

Computer Networks : Hoofdstuk 13 - ICMP

ICMP Messages

ICMPv4 and ICMPv6 Messages

Internet Control Message Protocol (ICMP) geeft feedback over issue gerelateerd aan het processen van IP pakketten onder verschillende condities.

- ICMPv4 is het messaging protocol voor IPv4. ICMPv6 is het messaging protocol voor IPv6 en bevat meer functionaliteiten.
- De ICMP berichten bevatten zowel voor ICMPv4 als ICMPv6:
 - Host reachability
 - Destination or Service Unreachable
 - Time Exceeded

Note

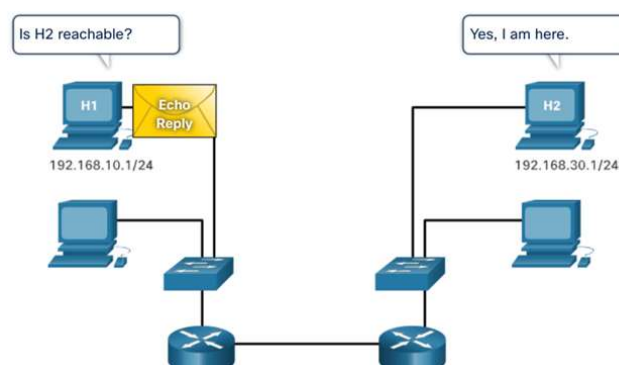
ICMP berichten zijn niet verplicht en vaak ook niet toegestaan binnen een netwerk voor veiligheids redenen.

Host Reachability

ICMP Echo berichten kunnen gebruikt worden om de **bereikbaarheid** van een host in een IP netwerk te testen.

Voorbeeld:

- De local host verstuurd een ICMP Echo Request naar een host.
- Indien de host beschikbaar is, zal de bestemmingshost antwoorden met een **Echo Reply**.



Destination or Service Unreachable

- Een ICMP Destination Unreachable bericht kan gebruikt worden om de bron te berichten dat een bestemming of een dienst niet beschikbaar is.
- Het ICMP bericht zal een code bevatten die aangeeft waarom het pakket niet geleverd kan worden.

A few Destination Unreachable codes for ICMPv4 are:	A few Destination Unreachable codes for ICMPv6 are:
<ul style="list-style-type: none">• 0 - Net Unreachable• 1 - Host Unreachable• 2 - Protocol Unreachable• 3 - Port Unreachable	<ul style="list-style-type: none">• 0 - No route to Destination• 1 - Communication with the destination is administratively prohibited (e.g., firewall)• 2 - Beyond scope of the source address• 3 - Address unreachable• 4 - Port Unreachable

Note

ICMPv6 heeft gelijkaardige codes met kleine verschillen voor Destination Unreachable berichten.

TTL = hop limit

Time Exceeded

- Wanneer het "Time to Live (TTL)" veld in een pakket verminderd is naar 0, dan zal een ICMPv4 Time Exceeded bericht verstuurd worden naar de bron host.
- ICMPv6 heeft ook een Time Exceeded bericht. In plaats van het IPv4 TLL veld, zal ICMPv6 het IPv6 Hop Limit veld gebruiken om te achterhalen als een pakket al dan niet vervallen is.

```
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 192.168.1.1: TTL expired in transit.
Reply from 192.168.1.1: TTL expired in transit.
Reply from 192.168.1.1: TTL expired in transit.
Reply from 192.168.1.1: TTL expired in transit.

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

ICMPv6 Messages

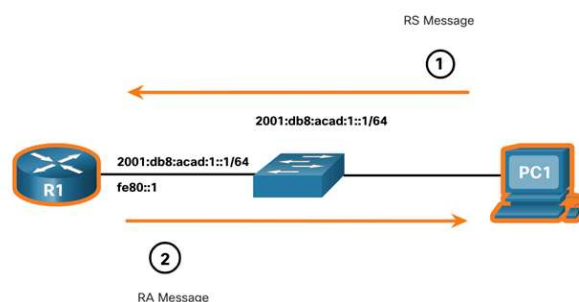
ICMPv6 Messages hebben nieuwe features en een verbeterde functionaliteit die we niet hadden in ICMPv4. Zoals vier nieuwe portocollen die onderdeel zijn van de Neighbor Discovery Protocol (ND of NDP)

- Het berichtenverkeer tussen een IPv6-router en een IPv6-apparaat, met inbegrip van dynamische adrestoewijzing, ziet er als volgt uit:
 - **Router Solicitation (RS)** bericht
 - **Router Advertisement (RA)** bericht
- Het berichtenverkeer tussen IPv6 toestellen inclusief het detecteren van duplicate adressen en adres resolution, ziet er als volgt uit:
 - **Neighbor Solicitation (NS)** bericht
 - **Neighbor Advertisement (NA)** bericht

Note

ICMPv6 ND bevat ook het redirect bericht. Dit heeft een gelijkaardige functie als het redirect bericht van IPv4

- RA berichten worden door IPv6-enabled routers elke 200 seconden uitgestuurd om adresseringsinformatie te voorzien aan IPv6-enabled hosts.
- RA berichten kunnen adresseringsinformatie bevatten van de host, zoals prefix lengte, DNS adres, en domeinnaam
- Een host die gebruik maakt van *Stateless Address Autoconfiguration* (SLAAC) zal zijn default gateway gelijk stellen aan het link-local adres van de router dat de RA stuurt.
- Een IPv6-enabled router zal een RA bericht uitsturen als een antwoord op een RS bericht.



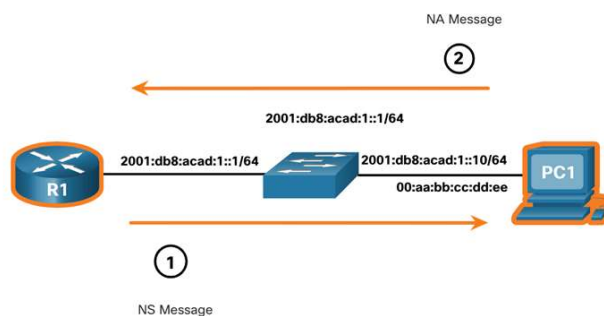
- Een toestel dat als adres een global IPv6 unicast of link-local unicast geassigneerd heeft, mag **duplicate address detection (DAD)** uitvoeren om te achterhalen of het IPv6 adres uniek is.

- Om te bekijken of een adres al dan niet uniek is, zal het toestel een NS bericht versturen met zijn eigen IPv6 adres als het adres waar naar gezocht wordt.
- Als een ander toestel op het netwerk dit adres heeft, zal het antwoorden met een NA bericht, en zo melden aan het toestel dat het bericht uitstuurt, dat dit adres reeds in gebruik is.

Note

DAD is geen vereiste, maar RFC 4861 raad te sterkste aan dat DAD uitgevoerd wordt op unicast adressen.

- Om te achterhalen wat het bestemmings MAC adres is zal het toestel een NS bericht sturen naar het **solicited node address**
- Het bericht zal het gekende (te zoeken) IPv6 adres bevatten. Het toestel met het te zoeken IPv6 adres zal antwoorden met een NA bericht dat zijn Ethernet MAC adres bevat.



Ping and Traceroute tests

Ping - Test Connectivity

- Het `ping` commando is een IPv4 en een IPv6 testprogramma dat gebruikt maakt van ICMP echo requesten en een echo reply berichten om de verbinding te testen tussen de host. Het geeft een samenvatting dat de succesratio geeft en de gemiddelde round-trip tijd naar de bestemming

```

S1#ping 192.168.20.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms

```

- Als een antwoord niet ontvangen is binnen de timeout, dan zal het `ping` commando een bericht weergaven dat meldt dat er geen antwoord ontvangen is.

```
RI#ping 2001:db8:acad:1::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:acad:1::2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Important

Het is veelvoorkomend dat de eerste **ping** een timeout genereert als address resolution (ARP of ND) uitgevoerd moet worden alvorens het ICMP Echo Request verstuurd wordt.

Ping the Loopback

Een **ping** commando kan gebruikt worden om intern de configuratie van IPv4 of IPv6 te testen op de lokale host.

- pingen van de het lokaal IPv4 loopback adres:

```
ping 127.0.0.1
```

- pingen van het lokaal IPv6 loopback adres:

```
ping ::1
```

→ ipv6 local host (loopback)

Ping the Default Gateway

Het **ping** commando kan ook gebruikt worden om te testen of een host kan communiceren met op het lokaal netwerk.

Hiervoor gebruiken we het default gateway adres, omdat de router meestal operationeel is.

- een succesvolle **ping** naar de default gateway geeft weer dat de host en de router interface die dient als de default gateway beide operationeel zijn binnen het netwerk
- indien de default gateway niet antwoord, kunnen we een **ping** sturen naar een andere host waarvan we weten dat die operationeel is binnen het lokaal netwerk

Ping a Remote Host

ping kunnen we ook gebruiken om te testen of een lokale host kan verbinden over een intern netwerk.

Een lokale host kan een host pingen op een extern netwerk. Een succesvolle **ping** over een intern netwerk bevestigt de communicatie op het lokale netwerk.

Note

Vele netwerkadministrators limiteren of verbieden het aantal ICMP berichten. Deze kunnen ook negatieve `ping` resultaten veroorzaken.

Traceroute - Test the Path

- Traceroute (`tracert`) is een programma dat kan gebruikt worden om het pad te testen tussen twee host. Het geeft een lijst van een aantal hops weer die sucsessvol bereikt werden over het pad.
- Traceroute voorziet een roundtrip tijd voor elke hop over het pad and geeft weer indien de hop faalt. **Een ster "*" geeft aan indien een hop verloren gaat of een pakket niet antwoord.**
- Deze informatie kan gebruikt worden om een problematische router te localiseren op het pad. Het kan ook aangeven of de router al dan niet geconfigureerd is om te antwoorden.

Note

Traceroute maakt gebruik van een functie van het TTL veld in IPv4 en van de Hop Limit voor IPv6 in de Laag 3 headers, samen met het ICMP Time Exceeded bericht.

```
R1#traceroute 192.168.40.2
Type escape sequence to abort.
Tracing the route to 192.168.40.2

 1  192.168.10.2      1 msec    0 msec    0 msec
 2  192.168.20.2     2 msec    1 msec    0 msec
 3  192.168.30.2     1 msec    0 msec    0 msec
 4  192.168.40.2     0 msec    0 msec    0 msec
```

- Het eerste bericht dat verstuurd wordt van traceroute zal een TTL veld hebben van 1. Dit zorgt ervoor dat de TTL time out op de eerste router. Deze router zal dan antwoorden met een ICMPv4 Time Exceeded bericht
- Traceroute zal dan progressief het TTL verhogen (2, 3, 4, ...) voor elke reeks berichten. Dit geeft de trace met de adressen van elke hop wanneer deze time outen over het hele pad.
- Het TTL veld wordt verder verhoogt tot wanneer de bestemming bereikt is. (of tot wanneer de maximum waarde bereikt is)