# **CISCO** Academy

# Packet Tracer - Wykrywanie sąsiadów IPv6

# Tabela adresowania

Urządzenie	Interfejs	IPv6 Adres/prefiks	Brama domyślna
RTA	G0/0/0	2001:db8:acad:1::1/64	nd.
	G0/0/1	2001:db8:acad:1::1/64	nd.
PCA1	karta sieciowa	2001:db8:acad:1::A/64	fe80::1
PCA2	karta sieciowa	2001:db8:acad:1::B/64	fe80::1
PCB1	karta sieciowa	2001:db8:acad:2::A/64	fe80::1

# Cele

Część 1: Odnajdywanie sąsiada sieci lokalnej IPv6

Część 2: Odnajdywanie sąsiada sieci zdalnej IPv6

# Wprowadzenie

Aby urządzenie mogło komunikować się z innym urządzeniem, adres MAC miejsca docelowego musi być znany. W przypadku protokołu IPv6 proces o nazwie Neighbor Discovery korzystający z protokołu NDP lub ND jest odpowiedzialny za określenie docelowego adresu MAC. Zbierzesz informacje PDU w trybie symulacji, aby lepiej zrozumieć proces. Nie ma punktów Packet Tracer dla tego ćwiczenia.

# Instrukcje

# Część 1: Odnajdywanie sąsiada sieci lokalnej IPv6

W części 1 tego ćwiczenia otrzymasz adres MAC urządzenia docelowego w tej samej sieci.

#### Krok 1: Sprawdź router w poszukiwaniu wykrytych sąsiadów.

- a. Kliknij na router RTA. Wybierz kartę CLI i wydaj polecenie **show ipv6 neighbors** z uprzywilejowanego trybu exec. Jeśli są wyświetlane jakieś wpisy, usuń je za pomocą polecenia **clear ipv6 neighbors**.
- b. Kliknij PC1, następnie wybierz kartę Desktop i kliknij Command Prompt.

#### Krok 2: Przełącz tryb Simulation, aby przechwytywać zdarzenia.

- c. Kliknij przycisk Simulation w prawym dolnym rogu okna topologii Packet Tracer.
- d. Kliknij przycisk **Show All/None** w lewym dolnym rogu panelu symulacji. Upewnij się, że niektóre **Event List Filters – Visible Events** wyświetlają **None**.
- e. Z wiersza polecenia na PCA1 wyprowadź polecenie ping —n 1 2001:db8:acad:1::b. Spowoduje to rozpoczęcie procesu ping do PCA2.
- f. Kliknij przycisk Play Capture Forward, który jest wyświetlany jako strzałka wskazująca w prawo z pionowym paskiem w polu Play Controls. Pasek stanu nad kontrolkami odtwarzania powinien rejestrować do 150.(Dokładna liczba może się różnić.)

g. Kliknij przycisk Edit Filters Wybierz kartę IPv6 u góry i zaznacz pola ICMPv6 i NDP .Kliknij czerwony X w prawym górnym rogu okna Edit ACL Filters. Przechwycone zdarzenia powinny być teraz wyszczególnione. Powinieneś mieć około 12 wpisów w oknie.

Dlaczego obecne są PDU ND?

h. Kliknij kwadrat w kolumnie Typ dla pierwszego zdarzenia, którym powinno być ICMPv6.

Ponieważ wiadomość zaczyna się od tego zdarzenia, istnieje tylko wychodzący PDU.Na karcie OSI Model, jaki jest typ wiadomości wymieniony dla ICMPv6?

Zauważ, że nie ma adresowania warstwy 2.Kliknij przycisk **Next Layer >>**, aby uzyskać wyjaśnienie dotyczące procesu ND.

i. Kliknij kwadrat obok następnego zdarzenia w Panelu Simulation. Powinien znajdować się w urządzeniu PCA1, a typem powinien być NDP.

Co zmieniło się w adresowaniu warstwy 3?

Jakie adresy warstwy 2 są wyświetlane?

Gdy host nie zna adresu MAC miejsca docelowego, specjalny adres MAC multicast jest używany przez odnajdowanie sąsiada IPv6 jako adres docelowy warstwy 2.

j. Wybierz pierwsze zdarzenie NDP na SwitchA.

Czy istnieje jakaś różnica między In Layers i Out Layers dla warstwy 2?

k. Wybierz pierwsze zdarzenie NDP na PCA2 .Kliknij na Outbound PDU Details.

Jakie adresy są wyświetlane dla poniższych?

**Uwaga**: Adresy w polach mogą być zawijane, dostosuj rozmiar okna PDU, aby ułatwić czytanie informacji adresowych.

Ethernet II DEST ADDR:

Ethernet II DEST ADDR:

IPv6 SRC IP:

IPv6 DST IP:

- I. Wybierz pierwsze zdarzenie NDP na RTA. Dlaczego nie ma żadnych Out Layers?
- m. Kliknij przycisk Next Layer >> do końca i przeczytaj kroki od 4 do 7, aby uzyskać dalsze wyjaśnienie.
- n. Kliknij następne zdarzenie ICMPv6 na PCA1 .

Czy PCA1 posiada teraz wszystkie niezbędne informacje do komunikowania się z PCA2?

o. Kliknij ostatnie zdarzenie ICMPv6 na PCA1 .Zauważ, że jest to ostatnia komunikacja na liście.

Jaki jest typ komunikatu echa ICMPv6?

- p. Kliknij przycisk **Reset Simulation** w Simulation Panel. W wierszu poleceń komputera PC1 wykonaj **ping** do komputera PC2.(Wskazówka: możesz nacisnąć strzałkę w górę, aby przywrócić poprzednie polecenie.)
- q. Kliknij 5 razy przycisk Capture Forward, aby zakończyć proces ping.

Dlaczego nie było żadnych zdarzeń NDP?

# Część 2: Odnajdywanie sąsiada sieci zdalnej IPv6

W części 2 tego ćwiczenia wykonasz kroki podobne do tych z części 1, z tym wyjątkiem, że host docelowy znajduje się w innej sieci LAN. Obserwuj, w jaki sposób proces wyszukiwania sąsiada różni się od procesu obserwowanego w części 1.Zwróć szczególną uwagę na niektóre dodatkowe kroki adresowania, które mają miejsce, gdy urządzenie komunikuje się z urządzeniem znajdującym się w innej sieci.

Pamiętaj, aby kliknąć przycisk **Reset Simulation**, aby usunąć poprzednie zdarzenia.

#### Krok 1: Przechwytywanie zdarzeń komunikacji zdalnej.

- a. Wyświetlaj i usuń wszelkie wpisy w tablicy sąsiadów IPv6 urządzenia, jak to zostało zrobione w części I.
- b. Przełącz PT do trybu symulacji. Kliknij przycisk **Show All/None** w lewym dolnym rogu panelu symulacji. Upewnij się, że niektóre **Event List Filters Visible Events** wyświetlają **None**.
- c. W wierszu polecenia na PCA1 wydaj polecenie **ping –n 1 2001:db8:acad:2::a**, aby wygenerować ruch do PCB1.
- Kliknij przycisk Play Capture Forward, który jest wyświetlany jako strzałka wskazująca w prawo z pionowym paskiem w polu Play Controls.Pasek stanu nad kontrolkami odtwarzania powinien rejestrować do 150.(Dokładna liczba może się różnić.)
- e. Kliknij przycisk **Edit Filters** Wybierz kartę IPv6 u góry i zaznacz pola **ICMPv6** i **NDP**. Kliknij czerwony X w prawym górnym rogu okna Edit ACL Filters. Wszystkie poprzednie wydarzenia powinny być teraz wyszczególnione. Należy zauważyć, że tym razem jest znacznie więcej wpisów.
- f. Kliknij kwadrat w kolumnie Typ dla pierwszego zdarzenia, którym powinno być ICMPv6.Ponieważ wiadomość zaczyna się od tego zdarzenia, istnieje tylko wychodzący PDU. Zauważ, że brakuje informacji warstwy 2, jak to miało miejsce w poprzednim scenariuszu.
- g. Kliknij pierwsze zdarzenie NDP na urządzeniu PCA1.

Jaki adres jest używany jako IP Src w przychodzącym PDU?

IPv6 Neighbor Discovery określi następne miejsce docelowe do przekazania wiadomości ICMPv6.

h. Kliknij drugie zdarzenie ICMPv6 dla **PCA1**.PCA1 ma teraz wystarczająco dużo informacji, aby utworzyć żądanie echa ICMPv6.

Jaki adres MAC jest używany jako docelowy MAC?

- i. Kliknij następne zdarzenie ICMPv6 na urządzeniu RTA. Zauważ, że wychodząca jednostka PDU z RTA nie ma docelowego adresu warstwy 2, oznacza to, że RTA musi ponownie wykonać Neighbor Discovery dla interfejsu, który ma sieć 2001:db8:acad:2::, ponieważ nie zna adresu MAC urządzeń w sieci LAN G0/0/1.
- j. Przejdź do pierwszego zdarzenia ICMPv6 dla urządzenia PCB1.

Czego brakuje w informacji wychodzącej warstwy 2?

- k. Kolejne kilka zdarzeń **NDP** kojarzy pozostałe adresy IPv6 do adresów MAC. Poprzednie zdarzenia NDP powiązały adresy MAC z adresami LLA.
- I. Przejdź do ostatniego zestawu zdarzeń ICMPv6 i zauważ, że wszystkie adresy zostały rozpoznane. Wymagane informacje są teraz znane, więc PCB1 może wysyłać wiadomości odpowiedzi echa do PCA1.
- m. Kliknij przycisk Reset Simulation w Simulation Panel.Z wiersza polecenia PCA1 powtórz polecenie do ping PCB1.
- n. Kliknij 9 razy przycisk Capture Forward, aby zakończyć proces ping.

Czy były jakieś zdarzenia NDP?

o. Kliknij jedyne zdarzenie PCB1 na nowej liście.

Co odpowiada docelowemu adresowi MAC?

Dlaczego PCB1 używa adresu MAC interfejsu routera do tworzenia PDU ICMP?

#### Krok 2: Sprawdź wyjścia routera.

- a. Powróć do trybu Realtime.
- b. Kliknij RTA i wybierz kartę CLI. Na routerze wydaj polecenie show ipv6 neighbors.
  Ile adresów jest wymienionych?

Z jakimi urządzeniami są powiązane te adresy?

Czy są jakieś wpisy na PCA2 (dlaczego lub dlaczego nie)?

- c. Wykonaj ping PCA2 z routera.
- d. Wydaj polecenie **show ipv6 neighbors**.

Czy są wpisy dla PCA2?

### Pytania refleksyjne

1. Kiedy urządzenie wymaga procesu odnajdywania sąsiada IPv6?

- 2. W jaki sposób router pomaga zminimalizować ilość ruchu IPv6 Neighbor Discovery w sieci?
- 3. Jak IPv6 minimalizuje wpływ procesu ND na hosty sieciowe?
- 4. Czym różni się proces odnajdywania sąsiada, gdy host docelowy znajduje się w tej samej sieci LAN i w zdalnej sieci LAN?