

# Enabling Resilient, Secure, and High Availability Voice Services in Microsoft OCS Deployments

December 2008

# Leveraging VX Series Intelligent Gateway for Increasing Enterprise Voice Security and Resiliency

## EXECUTIVE SUMMARY

Organizations are moving towards a centralized call processing model by leveraging the converged IP networks to save costs. But planning to consolidate infrastructure at the headquarters and extending the enterprise to include branch offices and remote sites, needs careful planning.

Any downtime in voice services either at the headquarters or the branch offices leads to loss of productivity, profitability, and competitiveness. In order to provide branch office employees the same voice experience as in the headquarters, organizations need to consider solutions that provide voice service continuity through resilient enterprise grade telephony architecture. A single point of failure architecture may render remote offices completely unreachable if the data network is down.

Banks, retail enterprises, government agencies, educational institutions, or any company with branch offices, needs a solution that:

- Minimizes or eliminates impact of service disruption
- Provides secure voice connectivity
- Defends against denial of service attacks
- Provides highly scalable architecture to meet the growing demands of the enterprise, and
- Consolidates infrastructure to reduce cost

NET product portfolio consists of Quintum Tenor Multipath Gateways and Switches for the small to medium enterprises and the VX Series Intelligent Voice Gateways for medium to large enterprises. The entire product line is architected to provide reliable voice services for the headquarters and at the branch/remote sites.

## PROVIDING HIGHLY AVAILABLE AND RESILIENT GATEWAYS FOR MICROSOFT OCS DEPLOYMENTS

Security threat to VoIP services and systems are real and may cripple the organization's ability to conduct business. Just as traditional PBXs, IP Telephony systems also have to offer high reliability and resiliency. A properly designed VoIP architecture should include features like high availability, load balancing, and security features such as encryption and firewall capabilities to thwart denial of Service attacks (DoS). The type of transport protocol supported by the network also has an impact on the resiliency of the voice services.

## SECURITY

Securing against malicious use, sabotage, and Denial of Service attacks is necessary for the successful implementation of VoIP. With access to public Internet and other external networks, security becomes an important issue to consider.

Toll Fraud is caused when malicious users try to make personal calls using an enterprise VoIP network. Under some conditions, certain gateways provide users with a secondary dial tone. A knowledgeable user may be able to make calls by dialing external access digit which is typically '9' in most organizations. Unlike other gateways, VX and Tenor Series gateways will never provide a secondary dial tone.

Other security issues such as eavesdropping and denial of service attacks can be mitigated by implementing encryption and firewall capabilities. The VX Series Intelligent Voice Gateways offer both TLS and SRTP encryption and a built-in firewall to protect against denial of service attacks.

## ENCRYPTION

In order to provide a high level of security, both signaling and media traffic needs to be encrypted. It is very easy to intercept SIP messages as it uses plain text for SIP Signaling. VX Series gateway uses Transport Layer Security (TLS) protocol to secure signaling information from intruders. Secure Real Time Protocol (SRTP) is used by the gateway to encrypt the media packets.

To protect callers on the network, VX Series gateway supports 128-bit Advanced Encryption Standard (AES) media encryption via SRTP. An X.509 digital certificate either created by the VX Series or supported by a third-party certificate authority provides the necessary encryption key. The encryption and secure key exchange supported by VX Series gateway enables mutual authentication using Message Digest 5 (MD5) Secure Hashing Algorithm (SHA).

Even as encryption provides voice security from eavesdropping, it creates a significant drain on call processing capacity. VX Series implementation of a separate hardware accelerator card within the VX chassis provides wire-speed encryption so there is no degradation of either call quality or capacity. VX Series supports up to 1000 simultaneous calls on a single box whether encryption is used or not.

## DENIAL OF SERVICE ATTACKS

Malicious users launch Denial of Service (DoS) attacks to cripple voice services in an organization. DoS attacks may be targeted to a specific end point or to the entire network by sending a large volume of traffic over the IP network. A VoIP aware gateway can be used to mitigate against DoS attacks.

The VX Series gateway provides protection through features like VLAN tagging and built-in firewall capabilities to stop DoS attacks. Using VLAN tagging, VoIP traffic can be separated from data traffic to provide additional security for voice. The built-in firewall in the VX Series gateway only allows VoIP traffic to pass through. Other packets that are not voice related are immediately dropped to minimize impact of DoS attacks.

## RELIABLE TRANSPORT USING TCP PROTOCOL

User Datagram Protocol (UDP) is a widely used protocol for streaming audio and video. Early SIP RFCs required vendors to support SIP over UDP communications only. Now, RFC 3261 requires support for both UDP and Transport Control Protocol (TCP). TCP transport provides reliable message delivery and connection-based communications protocol. Tenor and VX Series gateways from NET and Quintum support both UDP and TCP transport protocols for providing a reliable transport mechanism while also increasing the number of interoperable elements in the network.

## HIGH AVAILABILITY & LOAD BALANCING

The data networks may not always be operational due to a scheduled downtime or due to unscheduled events like power failure. A high availability solution ensures that the voice services are always available and the users are able to place and receive calls even under peak call rates or during network disruptions.

A pair of VX Series gateways configured in an Active-Active mode provides the necessary enterprise grade network resiliency for voice services through implementing high availability and load balancing architecture (see Figure 1). For incoming calls, VX series load balance across multiple mediation servers in a Microsoft OCS environment. The calls to the mediation server are then load balanced using round robin method. NET VX Series Intelligent Voice Gateways are engineered to handle up to 1000 simultaneous calls on a single node.

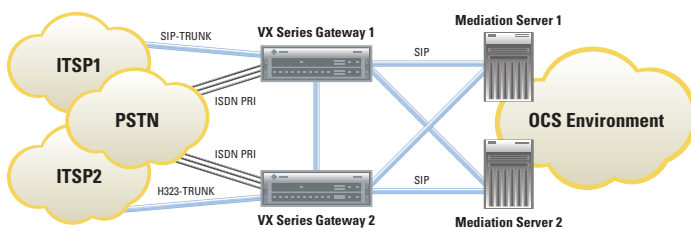


FIG. 1: VX Series gateways configured in an Active-Active mode provides enterprise grade network resiliency.

## RECOVERING FROM MAJOR DISRUPTIONS

Disruptions always happen and a resilient architecture provides protection for voice services from these interruptions. Availability of voice services can be impacted due to the following reasons:

- Hardware and power failure
- Link failure between sites

### Recovering from Hardware Power Failure

NET's VX1800 Series gateway comes with a redundant power supply to minimize failures.

## Recovering from Link Failures

Voice service can be disrupted due to failures of the IP network. VX Series Intelligent Media Gateways rely on Link Quality Management (LQM) functionality to monitor the quality of the network. LQM works by sending "I'm alive" messages periodically to establish availability of the next node in the network. This technique is used to check the health of the network and other VX nodes on the IP network. Using LQM statistics, VX Series gateway can collect statistics such as the average expected round trip time to the node, the average packet loss to a particular node on the network, and the node's availability. If the node is unreachable, then calls going to the node are skipped and the gateway will try alternate routes. In order to mark a node unreachable, the VX gateway:

- Sends an ICMP Ping command to the remote node's domain address. If the ICMP ping is unsuccessful, then the VX Series gateway determines that the node is unreachable and tries alternate routes to complete the call.
- If the remote node is a SIP application, SIP-OPTIONS message is used to check if the SIP application is alive or not. The Options method is used to measure the delay. Depending upon the thresholds reached, the VX series gateway may determine that the SIP application is unreachable and an alternate route is attempted to complete the call.

NET VX Series Gateway can be configured to reroute incoming calls to a PSTN or mobile network in case of failure of the IP networks. IT manager can configure up to 10,000 alternate routes on a single VX gateway to provide a high degree of business continuity for the enterprise.

## PROVIDING RELIABLE BRANCH OFFICE SOLUTION FOR MICROSOFT OCS DEPLOYMENTS

### Branch Office Availability

A centralized call processing model saves costs, reduces complexity, and increases management flexibility. However, the unintended consequence of the centralized model is reduced service reliability. Since voice traffic is carried through the data network, branch offices will remain isolated when the data network goes down. An enterprise grade gateway solution should ensure business continuity by restoring basic voice services at the branch office when the system failure occurs.

### VX Series providing Branch office Availability for OCS

NET's VX Series media gateways are designed to support both circuit-based and IP-based telephony within a distributed enterprise network. VX1200 and VX1800 rely on Link Quality Management (LQM) functionality to monitor the quality of the IP network.

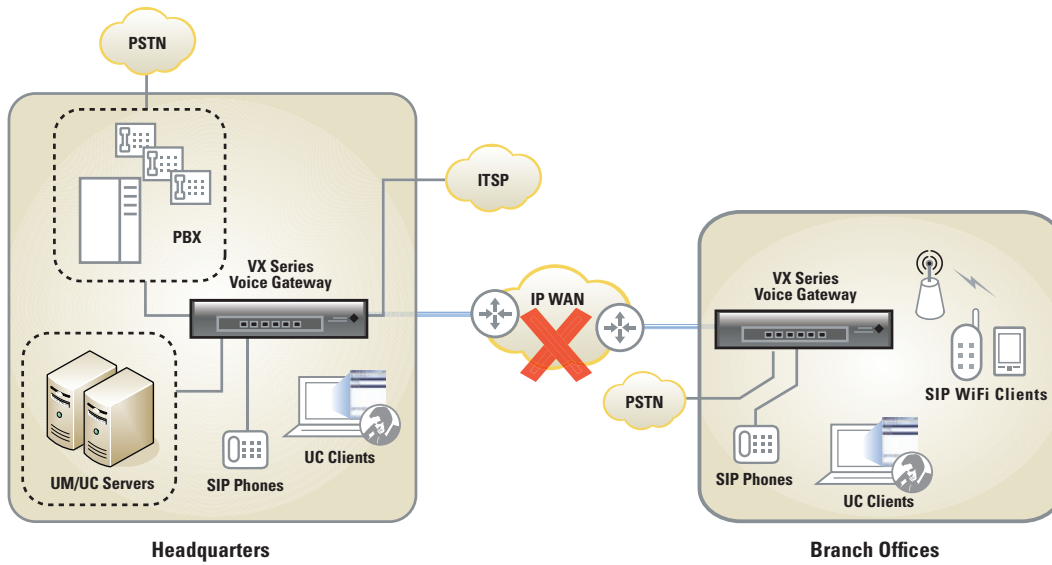
In the case the Link Quality thresholds are not reached, calls are routed through the PSTN. Employees continue to make calls through the VX series gateway for calls made within the organization. Incoming and outgoing calls to the external users are routed over the PSTN network.

VX Series can provide “Advanced call routing” functionality through integration of Active Directory/LDAP servers. IT manager can dynamically create routing decisions such that if the user is not reachable on their Microsoft Office Communicator client, then the call routing decisions can be configured to reach their mobile phone, home phone, or a SIP/Wi-Fi phone registered with the VX series gateway (see Figure 2). Provisioning alternate routes is simple and easy as most administrators already know how to use the Active Directory databases. VX Series maintains alternate routing numbers in the cache locally. Maintaining local cache on the VX Series node is especially useful in cases where IP network is down and it is not possible to reach the Active Directory server at the headquarters.

## CONCLUSION

As telephony networks are consolidated, organizations need a mature solution that provides highly resilient architecture for their unified communications deployments. NET VX Series gateways for Microsoft OCS, provides high-availability and secure solution which increases voice service reliability and improves business continuity both at the headquarters and at the branch offices.

**FIG. 2: VX Series detects LAN/IP WAN is down with no OCS connectivity and uses AD/LDAP to route call to any end point like a mobile phone, SIP phone, or an attendant.**



**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 Ridgeway Circle, Suite 100  
 Dulles, VA 20166, U.S.A.  
 T 703.948.1800  
 F 703.948.1850  
 E net\_federal@net.com



OEM Hardware Solutions  
 Information Worker Solutions  
 Networking Infrastructure Solutions

This document does not create any express or implied warranty by NET or about its products or services. NET's sole warranty is contained in the written product warranty for each product. The end-user documentation shipped with NET products constitutes the sole specifications referred to in the product warranty. The customer is solely responsible for verifying the suitability of NET products for use in its network. Specifications are subject to change without notice.

© 2008 Network Equipment Technologies, Inc. All rights reserved. NET, the NET logo are trademarks of Network Equipment Technologies, Inc., and its subsidiary, N.E.T. Federal, Inc. All other trademarks are the sole property of their respective companies.

IVGMSOCS-WP-1208