BRYANT WATKINS

CYSE 608 | Dr. Gladden

DNS & DHCP Research

2/18/26

Prompt: "How do DNS and DHCP protocols contribute to the efficiency and reliability of network communication in a Windows server 2019 environment? What strategies can be employed to address privacy and security concerns in the management of DNS and DHCP services on Windows Server 2019?"

DNS & DHCP Windows Server 2019 Contributions

DNS and DHCP make major contributions to the reliability and efficiency of Windows Server 2019 environment network communications. DNS (Domain Name System) plays the role of translating traditional web addresses, i.e. www.Google.com, into numeric addresses (Internet Protocol addresses) for the user. DNS's role is vital for reliable and efficient network communication in a Windows server 2019 environment. DNS's ability to automatically translate addresses for end users is incredibly important for efficiency, as this eliminates the hassle of users dealing with many different numerical sequences that would prove incredibly difficult to remember. DNS's ability to store all relevant information pertaining to internet protocol addresses also makes it reliable; users can rely on the DNS to get them to their desired destination and ensure that it is the correct destination.

DHCP, Dynamic Host Control Protocol, also makes major contributions to the reliability and efficiency of Windows Server 2019 environment network communications. DHCP plays the role of assigning internet protocol addresses for devices. DHCP assists the efficient network communications in a Windows server 2019 environment by providing address for the user and thus eliminates the need for that user to take those extra steps. Reliability of DHCP for Windows

Server 2019 environment network communications is another strong suit. The centralized management and autonomous nature of DHCP makes it very reliable. Centralized management works to ensure that no two addresses are given out at once, which eliminates the need for the user to check if their address is already in use. The autonomous nature of DHCP also ensures that it follows the same procedure every time and minimizes the chance of misconfiguration incidents and vulnerabilities.

Privacy and Security Concerns Managing DNS & DHCP Services on Windows Server 2019

There are numerous privacy and security considerations to know when attempting to manage DNS and DHCP services on a Windows Server 2019 environment. DNS has a few avenues to explore to help combat some common attacks. DNS can at times be vulnerable to – DNS Hijacking, DoS/DDos attacks, spoofing, and tunneling to name a few. Thankfully, there are mitigation tools and/or techniques for such vulnerabilities. One major cybersecurity tool for DNS is called DNSSEC, and this tool adds an additional layer of security. DNSSEC implements strong encryption, as well as digital signatures.

Response rate limiting is another effective tactic to combat malicious activity, specifically the threat of an DDoS attack. Response rate limiting is highly beneficial and secure due to its ability to ensure the network is not overloaded with traffic. DNS recursion configuration is yet another tactic for securely utilizing or managing DNS services in a Windows server 2019 environment. DNS recursion configuration mitigates the threat of malicious recursive queries and thus again combats threats faced by DoS attacks. DNS has many security factors at play in its operation and management.

DHCP provides a set of potential vulnerabilities as well. Common security risks when managing DHCP services are spoofing and Man-in-the-Middle attacks. These potential attacks allow bad actors to gain unauthorized access, obtain sensitive data/information, and the ability to tamper with data/information. There are, however, ways to mitigate these risks for DHCP like that of DNS services. One potential attack mitigation is any authentication protocols, as DHCP itself does not verify identities. DHCP Snooping is also highly effective, as this is a tool on a network that prevents communication with rogue or unauthorized DHCP servers. These security considerations are all critical for managing DNS and DHCP services in a Windows server 2019 environment.

WORK CITED

Gladden, Malik. “DNS Server Operation and Functionality.” *Windows Systems for Cybersecurity*, 18 Feb. 2026, Canvas, https://canvas.odu.edu/courses/202169/pages/03-%7C-dns-server-operation-and-functionality-2?module_item_id=9604355

Gladden, Malik. “DNS Security Protocols.” *Windows Systems for Cybersecurity*, 18 Feb. 2026, Canvas, https://canvas.odu.edu/courses/202169/pages/03-%7C-dns-security-protocols?module_item_id=9604356

Gladden, Malik. “DHCP Operation and Management.” *Windows Systems for Cybersecurity*, 18 Feb. 2026, Canvas, https://canvas.odu.edu/courses/202169/pages/03-%7C-dhcp-operation-and-management?module_item_id=9604357

Gladden, Malik. “DHCP Security Protocols.” *Windows Systems for Cybersecurity*, 18 Feb. 2026, Canvas, https://canvas.odu.edu/courses/202169/pages/03-%7C-dhcp-security-protocols?module_item_id=9604358

Gladden, Malik. “DHCP in IoT and BYOD environments.” *Windows Systems for Cybersecurity*, 6 Feb. 2026, Canvas, https://canvas.odu.edu/courses/202169/pages/03-%7C-dhcp-in-iot-and-byod-environments?module_item_id=9604359

Anfalovas, Ignas. “Understanding DHCP: A Guide to Dynamic Host Configuration Protocol.” IPXO, 4 Sept. 2024, www.ipxo.com/blog/what-is-dhcp/.

“Understanding DNS Security Threats and How to Mitigate Them.” *IP Pathways*, 6 June 2025, www.ippathways.com/understanding-dns-security-threats-and-how-to-mitigate-them/#:~:text=DNS%20security%20is%20critical%20for,protect%20your%20network%20from%20cybercriminals.