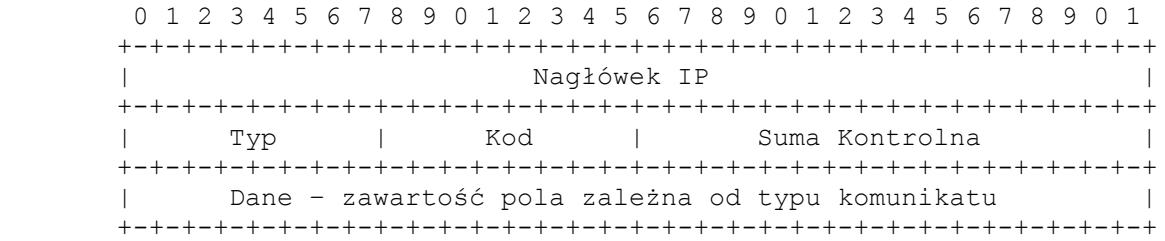
Protokół ICMP

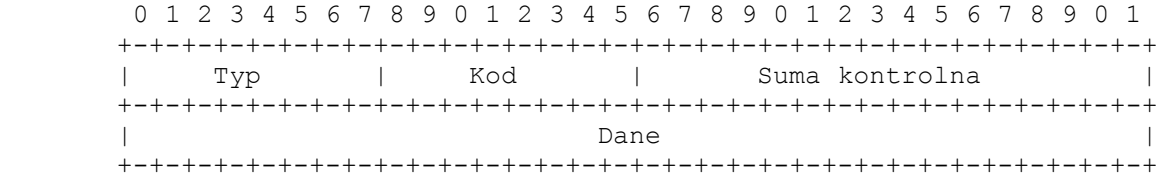
ICMP, opisany w dokumencie RFC 792, jest protokołem pomocniczym dla IP. Chociaż nie jest protokołem transportowym, to w modelu OSI znajduje się w warstwie czwartej, ponieważ komunikaty ICMP są przesyłane w pakietach IP. Protokół ten służy do przesyłania danych informacyjnych i komunikatów o problemach z transmisją pakietów. Ponieważ IP nie jest protokołem niezawodnym, tzn. nie zawiera mechanizmów gwarantujących dostarczenie pakietu do stacji docelowej, więc zaistniała konieczność stworzenia narzędzia pozwalającego w pewnych sytuacjach wykrywać przyczyny problemów z transmisją. Jeśli pakiet IP zawiera komunikat ICMP, to w polu „Protocol" nagłówka pakietu wpisana jest wartość 1. Nagłówek ICMP składa się z 4 lub więcej bajtów – długość nagłówka jest zależna od typu komunikatu – i znajduje się w polu danych pakietu IP, zaraz za nagłówkiem IP.

Ogólna budowa komunikatu ICMP:



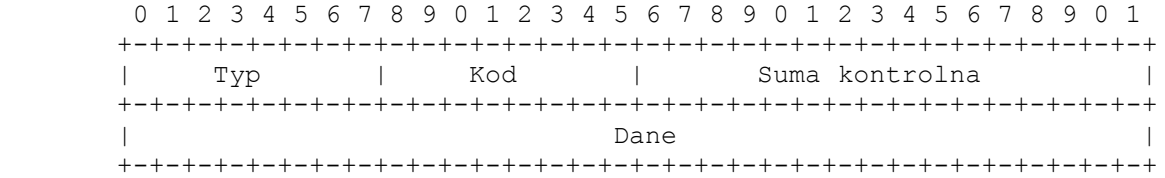
Rodzaje niektórych komunikatów ICMP
(pełna lista na stronie https://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml):

Przeznaczenie nieosiągalne (Destination Unreachable)
Typ: 3
Kod: 0 <- sieć nieosiągalna
1 <- host nieosiągalny
2 <- protokół nieosiągalny (określony w polu "Protocol" nagłówka IP)
3 <- port nieosiągalny (określony w polu 'Destination Port" nagłówka TCP lub UDP)
4 <- konieczna fragmentacja, ale jest ustawiony bit DF
5 <- niepowodzenie trasowania źródłowego



Komunikat wysyłany przez router do maszyny źródłowej, jeśli w tablicach trasowania routera nie ma informacji pozwalającej na przekazanie pakietu, albo jeśli nieosiągalny jest host docelowy, do którego router ma bezpośrednio przekazać pakiet. Host docelowy również może wysłać taki komunikat, jeżeli np. port docelowy jest nieaktywny. Jeszcze jedną przyczyną wysłania tego komunikatu przez router może być konieczność fragmentacji pakietu, ale ustawienie flagi DF na to nie pozwala.

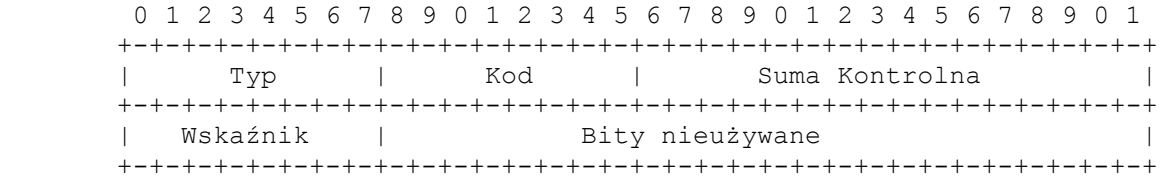
Przekroczenie czasu (Time Exceeded)
Typ: 11
Kod: 0 <- przekroczenie górnej granicy TTL
1 <- przekroczenie czasu składania pakietu z fragmentów



Kod 0 oznacza przekroczenie czasu życia pakietu (Time-to_Live exceeded), czyli wyzerowanie się pola TTL po dotarciu pakietu do n-tego routera na trasie, gdzie n jest początkową wartością pola TTL umieszczaną tam przez stację źródłową.

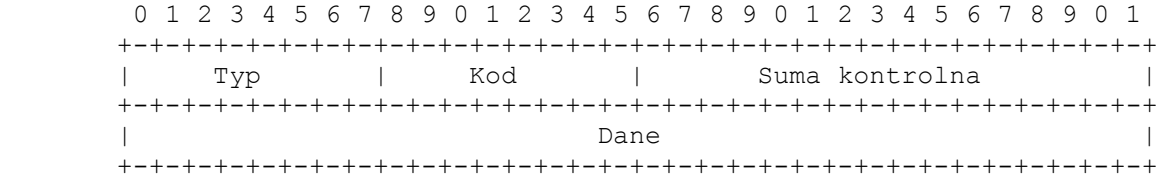
Komunikat z kodem 1 jest wysyłany do nadawcy przez stację docelową, ponieważ tylko ona składa z powrotem pakiet z fragmentów (nie robią tego routery).

Problem z parametrem (Parameter Problem)
Typ: 12
Kod: 0, problem jest identyfikowany przez wskaźnik



Oznacza problem z przetwarzaniem parametrów nagłówka IP. Wskaźnik identyfikuje pierwszy oktet pola parametru, np. 1 odpowiada polu ToS, 20 – kodowi pierwszej opcji.

Wygaszanie źródła (Source Quench)
Typ: 4
Kod: 0



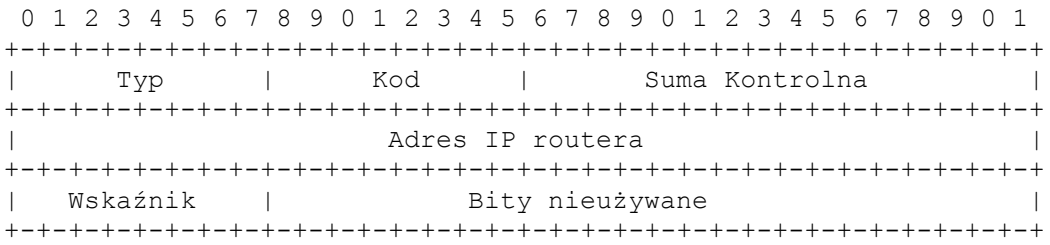
Komunikat wysyłany przez router lub host docelowy w przypadku, gdy nie nadąża on z przetwarzaniem napływających pakietów i następuje przepełnienie bufora. Po otrzymaniu takiego komunikatu maszyna źródłowa powinna zmniejszyć prędkość nadawania.

Przekierowanie (Redirect)
Typ: 5
Kod: 0 <- przekieruj te z następnych wysyłanych pakietów, które są zaadresowane do komputera, którego adres spowodował komunikat przekierowania, oraz te, które są zaadresowane do dowolnego komputera w jego sieci (obecnie nie jest stosowany ze względu na to, że adres sieci znajdującej się za routerem nie wynika z klasy adresu docelowego i nie jest możliwy do ustalenia);

Kod 1 <- przekieruj tylko te z następnych wysyłanych pakietów, które są zaadresowane do komputera, którego adres spowodował komunikat przekierowania;

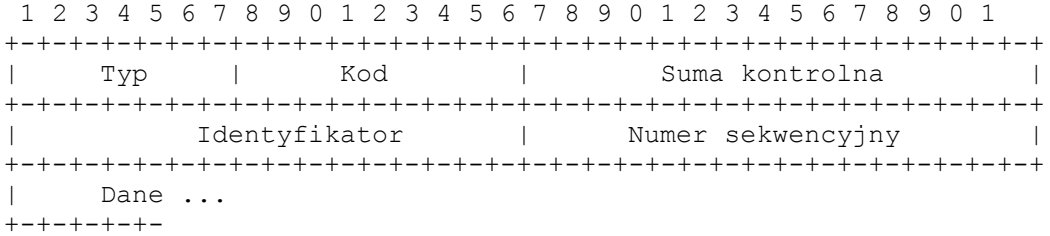
Kod 2 <- dotyczy pakietów określonych dla kodu 0, ale tylko tych, w których pole ToS jest takie samo jak w pakiecie, który spowodował komunikat przekierowania (obecnie nie jest stosowany z tego samego względu co komunikat z kodem 0);

Kod 3 <- dotyczy pakietów określonych dla kodu 1, ale tylko tych, w których pole ToS jest takie samo jak w pakiecie, który spowodował komunikat przekierowania.



Komunikat wysyłany przez router R1 w sytuacji, gdy maszyna źródłowa wysyła pakiet poza sieć lokalną, kierując go do routera R1, a router R1 przekazuje ten pakiet do interfejsu routera R2 znajdującego się w tej samej sieci co maszyna źródłowa. Komunikat ten informuje maszynę źródłową, ze powinna kierować pakiet bezpośrednio do R2.

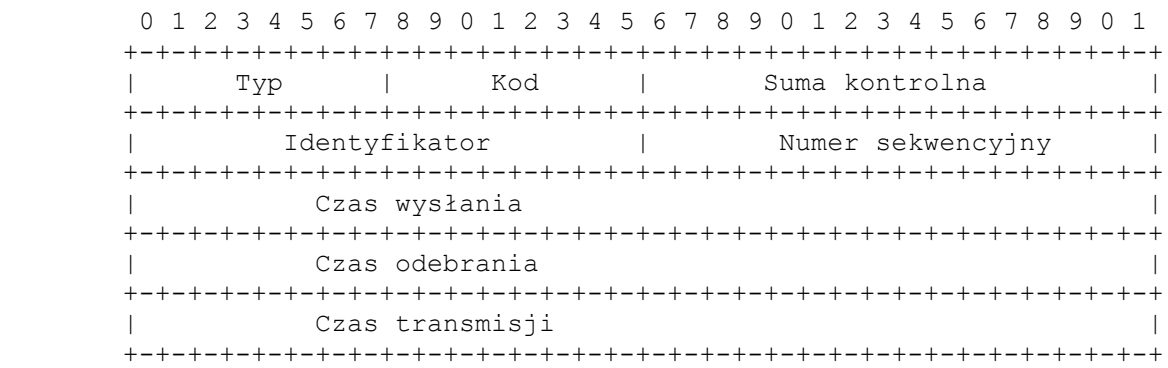
Żądanie echa lub odpowiedź na echo (Echo Request, Echo Reply)
Typ: 8, Kod: 0 <- Echo Request
Typ: 0, Kod: 0 <- Echo Reply



Identyfikator pozwala zestawić komunikaty Echo Request z odpowiadającymi im komunikatami Echo Reply. Na przykład, identyfikator może odgrywać rolę taką, jak numer portu w protokole TCP lub UDP, czyli identyfikować połączenie, natomiast numer sekwencyjny może być zwiększany o 1 w każdym kolejnym pakiecie Echo Request. W pakiecie Echo Reply są zwracane te same wartości.

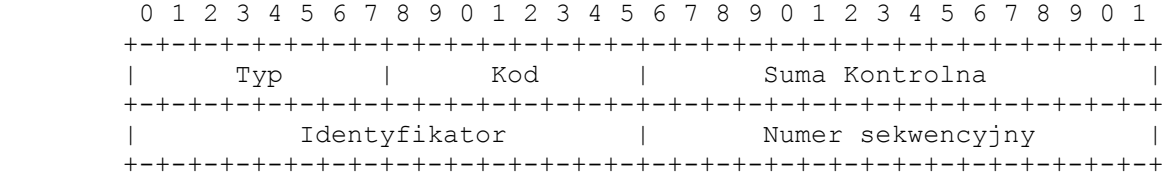
Stempel czasowy lub odpowiedź na stempel czasowy (Timestamp Request, Timestamp Reply)
Typ: 13 <- Timestamp
14 <- Timestamp Reply

Kod: 0



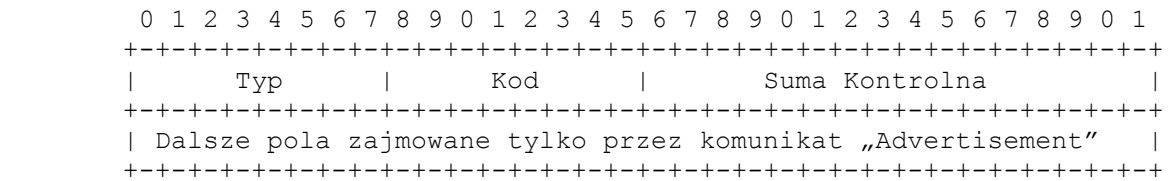
Żądanie informacji lub odpowiedź na żądanie informacji (Information Request, Information Reply)
Typ: 15 <- Information Request
16 <- Information Reply

Kod: 0



Wykrywanie routerów (Router Discovery)
Typ: 9 <- Router advertisement
10 <- Router solicitation

Kod: 0



Powyższe komunikaty mają na celu poinformowanie hostów o obecności routera w sieci, obecnie są rzadko stosowane, ponieważ zastępuje je protokół DHCP.

Testowanie komunikacji na poziomie IP - polecenie ping

Polecenie to wykorzystuje komunikaty ICMP „Echo Request" i „Echo Reply" do stwierdzenia, czy istnieje komunikacja w warstwie IP między maszyną lokalną, a wskazaną maszyną zdalną. Składnia polecenia w systemie Linux jest następująca:

ping opcje adres_lub_nazwa_maszyny_zdalnej

Oto niektóre przydatne opcje

-c liczba_pakietów : wysyła podaną liczbę komunikatów „Echo Request"

-n : wypisywane są adresy IP zamiast nazw, stosuje się w przypadku nie działających mechanizmów rozwiązywania nazw (DNS)

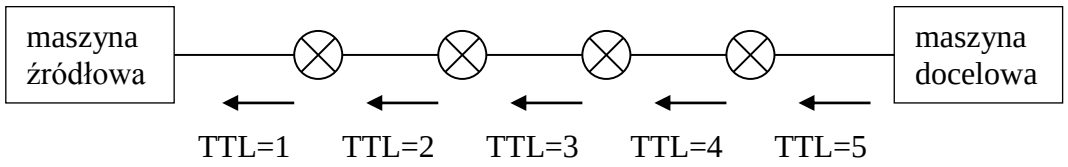
-s rozmiar_pakietu : wysyła komunikaty ICMP o wskazanej długości pola danych

-R : żądanie zapisywania trasy w polu opcji nagłówka IP

pozostałe opcje są opisane w podręczniku man (man ping).

Śledzenie trasy pakietów - polecenie traceroute

Polecenie traceroute generuje pakiety z małymi wartościami pola TTL. Dla przypomnienia, TTL (Time To Live) jest polem nagłówka IP mającym zapobiec powstawaniu pętli. Każdy router przekazujący pakiet zmniejsza wartość tego pola o 1. Router odrzuca każdy pakiet z wartością TTL równą zero i wysyła do nadawcy pakietu komunikat ICMP o przekroczeniu czasu (Time Exceeded). Przez wysyłanie po kolei pakietów z małymi wartościami TTL (1,2,3,...) traceroute powoduje, że routery znajdujące się na trasie pakietu wysyłają pakiety ICMP, identyfikując się w ten sposób. Pakiet z TTL równym 1 powoduje wysłanie komunikatu przez pierwszy router, z TTL równym 2 – przez drugi, itd.



Router wysyła komunikat ICMP przez ten sam interfejs, przez który otrzymał pakiet pochodzący od polecenia traceroute.. Adres tego interfejsu jest podawany w komunikacie ICMP jako adres źródłowy. Oprócz adresów IP, traceroute raportuje czas przesłania pakietu tam i z powrotem. Dodatkowe komunikaty ICMP messages (np. o nieosiągalnej maszynie lub sieci docelowej) są przedstawiane w postaci zakodowanej, na przykład `!N` oznacza nieosiągalną sieć, `!H` oznacza nieosiągalnego hosta, itd.

Składnia polecenia:

traceroute <opcje> <nazwa lub adres IP stacji docelowej>

niektóre opcje:

– f czas_TTL : ustawia początkową wartość wstawianą w pole TTL pierwszego wysyłanego pakietu (domyślnie 1)

– F : ustawia bit „nie fragmentuj”

– I : używa pakietów ICMP ECHO zamiast datagramów UDP

– m czas_TTL: ustawia maksymalną wartość wstawianą w pole TTL ostatniego wysyłanego pakietu (domyślnie 30)

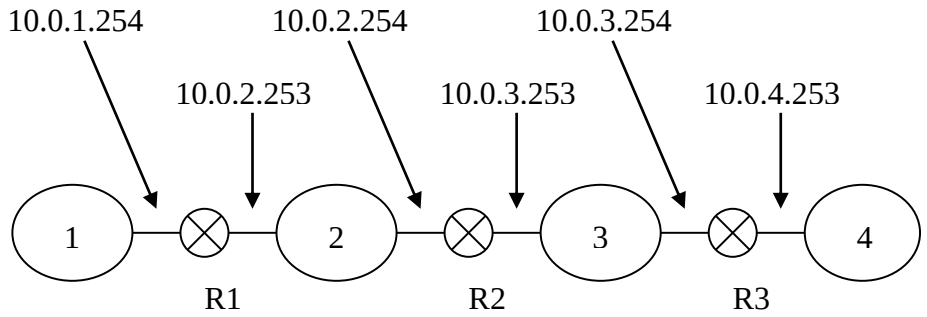
– n : wypisuje adresy IP zamiast nazw

– p bazowy_port_UDP : ustawia bazowy port UDP w pakietach wysyłanych jako datagramy UDP (domyślnie 33434), zakłada się, że w maszynie docelowej na portach od bazowy do bazowy + liczba_skoków – 1 nie nasłuchuje żadna aplikacja, a w konsekwencji host docelowy odpowie pakietem ICMP „PORT UNREACHABLE” (Port nieoiągalny)

– t wartość_TOS : ustawia żądaną wartość (dziesiętną) w polu TOS (domyślnie 0), opcja przydatna do badania, czy dla różnych wartości TOS pakiety przesyłane są różnymi trasami, przydatne wartości to 16 (małe opóźnienie), czy 8 (wysoka przepustowość)

pozostałe opcje są opisane w podręczniku man (man traceroute).

Konfiguracja sprzętu dla przykładów 1 i 2:



Polecenia konfigurujące router R1:

Konfiguracja interfejsów sieciowych:

ifconfig eth0 10.0.1.254 netmask 255.255.255.0 broadcast 10.0.1.255

ifconfig eth0:1 10.0.2.253 netmask 255.255.255.0 broadcast 10.0.2.255

Konfiguracja tablicy trasowania:

route add default gw 10.0.2.254

Polecenia konfigurujące router R2:

Konfiguracja interfejsów sieciowych:

ifconfig eth0 10.0.2.254 netmask 255.255.255.0 broadcast 10.0.2.255

ifconfig eth0:1 10.0.3.253 netmask 255.255.255.0 broadcast 10.0.3.255

Konfiguracja tablicy trasowania:

route add -net 10.0.1.0 netmask 255.255.255.0 gw 10.0.2.253

route add -net 10.0.4.0 netmask 255.255.255.0 gw 10.0.3.254

Polecenia konfigurujące router R3:

Konfiguracja interfejsów sieciowych:

ifconfig eth0 10.0.3.254 netmask 255.255.255.0 broadcast 10.0.3.255

ifconfig eth0:1 10.0.4.253 netmask 255.255.255.0 broadcast 10.0.4.255

Konfiguracja tablicy trasowania:

route add default gw 10.0.3.253

Przykład 1.Śledzenie pakietów przy pomocy polecenia ping

Wydaj polecenie ping na maszynie z sieci 10.0.1.0 do maszyny z sieci 10.0.4.0. Zaobserwuj otrzymywane komunikaty w przypadku, gdy włączone są wszystkie interfejsy routerów, oraz interfejsy maszyn źródłowej i docelowej. Następnie wyłączaj kolejno: interfejs maszyny docelowej, interfejs 10.0.4.253 routera R3, interfejs 10.0.3.254 routera R3, interfejs 10.0.3.253 routera R2, interfejs 10.0.2.254 routera R2, interfejs 10.0.2.253 routera R1, oraz interfejs 10.0.1.254 routera R1, obserwując przy tym otrzymywane komunikaty.

Przykład 2. Śledzenie pakietów przy pomocy polecenia traceroute

Na maszynie z sieci 10.0.1.0 wydaj polecenie traceroute, wskazując jako docelową, maszynę z sieci 10.0.4.0. Zaobserwuj otrzymywane komunikaty. Następnie, posługując się programem Wireshark, przeprowadź analizę pakietów generowanych przez polecenie traceroute.

Przykład 3. Analiza komunikatów Echo Request i Echo Reply

Skonfiguruj analizator Wireshark tak, aby przechwytywał tylko pakiety ICMP wymieniane między komputerami twoim i sąsiada. W tym celu użyj następującego wyrażenia filtrującego:

icmp and host <nazwa lub IP własnego komp.> and host <nazwa lub IP komp. sąsiada>

Następnie wydaj polecenie

ping – c3 <nazwa lub IP komp. sąsiada>

Przeanalizuj wysyłane i otrzymywane komunikaty ICMP (w sumie powinno ich być 6), szczególną uwage zwróć na pola „Identifier" i „Sequence Number" wystepujące w nagłówku ICMP.