

UNCLASSIFIED

Report Number: C4-059R-01

Guide to Securing Microsoft Windows 2000® DHCP

Systems and Network Attack Center (SNAC)



Updated: 25 June 2001
Version 1.2

National Security Agency
9800 Savage Rd. Suite 6704
Ft. Meade, MD 20755-6704

W2Kguides@nsa.gov

UNCLASSIFIED

UNCLASSIFIED

This Page Intentionally Left Blank

UNCLASSIFIED

Warnings

- **Do not attempt to implement any of the settings in this guide without first testing in a non-operational environment.**
- This document is only a guide containing recommended security settings. It is not meant to replace well-structured policy or sound judgment. Furthermore this guide does not address site-specific configuration issues. Care must be taken when implementing this guide to address local operational and policy concerns.
- The security changes described in this document only apply to Microsoft Windows 2000 systems and should not be applied to any other Windows versions or operating systems.
- SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE EXPRESSLY DISCLAIMED. IN NO EVENT SHALL THE CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
- See [Microsoft's web page](#) for the latest changes or modifications to the Windows 2000 operating system.

UNCLASSIFIED

This Page Intentionally Left Blank

UNCLASSIFIED

Acknowledgements

Some parts of this document were drawn from Microsoft copyright materials, with their permission.

Trademark Information

Microsoft, MS-DOS, Windows, Windows 2000, Windows NT, Windows 98, Windows 95, Windows for Workgroups, and Windows 3.1 are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and other countries.

All other names are registered trademarks or trademarks of their respective companies.

Table of Contents

Warnings..... iii

Acknowledgements v

Trademark Information vi

Table of Contents..... vii

Table of Figures viii

Table of Tables ix

Introduction xi

Getting the Most from this Guidexi

About the Guide to Securing Microsoft Windows 2000 DHCP xii

Chapter 1 Windows 2000 DHCP in the Network 1

DHCP Server Configurations 1

Chapter 2 Windows 2000 DHCP Server 3

DHCP Administrators and Users Group..... 3

DHCP File and Registry Permissions 3

DHCP Scope and Server Options..... 4

DHCP Auditing 4

DHCP Server Utilities 5

DHCP Server DNS Interaction 6

Chapter 3 Windows 2000 DHCP Client 7

DHCP Client Registry Permissions 7

DHCP Client TCP/IP Settings 7

DHCP Client and DNS 8

Automatic Private IP Addressing..... 8

DHCP Client Utilities 9

Appendix A Further Information..... 11

Appendix B References..... 13

Table of Figures

Figure 1 – DHCP with Internet Presence.....1
Figure 2 – DNS setting to allow only secure updates.....2
Figure 3 – DHCP Server’s Default DNS Settings6
Figure 4 – Recommended DNS Setting for DHCP Servers6
Figure 5 – DHCP Enabled Client7
Figure 6 – Default DNS Settings for Windows 2000 Clients.....8

Table of Tables

Table 1 - DHCP Server File Security Settings3
Table 2 – DHCP Server Registry Security Settings.....3
Table 3 – DHCP Audit Related Registry Settings.....5
Table 4 – DHCP Server Utility File Settings5
Table 5 – DHCP Client Registry Security Settings7
Table 6 – DHCP Client Utility File Settings.....9

UNCLASSIFIED

This Page Intentionally Left Blank

UNCLASSIFIED

Introduction

Dynamic Host Configuration Protocol (DHCP) is a TCP/IP standard that reduces the complexity and administrative overhead of managing network client IP addresses. The DHCP server automatically allocates IP addresses and related TCP/IP configuration settings to DHCP-enabled clients. By default, computers running Windows 2000 are DHCP-enabled clients.

The purpose of this guide is to inform the reader about the available security settings for the Windows 2000 DHCP Server and Clients, and how to properly implement them.

The ***Guide to Securing Microsoft Windows 2000 DHCP*** builds upon the recommendations presented in the other guides in this series for securing Windows 2000 Servers, and presents detailed information on how to configure DHCP to be secure.

This document is intended for Windows 2000 network administrators, but should be read by anyone involved or interested in Windows 2000 security.

Knowledge of Microsoft's DHCP server is assumed; this includes installation, configuration and administration.



NOTE: This is *not* a guide on how to install and set-up DHCP in your network. This guide does *not* address issues such as fault-tolerance, performance, general administration and troubleshooting. The focus of this guide is solely on the Security aspects of Microsoft DHCP servers and clients.

Getting the Most from this Guide

The following list contains suggestions for successfully using the Guide to Securing Microsoft Windows 2000 DHCP.



WARNING: This list does not address site-specific issues and every setting in this book should be tested on a non-operational network.

- ❑ Read the guide in its entirety. Subsequent chapters build on information and settings discussed in prior chapters. Omitting or deleting steps can potentially lead to an unstable system and/or network that will require reconfiguration and reinstallation of software.
- ❑ Perform pre-configuration recommendations:
 - Perform a complete backup of your system if this is not a new installation.
 - Ensure that the latest Windows 2000 service pack and hot fixes have been installed. For further information on critical Windows 2000 updates, see the [Windows Update for Windows 2000 web page](#).
- ❑ Configure Windows 2000 Server and Professional using the security recommendations presented in other guides in this series.
- ❑ Follow the recommended DHCP security settings contained herein that are appropriate for your environment.

About the Guide to Securing Microsoft Windows 2000 DHCP

This document consists of the following chapters:

Chapter 1, “Windows 2000 DHCP in the Network”, contains general DHCP recommendations for better network security.

Chapter 2, “Windows 2000 DHCP Server”, contains recommendations for safeguarding the DHCP Server during normal operations.

Chapter 3, “Windows 2000 DHCP Client”, contains recommendations for safeguarding DHCP Clients during normal operations.

Appendix A, “Further Information,” contains a list of the hyperlinks used throughout this guide.

Appendix B, “References,” contains a list of resources cited.

Windows 2000 DHCP in the Network

There are several deployment methods for DHCP in a Windows 2000 environment, defined by operational requirements. However, in general because DHCP is a protocol that lacks security, the DHCP services should not be exposed to the outside. Critical domain servers and essential client machines should be assigned “fixed” IP addresses that do not rely on DHCP.

DHCP Server Configurations

Figure 1 shows an example of a local area network that is serviced by a DHCP server and has connectivity to the Internet.

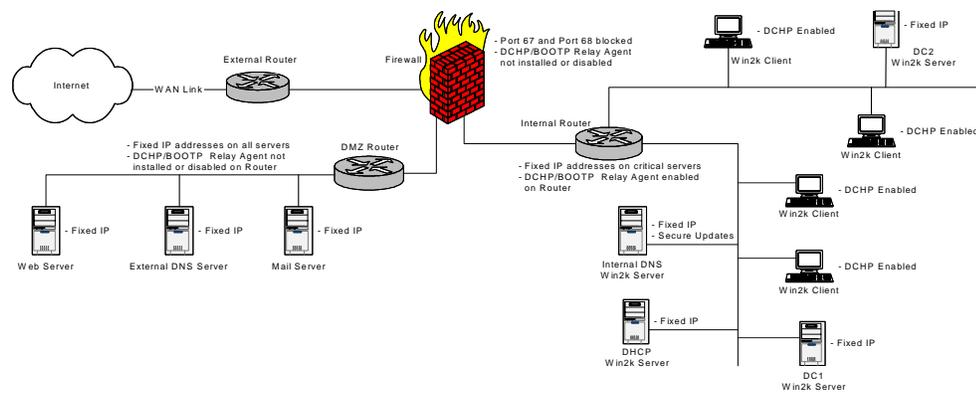


Figure 1 – DHCP with Internet Presence

General Configuration Guidance

To enhance security, the following measures are recommended:

- ❑ Block the DHCP ports (port 67 & port 68) at the Firewall protecting the Intranet from the Internet.
- ❑ Uninstall or disable the DHCP/BOOTP relay agent on the Firewall (if present).
- ❑ Assign “fixed” IP addresses to the DMZ router and DMZ servers.
- ❑ Uninstall or disable the DHCP/BOOTP relay agent on the DMZ router (if present).
- ❑ Install the DHCP server on a member server that is **not** a Domain Controller.
- ❑ Assign “fixed” IP addresses to all critical internal servers (including the DHCP servers) and stop the DHCP Client service on these machines.
- ❑ Assign “fixed” IP addresses to any critical internal clients and stop the DHCP Client service on these machines.

- ❑ On any DHCP server that is multihomed, disable service bindings for any connection that will not be used to listen and provide services to clients.
- ❑ Secure DHCP Server machines as described in **Chapter 2**.
- ❑ Secure DHCP Client machines as described in **Chapter 3**.

“Fixed” IP Address versus “Reserved” IP Address

The term “Fixed” IP address used in **Figure 1** and the general configuration guidance above, means the IP address is manually configured, i.e., hardcoded. This is opposed to an IP address, defined in a DHCP Reservation, which is permanently assigned to a particular machine. The use of DHCP Reservations for critical machines is discouraged.

Stop the DHCP Client Service on Critical Machines

The default for Windows 2000 Client and Server installations will have the DHCP Client service started and running as Local System. The DHCP servers and other critical client/server machines that utilize “Fixed” IP addresses do not require this service. Consequently, the DHCP Client service should be stopped and the service’s Startup type changed to Manual.

DHCP and DNS

Windows 2000 is reliant on the Domain Naming Service (DNS). Once client IP addresses are dynamically assigned by a DHCP server, the DNS tables need to be updated. It is recommended that the **Allow Dynamic Updates?** property of the DNS server be set to **Only Secure Updates** as shown in **Figure 2**.



Figure 2 – DNS setting to allow only secure updates

By default, DHCP clients will send an update to the DNS server after assignment of an IP address by the DHCP server. For client machines that do not support the DNS update function, e.g., Windows 95, the DHCP server must update the DNS entry on the client’s behalf. By default, the DHCP server is configured to update DNS entries at the request of clients. It is recommended that this feature be disabled.

Windows 2000 DHCP Server

The DHCP server service automatically allocates IP addresses and related TCP/IP configuration settings to DHCP-enabled clients. The DHCP server service runs as a Local System. To minimize potential damage from a compromise, it is recommended that the DHCP server be installed on a domain server that is **not** a Domain Controller. DHCP servers are critical so they should all have “Fixed” IP addresses and consequently the DHCP Client Service should be stopped and the startup type should be changed to manual.

DHCP Administrators and Users Group

When the DHCP server service is installed on a Windows 2000 server machine, two new local groups are created; DHCP Administrators and DHCP Users. These two groups are available for use if desired.

DHCP File and Registry Permissions

The DHCP database, recovery and audit files are stored in the %SystemRoot%\System32\DHCP folder. The recommended file security settings are listed in **Table 1**.

FOLDER OR FILE	USER GROUPS	RECOMMENDED PEISSIONS
<u>%SystemRoot%\System32\DHCP</u> folder, subfolders, and files	System DHCP Administrators DHCP Users	Full Control Full Control Read

Table 1 - DHCP Server File Security Settings

The recommended security settings for the DHCP Server Registry entries are listed in **Table 2**.

REGISTRY KEY	USER GROUPS	RECOMMENDED PEISSIONS
HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\DhcpServer	DHCP Administrator System	Full Control Full Control
HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Services\DhcpServer	DHCP Administrator System	Full Control Full Control
HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Services\Dhcp	System	Full Control

Table 2 – DHCP Server Registry Security Settings

DHCP Scope and Server Options

There are quite a few DHCP Options available. It is recommended that the options used be kept to a minimum. To reduce the risk to Client machines, the DNS Server option should **not** be used. Client machines should be assigned a “fixed” DNS address; see **Chapter 3**.

DHCP Auditing

The Windows 2000 DHCP service includes audit features that are enabled by default. The audit log files are found in the %SystemRoot%\system32\DHCP directory. To enable/disable auditing or change the directory where the audit log files are stored, use the **DHCP properties** page. Additional audit configuration information can only be changed through editing the Registry. **Table 3** lists the DHCP registry entries related to auditing along with the default values. See the Microsoft Windows 2000 Server Resource Kit [1] for additional details.



NOTE: Some of the DHCP Registry values listed in Table 3 are not present in the Windows 2000 Registry by default. When a Registry entry is not present, the default value is used.

Name:	DhcpLogMinSpaceOnDisk
Path:	HKLM\SYSTEM\CurrentControlSet\Services\DhcpServer\Parameters
Data Type:	REG_DWORD
Range:	0x0 - 0xFFFFFFFF <i>MB</i>
DefaultValue:	0x14 (20 MB)
Description:	Specifies the minimum amount of free disk space required for audit logging. DHCP periodically verifies that it has sufficient disk space to proceed with audit logging (the interval is specified in the value of DhcpLogDiskSpaceCheckInterval . This entry specifies the minimum value it requires. If the amount of free disk space is less than the value of this entry, the DHCP service does not write to the audit log. Logging is suspended until sufficient disk space is available.
Name:	DhcpLogDiskSpaceCheckInterval
Path:	HKLM\SYSTEM\CurrentControlSet\Services\DhcpServer\Parameters
Data Type:	REG_DWORD
Range:	0x0 - 0xFFFFFFFF <i>number of audit log entries</i>
DefaultValue:	0x32 (50 MB)
Description:	Determines how often DHCP verifies that disk space and file size are adequate for its audit log. The value of this entry represents the number of audit log records entered between each verification check.
Name:	DhcpLogFilePath

Path:	HKLM\SYSTEM\CurrentControlSet\Services\DhcpServer\Parameters
DataType:	REG_SZ
Range:	<i>Path name</i>
DefaultValue:	<i>Systemroot\System32\dhcp</i>
Description:	Specifies the directory where DHCP audit logs are stored. If you change the value of this entry, DHCP moves the audit log files to the new location. By default, the audit logs are stored in the same directory as the DHCP client information database.
Name:	DhcpLogFilesMaxSize
Path:	HKLM\SYSTEM\CurrentControlSet\Services\DhcpServer\Parameters
DataType:	REG_DWORD
Range:	0x0 - 0xFFFFFFFF <i>MB</i>
DefaultValue:	0x7 (7 MB)
Description:	Specifies the maximum combined size of one week's worth of DHCP audit logs. If the audit logs exceed the size specified by this value, DHCP stops writing to the audit log until sufficient space becomes available.
Name:	ActivityLogFlag
Path:	HKLM\SYSTEM\CurrentControlSet\Services\DhcpServer\Parameters
DataType:	REG_DWORD
Range:	0 – 1
DefaultValue:	0
Description:	Determines whether DHCP activity is audited and recorded in a log. Value 0 = No auditing or logging. Value 1 = DHCP activity is audited and logged.

Table 3 – DHCP Audit Related Registry Settings

DHCP Server Utilities

There are two DHCP utility programs available in the %systemRoot%\system32 folder, ipconfig.exe and netsh.exe. The recommended security settings for these files are listed in Table 4.

FOLDER OR FILE	USER GROUPS	RECOMMENDED PEMISSIONS
%SystemRoot%\System32\ipconfig.exe	System DHCP Administrators	Full Control Full Control
%SystemRoot%\System32\netsh.exe	System DHCP Administrators	Full Control Full Control

Table 4 – DHCP Server Utility File Settings

DHCP Server DNS Interaction

The DHCP server's default DNS configuration is shown in **Table 3**. It is configured to update DNS entries at the client's request. It is recommended that this feature be disabled by un-checking the **Automatically update DHCP client information in DNS** checkbox, see **Table 4**.

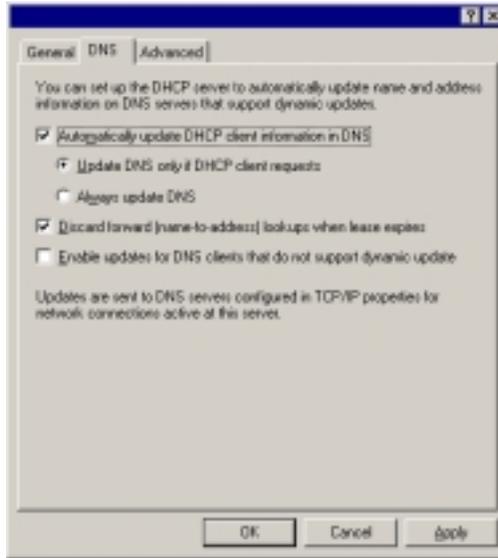


Figure 3 – DHCP Server's Default DNS Settings

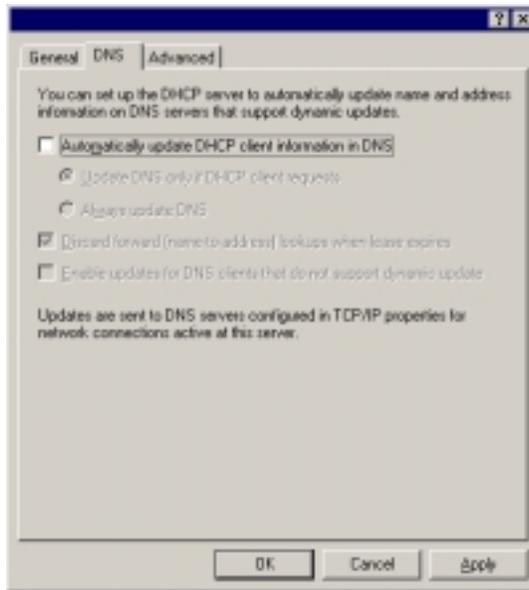


Figure 4 – Recommended DNS Setting for DHCP Servers



WARNING: By disabling this feature, all DHCP clients that rely on the DHCP server to update their DNS entries, e.g., Windows 95, must be given static IP addresses and corresponding DNS entries must be created.

Windows 2000 DHCP Client

The DHCP client service automatically queries the DHCP server for an IP address to assign to the client machine. This query is done at boot time and renewed, if needed, before the client machine’s lease expires. The DHCP client service is running as Local System on the client machine, consequently it is recommended that DHCP not be used on critical client machines. Critical client machines should use “Fixed” IP addresses and their DHCP Client service should be stopped and startup type changed to manual.

DHCP Client Registry Permissions

The recommended security settings for the DHCP Client Registry entries are listed in **Table 5**.

REGISTRY KEY	USER GROUPS	RECOMMENDED PERMISSIONS
HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Services\Dhcp	System	Full Control

Table 5 – DHCP Client Registry Security Settings

DHCP Client TCP/IP Settings

It is recommended that Clients only obtain their IP address, subnet mask, and Gateway information from the DHCP server. The DNS entry should be a “Fixed” entry (or set of entries), see **Figure 5**.

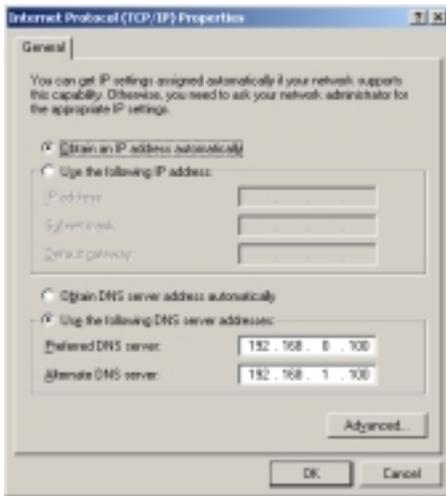


Figure 5 – DHCP Enabled Client

DHCP Client and DNS

Under Advanced TCP/IP Settings, the **Register this connection's address in DNS** is checked by default, see **Figure 6**.

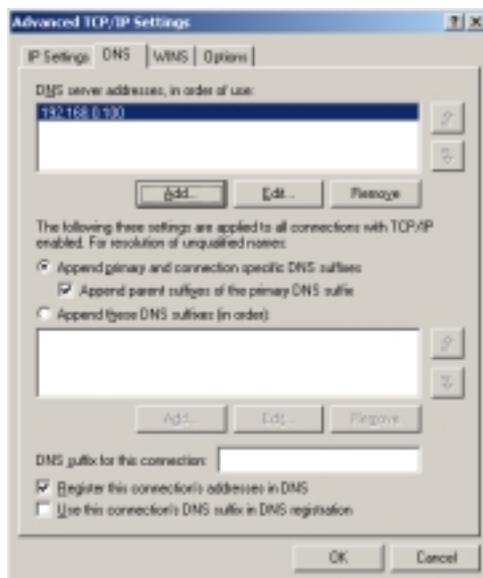


Figure 6 – Default DNS Settings for Windows 2000 Clients

This setting enables DHCP client's to update DNS once assigned an IP address by the DHCP server. Because DNS is configured to only accept secure updates, only valid client machines are able to change their DNS entries.

Automatic Private IP Addressing

Windows 2000 uses Automatic Private IP Addressing (APIPA) to assign an IP address to a machine when a DHCP Server is unavailable or the client's request for an address fails. Microsoft documentation states that the address assigned ranges from 169.254.0.1 through 169.254.255.254. This range of IP addresses, reserved by the Internet Assigned Numbers Authority (IANA), is not to be used on the Internet. It is recommended that this feature be disabled.

Disabling APIPA

To disable automatic address configuration:

- ❑ Open Registry Editor: click **Start**, click **Run**, type **regedt32**, and then click **OK**.



WARNING: Incorrectly editing the registry may severely damage your system. Before making changes to the registry, back up any valued data on the computer. Use the Last Known Good Configuration startup option if problems are encountered after manual changes have been applied.

- ❑ In Registry Editor, navigate to the following registry key:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\
Parameters

- ❑ Create the following entry:
 IPAutoconfigurationEnabled: REG_DWORD
- ❑ Assign a value of **0** to disable Automatic Private IP Addressing (APIPA) support for the selected network adapter.
- ❑ Close Registry Editor.



NOTE: User must be logged on as an administrator or a member of the Administrators group in order to complete this procedure.

If the *IPAutoconfigurationEnabled* entry is not present, a default value of 1 is assumed, which indicates that APIPA is used.

DHCP Client Utilities

There is a DHCP utility program available in the %SystemRoot%\system32 folder, ipconfig.exe. The recommended security setting for this file is listed in **Table 6**.

FOLDER OR FILE	USER GROUPS	RECOMMENDED PERMISSIONS
%SystemRoot%\System32\ipconfig.exe	System Administrators	Full Control Full Control

Table 6 – DHCP Client Utility File Settings

UNCLASSIFIED

This Page Intentionally Left Blank

UNCLASSIFIED



Further Information

[Microsoft's web page](http://www.microsoft.com)
<http://www.microsoft.com>

[Windows Update for Windows 2000 web page](http://www.microsoft.com/windows2000/downloads/default.asp)
<http://www.microsoft.com/windows2000/downloads/default.asp>

UNCLASSIFIED

This Page Intentionally Left Blank

UNCLASSIFIED

References

[1] Microsoft Windows 2000 Server Resource Kit, Microsoft Press, 2000.