














Wprowadzenie do sieci

- 1 Komunikacja sieciowa dziś 
- 2 Podstawy konfiguracji przełącznika i urządzenia końcowego 
- 3 Protokoły i modele 
- 4 Warstwa fizyczna 
- 5 Systemy liczbowe 
- 6 Warstwa łącza danych 
- 7 Przełączanie w sieciach Ethernet 
- 8 Warstwa sieci 
- 9 Odzworowanie adresów 
- 10 Podstawowa konfiguracja routera 
- 11 Adresowanie IPv4 

Komunikaty ICMP

13.1.1

Komunikaty ICMPv4 i ICMPv6



W tym temacie dowiesz się o różnych typach protokołu ICMP (Internet Control Message Protocol) oraz o narzędziach, które są używane do ich wysyłania.

Chociaż IP jest tylko protokołem działającym na zasadzie najlepszych starań, stos TCP/IP zapewnia komunikaty o błędach i komunikaty informacyjne podczas komunikacji z innym urządzeniem IP. Komunikaty wysyłane są za pomocą usług ICMP. Należy zauważyć, iż celem tych wiadomości jest informowanie zwrotnie nadawcy o realizowanej obsłudze przesyłania pakietu, nie zaś zapewnienie niezawodności protokołowi IP. Wiadomości ICMP nie są wymagane i są często blokowane w sieciach z powodów bezpieczeństwa.

Protokół ICMP jest dostępny dla obu protokołów IPv4 oraz IPv6. ICMPv4 to protokół powiadomień dla IPv4. ICMPv6 dostarcza identycznych usług dla IPv6, ale zawiera również dodatkowe funkcjonalności. W tym kursie termin ICMP będzie odnosił się zarówno do ICMPv4 jak i ICMPv6.

Rodzajów komunikatów ICMP i powodów dlaczego są wysyłane jest wiele. Komunikaty ICMP wspólne zarówno dla ICMPv4, jak i ICMPv6 i omówione w tym module obejmują:

- Dostępność hosta
- Przeznaczenie lub usługa niedostępna
- Przekroczenie czasu

13.1.2

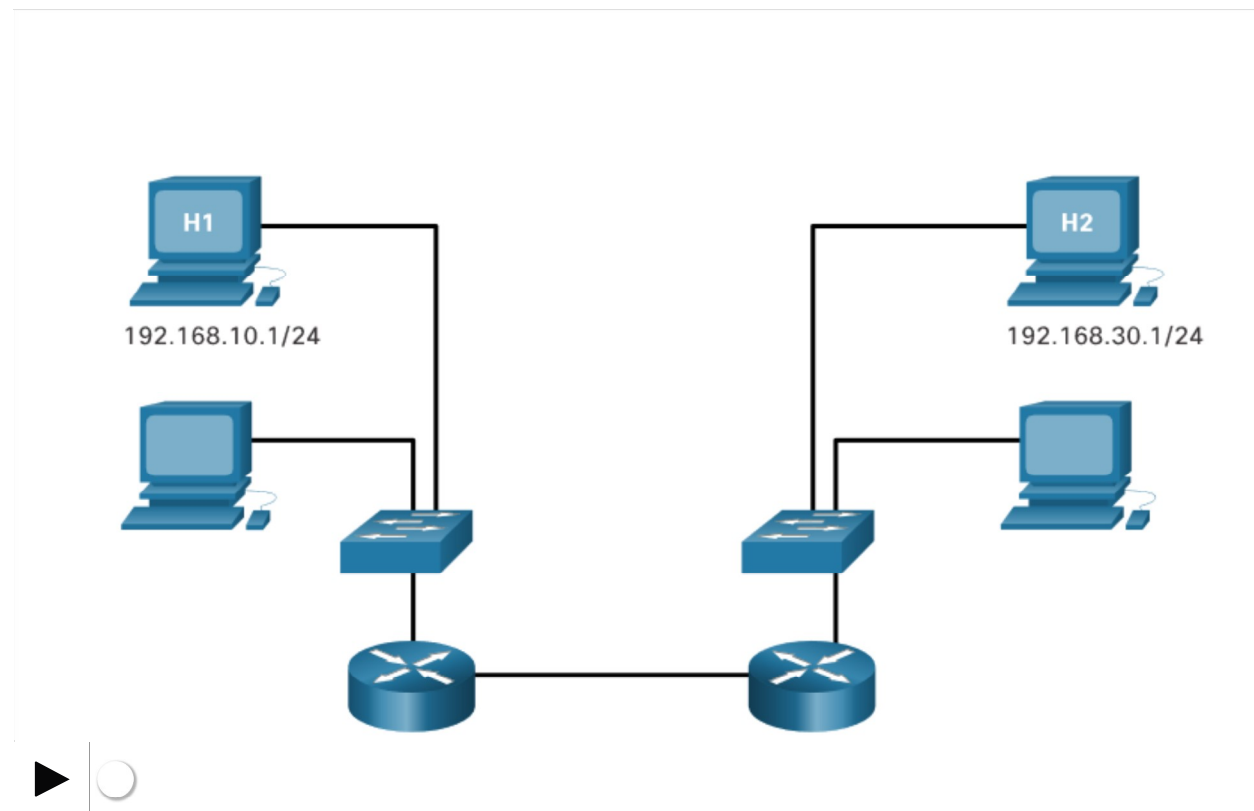


Wprowadzenie do sieci

- 1 Komunikacja sieciowa dziś ✓
- 2 Podstawy konfiguracji przełącznika i urządzenia końcowego ✓
- 3 Protokoły i modele ✓
- 4 Warstwa fizyczna ✓
- 5 Systemy liczbowe ✓
- 6 Warstwa łącza danych ✓
- 7 Przełączanie w sieciach Ethernet ✓
- 8 Warstwa sieci ✓
- 9 Odzworowanie adresów ✓
- 10 Podstawowa konfiguracja routera ✓
- 11 Adresowanie IPv4 ✓

Dostępność hosta

Komunikat echa ICMP może być użyty do przetestowania osiągalności hosta w sieci IP. Host lokalny wysyła żądanie echa (ICMP Echo Request) do hosta docelowego. Jeśli host docelowy jest dostępny, odpowiada komunikatem Echo Reply. Na rysunku kliknij przycisk Odtwórz, aby zobaczyć animację żądania/odpowiedzi echa ICMP. Ten sposób wykorzystania komunikatu ICMP jest podstawą funkcji **ping**.



13.1.3

Przeznaczenie lub usługa niedostępna



Wprowadzenie do sieci

1	Komunikacja sieciowa dziś	▼
2	Podstawy konfiguracji przełącznika i urządzenia końcowego	▼
3	Protokoły i modele	▼
4	Warstwa fizyczna	▼
5	Systemy liczbowe	▼
6	Warstwa łącza danych	▼
7	Przełączanie w sieciach Ethernet	▼
8	Warstwa sieci	▼
9	Odwzorowanie adresów	▼
10	Podstawowa konfiguracja routera	▼
11	Adresowanie IPv4	▼

Kiedy host lub brama otrzymują pakiet, który nie mogą nigdzie dostarczyć, mogą użyć komunikatu ICMP cel nieosiągnięty (ang. Destination Unreachable) w celu powiadomienia źródła pakietu, że host docelowy lub usługa jest niedostępna. Wiadomość będzie zawierać kod, który wskazuje dlaczego pakiet nie mógł być dostarczony.

Niektóre z kodów komunikatu Destination Unreachable dla ICMPv4 to:

- 0 – sieć niedostępna
- 1 – host niedostępny
- 2 – protokół niedostępny
- 3 – port niedostępny

Niektóre z kodów komunikatu Destination Unreachable dla ICMPv6 to:

- 0 – brak trasy do miejsca docelowego
- 1 – komunikacja z siecią docelową jest administracyjnie zablokowana (np przez zaporę)
- 2 – poza zakresem adresu źródłowego
- 3 – adres nieosiągalny
- 4 – port niedostępny

Uwaga: ICMPv6 ma podobne, ale lekko różniące się wartości kodów dla komunikatów Destination Unreachable.

13.1.4

Przekroczenie czasu



Komunikat ICMP przekroczony czas używany jest przez router aby poinformować, że pakiet nie może być przesłany dalej z powodu obniżenia wartości pola Czas życia (ang. Time to Live, TTL) w pakiecie do 0. Jeśli router otrzymuje pakiet i obniżając wartość pola TTL w pakiecie IPv4 otrzymuje wartość 0, niszczy pakiet i wysła komunikat przekroczony czas na adres źródłowy pakietu.

ICMPv6 również wysła komunikat przekroczono czas jeśli router nie może przesłać dalej pakietu IPv6 z tego samego powodu. IPv6 nie ma pola TTL, używa natomiast pola limit przeskoków w celu określenia czy pakiet wygaś.

Uwaga: Komunikaty o przekroczeniu czasu są używane przez narzędzie **traceroute**.

Wprowadzenie do sieci

- 1 Komunikacja sieciowa dziś ▼
- 2 Podstawy konfiguracji przełącznika i urządzenia końcowego ▼
- 3 Protokoły i modele ▼
- 4 Warstwa fizyczna ▼
- 5 Systemy liczbowe ▼
- 6 Warstwa łącza danych ▼
- 7 Przełączanie w sieciach Ethernet ▼
- 8 Warstwa sieci ▼
- 9 Odwzorowanie adresów ▼
- 10 Podstawowa konfiguracja routera ▼
- 11 Adresowanie IPv4 ▼

13.1.5

Komunikaty ICMPv6



Komunikaty i sygnalizacja błędów w ICMPv6 są podobne do wiadomości kontrolnych i sygnalizacji błędów zaimplementowanej w ICMPv4. Jednak ICMPv6 ma nowe cechy i poprawioną funkcjonalność w porównaniu z ICMPv4. Komunikaty ICMPv6 są enkapsulowane w IPv6.

ICMPv6 zawiera cztery nowe protokoły wchodzące w skład protokołu ND (Neighbor Discovery):

Przesyłanie wiadomości między routerem IPv6 a urządzeniem IPv6, w tym dynamiczne przydzielanie adresów, jest następujące:

- Komunikat Router Solicitation (RS)
- Komunikat Router Advertisement (RA)

Przesyłanie wiadomości między urządzeniami IPv6, w tym wykrywanie duplikatów adresów i odwzorowanie adresów, jest następujące:

- Komunikat Neighbor Solicitation (NS)
- Komunikat Neighbor Advertisement (NA)

Uwaga: ICMPv6 ND zawiera również komunikat przekierowania, który ma podobną funkcję do komunikatu przekierowania używanego w ICMPv4.



Kliknij każdy z nich, aby zobaczyć ilustrację i wyjaśnienie komunikatów ICMPv6.

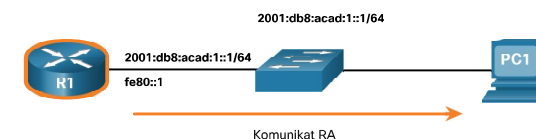
Komunikat RA

Komunikat RS

Komunikat NS

Wiadomość NA

Komunikaty RA są wysyłane przez routery z obsługą protokołu IPv6 co 200 sekund, aby dostarczyć informacje adresowe hostom obsługującym protokół IPv6. Mogą zawierać informacje o adresacji takie jak prefiks i długość prefiksu. Hosty używające SLAAC ustawią jako bramę domyślną adres link-local routera, który wysłał komunikat RA.














Wprowadzenie do sieci

- 1 Komunikacja sieciowa dziś ▾
- 2 Podstawy konfiguracji
przełącznika i urządzenia
końcowego ▾
- 3 Protokoły i modele ▾
- 4 Warstwa fizyczna ▾
- 5 Systemy liczbowe ▾
- 6 Warstwa łącza danych ▾
- 7 Przełączanie w sieciach
Ethernet ▾
- 8 Warstwa sieci ▾
- 9 Odzworowanie adresów ▾
- 10 Podstawowa konfiguracja
routera ▾
- 11 Adresowanie IPv4 ▾

R1 wysyła komunikat RA "Witam wszystkie urządzenia z obsługą protokołu IPv6. Jestem R1 i możesz użyć SLAAC do utworzenia globalnego adresu unicast IPv6. Prefiks to 2001:db8:acad:1::/64. Przy okazji, użyj mojego adresu link-local fe80::1 jako bramy domyślnej."



Wprowadzenie do sieci

- 1 Komunikacja sieciowa dziś 
- 2 Podstawy konfiguracji przełącznika i urządzenia końcowego 
- 3 Protokoły i modele 
- 4 Warstwa fizyczna 
- 5 Systemy liczbowe 
- 6 Warstwa łącza danych 
- 7 Przełączanie w sieciach Ethernet 
- 8 Warstwa sieci 
- 9 Odwzorowanie adresów 
- 10 Podstawowa konfiguracja routera 
- 11 Adresowanie IPv4 

13.1.6

Sprawdź, czy zrozumiałeś - Komunikaty ICMP



Sprawdź swoją wiedzę na temat komunikatów ICMP, wybierając NAJLEPSZĄ odpowiedź na poniższe pytania.

1. Jakie dwa typy komunikatów ICMP są wspólne dla ICMPv4 i ICMPv6? (Wybierz dwie odpowiedzi).

- ☐ Przeznaczenie lub usługa niedostępna
- ☐ Odwzorowanie hosta
- ☐ Konfiguracja IP
- ☐ Źródło nieosiągalne
- ☐ Przekroczenie czasu

2. Jaki typ komunikatu ICMPv6 wysyła host w celu uzyskania konfiguracji IPv6 podczas uruchamiania?

- ☐ Komunikat Neighbor Advertisement (NA)
- ☐ Komunikat Neighbor Solicitation (NS)
- ☐ Komunikat Router Advertisement (RA)
- ☐ Komunikat Router Solicitation (RS)

Sprawdź

Rozwiązanie

Resetuj

 13.0
Wprowadzenie

13.2
Testy ping i traceroute 