Putting the right SIP Trunk solution in place

A best practice guide for IT Professionals

wanstor

Contents

Introduction

SIP trunks are being deployed by businesses across the UK at a rapid rate. At Wanstor, we understand the potential for a rapid return on investment is a key driver of SIP trunk deployments.

However, maximum return on investment can only be achieved when IT Managers extend VoIP outside of the corporate LAN. In terms of infrastructure purchases, SIP trunks provide an immediate cost saving. They eliminate the need to purchase costly BRIs, PRIs or PSTN gateways.

The productivity benefits with SIP trunking are also significant. By extending the SIP capabilities of the corporate network outside the LAN, satellite offices, remote workers and even customers can use VoIP and other forms of real time communication applications to break down distance barriers in sharing ideas and increasing productivity.

In this white paper, we will cover the components necessary for selecting and deploying a successful SIP trunking solution.

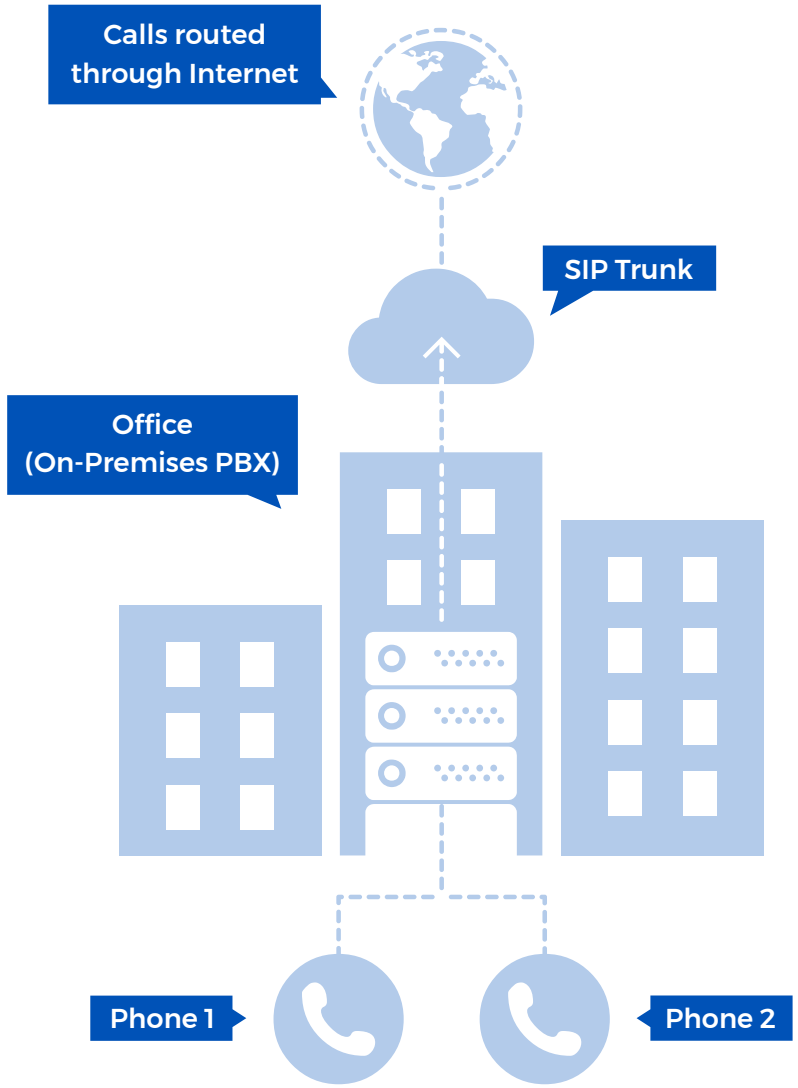
First things first: What is SIP Trunking?

Unlike traditional telephony, where bundles of physical wires were once delivered from the service provider to a business, a SIP trunk allows a company to replace these traditional fixed Public Switched Telephony Network (PSTN) lines with PSTN connectivity via a SIP trunking service provider on the Internet.

To enable SIP trunking, IT Managers should check that the PBX has a SIP-enabling trunking interface. It can either be an IP-based PBX communicating to all endpoints over IP, or a traditional TDM PBX.

The sole requirement is that an interface for SIP trunking connectivity is available. Over the Internet, the ITSP (Internet Telephony Service Provider) provides connectivity to the PSTN for communication with mobile and fixed devices.

The PBX on the LAN should then connect to the ITSP via the enterprise border element. The border element may be a SIP-capable firewall or a SIP-enabling edge device, attached to an existing non-SIP-capable enterprise firewall.



SIP Trunking Infrastructure

Now we have a definition of SIP trunking it is important IT Managers take the time to understand the SIP trunking infrastructure which will be required for a successful solution.

The first area for an IT Manager to consider is the PBX component. There are a wide variety of PBX components available on the market notably:

Traditional PBX : A PBX is a telephony exchange serving an organisations office. It performs the basic function of routing calls to their destination and a number of value added features such as call transfer, hold music, and redirects when a line is busy. The traditional TDM PBX is usually connected to a dedicated premises network that only carries voice traffic.

Line-side IP-enabled PBX : The LAN for data traffic is a later addition to the office than the telephony network. When it was first introduced it came in a separate parallel premises network. For many years these two network cable systems co-existed in the office serving separate but related communications functions.

The first IP-based PBXs, or IP-PBXs, focused on making the line side of the PBX, i.e. the side connecting to the telephones, run on IP protocols. The first benefit in doing so was that the two premises networks now could be converged into one common network. By the use of IP enabled telephones, these could be connected to the

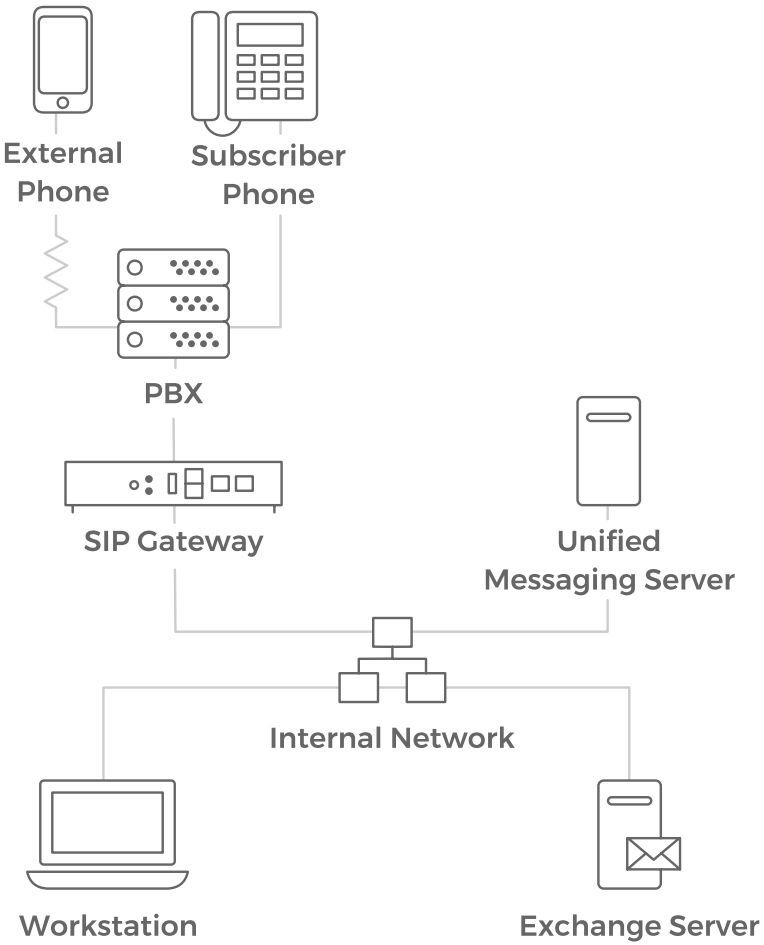


figure 1 : A traditional Private Branch Exchange or PBX

same physical cabling as the computers and servers, i.e. the LAN. Having made this change to a common premises infrastructure it then became possible to introduce PC-based soft clients instead of traditional telephone sets.

Some network engineers argue that voice and data traffic should not be mixed on the same LAN - or should at least be run on separate virtual LANs (VLANs).

The background to this is that voice traffic, due to its real time nature, is sensitive to delays or lack of bandwidth in the infrastructure resulting in poor voice quality. However, this issue can easily be solved on modern networks and should not stand in the way of realising the benefits of converged communication.

The bandwidth available on most enterprise LANs, 100Mbit/s or 1Gbit/s, is more than adequate for typical enterprise applications. By using appropriate quality of service techniques, businesses can make sure that voice traffic gets the appropriate priority to safeguard voice quality.

The IP-PBX : For many years businesses have used IP-based telephones connected through the corporate LAN. However, when calls needed to flow outside the corporate LAN they had to be routed to a local PSTN gateway and converted to traditional TDM-based telephony. Due to the inherently proprietary nature of TDM equipment and the fact that growth in network traffic inevitably leads to the need for additional hardware, this solution can be seen as expensive. In a world where more and more end points are running IP, there is a risk of deteriorating sound quality due to repeated transcodings between IP and TDM.

In light of the above, the next natural step is to use IP for the interface to the world outside your corporate LAN. This is done by IP-enabling the trunk interface on the PBX, completing its transformation into an IP-PBX.

In practice, this happens in one of two ways. For earlier TDM or IP-PBXs this can be achieved by placing an IP front-end on the trunk interface creating what is usually referred to as a hybrid IP-PBX.

This PBX contains both legacy TDM and IP-enabled parts. Newer IP-PBXs, or systems that are designed from the beginning, and are usually built with IP technology from the ground up, without the legacy TDM part.

There are a number of protocols available that could be used to IP-enable the trunk interface, including MGCP, H.323 and SIP. However, SIP is the protocol that has taken a lead in this battle of standards. It has a number of advantages over other protocols, the most important of which is that it supports a variety of communications - while H.323 is a voice-only protocol.

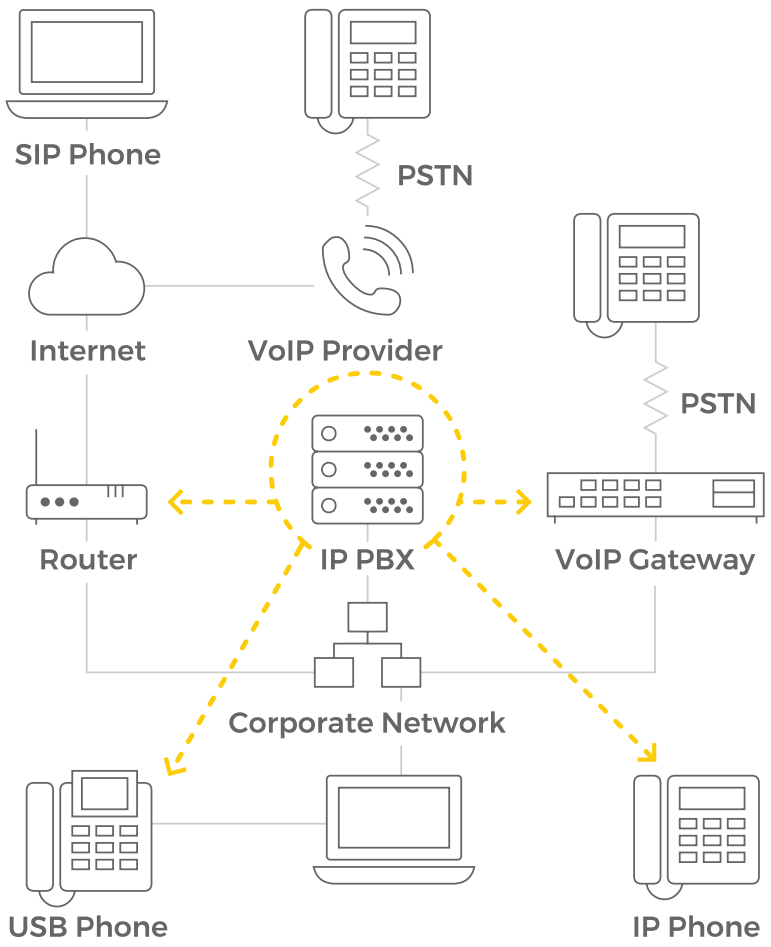


figure 2 : An Internet Protocol Private Branch Exchange (IP-PBX)

Why should you choose IP-based PBXs over legacy?

At Wanstor we believe there are a number of benefits for businesses in choosing IP-based PBXs, which include:

Easier user management : One of the main advantages of an IP-based PBX system is increased manageability. By using the existing data network, the need for separate wirings for a telephony system is eliminated and the phone becomes a computer, allowing administrators to easily make upgrades and force policies to each phone from a central management system.

Additionally, ID and configuration data will follow the phone regardless of where it is connected to the network, and users may log in to the device when they arrive at a new desk with profiles and information automatically loaded for them in advance.

Multi vendor end point connections : There is a trend in the PBX market to allow equipment from different vendors co-existence within the same PBX system. This allows the organisation to preserve investments made in phone endpoints even if the central PBX equipment is replaced. This allows users to select phones, media servers and switches from their preferred vendor. PBX vendors that choose to allow this believe the customer will be more likely to swap to their system if they can keep their existing phones.

However, some vendors continue to lock customers into their own equipment by making various proprietary extensions to systems at different points within the PBX lifecycle.

IP-based application integration : The SIP IP-PBX serves as the primary registrar of SIP users, and utilizes this information for routing purposes. But the fact that the PBX is now IP-based also means it can be integrated with other communication applications running on servers across the LAN.

One of the best examples of this is soft clients that can integrate voice capabilities with applications such as presence, instant messaging, file transfers and so on. Through such integration the PBX becomes part of a greater converged communication system, enabling the enterprise to benefit from productivity enhancing communications applications.

The Business Edge

The business edge may be a firewall with support for SIP - or an edge device connected to the firewall, handling the traversal of SIP traffic. When moving to VoIP, telephones and devices are connected to the Internet. It is therefore crucial to safeguard the system from attacks and other unwanted access. This is especially critical if end user devices and phones are always connected to the internet - for example, via broadband connection or a fixed line. A firewall protects end user devices by rejecting attacks and illegal data packets, allowing only approved traffic.

On a local area network where several devices 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 functionality is called NAT (Network Address Translation) and is usually integrated into the firewall.

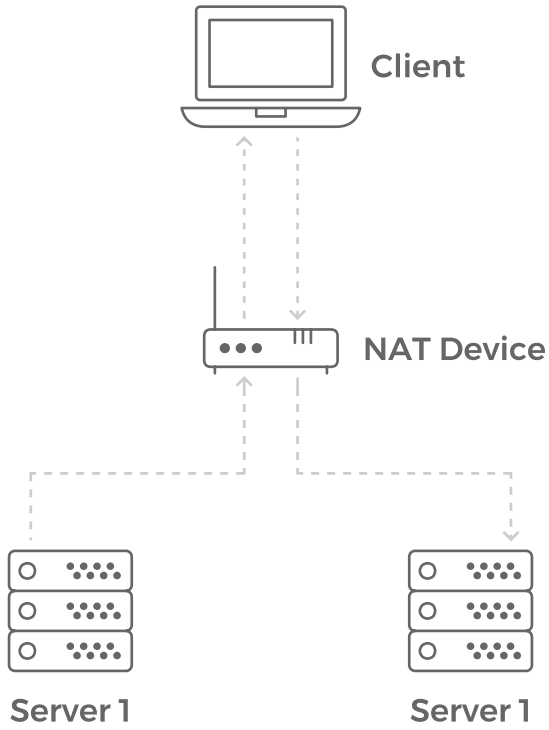


figure 3 : A one-to-one NAT, also known as a Full-cone NAT.

Firewalls and NAT routers are designed for data traffic that originates inside the private network. Because malicious attacks on the network frequently originate from outside, firewalls and NAT routers protect the business by blocking such malicious traffic. The problem, however, is that SIP traffic may be 'misunderstood' by traditional enterprise firewalls and NAT routers, and identified as unwanted traffic.

The biggest barrier for IT managers looking to SIP-enable their network is preparing the system to handle the traversal of SIP traffic across the firewall. The majority of current firewalls and NAT-routers are still not designed to handle full person-to-person communication, which as such will not reach users on the LAN unless the enterprise firewall has specific SIP support.

SIP traversal of firewalls and NATs is becoming a commodity in the sense that most vendors advertise support for the protocol. However, the basic SIP support offered by most of these vendors does not have the required features to fulfill the needs of a complex business IT environment.

It is therefore critical that IT Managers evaluate their current firewall solution to ensure there is proper SIP support for when new firewalls and NAT routers are installed. Several products or methods of doing so may resolve the issue of reaching users on a LAN. One addresses the problem's source – within the firewall itself.

Firewalls that have a SIP server (with SIP proxy, SIP registrar and possible 'Back to Back User Agent' that dynamically controls the firewall) have been available for many years.

This solution provides optimal flexibility, as SIP signaling can be rewritten and processed in a very flexible way - ensuring correct routing and interoperability with other systems built to RFC 3261 and related standards.

PBX and service provider equipment

Most basic call scenarios in a SIP trunking solution, using equipment from different vendors, work well. However, when more advanced features such as call transfer are used, problems occur when the standard is not strictly observed by all vendors. Additionally, as SIP is a flexible standard that leaves some room for adjustments, this means that at times two clients can have difficulties talking to each other even though none of them directly violate the standard.

To make the situation even more complex, some ITSPs and PBX vendors only implement parts of the standard, or add vendor-specific extensions to the standard. While performing traversal and security, these SIP-capable edge devices can also mediate between the PBX and service provider, offering an important function - they can process the SIP signaling and media in a way that is understood and expected by both the ITSP and the PBX.

Reliability

Thanks to its architecture with a full SIP proxy and registrar, an edge device can perform basic call routing functions. These functions can be used to increase the reliability and overall uptime of the total VoIP communications system.

There are edge devices that have a built-in function that detects whether contact with the central server is lost. The central server in this case could be either carrier equipment at the SIP trunking service provider or it could be an IP-PBX located at headquarters serving several branch offices.

The detection process will work whether contact is lost due to the central server being down or because the connection has failed.

In the case of failure, an edge device will take over the task of basic call routing, and depending on where the failure took place, ensure resurrection of the service either partly or fully. For example, if the central equipment fails, the edge device can route calls to alternative PSTN connectivity providers or a local PSTN gateway.

If the problem occurs because the last mile of Internet connection goes down, this device can at least make sure that local, intra-office communication still takes place.

Security

SIP-enabling edge devices can also add a layer of security to a business's communications, specifically in securing SIP media. Most security administrators will have serious concerns connecting a PBX system directly to the public Internet without any SIP-aware firewall in front of it. Like any server on the LAN, it needs to be protected by a firewall. A PBX is not built to withstand or recover from denial-of-service (DDOS) attacks and, in most cases, does not have filtering capabilities available to reduce traffic. Enterprise edge devices can secure SIP media and data traffic, and protect from eavesdropping.

Solutions for encryption of media and signaling using IETF proposed standards are recommended. These solutions include TLS (similar to SSL used for https) for signaling and SRTP (Secure Real Time Protocol) for media. Both are recommended in the SIP connect initiative.

An edge device can assume control of basic call routing in the event of service failure

Remote Working

To be able to extend the PBX features to remote workers in various locations, it is necessary to address the NAT traversal issue with SIP at the remote client end.

While many businesses are either replacing their existing firewalls with SIP-capable firewalls, or deploying SIP-enabling edge devices to solve this problem internally, the NATs at remote sites (wireless hotspots, hotels and such) are usually not SIP-capable. The result is that rich communication is not possible at remote locations.

There are connectivity solutions available – software solutions deployed in the enterprise edge device – that provide the necessary functionality to allow remote workers to connect to the central PBX. These include different ways of traversing the remote NAT without any special requirements on the client or server, outside the scope of SIP standards.

This far-end NAT traversal works well at wireless hot spots and the like, but does not work for enterprises with strict security policies, as the ports need to be open from the inside for this to work.

Branch office interconnections

When the PBX is IP-based, a host of new possibilities open up since communication between the PBX and other devices (including phones) are using a protocol (SIP) that works just as well over the internet as within the corporate LAN.

This means it is now possible to connect with other offices in the same organisation and partners and customers via IP, without the need to traverse the PSTN network and without the need for dedicated circuits. This actually enables an entire, multi-site business to use one centrally located IP-PBX instead of installing separate PBXs at each site.

When undertaking branch office interconnection of SIP-based systems, the same problems involved with traversing corporate firewalls and NATs as with SIP trunking itself will occur. A SIP-capable enterprise edge device will solve this problem as for SIP trunking. Some people even refer to such an inter-office connection within an enterprise as a SIP trunk.

Interoperability

Open standards are key to the success of voice over IP adoption. Back in the mid 1990s, both email and web browsing became universal practically overnight, driving the majority of people in the industrialized world to connect to the Internet. As mentioned before, the open standard for VoIP is the IETF standard, SIP.

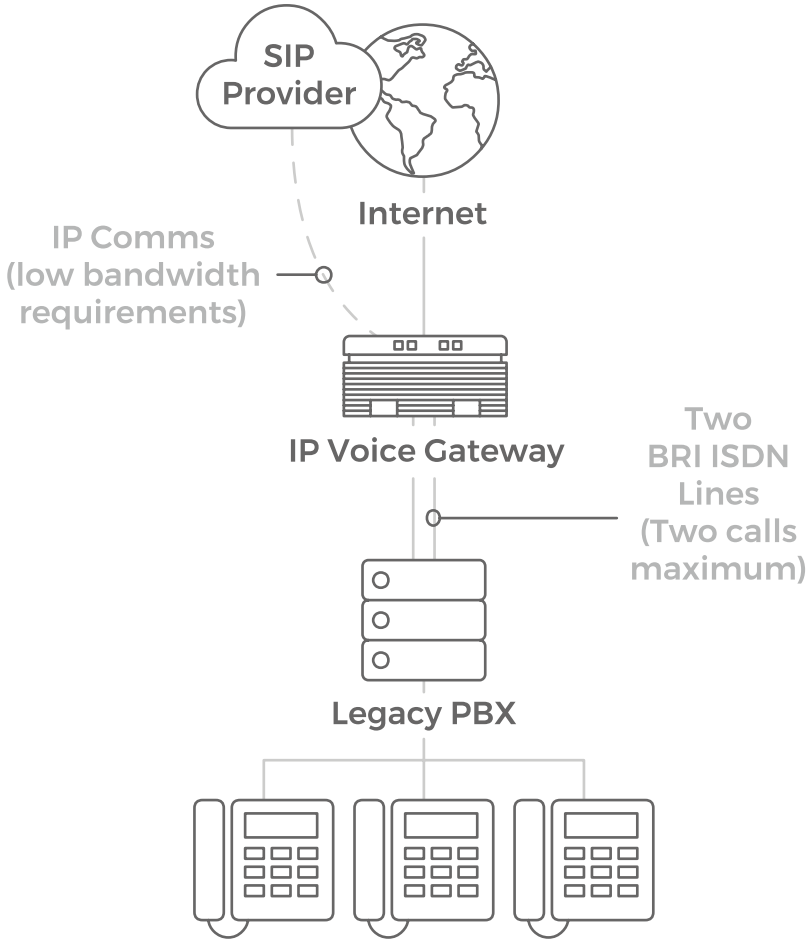


figure 4 : A basic SIP Trunking solution

We should expect that SIP will give rise to another period of exponential growth in Internet usage.

SIP stands for Session Initiation Protocol. It is used for setting up sessions between endpoints, which are often end-user devices or servers. SIP differs from the signaling protocol of the PSTN domain in that it allows for locating more intelligence in the endpoints rather than in centralised network elements, and is specified in a growing number of IETF RFCs.

Different groups with varied interests have taken part in adapting these standards. Some are PSTN operators who will try to redesign the PSTN world over SIP. Mobile operators and 3GPP IMS push for support of features like IM, presence, file sharing, video, and such.

As SIP is comprised of many specifications, most vendors do not implement all of them. SIP connect is an example of how a specific subset of these specifications can be used for defining a limited feature set (in this case, SIP trunking).

SIP connect was developed by the SIP Forum as a set of best practices for interfacing an enterprise PBX implementation with an ITSP that attempts to eliminate unknowns and incompatibilities.

The SIP connect specification defines how a PBX located at a business can connect to a VoIP service provider.

The primary service to be delivered by means of SIP connect is audio-based PSTN call origination and termination (voice). SIP connect refers to a number of existing IETF RFC specifications.

Thus, SIP connect provides a minimum set of requirements needed at both the SIP trunking service provider and the enterprise end to ensure interoperability. Compliance with SIP connect is vital to the overall success of SIP trunking deployments as it directly addresses, or eliminates, issues of interoperability.

Compliance also futureproofs the network; as new technologies based on SIP trunking are introduced, enterprises industry-wide can leverage whatever the next 'big thing' will be. SIP connect covers requirements in the following areas:

- DNS
- Signaling security
- Firewall and NAT traversal
- Authentication and accounting
- PSTN and SIP addressing
- Quality of service (QoS)
- Handling of media

Even though the SIP standard is written with interoperability in mind, integrating SIP equipment from different vendors takes time because, quite frequently, there are minor inconsistencies in how different vendors interpret the SIP specifications.

With regard to SIP trunking, different operators will use equipment from many gateway vendors who have varied requirements when it comes to the authentication of SIP trunk users.

If a company is looking to use SIP trunks from more than one vendor, perhaps to implement least-cost routing, they would normally have to deal with the complexities of interoperating with several SIP trunks that behave in different ways.

Compliance with SIP Connect is vital to SIP Trunking's success and the futureproofing of networks

As mentioned earlier, enterprise edge devices can mitigate these issues by addressing complexities of interoperability. These details and variations in handling approval from SIP trunks are handled by the device. From inside, the edge device will appear as one SIP trunk, even though it will then distribute traffic to several SIP trunks from different vendors outside.

As the device located closest to the operator, an edge device is well placed for this operation.

Another interoperability problem common with SIP trunking is when one endpoint is located behind a SIP-unaware NAT box (home users, hotels). When the edge device is first point of contact for such an endpoint, remote connectivity technology enables user participation in both outbound and inbound calls even though they are behind a SIP-unaware NAT.

Call transfer represents another interoperability problem. Some operators do not support this feature, and neither do some SIP user agents.

Additionally, a user who has a phone that supports call transfer cannot detect whether phones at the other end do so as well. If a call transfer attempt is made and fails, the call is often dropped. Edge devices can detect when a call is being made to or from an endpoint that does not support call transfer.

If someone still attempts to transfer a call to or from that endpoint, the device can perform this transfer itself in lieu of an endpoint that is unable to. The call will be transferred and the edge device makes sure that media is sent to another destination.

By using B2BUA within the device, a party that does not support call transfer will believe they have called the intended recipient.

Security for SIP trunking : What you need to know

Threats

Connecting devices exposes your entire network to various threats. Examples include brute force and Denial of Service (DDoS) attacks, where different systems are used to send large packet numbers, causing hosts to crash with the amount of traffic. These two are examples of traditional data communication attacks - but they, and many others, can easily be transformed into attacks on VoIP equipment.

To try and combat many of these instances, firewall vendors have developed significant expertise in securing data communications. They know how to design stable systems that are locked down to admit only services that have been configured to pass. Firewalls inspect and log traffic and, if intelligent enough, even block suspected attacks including traffic from known malicious sources.

It is important to note that firewalls alone cannot prevent DDoS attacks, but they can be built to withstand attacks. Firewalls can also lay the foundations for swift recovery. More importantly, they can be built to protect the enterprise LAN from being reached by DDoS attack.

Firewalls with a SIP server and full SIP proxy play a critical role in maintaining enterprise security, and securing SIP trunks. These can rewrite SIP signaling and process in a very flexible way, ensuring correct routing and interoperability with other systems built to RFC 3261 and related standards.

One important part of the SIP proxy is the SIP parser. The SIP parser verifies that the SIP message is valid and that it may be forwarded to the local LAN. The SIP parser must be robust enough to withstand any type of malformed SIP messages without crashing. To mitigate DoS attacks, the parser should be able to process a very large number of packets.

The SIP proxy should include support for an optional loop detection mechanism as defined in the SIP specification. This mechanism discerns whether a SIP message is looping and, if so, aborts such behaviour. This detection mechanism also protects against DDoS attacks where a SIP message is constructed to create loops, thus keeping the SIP proxy too busy to engage in useful processing.

In order to protect resources, e.g. a PSTN gateway, authentication of SIP users should also be supported. The standard means of authentication of SIP users is via the Digest protocol. SIP users' credentials should be stored in a centralized database such as a RADIUS server. This is more secure, and likely easier to maintain. SIP signaling consists of messages in ASCII text, and is therefore easy to read and manipulate. It is strongly recommended that SIP signaling is encrypted and authenticated, normally achieved by supporting TLS or MTLS. MTLS is the most secure method of doing so, as both server and client mutually authenticate each other using CA-signed certificates or certificate chains.

In order to provide greater and more flexible protection mechanisms, filters are useful features. A typical filter would include:

- SIP methods being allowed or prohibited on a network
- Authentication being enabled or disabled per network and SIP method
- SIP messages being filtered based on content type
- Incoming callers being restricted to a white list (individually enabled or disabled on a user by user basis)
- Filtering of from or to headers allowing or denying processing

Controlling media SIP proxy technology is an excellent way of adding control to the flow of SIP media. This control offers tremendous advantages with regard to security. The main purpose of SIP is to set up a media session between clients.

Media is handled by other protocols (often RTP). For media to traverse the enterprise edge, the SIP proxy must dynamically open the media ports for media to flow during the duration of the call.

Call Transfer represents an interoperability issue, with lack of support from numerous operators

As soon as the call is completed, media ports are closed. This behaviour is more secure than solutions with non-SIP-aware firewalls or border elements, where a media port range needs to be open constantly.

In general, the SIP proxy approach is more secure than IETF specified STUN/Turn/ICE methods, which require that ports are left open from inside the firewall in order to allow success in media port negotiation.

In addition to dynamic opening and closing of media ports, an edge device should only accept incoming media from endpoints receiving media. This protects against hackers injecting content from other endpoints or devices. To prevent media being intercepted by unauthorized persons, encryption comes into play. The industry seems to have chosen SRTP using descriptions for key exchange as the de facto standard for media encryption, effectively halting eavesdropping. Call integrity is stronger than ever before possible on PSTN.

Quality and reliability issues

A primary concern over VoIP and SIP trunking is quality of service and reliability. Will voice quality be good enough? Will the telephony service be available on demand? The answer to both questions is definitively yes. In fact, many people who use traditional PBXs are using VoIP without knowing it, as many service providers use IP in their backbone networks. Clearly IP is not the issue - both network planning and management are.

Quality of Service : Different service provider approaches

Online bottlenecks often occur over the last mile of connection to enterprise premises. Service providers utilise two methods in delivering adequate quality of service. In theory, only service providers controlling a link the entire way will guarantee an adequate level service quality; in practice, service providers relying on over-provisioning of links will also offer excellent quality.

Service provider controlling a connection in entirety : The service provider owns a connection and can control equipment all the way from the enterprise to their SIP trunking PSTN termination point. This makes it possible to prioritize voice traffic over data and also offer different Service Level Agreements (SLAs) to different customers.

Over-provisioning of links : Here, the SIP trunking service provider facilitates connection all the way to the subscriber. Any Internet connection is possible, as long as there is enough bandwidth. Good voice quality is achieved by over-provisioning of a link so that the last mile never becomes a problem.

Prioritization of voice traffic

To maximise utilisation of a given capacity, both data and voice should be delivered over the same connection. However, this makes prioritisation of voice traffic necessary. This can be based on:

- Services (protocol and port)
- Packet size
- SIP traffic
- IP-address and segments

This prioritisation should be possible for both outbound and inbound traffic. It should also be dynamic so that bandwidth dedicated to voice can automatically be used for data when it is available. The setting of Type of Service (TOS) and / or Diff Serv bits on packet level will allow routers on the Internet to make prioritizations. There is no guarantee, however, that all equipment will use these settings for prioritization.

In this case, it would help if the service provider controlled communication all the way out to customer premises.

Call admission control

Call admission control, also implemented in the edge device, ensures that it is impossible to initiate more calls than those that should fit within the link. Administrators define the amount of bandwidth dedicated to voice and the bandwidth available per call based on codecs used by the protocol. The edge device tracks all calls and when dedicated bandwidth is depleted, no more can be made or received. The response from an edge device in this case is 'service unavailable.' It is of course important to reserve call slot(s) for emergency calls.

Poor voice quality can be a client problem. It is commonly known that the general performance of a PC degrades over time due to badly managed software installations and fragmented hard disks. These issues affect voice quality. Additionally, many PCs (especially laptops) may not have a sound card optimised for voice.

At Wanstor, we advise all customers to invest in high-performance headsets with a built-in sound card if a PC is meant to be used as the primary phone device.

Another factor often overlooked is quality of service on the internal LAN. If the LAN represents a bottleneck, voice quality will be poor no matter how good an Internet connection may be.

MPLS

Many operators offer MPLS as a means of delivering quality service in a VoIP offering. The MPLS network is a provider-managed VPN. However, it is as easy to achieve good quality of service in an open standards-based SIP trunking connection as with MPLS.

One of the most important factors is whether the service provider controls the links from the enterprise to the PSTN termination, and not which protocol is used.

Also, SIP trunks are sometimes delivered over an MPLS connection for voice only. This means there is no support for global SIP connectivity over the Internet, and the solution can never be more than just a one-to-one replacement of traditional TDM lines.

Reliability of SIP trunks

Another point often raised by IT Managers is that a SIP trunking connection is less reliable as traditional TDM. It's true that internet connections are more dependent on electrical power, and TDM lines may have a slightly better average uptime in many parts of the world.

However, many enterprise telephony systems also rely on electrical power, so a policy with an uninterruptible power supply (UPS) that corresponds to desired uptime is a must. Furthermore a TDM line, when down, is truly dead. With SIP trunks, alternative backup solutions are available. The migration to SIP trunks will not happen overnight, so businesses might optionally choose to keep some traditional TDM / PSTN gateway capacity as a backup system. However, with the right choice of redundancy features and service provider, SIP trunking may offer greater reliability than many TDM-based networks.

SIP Trunking may be more reliable than traditional solutions

Due to inflexibility of the TDM in terms of line numbers, it is tempting to have a common PRI pool of lines at the headquarters also serving branch offices with PSTN connectivity. In many cases a SIP trunking connection may be more reliable than the traditional TDM in itself as it offers more backup alternatives, such as failover to a secondary SIP trunking provider, or failover to a secondary Internet service provider.

Bandwidth utilisation

The utilisation of bandwidth in a SIP trunking solution is often low with both telephony (TDM) and Internet lines. The telephony patterns in many businesses are distinguished by several hours a day comprising many calls, some with few and the rest a mixture. Internet data traffic, on the other hand, is for the most part erratic, with 'bursts' of traffic developing throughout the day.

In practice, when compared to real time communications (such as voice), data traffic is usually not as time critical. Combining both communication forms within the same connection will give maximum use of capacity.

By applying the correct quality of service settings, critical voice communication can be prioritized over data communication at all times.

Many IP-PBX installations appear similar to the left side of figure 5. This will provide a single point of failure combined with an unnecessary high load at headquarters.

The SIP trunking scenario on the right offers greater reliability, with different sites independently connected to the SIP trunking provider.

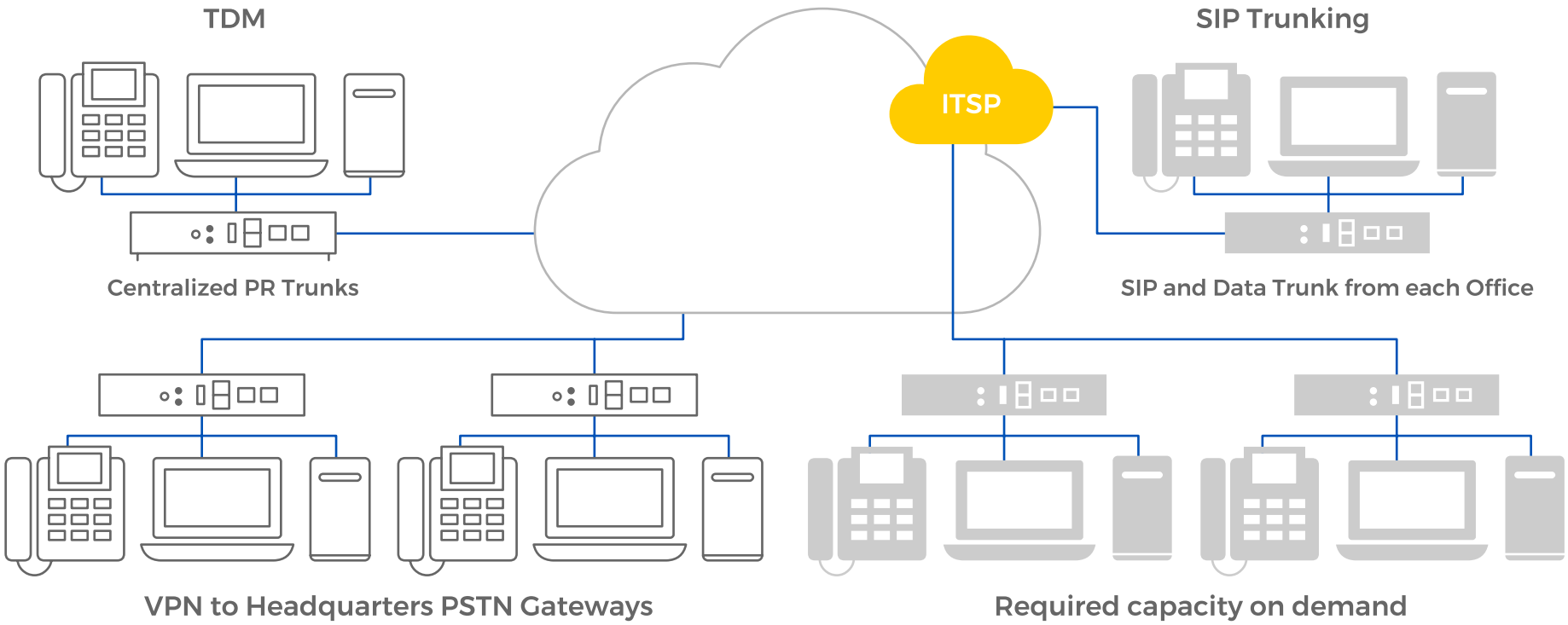


figure 5 : Time Division Multiplexing vs Session Initiation Protocol

With a SIP trunking solution, required capacity is always available. Instead of designing telephony for peak usage, it may instead be designed for average usage, allowing the dynamics of service quality to ensure that voice traffic always has the capacity it needs.

Flexibility to add new lines

Adding new lines with a SIP trunk connection is fairly linear - you only pay for extra lines that you need. When a TDM solution requires increased capacity, the following for each chunk of 23 (U.S.) or 30 (Europe) lines must be added:

- A new PRI subscription
- A new line card for PRI in the PSTN gateway

When capacity of the PSTN gateway and/or PRI connection is reached, it is necessary to invest in an additional PSTN gateway and / or PRI subscription. Unfortunately this is true even if you require only one more line. Going from one E1 / T1 to two always requires additional hardware, and can only be bought in steps of 23 / 30 lines.

Even if you move from an E1 / T1 to a higher level standard bundle like STM-1, the hardware will need replacing.

A SIP edge device will not have this problem. In a SIP trunk solution, the enterprise can increase one line at a time by:

- Purchasing additional software licenses for the edge device
- Allocating a greater percentage of the bandwidth for voice

Only if the total bandwidth capacity is utilised will the Internet connection eventually need to be upgraded.

Least Cost Routing (LCR)

The use of IP makes it possible to cost efficiently use SIP trunks from multiple service providers, dependent on optimal availability and best rates. In essence the business may become its own ‘Master Service Provider’, with subscriptions to service providers in countries where they have the highest calling volumes.

By routing calls to the cheapest service provider based on country codes, for example, significant savings can be achieved. These routing decisions can be made by the PBX or by the edge device.

The fact that this ability can be built into an edge device means that low functionality PBXs can also perform these routing functions. By ‘outsourcing’ this function to the edge device, the PBX need only send the number as it is, and let the edge device act depending on the destination.

Using multiple service providers offers a higher level of both security and reliability by way of:

- Failover to a secondary Internet service provider
- Failover to a secondary service provider or to a backup PSTN gateway

Making IP-to-IP calls when possible

Today, calls that could be transferred over IP are done so through TDM connections instead. These situations arise when calls are routed to a PSTN gateway on the LAN. In essence the true benefits of IP communications are not only unrealised but are also defeated as quality will suffer by analog or digital transcoding several times over.

ENUM (Electronic Number Mapping System, also known as Telephone Number Mapping) is a standardized address translation technology adopted by the IETF (Internet Engineering Task Force) using DNS (Domain Name Service) to link a phone number to a specific SIP address.

This feature is used to automatically look up phone numbers in determining whether they match a known SIP address, allowing the call to be completed over the Internet (instead of transferring it to the PSTN).

Since no traffic is placed on the PSTN, ENUM provides an additional means of cost savings for businesses that communicate with other enterprises using SIP. If a number is not found in the ENUM database, edge devices will route calls to the service provider for termination to the PSTN. With the growing base of installed SIP-based IP-PBXs, critical mass for widespread deployment of ENUM will arrive sooner rather than later.

It will not be long before the majority of calls are transferred directly via SIP over IP between calling parties instead of going over the PSTN.

SIP trunking: Unlocking higher productivity

Even though more difficult to calculate, it is perhaps with the gains achieved in improving productivity that SIP trunking delivers the fastest ROI of all.

Introducing SIP-based real time communication has a tremendous impact on how people work, how they collaborate and how they communicate both now and will do in future. SIP trunking is an important step, as it is the feature that moves communication from old PSTN connections to the Internet.

Once in place, the field is open for adoption of all productivity-enhancing features that SIP offers, including:

- Presence, in seeing who is currently online and available
- Instant Messaging (IM), text messaging in realtime
- File transfer
- Application sharing, collaboration on a single document
- Whiteboarding, writing and drawing on a common virtual whiteboard
- Video conferencing
- Machine-to-machine realtime communication
- The distribution of alarms

A wide range of rich communication options enable users to exchange ideas in the best possible way relating to their immediate situation. For instance, remote workers at a Wi-Fi enabled hotspot may find the best way to communicate with colleagues could be via IM and not VoIP.

The benefits of SIP trunking

Many businesses are already using VoIP - many others, however, are using it only for communication over the enterprise LAN. For all calls made outside of the LAN, a PSTN gateway on the enterprise edge is used.

These businesses realise a solid return on investment (ROI) just by lowering administrative costs and costs associated with calls made inside the company.

Many businesses only use VoIP as a one-to-one replacement for traditional wired telephony

With SIP trunking the potential for ROI is far greater, because SIP trunking takes the idea of VoIP a step further beyond this LAN application.

The full potential for IP communications can be realized only when communication is taken outside of the corporate LAN.

At Wanstor, we believe that SIP trunking delivers several benefits:

- Eliminates costly BRIs (Basic Rate Interfaces) and PRIs (Primary Rate Interfaces) subscriptions
- Eliminates investment in PSTN gateways and additional line cards as the business grows
- Edge devices offer cheaper investment paths in adding new lines as they are typically cheaper per line than corresponding PSTN gateways
- Optimal utilisation of bandwidth by delivering both data and voice within the same connection
- Maximum flexibility in line dimensioning and usage via avoidance of purchasing line capacity in chunks of 23 (T1) or 30 (E1) lines
- Flexible termination of calls to preferred providers; international calls can be made for the cost of local calls
- Redundancy with multiple service providers and links

The cost effectiveness of a SIP trunk is such that by replacing an existing PSTN gateway or PRI installation with an edge device or SIP trunk, ROI may be achieved in a matter of months.

For new installations, a SIP-capable edge device is most often a smaller investment than a PSTN gateway, making that investment cheaper.

It is almost impossible to calculate a 'standard' ROI for a SIP trunking investment as there are far too many service providers that offer services with widely differing conditions. However, from experience (and the points outlined within this white paper), we know that a SIP trunking solution offers significant ROI, with the majority of customers paying off their initial SIP trunking investment within 12 months.

Conclusion

In the end, it all boils down to this: can we trust SIP trunking? The answer is yes, so long as the right measures for securing media, ensuring interoperability, future proofing networks with standards-based equipment and SIP trunk deployment are in place.

By including SIP-capable edge devices as part of deployment, issues with security, quality of service and interoperability can be significantly reduced. We see SIP trunks as paving the way to an all-IP, all-SIP world where businesses can work without geographical constraints, employees can contribute equally regardless of location, and everyone can be reached anywhere and at any time with access to an internet connection.

This is the vision the IETF had when they first introduced the SIP protocol: the concept of true global connectivity. SIP trunking extends the concept of seamless connectivity within a business to customers, remote employees, and anyone operating outside of the corporate network.

This is the next evolution in telecommunications. Wanstor looks forward to working with you to make it happen for your business.