Inside Out Of Sharing Mechanism In Windows

Introduction

Most of the organization use shares to exchange some files or they share some resources like printer. But did we ever dig in to the details how Windows does this? Which protocols windows uses? This paper covers the information about the protocols windows uses to connect to the share on network. What are those protocols and under what circumstances windows uses which protocol? Which are the ports used by these protocols? How to disable these protocols on windows machines?

Windows uses two protocols to connect to shared resources over network

- SMB over TCP
- NetBIOS over TCP

So the question is under which circumstances Windows uses which protocol? How Windows determines the use of any of the protocol? First, Let us understand what each of this protocol is!!!

What is SMB?

SMB stands for "**S**erver **M**essage **B**lock". As defined in windows help, SMB is "A file-sharing protocol designed to allow networked computers to transparently access files that reside on remote systems over a variety of networks. The SMB protocol defines a series of commands that pass information between computers. SMB uses four message types: session control, file, printer, and message." Earlier till Windows NT, Windows used to run SMB on NetBIOS. From Windows 2000 onwards, Windows runs SMB directly over TCP/IP and started using TCP Port 445 for this purpose.

What is NetBIOS?

NetBIOS stands for "**Net**work **B**asic **I**nput **O**utput **S**ystem". As defined in windows Help, NetBIOS is - "An application programming interface (API) that can be used by programs on a local area network (LAN). NetBIOS provides programs with a uniform set of commands for requesting the lower-level services required to manage names, conduct sessions, and send datagrams between nodes on a network." This protocol is also used by windows for file/printer sharing over the network. NetBIOS uses TCP port 139 and 445.

How sharing works?

Connecting a shared resource in windows based network requires at least two windows machines. The machine, which tries to connect to the remote shared resource, is "**client**" and the machine where client will connect (having shared resource) is "**server**".

Now to understand which protocol client uses to connect to server, let us divide client in to two categories

- **When NetBIOS over TCP is enabled on the client**

  After windows 2000, When NetBIOS is enabled at client side which is a default behavior of any default installation, Client will try to connect to server at both the protocols, If SMB (TCP Port 445) responds, client will send a "RST" packet to server for NetBIOS protocol (TCP Port 139). If SMB does not respond then client continue connection using NetBIOS (TCP Port 139). If none of the protocol responds, client will consider the connection as fail.
- **When NetBIOS over TCP is disabled on the client**

  If NetBIOS is disabled at client, It will not try to connect to NetBIOS of the server even though it is enabled. Client will only try to connect to SMB over TCP (TCP Port 139)

of the server. If server has disabled SMB over TCP (TCP Port 139), client will consider the connection as fail.

Now let us see how to block each of this protocol. Make sure that you are not running or using any application which uses sharing mechanism. If you block these protocols, few applications will not work.

Blocking “SMB over TCP” (TCP Port 445)

1) Open registry editor using “regedit”.
2) Go to the Key - HKLM\SYSTEM\CurrentControlSet\Services\NetBT\Parameters
3) There will be value named “TransportBindName” of String type
4) Remove the value data for the value “TransportBindName”. This can be done by opening the value (double click on value to open it) and deleting the value data.
5) Reboot the system.

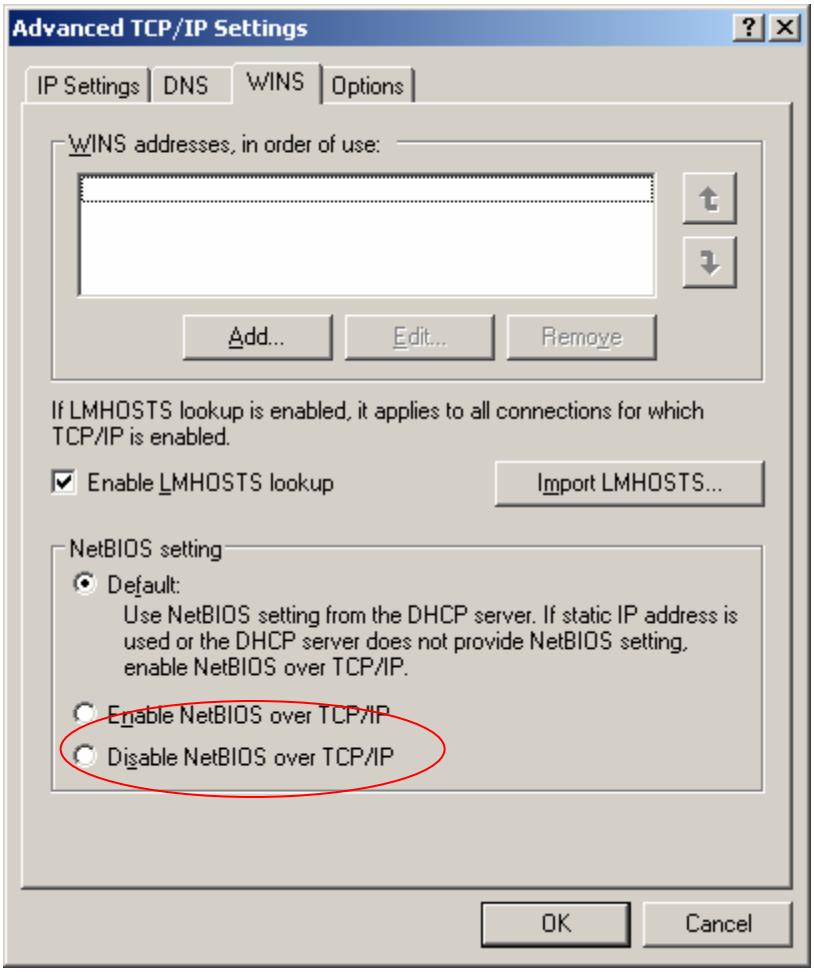
Above mentioned steps can be achieved by following batch file. Reboot the system after running the batch file.

```
echo off
reg delete "HKLM\SYSTEM\CurrentControlSet\Services\NetBT\Parameters" /v
TransportBindName /f
reg add "HKLM\SYSTEM\CurrentControlSet\Services\NetBT\Parameters" /v
TransportBindName /t REG_SZ
echo on
```

Blocking NetBIOS over TCP/IP (TCP Port 139, UDP Port 137, 138)

NetBIOS over TCP/IP is property of network interface. So needs to follow these steps for all the interfaces.

1) Open “Local Area Connection” (or the connection on which you want to block NetBIOS in case of multiple interfaces).
2) Click on properties to open “Local Area Connection Property” window.
3) Click on “Internet Protocol (TCP/IP)” and click on “Properties” to open “TCP/IP Property” window.
4) Click on “Advance” to open “Advanced TCP/IP Properties” window.
5) Click on WINS tab in the “Advanced TCP/IP Properties” window.
6) There is an option to disable “NetBIOS over TCP/IP” as shown in below screen. Select the option and click on OK.



7) This will disable NetBIOS over TCP/IP and close port 139 on the interface.

Note: All the information mentioned in this paper is true only after windows 2000.