Configuring Name Protection

7 out of 8 rated this helpful -

Applies To: Windows Server 2008 R2

Name squatting occurs when a non-Windows-based computer registers in Domain Name System (DNS) with a name that is already registered to a Windows-based computer. The use of name protection in Windows Server prevents name squatting by non-Windows-based computers. Name squatting does not present a problem on a homogeneous Windows network where Active Directory Domain Services (AD DS) can be used to reserve a name for a single user or computer.

Name protection is based on the Dynamic Host Configuration Identifier (DHCID) in the Dynamic Host Configuration Protocol (DHCP) server, and support for the new DHCID RR (resource record) in DNS. DHCID RR is described by the Internet Engineering Task Force (IETF) in RFCs 4701 and 4703.

DHCID is a resource record (RR) stored in DNS that maps names to prevent duplicate registration. This RR is used by DHCP to store an identifier for a computer, along with other information for the name such as the A/AAAA records of the computer. The unique position of DHCP in the name registration process allows it to request this match, and then refuse the registration of a computer with a different address attempting to register a name with an existing DHCID record.

DHCID prevents the following name squatting situations:

- Server name squatting by a client

- Server name squatting by another server

- Client name squatting by another client

- Client name squatting by a server

In addition, support for DHCP Unique Identifier (DUID) will be added to the IPv4 registration on the DHCP client. DUID is described by the IETF in RFC 4361.

Name protection can be configured for IPv4 and IPv6 at the network adapter level or scope level. Name protection settings configured at the scope level take precedence over the setting at the IPv4 or IPv6 level. If Name protection at the scope level is not configured at all, then the setting at the IPv4 or IPv6 network adapter takes precedence. DHCID protects names on a first come-first served basis.

To enable name protection at the IPv4 or IPv6 node level

1. Open the DHCP Microsoft Management Console (MMC) snap-in.
2. In the console tree, double-click the DHCP server you want to configure, right-click **IPv4** or **IPv6**, and then click **Properties**.
3. Click **DNS**, click **Advanced**, and then check **Enable Name Protection**.

To enable name protection at the scope level

1. Open the DHCP console.
2. In the console tree, double-click the DHCP server you want to configure, double-click **IPv4** or **IPv6**, right-click the scope you want, and then click **Properties**.
3. Click **DNS**, click **Configure**, and then check **Enable Name Protection**.