

Wireless Network Quality of Service

WHITE PAPER

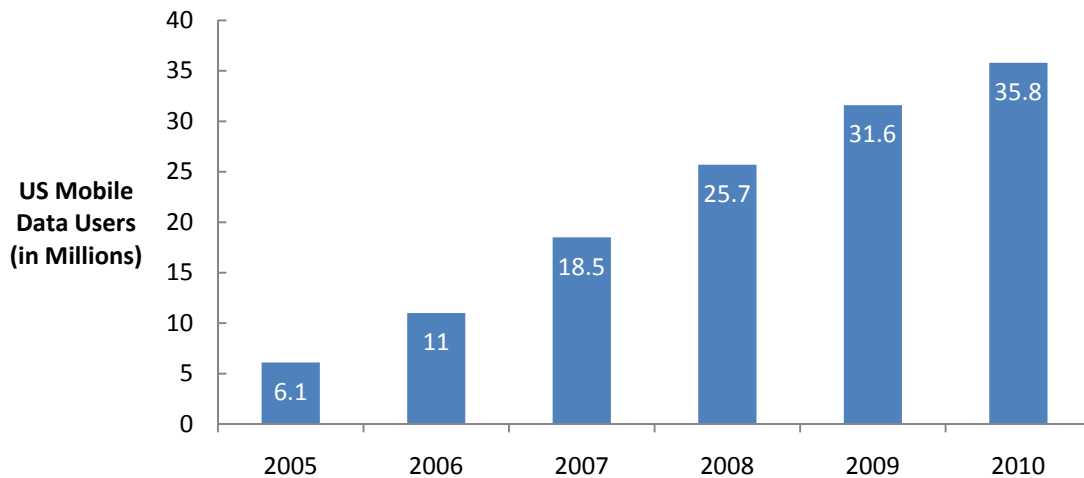
Overview

Yankee Group estimates that over 39% of the US workforce — 51 million workers — are mobile, spending 20% or more of their time away from the primary workspace¹. Furthermore, the number of mobile data users is growing rapidly and Yankee Group estimates it will exceed 35 million by 2010².

A key challenge faced by enterprise IT managers is how to ensure the productivity of this expanding population of mobile workers. Enterprise mobility offers significant opportunities to organizations. More time in the field meeting customers, prospects and partners can equate to stronger business relationships, increased revenue potential and greater efficiency. But providing mobility in today's enterprise environment is not a simple task. Successful mobile deployments require IT managers to take a holistic approach to managing all elements of the mobile deployment, including applications, wireless networks and devices.

Growth of the Mobile Workforce

Source: Yankee Group, 2006



Failures in mobile deployments are often attributable to an element entirely out of the hands of enterprise IT management — constrained bandwidth on public wireless networks. While there are management tools that allow control over bandwidth usage on private (managed) networks, most mobile workers rely on at least one and often more than one cellular data network to access corporate information and applications. To keep their mobile workers productive, enterprises need to employ Quality of Service (QoS) tools to ensure that critical applications and data operate efficiently regardless of the wireless network in use. When implemented properly, QoS solutions:

- Prevent non-critical applications from impeding critical ones
- Keep the mobile worker productive during periods of high network use
- Give priority to real-time streaming applications, such as voice-over-IP and video delivery
- Preserve quality and ensure timely delivery for media streams, by correcting for dropped packets
- Optimize the apparent performance of wireless networks

^{1,2} Yankee Group, "Optimize Enterprise Productivity Through Mobility: Choosing the Right VPN Solution," December 2006, p.1

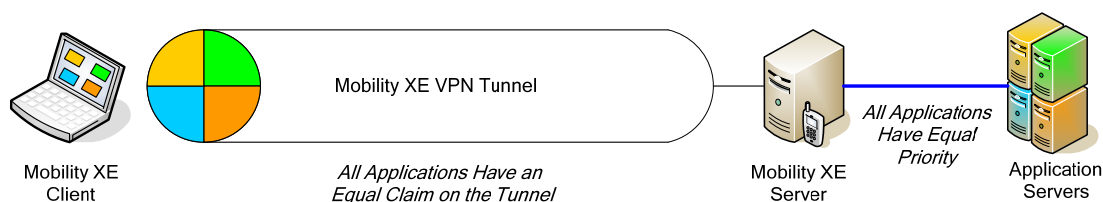
Mobility XE QoS

NetMotion Wireless' mobile VPN, *Mobility XE*, provides a robust suite of features that help workers stay productive by insulating applications from coverage gaps and other service disruptions. It enables seamless roaming between wireless networks and helps IT departments maintain security and enterprise control over their mobile workers, devices and networks.

Mobility XE also provides advanced QoS capabilities that let IT managers optimize mobile worker access to applications and data. These capabilities are part of the Mobility XE Policy Management module. By applying QoS policies, administrators can shape the data traffic transmitted through Mobility XE's secure VPN tunnel. They are able to designate which applications and processes receive higher bandwidth based on device, user, user group and more.

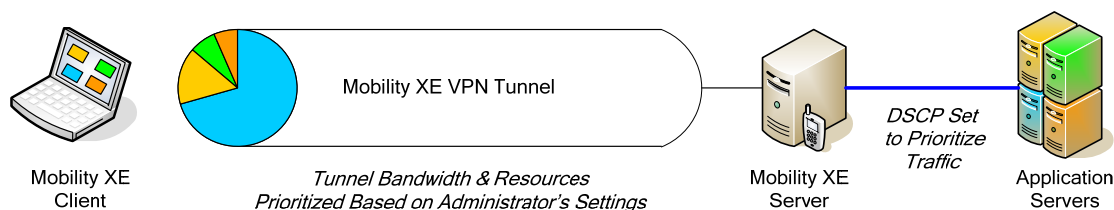
Without QoS

Without QoS, all applications have equal claim on the network bandwidth available between the mobile device and the Mobility XE server. Critical and non-critical applications, OS updates, antivirus updates, NetBIOS file-sharing and other traffic all compete for available bandwidth. Real-time applications (RTAs) such as VoIP and video are especially prone to quality problems because they are more susceptible than traditional "data" applications to deteriorated performance when bandwidth is constrained, or when there is appreciable latency or jitter. Real-time data flows are especially challenging for IT departments to control as they typically use randomly available ports to connect, making it impossible to know in advance which ports to block/allow for setting QoS policies.



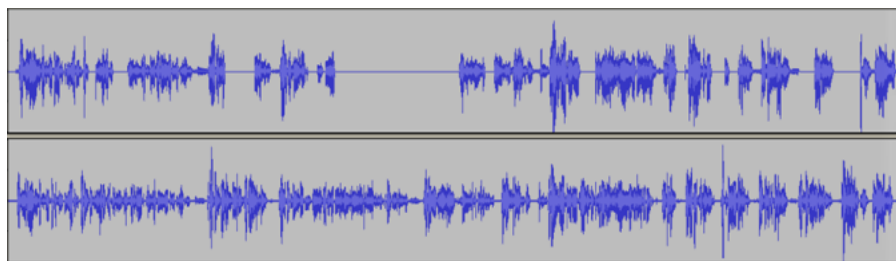
With QoS

Using QoS policies that are centrally administered and automatically deployed, Mobility XE can set the traffic-shaping priorities for each application over any wireless network. This allows the most critical application traffic to supersede all other data traffic, ensuring mobile worker productivity. Non-critical applications only receive bandwidth as it becomes available.



Mobility XE also supports DSCP tagging. This Internet standard uses TOS (Type of Service) bits in the TCP/IP packet header to allow network infrastructure components, such as routers and firewalls, to prioritize routing.

QoS policies are particularly well-suited for managing real-time applications because they can be applied based on application name so that they receive priority even though the ports they use may change.



The top waveform, of a voice conversation, exhibits 10% packet loss. Multiple words and an entire phrase are missing. Bottom, packet-loss reduction applied through Mobility XE QoS replaces the missing packets.

QoS policies also include the ability to perform Packet-Loss Recovery (PLR) for real-time applications. The PLR technique applied by Mobility XE uses a sophisticated mathematical technique that adds some additional payload to each packet. When packets are lost, PLR reconstructs them using information from the packets that were received. Using PLR for real-time application streams guards against breaks in the conversation or momentary picture loss, and improves the overall quality of the communication when networks lose packets or experience high latency or jitter.

The QoS settings in the Policy Management module are created and managed centrally via Mobility XE's management console and enforced on the remote devices. Should the settings need to be changed, administrators can modify them once (at the server) and they are automatically sent out to all subscribed mobile devices.

Device to DMZ

Mobility XE's QoS traffic shaping is enforced from the mobile device to the Mobility XE server, regardless of which wireless (or wired) networks are in between, and whether they are public or private. By contrast, QoS settings implemented by a wireless carrier in their network or as part of a WLAN are only active within the discrete network, representing only a portion of the path between the mobile device and the Mobility XE server. As a mobile deployment expands and workers connect to available wired, Wi-Fi or cellular data networks, maintaining control over quality and prioritization of the users' access to applications and data ensures their continued productivity.

Field Service Example

A field service organization has five key applications: billing, systems management for remote devices, corporate IM, a Web-based CRM application and e-mail. The field technicians carry laptops throughout the day, and use them occasionally at home and in a branch office. The laptops have a number of background applications which have been installed by the operating system, such as Windows Update, or come from third parties, such as automated antivirus or printer-driver updates.

The field technicians typically spend 32 hours a week in the field and 8 hours at a regional office. While in the field they are connected via a wireless carrier's data network. At the regional office they connect via an in-building wireless LAN.

QoS Solution using Mobility XE

Using Mobility XE's Policy Management module, the IT managers specify QoS priorities for each application. They give the billing application and remote-device systems management application the highest priority — as these are the applications essential for an on-site field technician. A moderate priority is given to Web CRM, corporate instant messaging and e-mail. All other applications are given a background priority — the

lowest setting. This set of policies prevents the field technician's productivity from being disrupted because some non-essential application is siphoning off bandwidth.

For example: The technician begins his workday in the field, boots his device and antivirus software attempts to download a large signature file over a cellular data network. QoS policies step in. The policy can either throttle back the download so it doesn't sap bandwidth from key working applications, or block the download temporarily. In the latter case, the policy prevents the download over the cellular data network, but allows it when the technician is at the corporate office connected to the wireless LAN.

Furthermore, QoS policy settings can be defined to behave differently depending on the time of day, the device, the user, etc. The field service organization, for example, might want certain applications such as file synchronization to only happen during off-hours. Or executives may want e-mail set to high priority when using Windows Mobile devices.

Conclusion

Quality of Service capabilities are one of the key building blocks for a successful mobile deployment. By implementing policies to govern access to enterprise data, IT management can better manage and enhance the productivity of their workers and protect their organizations. QoS gives IT managers complete power over their entire mobile deployment by letting them shape and control traffic across any network that their users may connect to. QoS also lets IT management handle the ever-growing population of mobile workers with tools that make even the largest deployment manageable.

Learning More

If you are a NetMotion Wireless customer, please see Tech Note 2212 on Configuring Quality of Service. If you are not a NetMotion Wireless customer, please see our website, <http://www.netmotionwireless.com> or contact sales@netmotionwireless.com for more information.

© 2009 NetMotion Wireless, Inc. All rights reserved. NetMotion and NetMotion Mobility are registered trademarks, and Mobility XE, Roamable IPSec, InterNetwork Roaming, Best-Bandwidth Routing and Analytics Module are trademarks of NetMotion Wireless, Inc. Microsoft, Microsoft Windows, Active Directory, ActiveSync, Internet Explorer, Windows Mobile, Windows Server, Windows XP, SQL Server, Windows XP Tablet PC Edition and Windows Vista are registered trademarks of Microsoft Corporation. All other trademarks, trade names or company names referenced herein are used for identification purposes only and are the property of their respective owners. NetMotion technology is protected by one or more of the following US Patents: 6,198,920; 6,418,324; 6,546,425; 6,826,405; 6,981,047; 7,136,645; 7,293,107; and Canadian Patent 2,303,987. Other US and foreign patents pending.