Network Equipment Technologies

TECHNICAL WHITE PAPER

Benefits of Using a Demarcation Device When Integrating Legacy Voice, SIP Trunks and Microsoft OCS R2

SIP Trunking

INTRODUCTION

The term "trunking" has been used in the telecom industry for a very long time. The term "SIP Trunking" is a VoIP-related term with Session Initiation Protocol (SIP) being used for initiating and tearing down calls. The SIP Trunking market has seen growing interest over the past two years and has now come into the mainstream with offerings from the major service providers. Organizations are now migrating from traditional Primary Rate Integrated Services Digital Network (PRI) based PSTN connectivity to IP-based converged networks using SIP at an increasing rate in order to achieve telecom cost savings.

Many organizations are already benefiting from VoIP by transporting calls over their IP networks. By implementing SIP trunks, enterprises can further reduce costs associated with PSTN access. Because SIP trunks are used for local and long distance calling, traditional TDM links can be significantly reduced and their use can be kept limited to providing PSTN backup and emergency 911 services only.

The far reaching benefit of deploying SIP trunks in the enterprise is the ease of implementing Unified Communications (UC). SIP trunks allow organizations to consolidate telephony into datacenters and allow branch offices to be linked with datacenters for providing same UC capabilities across the entire organization.

However, as UC is being adopted, enterprises need a solution that helps them gracefully migrate to UC from TDM environments. Any proposed solution should help organizations during the coexistent phase before TDM is completely replaced with UC.

This whitepaper provides general information about SIP Trunking and its benefits. It then describes the challenges faced by enterprises when deploying Microsoft OCS R2. Finally, this paper describes the benefits of using an NET demarcation device for solving protocol mediation, branch office survivability, failover redundancy, security, and interoperability problems encountered when connecting enterprise voice networks including OCS R2 with SIP Trunking service provider networks.

SIP TRUNKING DEFINED

A SIP trunk is a logical trunk over which an enterprise PBX/IP-PBX can peer with the service provider network. Calls are originated and terminated using the SIP protocol. A SIP Trunking service provider typically offers dial-tone, local, long-distance, and international calling features.

In a TDM environment, a typical PBX connection to the PSTN requires one or more T1/E1 PRI trunks. In a SIP Trunking environment, the PRI connection is replaced with an IP connection.

The incoming calls that used to traditionally ring on a PRI or an analog line will now receive a SIP INVITE to a WAN IP address. Similarly, the outgoing call is initiated by a SIP INVITE message to the carrier's Session Border Controller located inside the service provider network. There could be other elements such as soft switches and IP-PSTN gateways inside the carrier networks to convert the IP call to TDM before connecting the call to the PSTN user.

SIP trunks can be implemented over a variety of IP communications like Metro Ethernet, T1, DSL, Cable, WiMax, or 3G. SIP trunks can also be established over a public Internet connection by using unused bandwidth for voice traffic. While this arrangement provides a very high ROI, it is not the right enterprise grade solution because it lacks the necessary service guarantees.

Established LEC, ILEC, or CLECs are extending their existing QoS enabled IP-networks such as Multiprotocol Label Switching (MPLS) to provide SIP trunks to the enterprise.

THE BENEFITS OF SIP TRUNKING

SIP Trunking is now a major new opportunity for service providers. Carriers are building on their MPLS technology to offer VoIP. Both SMB and large enterprises have embraced SIP Trunking because of significant cost savings it provides them.

SIP Trunking offers cost and productivity gains for enterprises. They help organizations maximize their bandwidth utilization, reduce network complexity, and allow enterprises implement unified communications. Many service providers also support virtual and local telephone numbers.

Decreased Costs

SIP Trunks provide an average of 50 – 70% cost savings per trunk when compared to TDM circuits. Unlike TDM networks, where businesses have to buy in multiples of either 23 or 30 trunks depending on whether the interface is T1 or E1, a SIP trunk can be scaled in multiples of one. When coupled with line oversubscription, organizations stand to gain significant cost advantages.

For example, a 50 employee branch office might only buy 10 SIP trunks anticipating that there will only be 10 concurrent calls. In other words, only one SIP trunk is purchased for every 5 employees. Additionally, several service providers allow multiple calls to be delivered over a single SIP trunk, offering additional savings on communications costs.

Here is an example of an IT service company that saved telecom costs by deploying SIP trunks. The company has over 200 employees in one of their regional offices. In order to meet the needs of the 200 employees, it required 2 T1 PRI circuits. The month to month cost of PRI for both inward and outward dialing for PRI was $1000. The company makes roughly 20,000 minutes of long distance calling per month. The cost for local and long distance calling charges were $0.04/minute. When the company moved to SIP trunks, they purchased a 30 DID talk path for a cost of $900/month with unlimited inbound and local calling. The company had to incur a capital expense of $5,400 to purchase a demarcation device which was deployed as customer premise equipment.

The company leveraged their existing 10 MB broadband Internet Service connection. The overall bandwidth consumption using G.711 codec is ~3MB and drops to ~1MB when G.729 codec is used. Since most of the calls are

carried over IP networks, the long distance charges dropped to $0.02/minute. As a result of moving to SIP trunks, this company saved over 50% on their monthly operational expenses (See figure 1).

	TDM				SIP Trunks			
Capital Expenses	Item	Qty	Unit Cost	Total	Item	Qty	Unit Cost	Total
					Demarcation Device	1	$5,000	$5,000
					Install & Config	*4 hrs.	*$ 100	$ 400
Total Capex								**$5,400**
Operating Expenses	Monthly PRI	2	$1,000	$2,000	Monthly SIP Trunk	30	$30	$ 900
	Long Distance	20,000	$0.04	$ 800	Long Distance	20,000	$0.02	$ 400
Total Opex				**$2,800**				**$1,300**

***Installation rate and duration can vary depending upon the complexity of deployments**

Figure 1a: ROI calculation

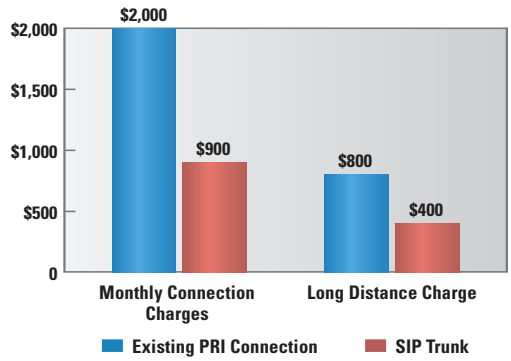

Figure 1b: Comparison of operating expense

ROI

As can be seen in the Figure 1a, there was a $1500 monthly operating expense savings by moving to SIP trunks. The first year ROI is over 333% and the payback period is less than four months. Since the equipment is fully paid up within the first four months, the cost savings in the first year and subsequent years became the key purchasing driver for this company. ROI for the second year and beyond is over 2000% because the company will only pay for the maintenance cost of the demarcation device while still saving over $18000 in yearly expenses.

Reduced Network Complexity

With SIP trunks, enterprises can evolve their traditional distributed voice architecture to a simple centralized and cost effective solution. A single centralized IP-PBX deployed in one location can now support multiple premises by linking the sites using the carrier SIP trunks. For example, a typical branch office may require one or more ISDN PRI circuits, a VPN circuit, and a voicemail circuit. With a converged SIP trunk from a service provider, all of the above elements can be replaced with a single IP link to a call processor such as an IP-PBX installed in a central location. Voice traffic is converged with the data traffic over a carrier's MPLS network and the central IP-PBX can support all branch offices resulting in cost savings and simplified voice network.

Improved Business Continuity

In the event of a network failure, business continuity can be very easily ensured by re-establishing connections with alternate SIP Trunking service providers.

Improved Bandwidth Utilization

SIP trunks allow organizations to better manage their bandwidth usage. Some service providers allow dynamic bandwidth allocation so that when certain sites use less bandwidth, the excess capacity can be dynamically allocated to high usage sites. Therefore, instead of buying additional capacity during peak usage, available capacity from low usage sites can be reused efficiently to meet on-demand needs of the enterprise.

Improved Voice Quality

SIP trunks also help reduce voice quality degradation. SIP trunks reduce the number of times a call has to be converted or transcoded from IP to TDM and from TDM to IP. The conversion happens only at the far-end PSTN termination point.

Enhanced Global Presence

Many SIP Trunking service providers offer Virtual Telephone Numbers (VTN's). VTN's enable organizations to assign local telephone numbers to users that are not physically located in the local calling area. Using this feature, a single site can support multiple local calling area numbers so that call center applications can be very easily established.

Increased Productivity

In addition to saving costs, SIP trunks are enablers of productivity improvement. Organizations can leverage SIP Trunking for implementing next generation unified communications, enterprise mobility solutions, and IP contact center applications.

Unified Communications technologies such as Microsoft OCS R2 are easy to implement using SIP trunks because a single IP connection can be used for voice, data, and video communication. A single IP network can carry multi-media, multi-modal communications including messaging, real-time voice and video communications across different domains so that customers, partners, and other stakeholders in a federation are able to collaborate effectively.

Another advantage of SIP Trunking is that it allows enterprises to connect their existing voice infrastructure and extend communications to users outside the enterprise. For example, mobile workers equipped with SIP devices can telecommute creating a good work/life balance for employees.

The IP contact center is a perfect example of an application that benefits from SIP Trunking. In a contact center, reaching the right resource may require repeated transfers especially when there are many resources dispersed among multiple sites. Using a SIP Trunking service, calls can be redirected an unlimited number of times without incurring huge recurring costs while improving overall call center productivity.

SIP TRUNKING BENEFITS FOR MICROSOFT OCS R2

Microsoft OCS R2 introduced several new enhancements, including support for SIP Trunking. Using any of the qualified service provider networks, an enterprise can connect their on-premise Microsoft OCS R2 with PSTN directly for PSTN origination, termination, and emergency services.

Any user inside or outside the corporate firewall can make local, long distance, or emergency calls. PSTN users can reach a corporate user by dialing an E.164 compliant Direct Inward Dialing (DID) number.

Figure 2 below depicts the topology supported by Microsoft in OCS R2. IP VPN is used for securely connecting enterprise OCS R2 with PSTN over a SIP Trunking service provider network.

Since a VPN or a private network is used for connecting the OCS R2 and the PSTN network, voice data security and the Quality of Service are guaranteed. In this topology, additional security with Transport Layer Security (TLS) for SIP signaling and Secure Real Time Protocol (SRTP) for media are not required. As a result of this, TCP for SIP signaling and RTP over UDP for the media are used and the messages are tunneled through the VPN router.

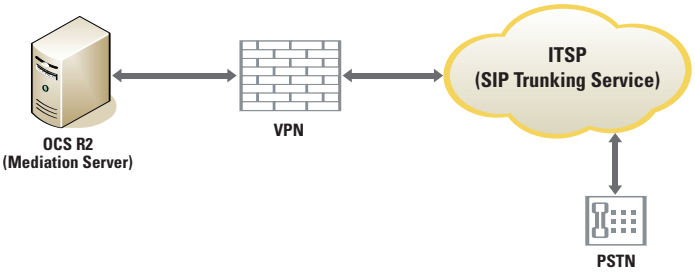

Figure 2: SIP Trunking topology supported by Microsoft

At the time of this writing, Microsoft has qualified three service providers – Sprint, Interoute, and Global Crossing - for interworking with Microsoft OCS R2.

SIP TRUNKING CHALLENGES FOR MICROSOFT OCS R2

Deploying a SIP Trunking solution in a Microsoft OCS R2 environment requires SIP trunks from a service provider, an Edge or Virtual Private Network (VPN) router, and several OCS R2 servers defined by Microsoft as server roles.

In the Microsoft SIP Trunking topology described in figure 2, the mediation server role performs the integration functionality and translates the SIP signaling and the media packets between OCS R2 and the ITSP network. It translates the Microsoft's proprietary RT Audio codec which is used in the OCS network to the standard G.711 codec commonly used in PSTN networks.

Even though the mediation server can be directly connected to the SIP Trunking service provider network, a demarcation device is preferred in order to support advanced enterprise demarcation capabilities such as protocol mediation, survivability, and for ensuring that the internal networks are not subjected to security risks inherent in an IP network. Without a demarcation device at the enterprise edge, enterprises face the following implementation difficulties:

- Standards are evolving, so interoperability may be an issue especially when customers have multiple legacy equipment along with OCS R2
- When organizations transition to SIP Trunking from TDM, internal networks may be vulnerable to security and denial of service attacks.
- Firewalls and NAT routers may block legitimate SIP traffic because existing firewalls and NAT routers are not SIP capable.
- SIP trunks from a single service provider may lead to a single point of failure. For a reliable service, multiple paths need to exist. Along with service reliability, multiple paths offer "Least Cost Routing" functionality. A reliable multipath link configuration is best supported by devices that are certified by a broad number of service providers.

The following section describes the implementation challenges in more detail.

Network Interoperability

Microsoft's software-powered VoIP solution supports either standalone OCS-only configurations or a coexistent configuration with the enterprise PBX.

In a stand-alone configuration, the PBX infrastructure is replaced with Microsoft OCS. The SIP Trunking topology, as discussed in the previous section (see figure 2), works extremely well for OCS R2 standalone deployments. In this deployment, it may be argued that a media gateway is not required. The mediation server performs the necessary translation between OCS R2 and the ITSP networks. However, most enterprises across many verticals like financial services, insurance, professional services, real estate, retail, and legal have many small offices in multiple geographical locations. Many of these companies and remote offices have multivendor, multi-generational TDM PBXs in their networks. Under this typical coexistent model, some users may be homed on existing PBXs while others may have migrated to OCS. In order for such a deployment to work effectively, either the PBX/IP-PBX should natively support SIP or alternatively, a media gateway is needed for providing the integration between OCS and the PBX as well as to provide seamless migration to OCS R2 from legacy PBX. A mediation server alone does not offer the necessary TDM – SIP, SIP – SIP, TDM – TDM interoperability required to seamlessly support OCS R2 in these diverse networks.

Additionally, many organizations are not comfortable with routing their calls directly into OCS R2 and prefer to take a phased approach by migrating users gradually from their legacy PBX to the new OCS R2 environment.

A media gateway that acts as a demarcation device while providing network interoperability to enable a seamless migration is an essential element for enabling SIP Trunking for Microsoft unified communications.

SIP Standards Compliance

While SIP is an open standard and the intention was to promote interoperability between vendors, the actual implementation leaves vendors a certain amount of freedom in the way the standards are interpreted. SIP Trunking solution providers may implement SIP over UDP while application vendors like Microsoft may need SIP transported over TCP or TLS (Transport layer security) for SIP signaling and RTP or SRTP (secure RTP) for media.

Additionally, some service providers have differences in their implementation of SIP in their call flows. For example, some providers may not support SIP REFER and may need to receive REINVITE messages for modifying calls during a transfer.

There are also differences in their support for codecs. Some service providers may support G.729 and G.711 codecs but not T.38 for fax. Even if T.38 fax over IP codec is supported, there may be interoperability issues. It has been found during interoperability testing with service providers that some carriers do not support T.38 REINVITE messages when the fax is sent using G.711 codec. This causes problems in rerouting fax message into Microsoft Exchange 2007 UM server.

There are also other protocol mediation issues. For example, the mediation server in the Microsoft OCS network that takes care of transcoding to Microsoft RT Audio codec, currently only recognizes G.711. Microsoft Exchange Server 2007 UM can only understand T.38 and G.711. However, some SIP Trunking service providers may prefer to support only G.729 codec. Under such conditions, a protocol mediation service offered by a demarcation device will ensure that G.729 codec is translated to G.711 before a mediation server translates it to RT Audio codec. Some demarcation devices may also offer additional value by translating G.729 to RT Audio directly without requiring an additional step of translating the codec into G.711 before passing on the message to the OCS environment.

NAT Traversal

Unlike the TDM environment, VoIP systems are vulnerable to malicious data and denial of service attacks (DoS).

Even for legitimate traffic, SIP messages may be blocked by Firewalls and NAT (Network Address Translation) due to the way SIP works. VoIP applications rely on separate streams of data - one for signaling stream and the other for the media stream. Well known ports are used for signaling whereas the Real Time Protocol (RTP) used for media randomly selects one of the 65000 available UDP ports. Since the port selection is dynamic, RTP needs a large range of UDP or TCP ports open on the firewall. Otherwise, SIP traffic may be completely blocked. A mechanism to dynamically open and close ports is needed to ensure that the SIP traffic is able to traverse the firewall.

To solve the firewall and NAT issues, enterprises can either upgrade existing firewalls to make them SIP-compliant or deploy a demarcation device that connects to the firewall and handles the traversal of SIP traffic through the firewall and the NAT device.

Security

Besides managing the firewall and the NAT traversal issues mentioned above, the VoIP solutions, like any other enterprise-class application, needs high levels of end-to-end security for ensuring communications reliability.

The TLS (Transport Layer Security) protocol protects signaling while the SRTP (Secured Real Time Protocol) protocol provides a mechanism for secure transmission of voice packets across various data interfaces. But encryption adds to overhead and reduces overall call capacity. Furthermore, because the signaling messages and the media are encrypted, many firewalls are unable to track call state which is an essential requirement for dynamically opening and closing ports.

Some organizations also need a separate device in their networks that they can trust for safely opening and closing the required ports on their firewall.

A demarcation device deployed at the enterprise edge ensures that the internal networks are protected from various security threats such as spoofing, eavesdropping, and denial of service attacks to ensure high availability of SIP trunks and to protect internal networks from these threats.

Service Assurance

Another important concern for organizations is the impact on the voice quality when they transition to SIP trunks from TDM. Most service providers can deliver end-to-end QoS because they own the connection to the enterprise or because they have QoS-based interconnection agreements with their partners. If a service provider does not own the local access facility to the enterprise, they ask that the local access be over provisioned to ensure QoS. In the former case, service providers usually have a managed Customer Premise Equipment (CPE) that ensures that voice gets higher priority over other data traffic that travels over the SIP trunk. However, traffic prioritization alone is not enough. In addition to traffic prioritization, call admission control (CAC) is necessary to ensure that the network does not initiate more calls than can be transported over the SIP trunks.

In TDM networks, the CAC functionality is inherent to the network interface because there cannot be more calls possible than there are time slots available on the channel. On the other hand, CAC functionality needs to be introduced in an IP network.

While the service provider managed CPE such as a router may handle the traffic prioritization function, a demarcation device will be needed for controlling the number of calls. A demarcation device will have the ability to reroute legitimate voice calls to an alternative SIP Trunking provider or to a PSTN connection when the number of call requests exceeds the available bandwidth or if the thresholds for maximum calls allowed are reached.

In addition to providing call admission control, a demarcation device can also manage the available IP bandwidth to ensure optimum user experience. The amount of bandwidth required depends on the voice codec selected. Compressed codecs like G.729 can transport more calls while uncompressed codecs such as G.711 require more bandwidth and hence transport fewer calls than G.729. The demarcation device's transcoding functionality will ensure the right codec is used based on application for efficiently managing the available bandwidth.

Certification & Vendor Qualifications

Service provider certification is extremely important and assures users that any interoperability issues have already been resolved by vendors before the equipment is installed. However, SIP Trunking service provider certification alone is not sufficient. A demarcation device that is qualified for Microsoft OCS R2 as well as certified by the service provider is the only proven method for guaranteed interoperability.

Reliability, High Availability, and Branch Office Survivability

Traditional TDM is a very reliable service and organizations expect the same level of reliability for VoIP. When organizations completely transition to IP, if a failure condition occurs either because there is no contact with the service provider network or there is degradation in the QoS over the SIP trunks, the lifeline of business is impacted.

A demarcation device with a SIP registrar and intelligent routing capability, addresses the risk of service disruption. This is especially true for branch office and remote office employees. When a connectivity loss is detected, a demarcation device can automatically restore telephone service at the branch office for intra-branch and PSTN calling.

Finally, many customers for various reasons may want to retain the relationship with their existing service provider but may not be able to do so because the service provider networks may not be officially qualified to work with OCS R2. At the time of this writing, Microsoft has qualified only three service providers to interwork with OCS R2. A demarcation device complements the list from Microsoft with its own set of qualified service providers. Because there is a larger set of service providers to choose from, organizations can design a very reliable telephony network for their Microsoft OCS deployments.

Authentication and Registration

Registration and Authentication with service provider may be necessary to ensure that only registered users are allowed access to the service. However, not all PBXs and IP-PBXs can support authentication to service provider networks natively. A demarcation device sitting at the edge of the enterprise network can ensure that the endpoints are properly authenticated before connecting to the SIP Trunking network.

OA&M Support

Both Service providers and enterprises need solutions that enable them to drive down the total cost of operations and support. Separate OA&M equipment besides increasing management complexity, will not be able to provide the required end-to-end quality metrics needed in an enterprise grade deployment.

A good demarcation device built for Microsoft OCS R2 will be able to integrate with both service provider networks and the Microsoft QoE server to offer true end-to-end operations and management.

NET'S SOLUTION WITH VX SERIES DEMARCATION DEVICE

SIP Trunking Solution Architecture for Microsoft OCS R2

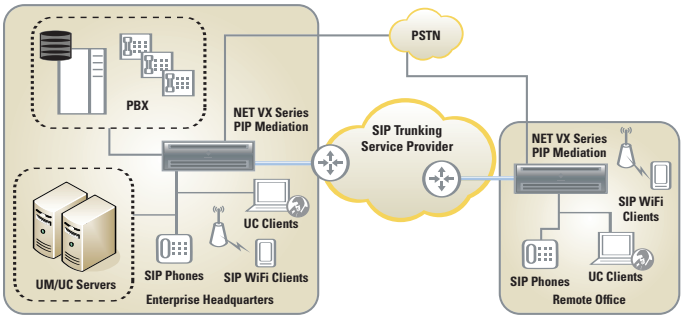

Figure 3: Solution Architecture

The VX Series intelligent voice gateway is a fully integrated multi-service voice switch that provides high-performance secure VoIP communications for the enterprise OCS deployments (See figure 3). It secures both signaling and media through standard protocols such as TLS and SRTP. The in-built firewall capabilities further extend the security by protecting the nodes from denial of service attacks. It is the industry's first fully integrated gateway with Any-to-Any protocol switching functionality, high call capacity, and security, creating a next-generation solution for enterprise VoIP and Unified Communications applications. VX Series gateways, including the popular VX1200 and VX1800, are Microsoft OCS 2007 R2 Qualified.

This section provides the technical details of NET gateways and their unique capabilities for integrating legacy voice infrastructure and OCS R2 with SIP Trunking service provider networks.

Any-to-Any Protocol Conversion

Working as a back-to-back user agent, NET gateways provide true, any-to-any protocol translation and media interworking between H.323, SIP, TDM signaling, DTMF encoding while, supporting a large number of codecs including RT Audio. For example, a VX gateway can convert in-band DTMF often used by SIP trunk providers to RFC 2833 DTMF relay commonly used in enterprise SIP networks.

Using a VX gateway, virtually any PBX can be connected to a SIP trunk provider network making them SIP capable. Also, a VX gateway deployed as a demarcation device provides supplementary services and feature transparency between on-net and off-net users. Basic supplementary services like call hold, call transfer, call waiting, three-way conferencing, call line identification (caller id), calling name are all supported by the VX Series.

It is extremely important to be able to support modem and fax calls over SIP trunks. VX gateways support T.38 for fax over IP. Finally, NET VX gateways support a wide variety of PSTN protocols for T1/E1 connectivity – MF-R1, T1 CAS (E&M, Loopstart), E1 CAS (MFC-R2), 4ESS, 5ESS, DMS-100, Euro ISDN, QSIG, NTT InsNet(Japan), Harris 20/20, CoreNet, and NI-2. NET VX Series gateways are certified to interoperate with several SIP Trunking service providers and are qualified for interoperability with Microsoft OCS R2.

Enterprise Class Intelligent Call Routing

Due to the diverse set of call processing equipment in an enterprise, the dial plans may need to be modified to either append or strip digits to normalize routing between the SIP trunks and the specific PBX. For example, Microsoft OCS and some service providers require a "+" to be added in front of a phone number. A simple translation rule in the VX gateway accomplishes this task.

NET VX Series gateways provide "Advanced Call routing" functionality through integration with Active Directory and LDAP servers. IT managers can dynamically create routing decisions such that if the user is not reachable on the IP network, then calls are routed to their mobile phone, home phone, or a SIP phone registered with the VX gateway. Additionally, the VX Series provides least cost routing to alternate service providers. A single VX gateway can register up to 5000 SIP phones and can configure up to 10000 call routes. VX Series gateways can function as a SIP registrar, Registrant, or in a Proxy Like mode.

Multipath Networks

NET VX Series gateways support a wide variety of telecom interfaces and can be deployed through satellites, Gigabit Ethernet, and Wireless LAN networks using 802.11x.

Bandwidth Utilization and Call Admission Control

Voice quality is a major concern for organizations. QoS and reliability are important factors for successful deployment of a SIP Trunking solution in an enterprise. A poorly designed network can congest and overwhelm access routers, degrading network performance and audio quality.

NET's proprietary BESTflow™ technology and the BEST™ Signaling Protocol (BSP) help reduce bandwidth requirements. Other frame packing technologies place multiple samples from a single call into one packet resulting in increased voice latency as packets wait to be filled. Using NET's Voice Transport Protocol (VTP), the NET VX increases network performance. The throughput of a router increases when inspecting a smaller number of larger sized packets as opposed to inspecting large number of smaller size packets for each call.

In addition to efficient bandwidth utilization, the NET VX can ensure that the network does not receive more calls than can be reliably transported over the SIP network. By providing a mechanism to limit the number of calls, the NET VX provides the first line of network defense against the denial of service attacks.

When calls enter an enterprise network on a SIP trunk, bandwidth consumption depends on the codec used. The SIP INVITE that arrives from the service provider includes the codec that the calling endpoint and service provider configuration has chosen. The NET VX, acting as a demarcation device through its codec transcoding functionality, ensures that only valid codecs are passed towards the enterprise network. Finally, the NET VX assures that only a specified number of calls are allowed per trunk group. This mechanism controls the maximum number of simultaneous calls allowed to enter the enterprise network. Each call is counted on the trunk group. When the number of calls exceeds the configured amount, the SIP INVITE request can be rejected or diverted to an alternative route.

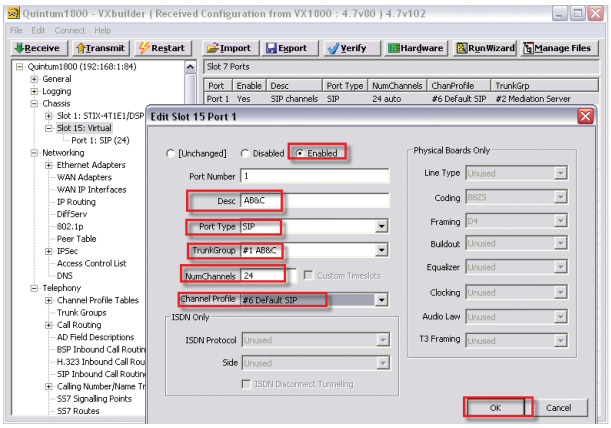

Figure 4: Configuring a Virtual SIP port for each trunk group

In the NET VX, a trunk group can be limited to a certain number of simultaneous calls. For example, in figure 4, THE NET VX only allows 24 simultaneous calls. A virtual SIP port is defined for each trunk group. The number of channels corresponds to the number of simultaneous SIP calls purchased from the service provider.

Security

Acting as a back-to-back user agent (B2BUA), the NET VX gateway can terminate encryption, make necessary firewall openings, and then re-encrypt traffic before it goes on to the next destination. A hardware based encryption model ensures that call processing capacity is not reduced even when calls are encrypted. NET VX series gateways use Transport Layer Security (TLS) protocol to secure signaling information and Secure Real Time Protocol (SRTP) for media packets. SRTP specifies how to securely transport real-time media. It is built on the foundation of RTP and adds the necessary encryption such as AES to the media packets making the voice traffic secure and reliable.

Additionally, an on-board firewall only allows VoIP traffic to pass through the VX in order to protect the network from DoS attacks. VX gateways also support VLAN tagging to isolate networks to further enhance security.

NAT Traversal

Most NAT & firewalls are not session aware or stateful. They block all unsolicited sessions originating from outside on most TCP and UDP ports. As the media control elements of the VoIP signaling protocols randomly select one port out of a large pool of 65000 UDP ports per call, the firewalls must keep open a large number of pinholes to support VoIP, causing security risks. Furthermore, as IP addresses are buried deep inside the signaling protocol messages, NAT will not work. If high security TLS is used, then the firewall cannot examine the packets as the packets are encrypted.

Expensive firewall upgrades may solve these firewall and NAT traversal issues. However, most organizations would like to extend the life of their security infrastructure. Additionally, some SIP Trunking service providers require that only a limited number of ports are open at any time. Typically this number is up to five ports. Therefore, in lieu of such an expensive upgrade, NET's proprietary VoIP signaling protocol, BSP (Bestflow™ signaling protocol), enabled between NET nodes placed on either side of the firewall solves the

aforementioned NAT traversal issue while providing increased message security between the nodes (see figure 5).

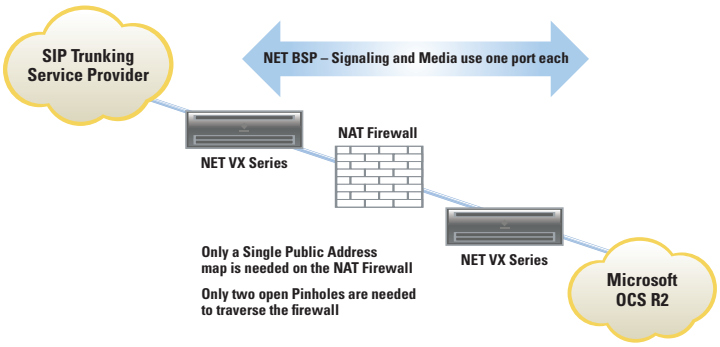

Figure 5: As a demarcation device, the NET VX solves NAT Firewall and Security problems by tunneling voice and signaling over two fixed ports.

NET's Bestflow™ technology uses only two UDP ports to carry both signaling and media traffic. Only these two ports have to be opened on the firewall, reducing the security risk for devices inside the firewall.

High Availability, Resiliency, and Survivability

In order for enterprise customers to adopt SIP trunks, the solution should offer the same high availability and resilient architectures that they have come to expect from TDM.

NET VX gateway offers enterprises flexibility in implementing SIP Trunking solution with Microsoft OCS R2. This flexibility can potentially provide the same level of reliability as offered by the traditional PSTN networks.

Using the NET VX gateway, organizations can deploy SIP trunks from multiple service providers and use load balancing or failover between them when necessary (See figure 6). In the case of IP network failure, calls can automatically failover to alternate SIP Trunking service provider or to a traditional PSTN access to improve the overall reliability (see figure 9).

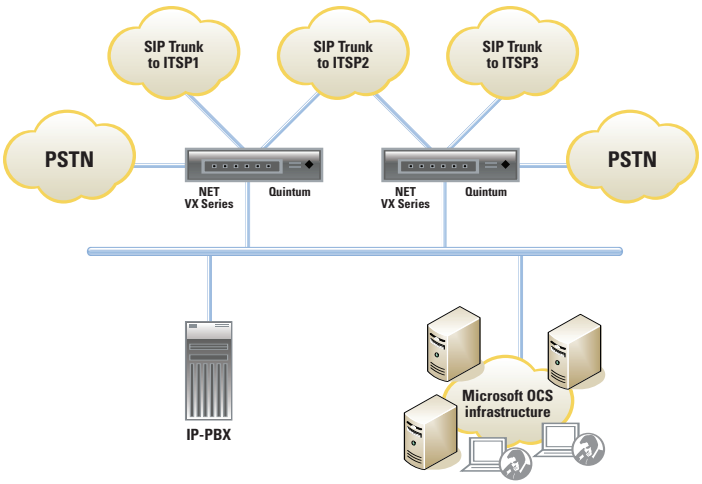

Figure 6: HA configuration

The VX gateway constantly monitors the IP network for failures with SIP OPTIONS, ICMP, or proprietary Link Quality Management (LQM) module. The "keep alive" messages offered by these techniques provide administrators results about the health of the IP connectivity. Based on the thresholds established by the administrator, the VX gateway can apply alternate routing. For example, the VX gateway can be configured to failover to a secondary SIP proxy (or a secondary border element) inside the carrier network when the primary proxy server fails.

In figures 7a and 7b, call routes are defined to the Primary and Secondary Border Elements inside the SIP Trunking service provider network.

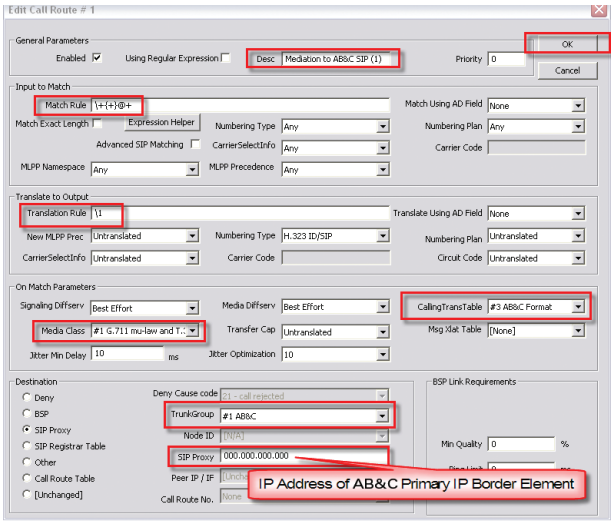

Figure 7a: Defining a primary border element inside a service provider network

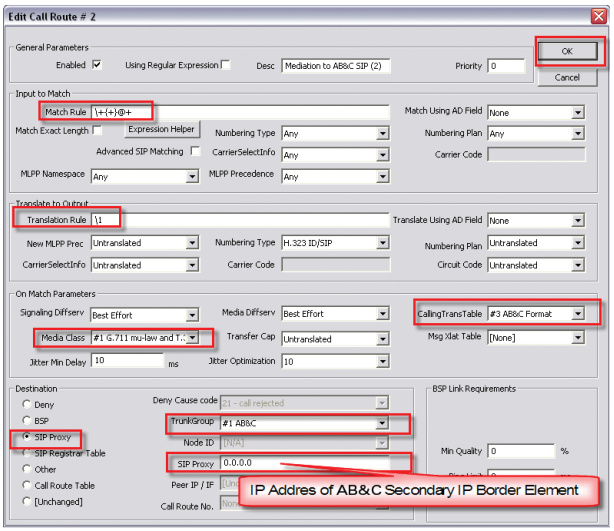

Figure 7b: Defining a secondary border element inside a service provider network

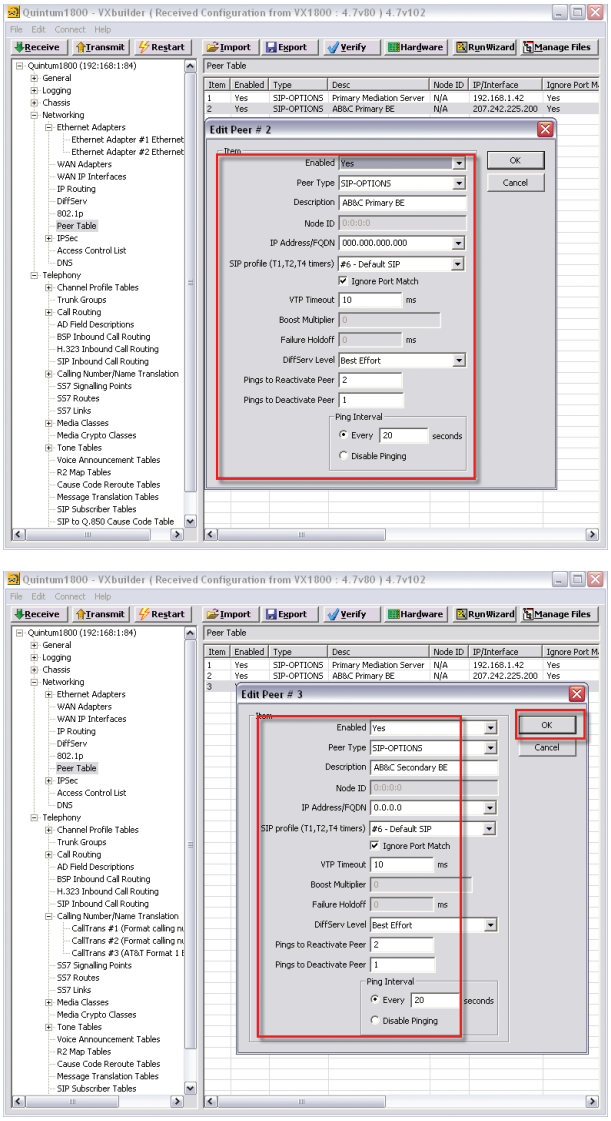

Figure 8: Both the Primary and Secondary Border Elements are configured as peers.

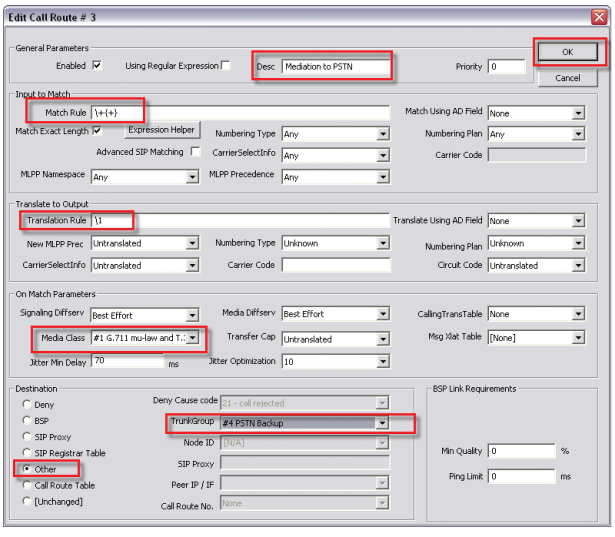

Figure 9: A call route is defined for PSTN failover

Network Management

VX Series gateways have a network management tool for real-time monitoring of the nodes. The management software displays status and alarms for all the channels configured on the VX node. It provides call detail records (CDRs) and also provides end-to-end voice quality metrics and provides statistics to Microsoft QoE servers.

SUMMARY

In conclusion, SIP Trunking provides on average 50 – 70% savings in telecommunications costs. In addition to cost savings, SIP trunks offer organizations productivity benefits and offer some new services like virtual telephone number that were not possible or difficult to provide in TDM networks.

Microsoft supports SIP Trunking natively in OCS R2. Deployed in a standalone mode, OCS R2 offers direct connectivity to ITSP networks. Given the complexities associated with interfacing multivendor and multigenerational PBXs and IP-PBXs with OCS, most enterprises need a demarcation device that provides the interface functions securely with legacy PBXs and ITSP networks. Another reason that is driving demand for a demarcation device is the need for enterprises to gradually migrate to OCS as most organizations are not likely to route calls directly to OCS. SIP Trunking service provider diversity is extremely important to offer the necessary failover reliability. At the time of this writing, only three service providers are qualified to interwork with OCS R2. That may not be sufficient for enterprise deployments especially when the enterprise may want to have a choice of service providers as well as for implementing some business critical applications like least-cost-routing and high availability.

A demarcation device is a very important component for interconnecting OCS R2 and existing voice infrastructure with SIP Trunking service provider networks. A good demarcation device has advanced capabilities like protocol mediation, branch office survivability, failover redundancy, and provides security against denial of service attacks.

The NETVX gateway is a good complement to existing TDM and IP infrastructure and helps connect diverse telephony equipment over a SIP Trunking solution provider network.

The solution from NET offers the following benefits:

- Is qualified for Microsoft OCS R2
- Is certified to interwork with several SIP Trunking service providers offering organization a wide choice of service providers to work with
- Provides interoperability with a wide variety of TDM and IP based PBXs
- Secures VoIP traffic and mitigates against denial of service attacks
- Repairs SIP messages to offer feature transparency across TDM and IP domains
- Connects mobile, remote workers with enterprise PBX users and offers branch office survivability
- Provides NAT, Firewall traversal for SIP messages

The following table provides a partial list of features supported by NET's demarcation device.

Feature	Supported	Comments
Call Admission Control	✓	
Modify SIP Message Headers	✓	
Dial Plan Modification	✓	
Fax	✓	Both T.38 and G.711
MidCall Codec Renegotiation	✓	
DTMF Methods	✓	RFC2833 In band DTMF
SIP Registrar, Proxy like mode, Registrant	✓	5000 SIP UAs can be registered. Requests from SIP UAs can be routed to any phone based on the dial plan. SIP UAs can reside behind a NAT GUI based management tool allows monitoring all 5000 SIP UAs
SIP Authentication	✓	
Transfer (REFER)	✓	REFER methods are not passed if the far side does not support REFER and sends an INVITE instead
Failover to Secondary Border Element	✓	SIP OPTIONS with configurable frequency or ICMP Ping
Calling Name Delivery	✓	
Calling Name Privacy	✓	
Call Hold and Resume	✓	
Voice mail Redirect	✓	Voice mail can be delivered to Microsoft Exchange 2007 UM or to another voice mail server
302 Redirect	✓	302 Redirect is not passed if the far side does not support but sends an INVITE instead
Survivability to PSTN	✓	

LEADERS IN NETWORK EVOLUTION

net™ Network Equipment Technologies

Corporate Headquarters
6900 Paseo Padre Parkway
Fremont, CA 94555 U.S.A.
T 510.713.7300
F 510.574.4000
E info@net.com
www.net.com

N.E.T. Federal
21660 Ridgetop Circle, Suite 100
Dulles, VA 20166, U.S.A.
T 703.948.1800
F 703.948.1850
E net_federal@net.com

Microsoft GOLD CERTIFIED Partner

OEM Hardware Solutions
Information Worker Solutions
Networking Infrastructure Solutions