At a glance:

- The Next-Generation TCP/IP stack
- User-focused networking tools
- Improving network security
- Simplifying network management

Enterprise networking with Windows Vista

Jason Leznek

When was the last time you tried working for an entire day without being connected to your corporate network? Think about it – no access to e-mail. No browsing the Internet. You couldn't use printers or file shares. You couldn't access your essential data in sales databases. You wouldn't be able to do your job at all.

Network connectivity is critical to most people's ability to function at work. Likewise, there are more expectations from users to be mobile, connecting their corporate-owned laptops to virtually any public or home network anywhere. Do you shudder at the security ramifications?

The engineers in the Windows Vista networking team know how important connectivity is, and they have been hard at work making the best set of networking innovations since Windows® 95. With Windows Vista, networking becomes simpler to use, more secure, easier to manage and scalable to the largest of networks.

It's been five years since Windows XP was released. A lot has changed in that time, including a need for more ubiquitous wireless networking capabilities wherever users may be; governmental or industrial regulations like Sarbanes-Oxley and HIPAA; and the need to reduce costs and utilise current investments more efficiently. Users expect

This article is based on a pre-release version of Windows Vista. All information herein is subject to change.

network resources to 'just be there' and become frustrated with the slightest hint of a connectivity problem. Finally, users are more mobile than ever before, and they may not be connecting to just your corporate network – they could be connecting to virtually any network around town.

Start with the stack

Windows Vista includes an updated implementation of the TCP/IP stack, which features significant improvements that address several top networking issues, offering greater performance and throughput, a native Wi-Fi architecture, and APIs for network packet inspection.

Maximising network utilisation requires complex tuning of TCP/IP configuration settings. Windows Vista eliminates the need to do this manually by detecting network conditions and automatically optimising performance. On high-loss networks, such as wireless networks, Windows Vista can better recover from single and multiple packet losses. It can dynamically increase or decrease the TCP receive window to fully utilise the link. Users transferring files across a high-speed/high-latency WAN or downloading files from the Internet should notice much faster transfer times.

Windows Vista also includes a native wireless networking architecture (Native WiFi) as part of its core networking stack. The benefits include flexible deployment across many hardware brands and models, similar user experiences regardless of the hardware, and more reliable third-party wireless NIC drivers. Wireless networking in Windows Vista can be centrally managed, supports the latest security protocols and provides the user with a more seamless network experience.

The Windows Filtering Platform (WFP) is a new architecture in the Next-Generation TCP/IP stack that provides APIs which third-party software developers can use to participate in the filtering decisions that take place at several layers in the TCP/IP protocol stack without having to write their own kernel-mode applications. The platform also provides support for next-generation firewall features such as authenticated communication and dynamic firewall configuration based on an application's use of the Windows Sockets API (application-based policy).

Empowering the user

The Network and Sharing Center is a single place for users to check network status – if they are connected, what they're connected to, and whether they are on the local network or the Internet (see **Figure 1**). They can also view the status of various network services on their computers. Is the computer discoverable on the local network? Are any folders or printers shared? The user can also create or connect to an existing network, whether it is an ad hoc or infrastructure wireless network, VPN or home broadband connection.

Windows Vista can also diagnose and resolve many connectivity issues without the user needing to call the help desk. The Network Diagnostics Framework provides Windows Vista with the ability to identify the root cause of the connectivity problem from the context of the application's action. For example, if the user can't reach an Internet site, Network Diagnostics will attempt to trace the problem, from whether there's an active wireless connection and a valid IP address, through accessing the DNS server, finding the proxy server, and getting a response from the Web server.

If a problem is found, the user gets a message clearly identifying the problem and how

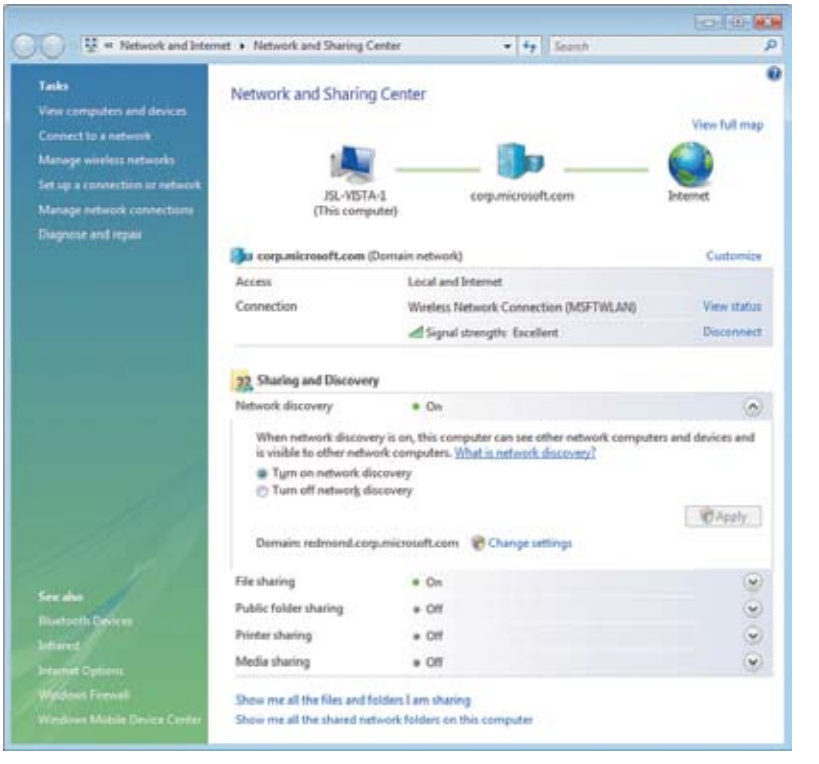

Figure 1 **Network and Sharing Center**

to resolve it (see **Figure 2**). Sometimes it's as simple as clicking a response. Other times, the user must make a configuration change, and the dialog box will bring the user to the exact location. Sometimes the user simply can't take the appropriate action because of lack of knowledge or administrative privileges; richer information is logged to the Event Viewer so the help desk can work on resolving the problem quickly instead of spending hours troubleshooting.

Windows Vista has Network Awareness APIs that applications can call to get connectivity status, enabling an application to become aware of changes in connectivity and to identify the type of network – domain, public or private – the computer is currently connected to. When Windows Vista can access the Domain Controller across the network, it switches into the Domain profile automatically. No other networks can be placed in this category. All other networks are categorised as public unless a user or application identifies the network as private. Networks that represent direct connections to the Internet or are in public places, such as airports and coffee shops, should be left public. Only networks located behind a private gateway device should be identified as private, such as home or small business networks.

Windows Vista improves the behaviour of the wireless client to mitigate wireless attacks.

With Network Awareness, applications such as Windows Firewall with Advanced Security (discussed later) can have different configurations based on the type of network currently connected to, and switch between configurations automatically when the network type changes. For example, the administrator may have configured the firewall to open up specific ports for desktop management software while the computer is connected to the domain network, but those same ports should be automatically closed when the user is working at a public hotspot.

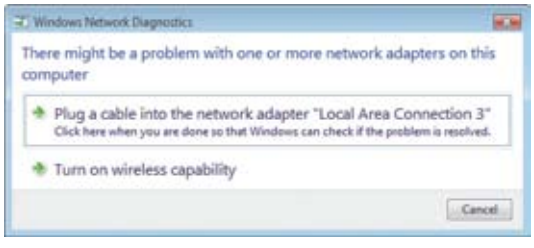

Figure 2 **Troubleshooting a connectivity problem**

Group Policy is also network-aware in Windows Vista: it automatically knows when the computer is on the domain network and begins processing any new Group Policy settings without having to wait for the next refresh cycle. This means that Windows Vista will automatically check for new Group Policy settings when it connects to the domain network even if it is coming out of hibernation. This allows administrators to deploy security settings faster when time is of the essence.

Securing the network

There are many types of threats – users accessing wireless networks that are not as they seem, unhealthy guest PCs connecting to a corporate network, and unmanaged resources attempting to access resources they shouldn't have access to. It's enough to keep a network administrator busy all day and worrying all night. Windows Vista can help with all of these scenarios, with enhanced network security features that are comprehensive yet easy to configure.

The native Wi-Fi architecture in Windows Vista has wide support for the latest security protocols, including Wi-Fi Protected Access (WPA) 2 Enterprise and Personal, PEAP-TLS, and PEAP-MS-CHAP v2 (Protected Extensible Authentication Protocol with Transport Layer Security and with Microsoft Challenge Handshake Authentication Protocol). This broad support ensures interoperability between Windows Vista and almost any wireless infrastructure. The capabilities of the wireless network card are examined by Windows Vista and the most secure protocol is chosen by default when connecting to or creating wireless networks. Using the EAP-HOST framework, Windows Vista is able to support custom authentication mechanisms defined by a hardware vendor or by an organisation.

Windows Vista includes many improvements to the behaviour of the wireless client to mitigate common wireless attacks. The cli-

ent will automatically connect only to networks the user has explicitly requested or identified as preferred networks and will not automatically connect to ad hoc networks. The client also provides a warning if the user is about to initiate a connection to an unsecured network. Additionally, the client will actively probe for fewer preferred networks and only if instructed to do so by the user, making it more difficult for attackers to identify what network the client is trying to connect to and create a rogue network with the same name.

The Windows Vista native wireless client supports a single sign-on (SSO) feature, which executes Layer 2 network authentication at the appropriate time given the network security configuration, while at the same time integrating with the user's Windows logon experience. Once a single sign-on profile is configured, network logon will precede the Windows logon. This feature enables scenarios such as Group Policy updates, logon scripts and wireless bootstraps, which require network connectivity prior to user logon.

Windows Firewall with Advanced Security brings a new level of network security to the Windows platform, providing support for both inbound and outbound filtering as well as Windows Service Hardening. If the firewall detects a Windows service behaving abnormally as defined by the Windows Service Hardening network rules, the firewall will block it. Windows Firewall with Advanced Security also supports Authenticated Bypass, which enables certain computers authenticated with IPsec to bypass firewall rules for such tasks as remote management.

One of the most significant changes in Windows Firewall is its integration with IPsec. In the past, administrators needed to rely on two separate tools – a firewall and an IPsec deployment and management tool – to create a layered set of network security rules. With Windows Vista, administrators can create simple network security rules that may combine both firewall port and IPsec rules to protect the network from unauthorised access. This integration provides a simple way to enforce authenticated, end-to-end network communications, providing scalable, tiered access to trusted network resources and/or protecting the confidentiality and integrity of data.

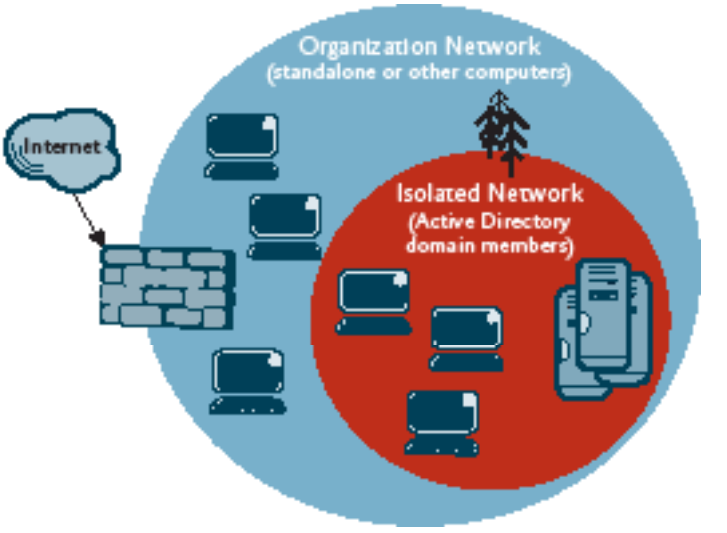

Figure 3 **Server and domain isolation**

The administrator can logically isolate the corporate network into zones that can be accessed by any computer (including guests) or by just those computers that have authenticated to the domain (Domain Isolation). The administrator can further isolate specific servers that should only be accessed by a specific set of users or computers, such as an HR application server being restricted to computers in the HR group (Server Isolation) as shown in **Figure 3**.

Viruses or worms can enter private networks through a mobile laptop and quickly infect other computers. Windows Vista, when connecting to a network infrastructure based on Windows Server code-named 'Longhorn' (the next version of Windows Server) will support Network Access Protection (NAP) to reduce the risks of connecting unhealthy computers to private networks directly or across a VPN connection. If a computer running Windows Vista lacks current security updates, virus signatures, or otherwise fails to meet corporate security requirements, NAP blocks the computer from full access to the network. Instead, it will be connected to a restricted network where it can download and install the updates, antivirus signatures, or configuration settings that are required to comply with current health requirements.

Simplifying Network Management

The networking features in Windows Vista have been designed to support high levels of manageability to help reduce the cost of deploying wireless networks and network secu-

rity policies, as well as to provide quality of service for applications and users. Windows Vista uses Group Policy or command-line scripting via the Network Shell (NETSH) extensively to manage network features, so you don't need to learn or deploy a new management tool, and you can take advantage of your existing investment in Active Directory and the Organizational Unit (OU) structure you have already created.

Deployment and management of network security rules – combining firewall and IPsec policies – is made easier within a single wizard-driven Microsoft Management Console (MMC) snap-in called Windows Firewall with Advanced Security (see **Figure 4**) or command-line scripting via NETSH. The new snap-in provides a simple way to deploy inbound or outbound filtering and connection security rules that limit access by specific users, computers or applications while providing a granular level of administrative control. IPSec can request or require authentication by user, computer or health certificate (integrating with Network Access Protection) to provide a scenario-based security policy. The snap-in makes the creation of server or domain isolation rules easy and, since it is Group Policy-based, you can target these rules based on your business structure.

Using Group Policy, you can also define how mobile clients connect to and operate on wireless networks. For example, a company may define a policy that requires all wireless connections to use a certain protocol or that all connections must be limited to a certain wireless network. Because these settings are made via Group Policy, the end user can be prevented from changing these settings.

NETSH enables automation and scripting to assist in troubleshooting wireless network connections. Using the command-line interface, administrators can verify, change or remove a client's wireless network configuration profiles. These configuration profiles can also be exported to and imported from other computers to expedite provisioning of multiple computers.

Network quality can diminish because high-bandwidth applications tend to consume all available capacity, and applications are not written to give central bandwidth control to IT administrators. Adding more bandwidth may not solve these problems; instead, it only leads to the same applications consuming the newly available capacity. With policy-based quality of service (QoS), administrators can prioritise and/or throttle outbound network traffic without requiring applications to be modified. Policies can either mark outbound traffic with a Differentiated Services Code Point (DSCP) value for routers to prioritise or let Windows Vista throttle the amount of outbound traffic sent, regardless of the router configuration. Combining both techniques provides even greater flexibility. **Figure 5** shows the creation of the QoS policy.

Scaling to the enterprise and beyond

Enterprise-level organisations often worry about scalability issues when supporting their network. For example, you may begin running out of available IP addresses, espe-

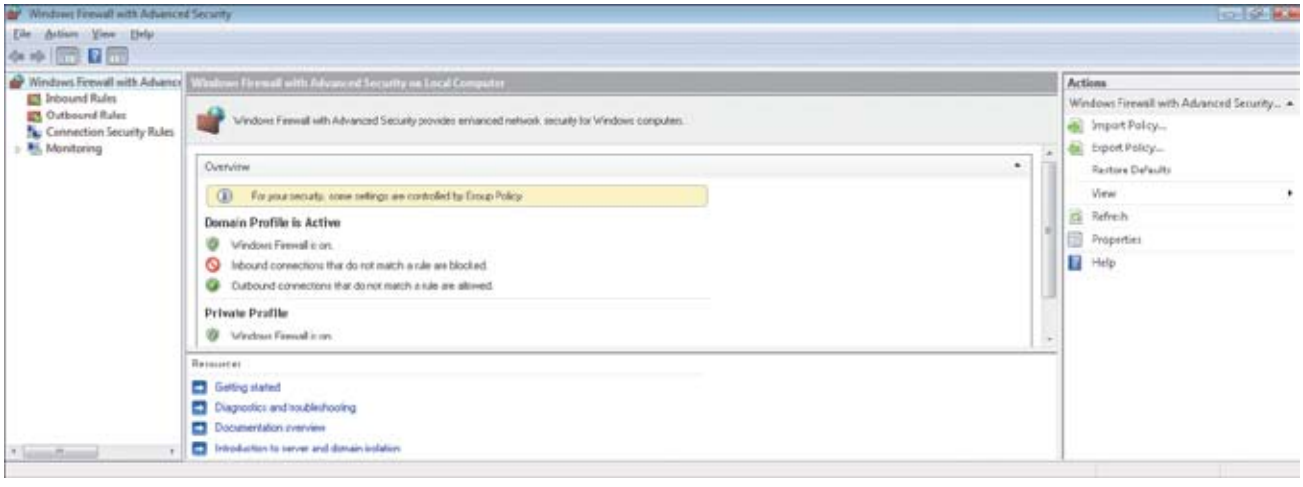

Figure 4 **Windows Firewall with advanced security**

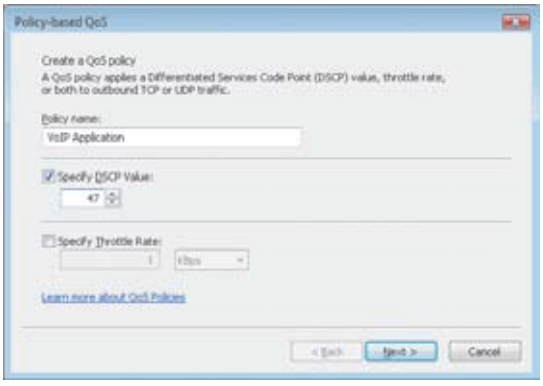

Figure 5 **Creating a QoS policy**

Windows Vista is the most significant update to Windows networking since Windows 95.

cially when business demands introduce multiple networked devices per user, such as additional laptops and mobile devices like Smartphones. Likewise, while you may be interested in providing additional network services such as IPsec, you may also be concerned about the impact on CPU load. Windows Vista addresses network scalability concerns by supporting IPv6 and hardware offload capabilities.

To solve problems with limited public IPv4 addresses, many governments, ISPs and other organisations are transitioning to IPv6, the next version of the network protocol that drives the Internet. Windows Vista supports IPv4 and IPv6 together through a dual-layer IP stack architecture. IPv6 is enabled by default, and the dual-layer stack support enables you to migrate gradually using IPv6 transition technologies that can tunnel IPv6 traffic across a private IPv4 network or the Internet. Windows Vista natively supports PPPv6 and Layer 2 Tunneling Protocol (L2TP/IPv6) virtual private networks (VPNs), enabling remote access users to take advantage of the benefits of IPv6 networks.

Windows Vista supports offloading network traffic processing to specialised network adaptors. New offload capabilities include IPv6 and TCP Chimney offload. These architectural innovations optimise performance and network throughput to achieve the performance and operational gains made possible by today's high-speed networks. Utilising compatible network adaptor hardware can remove bottlenecks related to network packet processing such as CPU overhead and available memory bandwidth, without requiring changes to existing applications or network management tools.

The network stack also supports Receive-side Scaling, which dynamically balances inbound network connections so the load can be shared across multiple processors or cores, reducing potential bottlenecks in processing network traffic.

Summary

Windows Vista represents the most significant update to Windows networking since Windows 95. Users will find it easier to take advantage of wired and wireless networks as they travel. With the new auto-tuning network stack, file transfers will be faster. Enterprises will appreciate the reduced security risks, including improved protection from threats introduced by mobile and wireless users.

Systems administrators will find Windows Vista easier to manage, with the ability to create granular security policies for network traffic as well as QoS for mission-critical apps. These new features let you do more with your network infrastructure while minimising administration effort and maximising end-user productivity. ■

Additional resources

- **New Networking Features in Windows Server 'Longhorn' and Windows Vista**
  microsoft.com/technet/itsolutions/network/evaluate/new_network.mspx
- **Next Generation TCP/IP Stack in Windows Vista and Windows Server 'Longhorn'**
  microsoft.com/technet/community/columns/cableguy/cg0905.mspx

Jason Leznek *is the Senior Product Manager for Windows Vista Networking. He has been with Microsoft for almost ten years and was the Product Manager for Windows Server Update Services and Group Policy prior to joining the Windows Vista team. Prior to that, he spent seven years in the field working with Microsoft enterprise customers.*