8. Tworzenie pytań: Zadaj uczniom, aby sami przygotowali pytania związane z omawianą tematyką. To wymaga dogłębnego zrozumienia, aby sformułować odpowiednie pytania.

Zachęcam uczniów do stworzenia własnych pytań związanych z tematyką DNS i Active Directory. Kilka przykładowych pytań, które mogą posłużyć jako inspiracja:

1. **DNS:**
   - Jakie są główne zadania systemu DNS w sieci komputerowej?
   - Co to jest rekurencyjny resolver w kontekście DNS?
   - Jakie są różnice między rekordem A a rekordem MX w DNS?
2. **Struktura i Hierarchia DNS:**
   - Wyjaśnij, jak hierarchia domen w DNS odzwierciedla strukturę organizacyjną sieci.
   - Co to jest etykieta domeny w DNS i jakie są zasady tworzenia etykiet?
3. **Proces Działania DNS:**
   - Opisz kroki, jakie zachodzą podczas odpytywania DNS w celu uzyskania adresu IP dla danej nazwy domeny.
   - Jaki jest wpływ czasu życia (TTL) rekordu DNS na efektywność działania sieci?
4. **Rola DNS w Active Directory:**
   - Jak DNS wspiera proces autentykacji użytkowników w kontekście Active Directory?
   - Dlaczego poprawna konfiguracja stref DNS jest istotna dla prawidłowego funkcjonowania Active Directory?
5. **Dynamiczne Aktualizacje DNS:**
   - Co to jest dynamiczna aktualizacja DNS i dlaczego jest ważna w środowisku z dynamicznie przydzielanymi adresami IP?
   - Jakie mechanizmy zapewniają zabezpieczenia w przypadku dynamicznych aktualizacji DNS?
6. **Porównanie DNS i WINS:**
   - Jak różni się rola DNS od roli usługi WINS (Windows Internet Name Service) w systemie Windows?

- Kiedy warto używać DNS, a kiedy WINS, aby rozpoznać nazwy w sieci?

7. **Active Directory:**
   - Jakie informacje przechowuje Active Directory i w jaki sposób są one zorganizowane?
   - Jakie są korzyści wynikające z centralnego zarządzania zasobami przy użyciu Active Directory?
8. **Integracja DNS z AD:**
   - W jaki sposób DNS integruje się z usługą autentykacji Kerberos w Active Directory?
   - Co to jest rekord SRV w DNS i jaka jest jego rola w kontekście usług sieciowych?
9. **Zabezpieczenia w DNS i AD:**
   - Jakie kroki można podjąć, aby zabezpieczyć serwery DNS przed atakami typu cache poisoning?
   - Jakie są podstawowe zasady zarządzania uprawnieniami w Active Directory?
10. **Zastosowanie DNS poza AD:**
    - Jakie są inne obszary zastosowania DNS poza środowiskiem opartym na usłudze Active Directory?
    - Dlaczego DNS jest istotny w kontekście globalnej komunikacji internetowej?

Uczniowie mogą wykorzystać te przykładowe pytania lub dostosować je do własnych potrzeb, aby przetestować swoją wiedzę na temat DNS i Active Directory.

Odpowiedzi do przykładowych pytań, które zostały wymienione wcześniej:

1. **DNS:**
   - Główne zadania systemu DNS to tłumaczenie nazw domenowych na adresy IP i odwrotnie oraz zapewnianie hierarchicznej struktury do organizacji nazw w sieci.
   - Rekurencyjny resolver w kontekście DNS to serwer DNS, który odpytuje inne serwery DNS w imieniu klienta w celu uzyskania odpowiedzi na zapytanie.
2. **Struktura i Hierarchia DNS:**
   - Hierarchia domen w DNS odzwierciedla strukturę drzewiastą, z domenami nadrzędnymi i podrzędnymi.
   - Etykieta domeny w DNS to część pełnej nazwy domeny, oddzielona kropkami, np. "example" w "example.com".

3. **Proces Działania DNS:**
   - Proces odpytywania DNS zaczyna się od lokalnego resolvera, który kieruje zapytanie do serwera DNS w domenie nadrzędnej, aż dojdziesz do serwera odpowiedzialnego za daną domenę.
   - TTL (czas życia) rekordu DNS określa, jak długo inny serwer może przechowywać tę informację w pamięci podręcznej.
4. **Rola DNS w Active Directory:**
   - DNS wspiera autentykację użytkowników poprzez dostarczanie informacji o lokalizacji kontrolerów domeny i innych usług AD.
   - Poprawna konfiguracja stref DNS jest istotna, aby komputery i usługi w sieci mogły poprawnie identyfikować i komunikować się w środowisku AD.
5. **Dynamiczne Aktualizacje DNS:**
   - Dynamiczna aktualizacja DNS pozwala komputerom w sieci na automatyczne rejestrowanie i aktualizowanie swoich rekordów DNS.
   - Mechanizmy zabezpieczeń w dynamicznych aktualizacjach DNS obejmują rejestrację zabezpieczoną kluczami i ograniczenia na poziomie serwera.
6. **Porównanie DNS i WINS:**
   - DNS tłumaczy nazwy domenowe na adresy IP, podczas gdy WINS tłumaczy nazwy NetBIOS na adresy IP.
   - DNS jest bardziej skalowalny i uniwersalny, podczas gdy WINS jest bardziej związany z systemami Windows.
7. **Active Directory:**
   - Active Directory przechowuje informacje o obiektach w sieci, takie jak użytkownicy, grupy i zasoby, w hierarchicznej strukturze.
   - Jest to centralny system zarządzania dostępem i autoryzacją w środowisku Windows.
8. **Integracja DNS z AD:**
   - DNS integruje się z usługą autentykacji Kerberos poprzez dostarczanie rekordów SRV, które wskazują na usługi dostępne w domenie.

- Rekord SRV jest specjalnym rekordem DNS, który informuje o dostępności usług sieciowych w danej domenie.

9. **Zabezpieczenia w DNS i AD:**
   - Aby zabezpieczyć przed atakami typu cache poisoning, można korzystać z technik, takich jak DNSSEC.
   - W zarządzaniu uprawnieniami w Active Directory ważne jest ustalenie dokładnych zasad dostępu do zasobów i kontrola nad grupami.
10. **Zastosowanie DNS poza AD:**
    - Poza AD, DNS jest niezbędny do przetłumaczenia nazw domenowych na adresy IP podczas globalnej komunikacji w internecie.
    - W sieci internetowej, DNS umożliwia użytkownikom dostęp do witryn internetowych poprzez wpisywanie czytelnych nazw zamiast adresów IP.