

Security Bits & Bites

Windows NetBIOS Protection: Closing the Door Ajar @ Home (Level 200) Revision 1.10, 15 Aug 2004 by Lee Desmond (dot com)

High-level Summary

This document directs attention to an important topic that is largely ignored or given light treatments in other publications – Windows NetBIOS Protection.

NetBIOS interaction with the outside world (“Internet”) is redundant since Internet access merely requires the TCP/IP suite of protocols to function correctly. Outside a typical corporate LAN environment, NetBIOS has no real reason to exist as well. Disabling unwanted services will not only improve security (*e.g.* against exploits such as Blaster) but also system performance in general.

Target audience group is the average remote user, utilizing his/her private home machine or company-issued computer while on the road. In both instances, they are independent and operate outside the protective confines of an organization’s perimeter network.

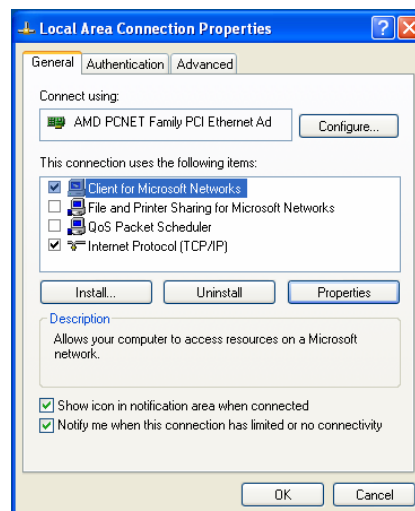
Windows Platforms

Tested on Windows 2000 SP4 and XP (including Win XP SP2).

Network Interface

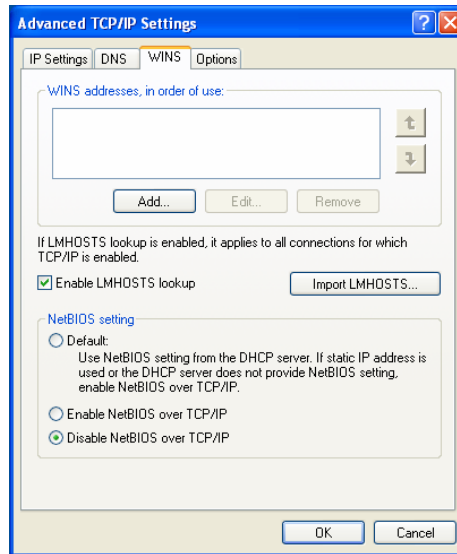
By default, Windows enables a host of network services that are not essential when operating in a remote environment. Therefore, deactivating them should be the first logical step to take.

1. Uncheck File and Printer Sharing for Microsoft Networks. This is located under **Properties** for all network interface types (wired or wireless).

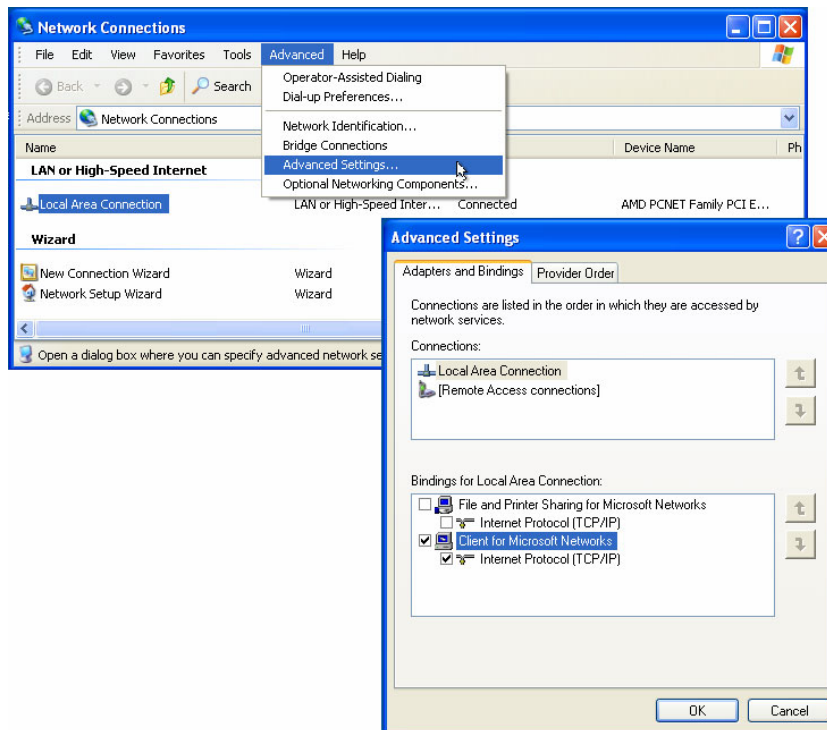


2. Uncheck QoS Packet Scheduler if it is installed (optional).

- Pick Disable NetBIOS over TCP/IP on the **WINS** tab (Internet Protocol (TCP/IP) → Properties → Advanced).



An alternative configuration method is shown below:



NT Services

Several NT Services turned on by default are not necessary. Besides, standard client machines should not be serving out files and revealing their identity to the world (all without the user's knowledge). Use the table below as a reference to achieve a basic level of NetBIOS Protection.

SERVICE DISPLAY NAME	SERVICE NAME	SERVICE STARTUP TYPE	
		DEFAULT	RECOMMENDED
Server	lanmanserver	Automatic	Manual
TCP/IP NetBIOS Helper	lmhosts	Automatic	Manual
Computer Browser	browser	Automatic	Manual
Workstation	lanmanworkstation	Automatic	Manual; leave the default of Automatic if frequent access to SMB resources is needed

The recommended set of minimum changes will not prevent Internet connectivity or access to typical share resources hosted on SMB¹ resources (*e.g.* File Server).

Caveats

Hardware Profiles

Unfortunately, disabling any of the properties shown in the “Network Interface” section will affect each and every Windows “Hardware Profiles”. This useful feature facilitates selective start/stop of hardware devices and services, and is vital to enable Win NT 4 to properly run on laptop systems. The behavior is not any different on Win 200x / XP platforms.

Network Neighborhood

Browsing of “Microsoft Windows Networks” resources using Windows Explorer or the command line (*e.g.* net view) will be greeted with errors or incomplete results. Login scripts that rely on user-friendly names such as \\machine_name\share_name will also break. Nevertheless, access to remote SMB resources is still possible without any visible loss of functionality.

NetBIOS name resolution will cease to work – workaround is to use IP Address instead
i.e. net use P: \\192.168.123.45\share_name

Final Words

A hardware “combi-device” that provides capabilities such as routing, switching, firewall / NAT² and WiFi (wireless) is highly indispensable in a remote location setup. A small investment will significantly enhance the overall security of any client machine, particularly ubiquitous Windows-based ones. Unsolicited traffic will be silently dropped and common NetBIOS assaults from the Internet will be blocked right at the front door.

Anti-virus software with current AV signatures, in conjunction with a properly configured desktop firewall application, round up the essential defense arsenal of any Windows-based machine that is part of the Internet community.

And of course, do not forget to maintain and apply published security patches against known vulnerabilities in a timely manner!

- end -

¹ Server Message Block

² Network Address Translation