SIP – The Next Big Step

Voice over IP Communications

Presented By:
Stephen J. Guthrie
VP of Operations
Blue Ocean Technologies

Goals

- **What are our Goals for Today?**
- **Executive Summary:**

It is expected that real-time person-to-person communication, like IP telephony (VoIP),presence, instant messaging, voice, video and data collaboration will be the next big wave of Internet usage. The Internet standard for such communication is SIP (Session Initiation Protocol). For businesses looking to join this burgeoning SIP user community, it is important to ensure that the enterprise network is adequately prepared and safeguarded. However, universal connectivity across the Internet is frequently thwarted because the NATs and Firewalls in an existing network are not SIP capable – a common situation for businesses of all sizes.

The Next Big Step of Internet Usage – Person-to-Person Communication

When the Internet first started as a defense, research and university network, few anticipated just how widely accepted its use would be. Email applications and Web surfing have become so popular that today they are used on a daily basis by nearly every company around the world. Yet these applications do not support real-time communication between individuals, a capability that is fast becoming a necessary business tool as more and more enterprises utilize broadband or have a fixed connection to the Internet.

The Next Big Step of Internet Usage – Person-to-Person Communication

The next big step of Internet usage will be person-to-person communication. Applications include:

- Voice (of which IP telephony or VoIP just is one component)
- Video
- Presence (information of when, where and how a person you wish to contact is available)
- Instant messaging
- Conferencing with voice, video and data collaboration
- and more…

Several forms of person-to-person communication over the Internet have been in use for several years. However, it is only recently that SIP has become the generally accepted Internet protocol. Now that a standard has been established, and more companies than ever before have a broadband or fixed connection to the Internet, these types of person-to-person applications are becoming increasingly available and widely used.

What's the big deal?

Session Initiation Protocol, or SIP, is a protocol for person-to-person real time communication over the Internet.

It is standardized by IETF, the standardization organization of the Internet world. Henning Schulzrinne at Columbia University and Jonathan Rosenberg at Dynamicsoft are considered to be the authors of SIP.

SIP began, as indicated by the name, as a way to start sessions between users on the Internet. It has since become the basis for a wide variety of applications.

SIP is frequently used for "ordinary telephony," i.e., voice with 3 kHz bandwidth and common number dialing, over IP networks (VoIP). It is also the basis for IP telephony with video, presence and instant messaging.
In the future, it is expected that SIP will enable applications such as games, conference calls with video, application sharing and monitoring and control of the smart home.

In addition, SIP has grown beyond the desktop – it has become the standard protocol for multimedia in the third generation mobile phone system (3G, IMS).A powerful force driving the acceptance of – and development of applications for – SIP is the development of Microsoft® Office Live Communication Server 2003 (now known as Windows 2008R2 Linc), a package of RTC services for the Windows 2003 server.

What’s the big deal?

In addition, SIP has grown beyond the desktop – it has become the standard protocol for multimedia in the third generation mobile phone system (3G, IMS).A powerful force driving the acceptance of – and development of applications for – SIP is the development of Microsoft® Office Live Communication Server 2003 (now known as Windows 2008R2 Linc), a package of RTC services for the Windows 2003 server.

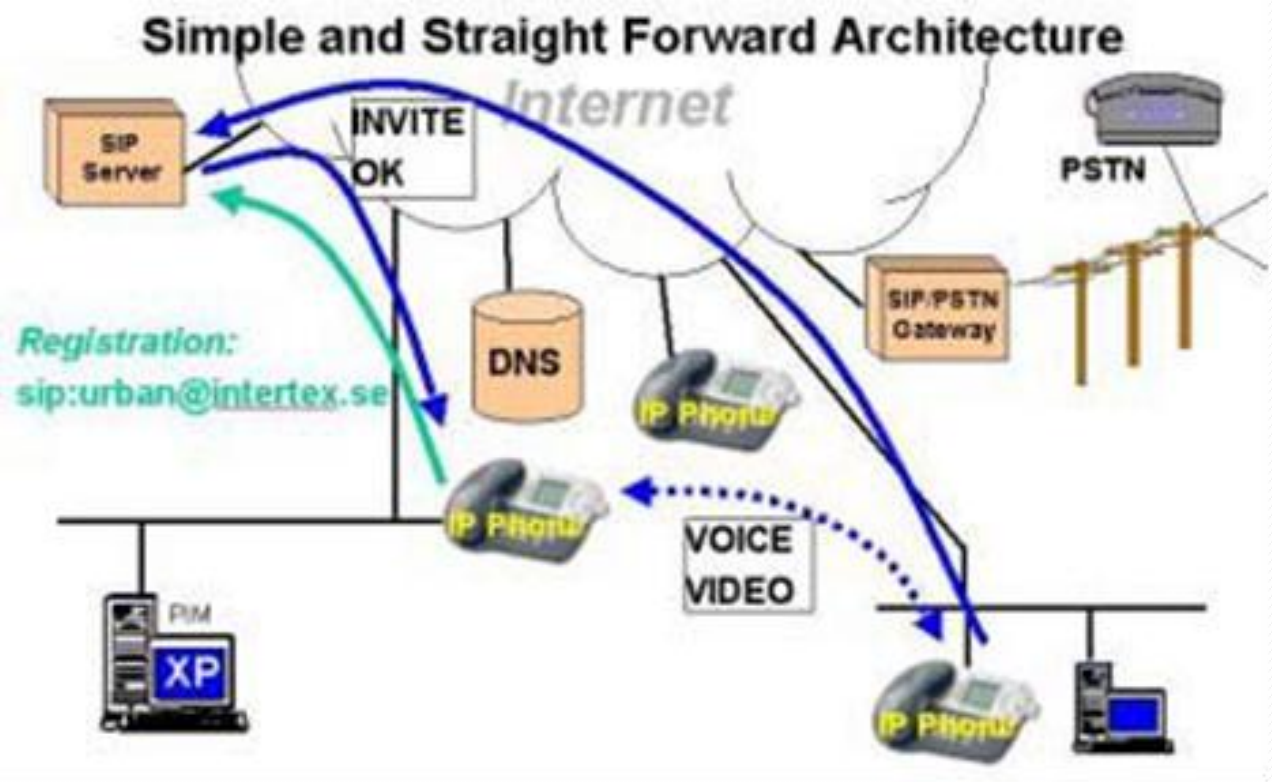
Person to Person Communications

SMTP created email

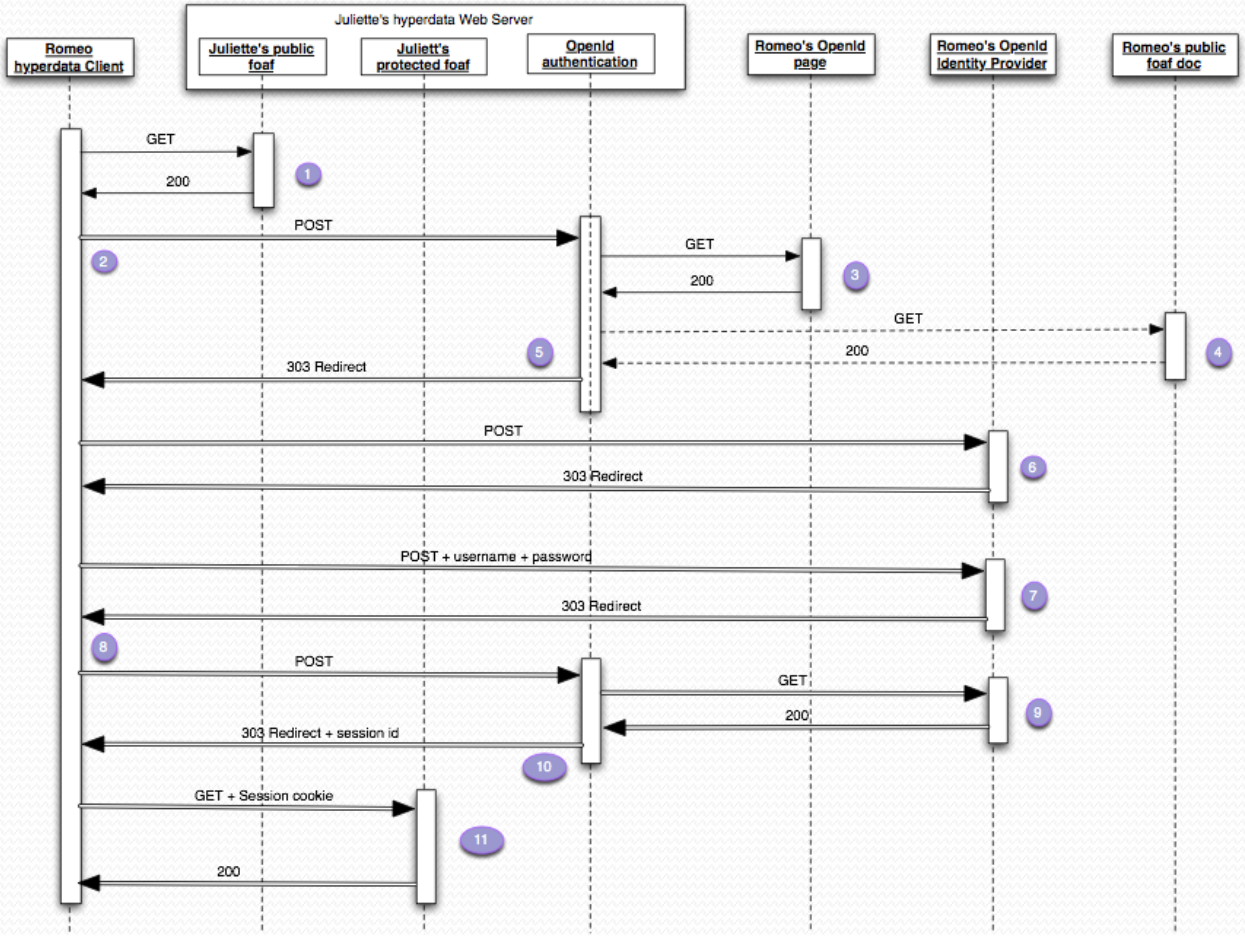
HTTP created the web

SIP will create person to person communication

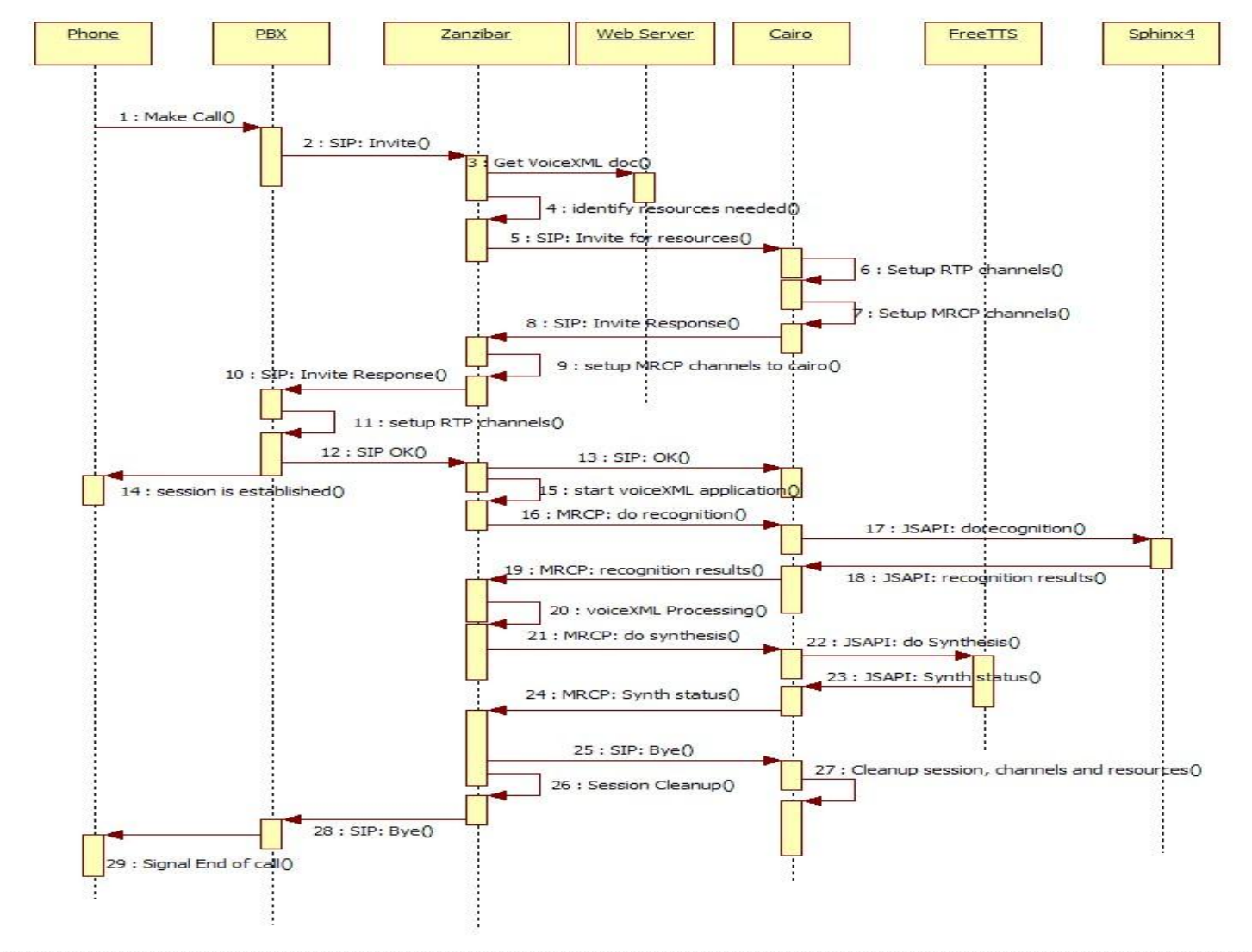
SIP Architecture Perspetive



HTML Sequence Diagram



SIP Sequence Diagram

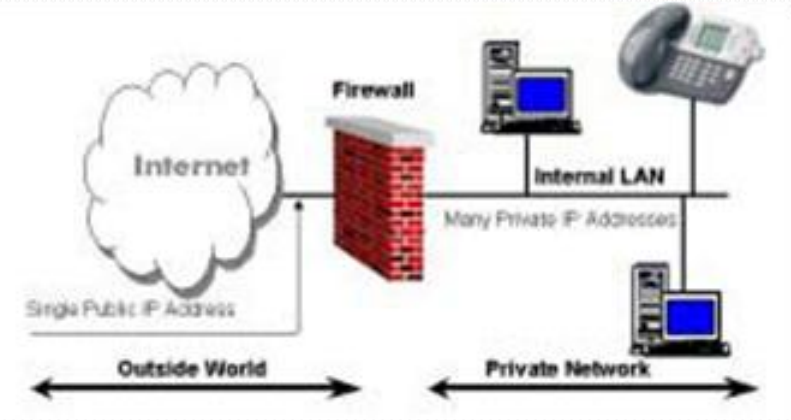


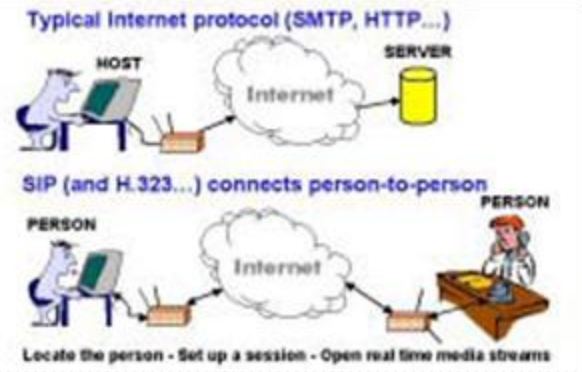
Firewalls, NATS and Routers

When connecting a PC to the Internet, it is imperative to safeguard the system from hacker attacks and other unwanted accessibility. This is especially critical if the PC is constantly connected, for example *via* broadband or a fixed line. A firewall protects the PC by rejecting attacks and illegal data packets, allowing only approved traffic.

On a local area network (LAN), where several PCs or other equipment is connected, it is common to have private IP addresses on the LAN and a single common public IP address to the Internet. This is called NAT (Network Address Translation) and is often an integrated part of the firewall.

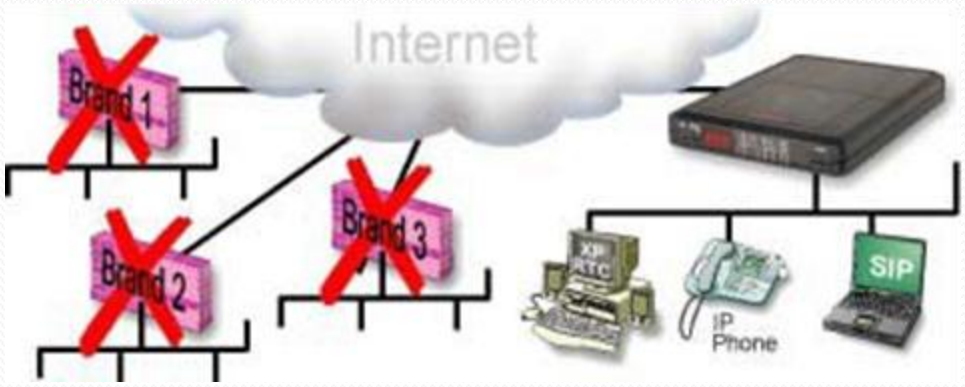
Firewalls, NATs and Routers





Firewalls are ticking time bombs!

The biggest hurdle for IT managers looking to SIP-enable their network (or enable for similar protocols like e.g. H.323) is prepping the system to handle the traversal of this type of traffic. The most overlooked communications hub is the firewall. The majority of current firewalls and NAT-routers are not designed to handle person-to-person communication, which will not reach users on the LANs unless the enterprise firewall has specific SIP support. It is critical that IT managers evaluate their current firewall solution to ensure there is proper SIP support when new firewalls and NAT routers are installed. It is a common misunderstanding that firewalls can be reconfigured to handle SIP traffic. One problem is that the media streams (e.g. voice and video packets) are transferred over dynamically assigned UDP ports that generally are closed. Another problem is that the SIP clients inside the firewall cannot be reached by IP addresses since these most often are private and local to the LAN. Communication simply does not take place, unless there is specific SIP support in the firewall.



Think of packets as a train

These are the private packets being sent.

This is the public reply being received.

The outbound freight is originally green!
We change it to black with NAT.

NAT concepts

Several firewall vendors develop models with an SIP ALG (Application Layer Gateway). These ALGs usually work at a lower level than a proxy, adjusting the data packets “on the flight.”

Cisco is developing firewalls with ALGs that also handle incoming calls to multiple users, while other more simple implementations may only support a single SIP user on the LAN.

A common limitation of the ALG architecture is that it cannot handle secure SIP signaling via TLS (Transport Layer Security). TLS is strongly recommended by Microsoft to be used with their SIP enterprise solution, RTC Server.

Other solutions are also being developed to enable SIP firewall and NAT traversal. For instance, STUN is a method for shuttling SIP through existing NATs.

It works by keeping holes open in the NAT with dummy traffic and having the SIP clients emulate their identity from the outside of the protected LAN.

One disadvantage with STUN is that it will not work for all NATs. It also does not ensure the security of the network, and may have scalability and security issues. The SIP client must be able to implement STUN and integrate it in the SIP stack to make it work.

There are also various tunneling approaches, i.e., creating a tunnel through the firewall and then having an ALG in a central place at the “SIP operator” to cope with the separate address space of the private LANs and their individual users. This requires special equipment at the SIP operator, or special equipment and software on the LAN or within the SIP clients.

NAT concepts

With this approach, users are locked into a specific SIP operator. This approach can normally not handle complex configurations, such as interworking between an operator and the Microsoft RTC Server architecture, where a local SIP server on the LAN is used.

For home users, Microsoft has suggested an extension to UPnP (Universal Plug and Play) to allow Windows to control the NAT or firewall. Several small, inexpensive NATs have implemented these UPnP extensions, and thus allow SIP traversal for Windows Messenger (which is SIP based).

However, this solution is not secure enough to allow every PC on the LAN to open the firewall (in the RTC Server architecture, Microsoft recommends that UPnP be disabled for high security).

Another limitation is that UPnP control from Windows clients will not help other SIP products (e.g. SIP phones) traverse a NAT or firewall.

Conclusion

Real-time person-to-person communication is fast becoming a critical communications tool for enterprises of all sizes. With the standardization of SIP as the Internet protocol for applications such as VoIP, instant messaging, video, presence and IP telephony, businesses are eager to adapt their existing hardware to accept SIP – which is expected to generate the next big wave of Internet usage since SMTP created email and HTTP gave us the Web. In all new installations of firewalls and NAT routers, proper SIP is critical to allow the users on the LANs to utilize real-time person-to-person communication.

There are a number of solutions for firewall and NAT traversal. The most reliable solution solves the problem where it occurs, in the firewall or NAT itself. By including a SIP proxy and SIP registrar for controlling the NAT and firewall, it is possible to handle complex SIP scenarios and even use TLS for secure and private signaling.

Contact Information

Stephen J. Guthrie
Chief Operating Officer
Blue Ocean Technologies
1500 1st Ave N
Unit 2
Birmingham, AL 35203
Email: Steve.Guthrie@blueotech.net
Voice: 205-776-6902
Mobile: 205-422-6508