

## **Temat: Serwer DHCP, instalacja i konfiguracja.**

**Cel ogólny lekcji:** Przedstawienie roli DHCP (Dynamic Host Configuration Protocol - Dynamiczny Protokół Konfiguracji Hosta) w sieciach komputerowych oraz omówienie procesu instalacji i konfiguracji serwera DHCP w systemach Windows Server 2016, 2019 i 2022.

### **Cele szczegółowe lekcji:**

#### **1. rola DHCP w sieciach komputerowych:**

- a. Omówienie roli protokołu DHCP w procesie automatycznego przydzielania adresów IP urządzeniom w sieci.
- b. Wyjaśnienie korzyści wynikających z użycia DHCP, takich jak skalowalność, zarządzanie konfiguracją i unikanie konfliktów adresów IP.

#### **2. Instalacja roli serwera DHCP:**

- a. Przedstawienie kroków instalacji roli serwera DHCP w systemach Windows Server 2016, 2019 i 2022 za pomocą narzędzia "Dodawanie ról i funkcji". Uczestnicy dowiedzą się, jak poprzez Menedżera Serwerów zainicjować instalację roli oraz jakie komponenty są wymagane.
- b. Omówienie nowości i usprawnień w kolejnych wersjach systemu. Uczestnicy zrozumieją, jak nowości w tej wersji systemu mogą wpłynąć na instalację i konfigurację serwera DHCP.

#### **3. Konfiguracja podstawowych parametrów DHCP:**

- a. **Zakres adresów IP:** Wyjaśnienie, jak definiować zakres adresów IP, jakie zostaną przydzielane przez serwer DHCP. Uczestnicy dowiedzą się, jak dobrać zakres zgodnie z ilością urządzeń w sieci.
- b. **Maska podsieci:** Omówienie wpływu maski podsieci na przydzielanie adresów IP. Uczestnicy zdobędą wiedzę na temat znaczenia maski podsieci w kontekście zarządzania siecią.
- c. **Brama domyślna: Wyjaśnienie,** jak skonfigurować bramę domyślną w serwerze DHCP. Uczestnicy dowiedzą się, jakie jest jej znaczenie dla komunikacji między sieciami.
- d. **Serwery DNS:** Omówienie konfiguracji serwerów DNS w serwerze DHCP. Uczestnicy zdobędą umiejętność ustalania serwerów DNS dla urządzeń w sieci.
- e. **Rezerwacje DHCP:** Wyjaśnienie, co to są rezerwacje DHCP i jak można je tworzyć. Uczestnicy nauczą się, jak przydzielać stałe adresy IP wybranym urządzeniom w sieci.

f. **Zakresy wykluczone:** Przedstawienie, w jaki sposób definiować zakresy wykluczone, aby serwer DHCP nie przydzielał pewnych adresów IP. Uczestnicy zrozumieją, dlaczego wykluczanie adresów jest czasem niezbędne.

#### 4. Konfiguracja opcji zaawansowanych:

a. **Adresy IP alternatywnych serwerów DNS:** Omówienie, jak skonfigurować alternatywne serwery DNS w serwerze DHCP. Uczestnicy dowiedzą się, jak zapewnić redundancję w przypadku niedostępności głównego serwera DNS.

b. **Serwery NTP:** Wyjaśnienie, jak skonfigurować serwery NTP (Network Time Protocol) w serwerze DHCP. Uczestnicy zdobędą umiejętność synchronizacji czasu w sieci.

c. **Konfiguracja klientów PXE:** Przedstawienie, jak skonfigurować serwer DHCP, aby umożliwiać uruchamianie systemu operacyjnego przez sieć (PXE) dla klientów. Uczestnicy zdobędą wiedzę o tym zaawansowanym aspekcie DHCP.

5. **Audyt i monitorowanie serwera DHCP:** Przeprowadzenie omówienia, jak monitorować działanie serwera DHCP oraz analizować dzienniki zdarzeń w celu identyfikacji ewentualnych problemów lub anomalii w pracy serwera.

6. **Zabezpieczenia DHCP:** Przedstawienie metod zabezpieczania serwera DHCP przed nieautoryzowanym dostępem oraz unikaniem konfliktów adresów IP w sieci.

**Wprowadzenie:** Lekcja dotyczy serwera DHCP (Dynamic Host Configuration Protocol) oraz jego instalacji i konfiguracji w systemach Windows Server 2016, 2019 i 2022 zapewnia uczestnikom umiejętności niezbędne do efektywnego zarządzania adresacją IP.

Protokół DHCP umożliwia automatyczne i dynamiczne przydzielanie adresów IP urządzeniom w sieci, co przyczynia się do usprawnienia administracji i efektywnego wykorzystania dostępnych adresów.

W trakcie tej lekcji skupimy się na instalacji i konfiguracji serwera DHCP w systemach Windows Server 2016, 2019 i 2022. Omówienie procesu instalacji i konfiguracji, włączając zaawansowane opcje i nowości w różnych wersjach systemu, co pozwoli uczestnikom lepiej zrozumieć i wykorzystać protokół DHCP w ich sieciach.

#### A. Omówienie roli DHCP w sieciach komputerowych:

**DHCP (Protokół Dynamic Host Configuration Protocol - Protokół dynamicznej konfiguracji hosta/węzła)** pełni kluczową rolę w zarządzaniu adresacją IP w sieciach komputerowych. Jego głównym zadaniem jest automatyczne i dynamiczne przydzielanie klientom ustawień TCP/IP, takich jak adres IP,

maska podsieci, brama domyślna i serwer DNS oraz innych konfiguracji sieciowych urządzeniom, takim jak komputery, drukarki, telefony czy inne urządzenia sieciowe.

Usługa DHCP oferuje możliwość automatycznego pobrania z serwera konfiguracji TCP/IP, czyli adresu IP, maski podsieci, domyślnej bramy w sieci, serwerów DNS.

Klient DHCP pobiera dane konfiguracyjne od pierwszego serwera DHCP, od którego może je uzyskać. Aby uniknąć problemów, w sieci powinien być jeden serwer DHCP lub inne rozwiązania gwarantujące przydzielanie odpowiednich danych.

Poniżej omówione są kluczowe aspekty roli i znaczenia protokołu DHCP w sieciach komputerowych:

1. **Automatyczne przydzielanie adresów IP:** Tradycyjnie, ręczne przypisywanie adresów IP do każdego urządzenia w sieci mogło być skomplikowane i czasochłonne, szczególnie w przypadku dużych sieci. DHCP eliminuje tę pracochłonną procedurę, umożliwiając automatyczne przydzielanie adresów IP urządzeniom w momencie ich dołączenia do sieci.
2. **Dynamiczne zarządzanie adresami IP:** DHCP umożliwia dynamiczne zarządzanie dostępnymi adresami IP w puli adresowej. Kiedy urządzenie opuszcza sieć, adres IP jest zwalniany i staje się dostępny do ponownego przydzielenia. Dzięki temu możliwe jest efektywne wykorzystanie dostępnych adresów IP, nawet w sieciach o zmiennej liczbie urządzeń.
3. **Skalowalność sieci:** W sieciach o dużym rozmachu, ręczne konfigurowanie adresów IP dla każdego urządzenia byłoby uciążliwe i podatne na błędy. DHCP pozwala na elastyczne zarządzanie konfiguracją adresów IP, co jest kluczowe w przypadku dynamicznie rozwijających się sieci.
4. **Zarządzanie konfiguracją:** Oprócz adresów IP, protokół DHCP może przydzielać inne konfiguracje, takie jak maska podsieci, brama domyślna, serwery DNS i inne opcje sieciowe. To ułatwia dostęp do zasobów sieciowych oraz zapewnia spójność konfiguracji urządzeń w sieci.
5. **Zapobieganie konfliktom adresów:** DHCP kontroluje proces przydzielania adresów IP, co pomaga uniknąć konfliktów adresów w sieci. Dzięki temu nie ma ryzyka, że dwa urządzenia będą miały ten sam adres IP, co mogłoby prowadzić do problemów komunikacyjnych.
6. **Łatwa migracja i zmiana konfiguracji:** W przypadku zmiany infrastruktury sieciowej, takiej jak zmiana adresów bram domyślnych czy serwerów DNS, zmiana tych ustawień na wszystkich urządzeniach w sieci byłaby pracochłonna. DHCP ułatwia wprowadzenie takich zmian poprzez centralne zarządzanie konfiguracją.

**Podsumowując:** Rola protokołu DHCP w sieciach komputerowych polega na zapewnieniu efektywnego i automatycznego przydzielania dynamicznych adresów IP oraz innych konfiguracji

sieciowych dla urządzeń. Dzięki temu sieci stają się bardziej skalowalne, łatwiejsze w zarządzaniu i bardziej odporne na błędy związane z konfiguracją adresów IP.

## **B. Instalacja roli serwera DHCP:**

Instalacja roli serwera DHCP jest kluczowym krokiem w tworzeniu infrastruktury sieciowej, umożliwiającej automatyczne przydzielanie adresów IP i konfiguracji sieciowej urządzeniom. Poniżej omówione są kroki instalacji roli serwera DHCP w różnych wersjach systemów Windows Server: 2016, 2019 oraz 2022.

### **a. Windows Server 2016:**

W systemie Windows Server 2016 instalacja roli serwera DHCP odbywa się poprzez Menedżera Serwerów. Oto kroki do wykonania:

1. Otwórz Menedżera Serwerów poprzez narzędzie "Server Manager".
2. Wybierz opcję "Dodaj role i funkcje".
3. W oknie "Dodawanie ról i funkcji" postępuj zgodnie z kierunkami kreatora, aż do osiągnięcia kroku "Role serwera".
4. Znajdź i zaznacz "Serwer DHCP", a następnie kliknij "Dalej".
5. W kolejnych krokach kreatora postępuj zgodnie z wytycznymi, akceptując domyślne ustawienia lub dostosowując je według potrzeb.
6. Po zakończeniu kreatora, rolę serwera DHCP możesz skonfigurować i zarządzać za pomocą narzędzia "Menedżer DHCP".

### **b. Windows Server 2019:**

Proces instalacji roli serwera DHCP w systemie Windows Server 2019 jest podobny do wersji 2016, jednak nowości w tej wersji systemu mogą wpłynąć na instalację i konfigurację. Przykładowe nowości to ulepszona obsługa IPv6, lepsza kontrola nad zakresem przydzielanych adresów IP czy wsparcie dla funkcji Failover DHCP.

### **c. Windows Server 2022:**

Chociaż Windows Server 2022 to najnowsza wersja systemu, instalacja roli serwera DHCP nadal opiera się na podobnych krokach co w poprzednich wersjach. Możesz spodziewać się ewentualnych udoskonaleń i dostosowań, które Microsoft wprowadził w najnowszym systemie.

Wszystkie trzy wersje systemu umożliwiają instalację roli serwera DHCP za pomocą narzędzia "Dodawanie ról i funkcji" w Menedżerze Serwerów. Po zainstalowaniu roli, konfigurację i zarządzanie serwerem DHCP można przeprowadzić za pomocą narzędzia "Menedżer DHCP". Kluczowym aspektem konfiguracji jest definiowanie zakresów adresów IP, udostępnianie opcji konfiguracji sieciowej oraz ewentualne ustawienia failover DHCP dla zapewnienia wysokiej dostępności usługi.

Podsumowując, instalacja roli serwera DHCP w różnych wersjach systemów Windows Server polega na wykorzystaniu narzędzi dostępnych w Menedżerze Serwerów oraz dalszej konfiguracji za pomocą narzędzia Menedżera DHCP. Choć nowości mogą wpłynąć na pewne aspekty instalacji, ogólna procedura pozostaje podobna i umożliwia efektywne zarządzanie adresacją IP w sieci.

### C. Konfiguracja podstawowych parametrów DHCP:

#### a. Zakres adresów IP:

Definiowanie zakresu adresów IP to kluczowy krok w konfiguracji serwera DHCP. Zakres obejmuje pewny przedział adresów IP, które serwer DHCP może przydzielać urządzeniom w sieci. Dobre dopasowanie zakresu do ilości urządzeń w sieci jest istotne, aby uniknąć wyczerpania dostępnych adresów lub nadmiernego marnotrawstwa. Zakres adresów IP jest określany przez początkowy i końcowy adres IP oraz jest związany z konkretną podsiecią.

#### b. Maska podsieci:

Wpływa na to, jak duży jest dostępny pul rezerwacji adresów IP w danej podsieci. Im krótsza maska podsieci, tym większa liczba dostępnych adresów. Maska podsieci określa, które bity w adresie IP identyfikują sieć, a które identyfikują hosta. Dla przykładu, w masce 255.255.255.0, pierwsze 24 bity to identyfikacja sieci, a ostatni ósmy bit to identyfikacja hosta.

#### c. Bramy domyślnej:

Konfiguracja bramy domyślnej w serwerze DHCP polega na określeniu adresu IP routera, który służy jako punkt wyjścia z lokalnej sieci do innych sieci lub do Internetu. Adres bramy domyślnej jest przesyłany do urządzeń w sieci wraz z adresem IP, aby umożliwić im komunikację z innymi sieciami.

#### d. Serwery DNS:

W konfiguracji serwerów DNS w serwerze DHCP definiuje się adresy IP serwerów DNS, które zostaną przekazywane urządzeniom w sieci w celu przekształcania nazw domenowych na adresy IP.

To umożliwia urządzeniom poprawne zlokalizowanie zasobów w sieci lub w Internecie.

### e. Rezerwacje DHCP:

Rezerwacje DHCP pozwalają przydzielić stałe adresy IP określonym urządzeniom, na podstawie ich adresów MAC. Jest to przydatne w przypadku urządzeń, które zawsze muszą korzystać z tego samego adresu IP, na przykład drukarek lub serwerów. Rezerwacje zapewniają pewność, że te urządzenia zawsze otrzymają sprecyzowany adres.

### f. Zakresy wykluczone:

Niektóre adresy IP w danym zakresie mogą być zarezerwowane lub nie mogą być przydzielane przez serwer DHCP. Dlatego tworzy się zakresy wykluczone, aby uniknąć przydzielania tych adresów.

Przykładowe przypadki to adresy IP używane jako bramy domyślne lub adresy przypisane do serwerów, które nie powinny być dynamicznie zmieniane.

### g. Zarządzania serwerem DHCP w środowisku graficznym:

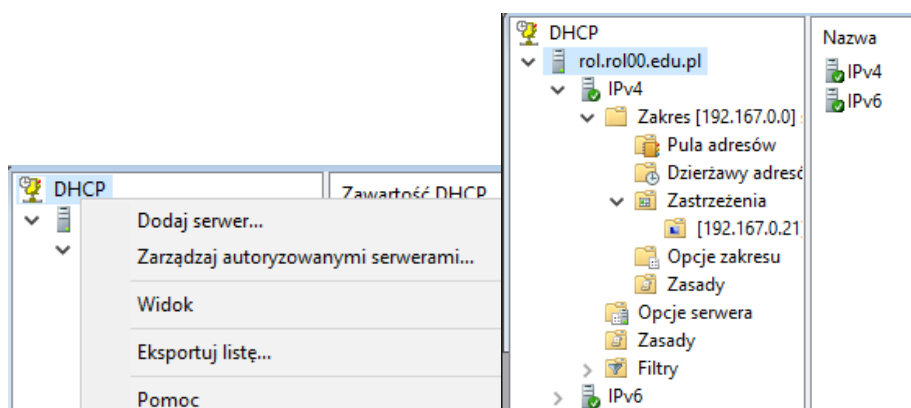
W oknie zarządzania serwerem DHCP dostępne są zakładki zawierające informacje o użyciu zakresu:

- **Pula adresów** - zakres adresów IP przydzielanych klientom oraz adresy wykluczone,
- **Dzierżawy adresów** - adresy aktualnie dzierżawione przez klientów,
- **Zastrzeżenia** - adresy zarezerwowane do przypisywania adresów IP na podstawie adresu MAC.

Aby zarezerwować nowy adres, należy kliknąć prawym przyciskiem myszki na Zastrzeżenia, a następnie z menu kontekstowego wybrać Nowe zastrzeżenie. W otwartym oknie wpisać nazwę, rezerwowany adres IP i adres MAC urządzenia, dla którego ma być zachowany adres IP.

- **Opcje zakresu** - ustawienia pobierane przez klientów, np. adres bramy, serwery DNS.

W sytuacji, gdy na interfejsie nie ustawiono statycznego adresu IP, a stacja nie mogła pobrać adresu z serwera DHCP, system Windows ustawia adres automatyczny z puli 169.254.x.x z maską sieci 255.255.0.0.



	Początkowy adres IP	Końcowy adres IP	Opis
	192.167.0.20 192.167.0.51	192.167.0.200 192.167.0.59	Zakres adresów do rozpowszechniania Adresy IP wykluczone z rozpowszechniania

Właściwości: Zakres [192.167.0.0] szkola.x

Ogólne DNS Zaawansowane

Zakres

Nazwa zakresu:

Początkowy adres IP:

Końcowy adres IP:

Maska podsieci:  Długość: 24

Czas trwania dzierżawy dla klientów DHCP

Ograniczony do:

Dni:  Godziny:  Minuty:

Właściwości: Zakres [192.167.0.0] szkola.x

Ogólne DNS Zaawansowane

Możesz skonfigurować serwer DHCP tak, aby automatycznie aktualizował autorytatywne serwery DNS rekordami hosta (A) i wskaźnika (PTR) klientów protokołu DHCP.

Włącz aktualizacje dynamiczne DNS zgodnie z tymi ustawieniami:

Aktualizuj dynamicznie rekordy DNS tylko na żądanie klientów DHCP

Zawsze aktualizuj dynamicznie rekordy DNS

Odrzuć rekordy A i PTR po usunięciu dzierżawy

Aktualizuj dynamicznie rekordy DNS dla klientów DHCP, którzy nie żądają aktualizacji (np. dla klientów z systemem Windows NT 4.0)

Wyłącz aktualizacje dynamiczne rekordów PTR DNS

Ochrona nazwy

Ochrona nazwy DHCP jest wyłączona w tym zakresie.

Właściwości: Zakres [192.167.0.0] szkola.x

Ogólne DNS Zaawansowane

Przypisz dynamicznie adresy IP następującym klientom:

DHCP

BOOTP

Oba

Czas trwania dzierżawy dla klientów BOOTP

Ograniczony do:

Dni:  Godziny:  Minuty:

Nieograniczony

Konfiguracja opóźnienia

Określ opóźnienie (w milisekundach), z jakim serwer DHCP dystrybuuje adresy

Opóźnienie podsieci:  ms

	Adres IP klienta	Nazwa	Wygaśnięcie dzierżawy	Typ
	192.167.0.20 192.167.0.21	DESKTOP-VNM5D... 21	16.09.2019 02:09:08 Zastrzeżenie (aktywne)	DHCP Brak

DHCP

rol.ro100.edu.pl

IPv4

Zakres [192.167.0.0]

Pula adresów

Dzierżawy adresów

Zastrzeżenia

Opcje zakresu

Zasady

Opcje serwera

Zasady

Filtry

IPv6

Zastrzeżenia

[192.167.0.21] 21

Właściwości: [192.167.0.21] 21

Ogólne DNS

Klient zastrzeżony

Nazwa zastrzeżenia:

Adres IP:

Adres MAC:

Opis:

Obsługiwane typy














Oba

DHCP

BOOTP







	Nazwa opcji	Dostawca	Wartość
	003 Router	Standardowy	192.167.0.1
	006 Serwery DNS	Standardowy	192.167.0.1
	015 Nazwa domeny DNS	Standardowy	rol100.edu.pl

Ikony DHCP mają określone znaczenie i przekazują ogólne informacje o aktualnym stanie obiektów konsoli. Przykłady poniżej:

Ikona	Opis
	Oznacza to, że konsola próbuje połączyć się z serwerem.
	Często oznacza to, że DHCP utracił połączenie z serwerem.
	Serwer DHCP dodany do konsoli.
	Serwer DHCP podłączony i aktywny w konsoli.
	Serwer DHCP podłączony, ale nie autoryzowany w Active Directory do użytku w Twojej sieci.
	Serwer DHCP podłączony, ale bieżący użytkownik nie ma uprawnień administracyjnych do zarządzania serwerem.
	Ostrzeżenie serwera DHCP. Dostępne adresy dla zakresów serwerów są dzierżawione i używane w co najmniej 90 procentach. Oznacza to, że na serwerze są prawie wyczerpane dostępne adresy do dzierżawy klientom.
	Alarm serwera DHCP. W zakresach serwerów nie są dostępne żadne adresy, ponieważ maksymalna (100 procent) adresów przydzielonych do użycia jest obecnie dzierżawiona. Oznacza to awarię serwera DHCP w sieci, ponieważ nie jest on w stanie dzierżawić ani obsługiwać klientów.
	Zakres lub superzakres jest aktywny.
	Zakres lub superzakres jest nieaktywny.
	Ostrzeżenie dotyczące zakresu lub superzakresu. Ostrzeżenie dotyczące zakresu: co najmniej 90 procent adresów IP zakresu jest w użyciu. Ostrzeżenie o superzakresie: Jeśli jakikolwiek zakres w superzakresie ma ostrzeżenie, superzakres też je ma.
	Alert dotyczący zakresu lub superzakresu. Alert dotyczący zakresu: wszystkie adresy IP zostały przydzielone przez serwer DHCP i są używane. Żaden klient nie może uzyskać adresów IP z serwera DHCP, ponieważ nie ma on już adresów IP do przydzielenia. Alert superzakresu: co najmniej jeden zakres zawarty w superzakresie ma wszystkie adresy IP przydzielone przez serwer DHCP. Żaden klient nie może uzyskać adresu IP z zakresu zdefiniowanego w zakresie przydzielonym w 100%. Jeśli inne zakresy w superzakresie zawierają dostępne adresy, serwer DHCP może przydzielić adresy z tych zakresów.
	Folder zawierający listę opcji serwera.



	Opcja serwera.
	Folder zawierający listę opcji zakresu.
	Opcja zakresu.
	Opcja rezerwacji.
	Folder zawierający listę aktywnych dzierżaw.
	Aktywna dzierżawa: ten adres nie jest dostępny do dzierżawy przez serwer DHCP.
	Wygasła dzierżawa: ten adres jest dostępny do dzierżawy przez serwer DHCP.
	Aktywna dzierżawa, oczekująca dynamiczna aktualizacja DNS. Adres ten nie jest dostępny do dzierżawy przez serwer DHCP.
	Aktywna dzierżawa rezerwacji: ten adres jest aktywną dzierżawą zarezerwowanego adresu IP. Ten adres IP nie jest dostępny do dzierżawy przez serwer DHCP.
	Klient łączy się poprzez serwer dostępu zdalnego.
	Katalog główny konsoli DHCP.
	Folder puli adresów.
	Zakres alokacji zakresu. Adresy z tego zakresu przydzielane są do dostępnej puli adresów wykorzystywanej do oferowania klientom dzierżawy.
	Zakres wykluczenia zakresu. Adresy z tego zakresu są wyłączone z dostępnej puli adresów wykorzystywanej do oferowania klientom dzierżawy.
	Folder zawierający listę rezerwacji.
	Tabela protokołu Bootstrap (BOOTP).
	Wpis BOOTP w tabeli zawierający informacje zwracane do klienta BOOTP (np. nazwa pliku obrazu rozruchowego, nazwa serwera plików).
	Folder zawierający foldery filtrów Zezwól i Odmów.

	Folder zawierający listę filtrów dozwolonych, gdy filtrowanie jest włączone. Zezwalaj na filtry klienta na liście.
	Folder zawierający listę filtrów dozwolonych, gdy filtrowanie jest wyłączone. Zezwalaj na filtry klienta na liście nie będą miały zastosowania.
	Zezwalaj na filtr klienta. Ten klient będzie mógł uzyskać dzierżawę od tego serwera DHCP, jeśli jego adres MAC znajduje się na liście.
	Folder zawierający listę filtrów odmowy, gdy filtrowanie jest włączone. Zastosowane zostaną filtry Odmów klienta na liście.
	Folder zawierający listę filtrów odmowy, gdy filtrowanie jest wyłączone. Filtry Odmów klienta na liście nie będą miały zastosowania.
	Odrzuć filtr klienta. Klienci z tymi adresami MAC nie będą mogli uzyskać dzierżawy od tego serwera DHCP.

Podsumowując, konfiguracja roli serwera DHCP obejmuje definiowanie zakresu adresów IP, maski podsieci, bramy domyślnej, serwerów DNS oraz ewentualne tworzenie rezerwacji i zakresów wykluczonych. Odpowiednie ustawienia pozwalają na efektywne zarządzanie adresacją IP w sieci, zapewniając urządzeniom poprawne przydzielanie adresów i dostęp do niezbędnych zasobów.

#### D. Konfiguracja opcji zaawansowanych:

##### a. Adresy IP alternatywnych serwerów DNS:

Konfiguracja alternatywnych serwerów DNS w serwerze DHCP polega na wskazaniu dodatkowych adresów IP serwerów DNS, które będą używane przez urządzenia w przypadku niedostępności głównego serwera DNS. To zapewnia redundancję i niezawodność w przypadku awarii serwera DNS. Jeśli główny serwer DNS przestanie działać, urządzenia automatycznie przełączą się na alternatywne serwery DNS, co pozwala utrzymać dostępność do usług sieciowych.

##### b. Serwery NTP:

Serwery NTP (Network Time Protocol) są używane do synchronizacji czasu w sieci. Konfiguracja serwerów NTP w serwerze DHCP polega na wskazaniu adresów IP serwerów NTP, które dostarczą dokładny czas dla urządzeń w sieci. Dzięki temu wszystkie urządzenia w sieci będą miały zsynchronizowany czas, co jest istotne w kontekście logów, zabezpieczeń i innych operacji czasochłonnych.

### c. Konfiguracja klientów PXE:

PXE (Preboot Execution Environment) umożliwia klientom uruchamianie systemu operacyjnego przez sieć. Konfiguracja serwera DHCP w celu obsługi klientów PXE jest bardziej zaawansowanym aspektem. Wymaga ustawienia opcji DHCP, takich jak "Boot Server Host Name" (66) i "Bootfile Name" (67), aby wskazać, które pliki uruchamialne powinny zostać dostarczone klientom. To umożliwia zdalne instalacje systemów operacyjnych lub narzędzi diagnostycznych bez konieczności korzystania z nośników fizycznych.

Opcje "Boot Server Host Name" (66) i "Bootfile Name" (67) są obydwie związane z konfiguracją serwera DHCP w kontekście klientów używających PXE (Preboot Execution Environment) do zdalnego uruchamiania systemu operacyjnego lub narzędzi diagnostycznych przez sieć. Oto różnice między nimi:

#### "Boot Server Host Name" (66):

- Ta opcja wskazuje nazwę serwera, który działa jako serwer PXE.
- Gdy klient PXE inicjuje proces uruchamiania przez sieć, dostaje od serwera DHCP informację o nazwie hosta serwera PXE, który ma obsłużyć proces uruchamiania.
- Klient PXE użyje tej informacji, aby nawiązać połączenie z odpowiednim serwerem PXE i pobrać niezbędne pliki startowe, takie jak pliki bootujące lub obrazy systemów operacyjnych.

#### "Bootfile Name" (67):

- Ta opcja wskazuje nazwę pliku, który ma być dostarczony klientowi PXE przez serwer DHCP.
- Po odebraniu odpowiedzi DHCP z tą opcją, klient PXE użyje jej jako wskazania, które pliki powinien pobrać i uruchomić z serwera PXE.
- Ten plik może być plikiem startowym (np. bootloaderem), który umożliwia uruchomienie systemu operacyjnego lub narzędzi diagnostycznych.

"Boot Server Host Name" wskazuje na serwer PXE, który ma obsłużyć klienta PXE, natomiast "Bootfile Name" określa nazwę pliku, który klient PXE powinien pobrać i uruchomić z tego serwera.

Podsumowując, konfiguracja adresów IP alternatywnych serwerów DNS pozwala na zapewnienie redundancji w przypadku awarii głównego serwera DNS, serwery NTP synchronizują czas w sieci, a konfiguracja klientów PXE umożliwia zaawansowane operacje uruchamiania systemów operacyjnych

przez sieć. Wszystkie te elementy przyczyniają się do bardziej niezawodnego i zintegrowanego zarządzania siecią.

## **E. Audyt i monitorowanie serwera DHCP:**

Monitorowanie i audyt serwera DHCP są kluczowymi działaniami, które pomagają w utrzymaniu stabilnej i niezawodnej infrastruktury sieciowej. Obejmują one analizę działania serwera DHCP, identyfikację problemów oraz reagowanie na wszelkie anomalie. Audytu i monitorowania serwera DHCP to:

### **1. Monitorowanie działania serwera DHCP:**

- **Dzienniki zdarzeń:** Serwer DHCP generuje dzienniki zdarzeń zawierające informacje o różnych działaniach, takich jak przydzielanie adresów IP, odnowienie dzierżawy, błędy itp. Te dzienniki można analizować, aby monitorować zdrowie i działanie serwera DHCP.
- **Narzędzia do monitorowania:** Istnieje wiele narzędzi dostępnych na rynku, które pozwalają na monitorowanie działania serwera DHCP. Mogą one dostarczać informacje o obciążeniu, dostępności, liczbie dzierżaw i wiele innych parametrów.
- **Monitorowanie wydajności:** Monitorowanie zasobów serwera, takich jak zużycie CPU, pamięci, dysku i sieci, pozwala na wczesne wykrycie potencjalnych problemów wydajnościowych.

### **2. Audyt i analiza dzienników zdarzeń:**

- **Analiza dzienników zdarzeń:** Regularna analiza dzienników zdarzeń DHCP pozwala na identyfikację potencjalnych problemów, błędów lub nieprawidłowości w działaniu serwera. Wpisy w dziennikach mogą zawierać informacje o odmowie przydzielenia adresu IP, błędach konfiguracji, zbyt dużym obciążeniu serwera itp.
- **Alarmy i powiadomienia:** Występowanie określonych zdarzeń lub błędów w dziennikach zdarzeń może spowodować generowanie alarmów lub powiadomień, które ostrzegają administratorów o problemach. To umożliwia szybką reakcję na awarie lub awarie.
- **Historia dzierżaw:** Analiza historii przydzielonych adresów IP może pomóc w identyfikowaniu trendów, takich jak ilość dzierżaw w danym okresie, częstotliwość odnowień dzierżaw itp.

### 3. Zapobieganie problemom i optymalizacja:

- **Regularna konserwacja:** Regularne przeglądy i konserwacja serwera DHCP, w tym czyszczenie niepotrzebnych dzierżaw, mogą pomóc w uniknięciu problemów związanych z brakiem dostępnych adresów IP.
- **Optymalizacja konfiguracji:** Analiza dzienników może pomóc w identyfikacji obszarów, które wymagają optymalizacji, takich jak zakresy adresów IP, dzierżawy, czasy dzierżaw, serwery DNS, bramy itp.

### 4. Zapasowy serwer DHCP:

- **Redundancja:** Wdrożenie zapasowego serwera DHCP w sieci zapewnia redundancję w przypadku awarii głównego serwera DHCP. Dzięki temu sieć może nadal dynamicznie przydzielać adresy IP, nawet jeśli jeden serwer ulegnie awarii.

### 5. Utrzymywanie aktualnych systemów i oprogramowania:

- **Regularne aktualizacje:** Regularne aktualizacje systemów operacyjnych i oprogramowania serwera DHCP są kluczowe dla zapewnienia bezpieczeństwa i wydajności. Aktualizacje mogą również wprowadzać nowe funkcje lub poprawiać działanie serwera DHCP.

Podsumowując, audyt i monitorowanie serwera DHCP są nieodzowne dla utrzymania stabilnej i wydajnej sieci komputerowej. Regularna analiza dzienników zdarzeń, monitorowanie wydajności i wdrażanie odpowiednich działań naprawczych pomagają w identyfikacji, zapobieganiu i reagowaniu na wszelkie problemy lub anomalie w pracy serwera DHCP.

### F. Zabezpieczenia DHCP:

Serwer DHCP jest kluczowym elementem infrastruktury sieciowej, a jego zabezpieczenie jest niezwykle ważne, aby uniknąć potencjalnych problemów z nieautoryzowanym dostępem lub konfliktami adresów IP. Oto kilka metod zabezpieczania serwera DHCP:

1. **Filtracja MAC (Media Access Control):** Wprowadzenie listy dozwolonych adresów MAC umożliwia przydzielanie adresów IP tylko urządzeniom znajdującym się na liście. To zapobiega nieautoryzowanym urządzeniom uzyskiwaniu adresów IP z serwera DHCP.
2. **Autoryzacja serwera DHCP:** Tylko autoryzowane serwery DHCP są uprawnione do udostępniania adresów IP w sieci. System Windows Server umożliwia autoryzację serwera DHCP w usłudze Active Directory. Nieautoryzowany serwer DHCP nie będzie działać.

3. **Zabezpieczenia fizyczne:** Umieszczenie serwera DHCP w odpowiednio zabezpieczonym pomieszczeniu, takim jak pomieszczenie serwerowe, pomaga w ograniczeniu dostępu nieautoryzowanych osób do sprzętu.
4. **Unikanie konfliktów adresów IP:**
  - **Zdefiniowane zakresy:** Właściwie skonfigurowane zakresy adresów IP pomagają uniknąć konfliktów poprzez zapewnienie, że każdy adres IP jest przydzielany tylko raz.
  - **Przydzielanie stałych adresów IP:** W przypadku niektórych urządzeń, takich jak drukarki lub serwery, warto przypisać stałe adresy IP, aby uniknąć przypadkowych konfliktów.
5. **Użycie zakresów wykluczonych:** Możliwość definiowania zakresów wykluczonych, które nie są przydzielane przez serwer DHCP, pomaga w uniknięciu konfliktów z adresami IP, które są już w użyciu.
6. **Monitorowanie i analiza zdarzeń:** Regularna analiza dzienników zdarzeń DHCP pozwala na wykrycie potencjalnych problemów lub prób nieautoryzowanego dostępu. Alarmy i powiadomienia mogą ostrzec o nieprawidłowych działaniach.
7. **Zabezpieczenia sieciowe:** Odpowiednia konfiguracja zabezpieczeń sieciowych, takich jak firewalle, może pomóc w ograniczeniu dostępu do serwera DHCP z zewnątrz sieci.
8. **Regularne aktualizacje:** Regularne aktualizacje systemu operacyjnego oraz oprogramowania DHCP pomagają w zapewnieniu bezpieczeństwa i eliminacji potencjalnych luk w zabezpieczeniach.
9. **Odpowiednia konfiguracja uprawnień:** Nadanie odpowiednich uprawnień dostępu do serwera DHCP dla administratorów oraz ograniczenie dostępu dla innych użytkowników jest istotne dla zabezpieczenia serwera przed potencjalnymi zagrożeniami.
10. **Audyt zdarzeń:** Włączenie audytu zdarzeń w serwerze DHCP pozwala na rejestrowanie wszystkich zdarzeń związanych z przydzielaniem adresów IP. To ułatwia monitorowanie i analizę działań serwera.

Podsumowując, zabezpieczanie serwera DHCP to kluczowy krok w utrzymaniu stabilnej, wydajnej i bezpiecznej sieci komputerowej. Kombinacja fizycznych, sieciowych i programowych zabezpieczeń, w połączeniu z odpowiednią konfiguracją oraz monitorowaniem, pomaga w minimalizowaniu ryzyka wystąpienia problemów związanych z nieautoryzowanym dostępem lub konfliktami adresów IP.

#### 11. Unikanie konfliktów adresów IP:

Konflikty adresów IP to sytuacje, w których dwa lub więcej urządzeń w sieci próbuje używać tego samego adresu IP. Tego rodzaju konflikty mogą prowadzić do problemów z komunikacją i działaniem urządzeń w sieci. Aby uniknąć konfliktów adresów IP, istnieje kilka praktyk i mechanizmów:

- a. **Zakresy adresów IP:** Starannie zdefiniowane i dobrze zarządzane zakresy adresów IP pomagają uniknąć konfliktów. Upewnij się, że zakresy nie nakładają się na siebie i że każdy adres IP jest przydzielany tylko raz.
- b. **Rezerwacje DHCP:** Rezerwacje DHCP to metoda, w której konkretnym urządzeniom jest przypisywany stały adres IP. To szczególnie przydatne w przypadku urządzeń wymagających zawsze tego samego adresu, takich jak serwery czy drukarki. Dzięki temu eliminuje się możliwość przypadkowego konfliktu.
- c. **Zakresy wykluczone:** Możesz zdefiniować zakresy adresów IP, które są wykluczone z puli przydzielanych przez serwer DHCP. Dzięki temu możesz zabezpieczyć określone adresy IP, np. te, które są już używane w sieci.
- d. **Analiza dzienników zdarzeń:** Regularna analiza dzienników zdarzeń DHCP pozwala na wykrycie ewentualnych prób konfliktów lub nieprawidłowych działań. Alarmy i powiadomienia mogą być skonfigurowane, aby ostrzegać o nadmiernych próbach uzyskania adresów IP.
- e. **Dynamiczne aktualizacje DNS:** Jeśli serwer DHCP i serwer DNS są zintegrowane, dynamiczne aktualizacje DNS mogą pomóc w uniknięciu konfliktów, poprzez śledzenie i aktualizowanie informacji o adresach IP w serwerze DNS.
- f. **Monitorowanie dostępności urządzeń:** Regularne monitorowanie dostępności urządzeń w sieci może pomóc w wykryciu przypadków, w których dwa urządzenia próbują używać tego samego adresu IP.
- g. **Edukacja użytkowników:** Warto poinformować użytkowników o konieczności zgłaszania problemów związanych z komunikacją czy dostępnością sieciowych urządzeń, aby uniknąć przypadkowych prób konfliktu adresów.

Ważne jest, aby tworząc infrastrukturę sieciową, starannie planować i konfigurować serwer DHCP, aby uniknąć konfliktów adresów IP. Przy odpowiedniej konfiguracji i monitorowaniu można zminimalizować ryzyko wystąpienia tego rodzaju problemów, co przyczyni się do płynnego działania sieci komputerowej.

**Podsumowanie:** Lekcja dotycząca instalacji i konfiguracji serwera DHCP na systemach Windows Server 2016, 2019 i 2022 zapewnia uczestnikom umiejętności niezbędne do efektywnego zarządzania adresacją IP w sieciach komputerowych. Rozszerzone omówienie procesu instalacji i konfiguracji, włączając zaawansowane opcje i nowości w różnych wersjach systemu, pozwoli uczestnikom lepiej zrozumieć i wykorzystać protokół DHCP w ich sieciach.