DNS and DHCP in Windows Server 2019

Wesley Faxlanger

School of Cybersecurity

CYSE:608 Cyber War

Dr. Malik A. Gladden

13 September 2026

DNS and DHCP in Windows Server 2019

Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) both play a role in ensuring that a network functions reliably. DNS provides name resolution by mapping computer names to IP addresses, allowing users and applications to locate network resources without the need to recall numerical addresses. In Windows Server environments, DNS is particularly important because Active Directory Domain Services relies on DNS to locate domain controllers for authentication, updates, and searches (Microsoft, 2025). Windows Server DNS provides caching, which allows future requests to be processed faster and more effectively. Forwarding and conditional forwarding can further improve efficiency by directing DNS requests to appropriate servers rather than requiring unnecessary queries throughout the network (Microsoft, 2025).

While DNS and DHCP work in unison to improve network efficiency, they each serve a unique function. DHCP assigns the necessary network settings to clients, hence the name Dynamic Host Configuration Protocol. Microsoft (2025) explains that Windows Server DHCP centralizes IP address management, reduces manual configuration, and helps minimize addressing errors. DHCP and DNS ultimately work in unison to achieve maximum efficiency. DHCP provides critical information such as IP address, default gateway, DNS servers, and DNS domain name. This automation becomes especially useful as networks grow, as administrators will not have to manually configure every device, ultimately improving availability. DHCP can also work with DNS through dynamic updates, allowing DNS records to be updated when DHCP leases are assigned or renewed (Microsoft, 2025). In summary, DNS is the map, and DHCP helps a device join a network. Reliability can also be improved through DHCP failover. Windows Server 2019 allows two DHCP servers to share lease and scope information. If one server

becomes unavailable, the other can continue servicing DHCP clients using replicated information (Microsoft, 2024).

In the context of a Windows Server 2019 environment, these tools are invaluable as they not only support aspects of basic network functions but also enable scalability. But also automate steps that would be tedious for network administrators. Security is a major concern in the context of DNS and DHCP, as attackers could potentially redirect network traffic or provide clients with malicious network configurations. For example, configuring a device so that it becomes vulnerable to attack or filtering network traffic in a manner that allows attackers to capture sensitive data. One important strategy is using Active Directory-integrated DNS zones with secure dynamic updates. Microsoft states that when a zone is Active Directory-integrated, Windows Server DNS enables only secure dynamic updates by default (Microsoft, 2025). This helps prevent unauthorized systems from modifying DNS records. DNSSEC provides additional protection by using cryptographic signatures to allow DNS responses to be validated. According to Microsoft (2023), DNSSEC provides “origin authority, data integrity, and authenticated denial of existence,” making DNS less vulnerable to DNS spoofing attacks.

In conclusion, in the context of Windows Server 2019, DNS and DHCP are both critical tools in an effective network. However, the potential security risks cannot be ignored. According to Microsoft (2025), administrators should use DHCP audit logging to monitor lease assignments and renewals, restrict administrative permissions, regularly apply updates, and review DNS and DHCP activity for suspicious changes. Combining secure dynamic updates, DNSSEC, DHCP authorization, logging, controlled administrative access, and failover allows administrators to maintain efficient and reliable network communication while reducing security and privacy risks.

References

Microsoft. (2023, June 13). What is DNSSEC on DNS Server in Windows Server? Learn.Microsoft.Com. https://learn.microsoft.com/en-us/windows-server/networking/dns/dnssec-overview

Microsoft. (2025, March 27). *DHCP failover in Windows Server*. MicrosoftLearn. https://learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-failover

Microsoft. (2025, March 24). *Dynamic DNS Update in Windows and Windows Server*. Microsoft.Com. https://learn.microsoft.com/en-us/windows-server/networking/dns/dynamic-update

Microsoft. "What Is DHCP Server in Windows Server?" *What Is DHCP Server in Windows Server? | Microsoft Learn*, 13 May 2025, learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top.

Microsoft. "Domain Name System (DNS) in Windows and Windows Server." *Domain Name System (DNS) in Windows and Windows Server | Microsoft Learn*, 15 May 2025, learn.microsoft.com/en-us/windows-server/networking/dns/dns-overview.