Bevezetés a hálózatok világába

ICMP (Internet Control Message Protocol)

Habár maga az IP nem megbízható protokoll, a TCP/IP protokollcsalád tartalmaz olyan üzeneteket, amelyek bizonyos hibák előfordulása esetén küldhetők. Ezeket az üzeneteket.az ICMP protokoll szolgáltatásaival küldik el. A céljuk nem az, hogy megbízhatóvá tegyék az IP protokollt, inkább az IP csomagok feldolgozása során felmerült jelenségekről küldenek visszajelzést bizonyos esetekben. Az ICMP üzenetek nem szükségesek, bizonyos hálózatokon belül biztonsági okokból sokszor nem is engedélyezettek.

Az ICMP IPv4 és IPv6 esetén egyaránt rendelkezésre áll. Az IPv4 üzenetküldő protokollja az ICMPv4. Az ICMPv6 ugyanezeket a szolgáltatásokat nyújtja az IPv6 felé, de további funkciókat is tartalmaz. Ha ebben a kurzusban az ICMP kifejezést használjuk, akkor azt egyaránt értjük az ICMPv4-re és az ICMPv6-ra is.

Az ICMP üzenetek száma és az ok, ami miatt kiküldik őket, nagyon kiterjedt. Most csak a leggyakoribbak egy részét tárgyaljuk.

Az ICMPv4 és ICMPv6 közös ICMP üzenetei például:

- Állomás elérhetősége (Host reachability)
- Cél vagy szolgáltatás nem elérhető (Destination or Service Unreachable)
- Időtúllépés (Time exceeded)

Állomás elérhetősége

Az ICMP visszhang kérés üzenetet annak a megállapítására használhatjuk, hogy egy állomás üzemel-e. A helyi gép ICMP visszhang kérés üzenetet küld az állomásnak. Ha az állomás elérhető, visszhang válasz üzenettel válaszol. Játsszuk le az ábra animációját az ICMP visszhang kérés/visszhang válasz üzenetek megtekintéséhez. Az ICMP visszhang üzenetei képezik a ping segédprogram alapját is.

Cél vagy szolgáltatás nem elérhető (Destination vagy Service Unreachable)

Ha egy állomás vagy átjáró olyan csomagot kap, amelyiket nem tud kézbesíteni, az ICMP cél nem elérhető üzenetét használhatja arra, hogy a küldőt értesítse a cél vagy a szolgáltatás elérhetetlenségéről. Az üzenet tartalmaz egy kódot, amely leírja, hogy a csomagot miért nem sikerült kézbesíteni.

Az ICMPv4 cél nem elérhető üzenetének néhány kódja és jelentésük:

- 0 - Hálózat nem elérhető
- 1 - Állomás nem elérhető
- 2 - Protokoll nem elérhető
- 3 - Port nem elérhető

Az ICMPv6 cél nem elérhető üzenetének néhány kódja és jelentésük:

- 0 - Nincs útvonal a célig
- 1 - Célállomással való kommunikáció adminisztratív módon tilos (pl. tűzfal miatt)
- 2 - Forráscím hatókörén túl található
- 3 - Cím elérhetetlen
- 4 - Port nem érhető el

Megjegyzés: Az ICMPv6 hasonló, de kissé más kódokat használ a cél nem elérhető üzenetekben.

Időtúllépés

Az ICMPv4 időtúllépés üzenetet forgalomirányítók használják akkor, ha a csomagot nem továbbíthatják, mert az élettartam (Time To Live, TTL) mezőjének értéke nullára csökkent. Ha egy forgalomirányító elfogad egy csomagot, és a TTL érték csökkentése után az új érték nulla lesz, eldobja a csomagot, majd időtúllépés üzenetet küld a küldőnek.

Az ICMPv6 szintén időtúllépés üzenetet küld, ha a forgalomirányító nem tudja továbbítani az IPv6 csomagot, mert az élettartama lejárt. Az IPv6-nál nem TTL mezőt használnak, hanem az ugrás korlát (hop limit, ugrás limit) nevű mező jelzi, ha a csomag élettartama lejárt.

ICMPv6 üzenetek

Az ICMPv6 információs- és hibaüzenetei nagyon hasonlóak az ICMPv4-ben megvalósított vezérlő- és hibaüzenetekhez. Azonban az ICMPv6 olyan funkciókat és fejlesztéseket is tartalmaz, melyek az ICMPv4-ben még nincsenek jelen.

Az ICMPv6 négy új protokollt tartalmaz a Szomszéd Felderítő Protokoll (Neighbor Discovery Protocol, ND, NDP) részeként:

- Forgalomirányító keresés üzenet (Router Solicitation)
- Forgalomirányító hirdetés üzenet (Router Advertisement)
- Szomszéd keresés üzenet (Neighbor Solicitation)
- Szomszéd hirdetés üzenet (Neighbor Advertisement)

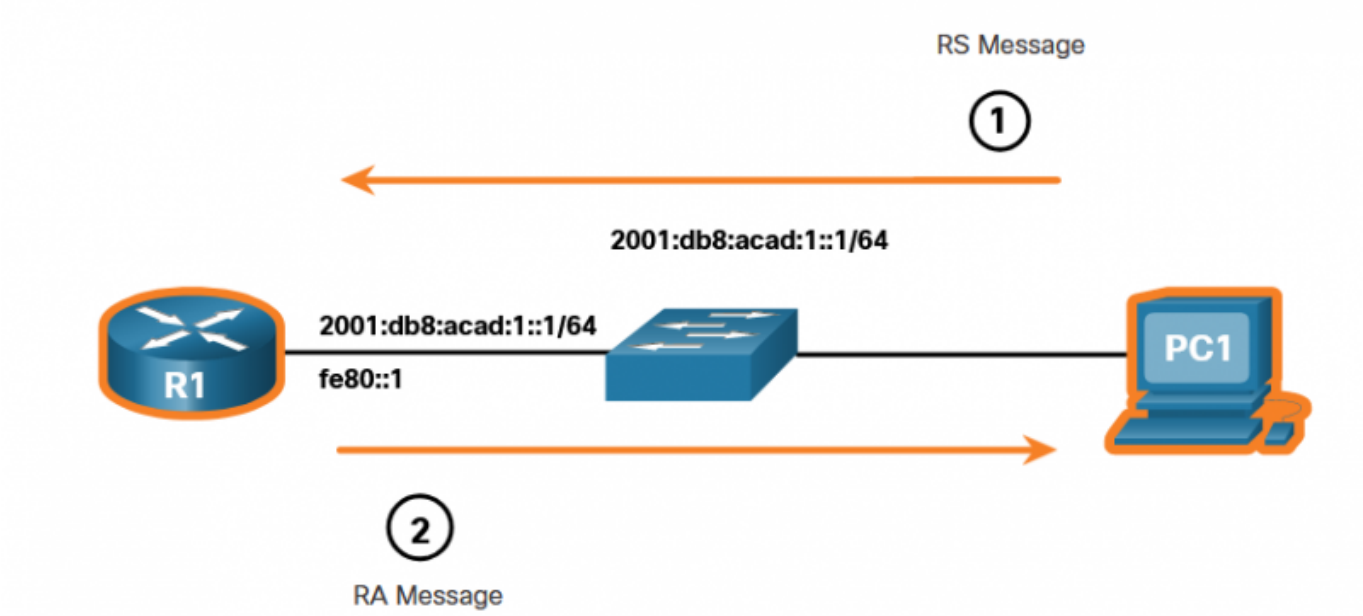
Forgalomirányító keresés és forgalomirányító hirdetés üzenetek

Az IPv6-képes eszközöket két kategóriába sorolhatjuk: forgalomirányítók és állomások. A forgalomirányító keresés és a forgalomirányító hirdetés üzenetek állomások és forgalomirányítók között zajlanak.

- **Forgalomirányító keresés (Router Solicitation, RS) üzenet**: Az állomás akkor fog RS üzenetet küldeni a forgalomirányítónak, amikor úgy állítjuk be, hogy a címzési információját

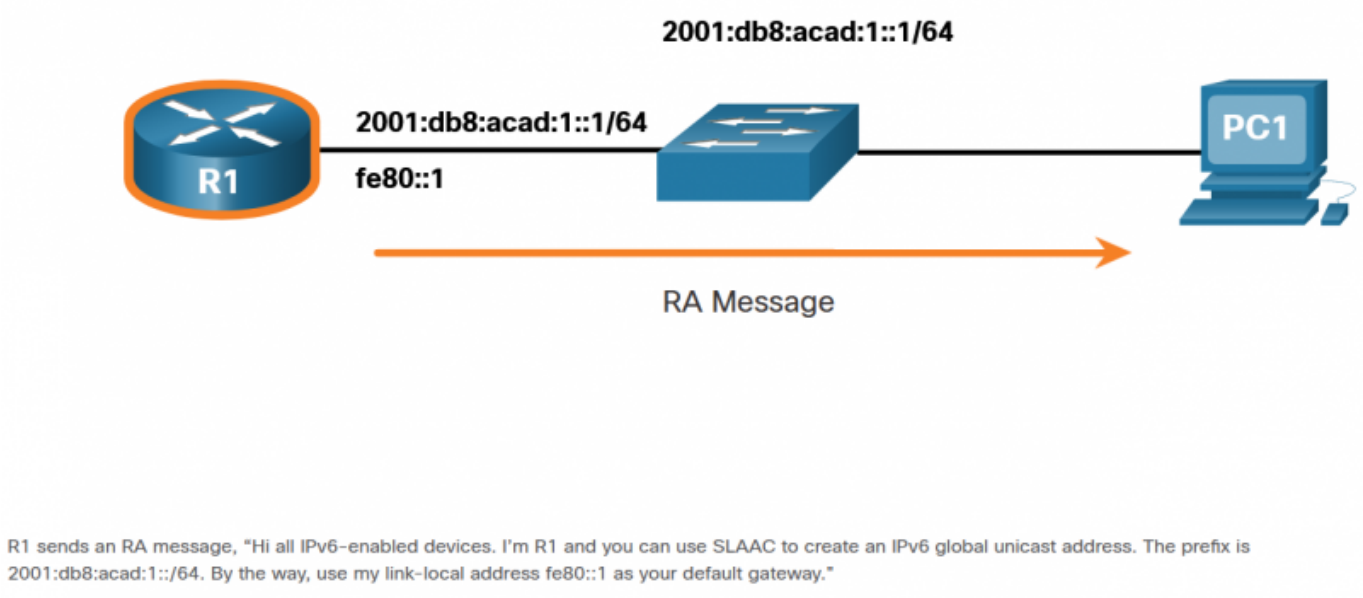
automatikusan szerezze be állapotmentes cím autokonfiguráció (SLAAC) segítségével. Az állomás ezt az RS üzenetet az IPv6 minden router multicast címre küldi el.

- **Forgalomirányító hirdetés (Router Advertisement, RA) üzenet**: Az RA üzeneteket a forgalomirányítók küldik, hogy címzési információt biztosítsanak az SLAAC-t használó állomások számára. Az RA üzenet olyan címzési információkat adhat az állomásnak, mint az előtag és az előtag hossza. A forgalomirányító rendszeresen, vagy egy RS üzenetre válaszolva küld ki az RA üzeneteket. Alapértelmezés szerint a Cisco forgalomirányítók 200 másodpercenként küldenek RA üzenetet. Az RA üzeneteket az IPv6 minden állomás multicast címre küldik. Az SLAAC-t használó állomás az alapértelmezett átjáróját az RA üzenetet küldő forgalomirányító link-local címére állítja be.



R1 replies to the RS with an RA message.

1. PC1 sends an RS message, “Hi, I just booted up. Is there an IPv6 router on the network? I need to know how to get my IPv6 address information dynamically.”
2. R1 replies with an RA message. “Hi all IPv6-enabled devices. I’m R1 and you can use SLAAC to create an IPv6 global unicast address. The prefix is 2001:db8:acad:1::/64. By the way, use my link-local address fe80::1 as your default gateway."



ICMPv6 szomszéd keresés (Neighbor Solicitation) és szomszéd hirdetés (Neighbor Advertisement) üzenetek

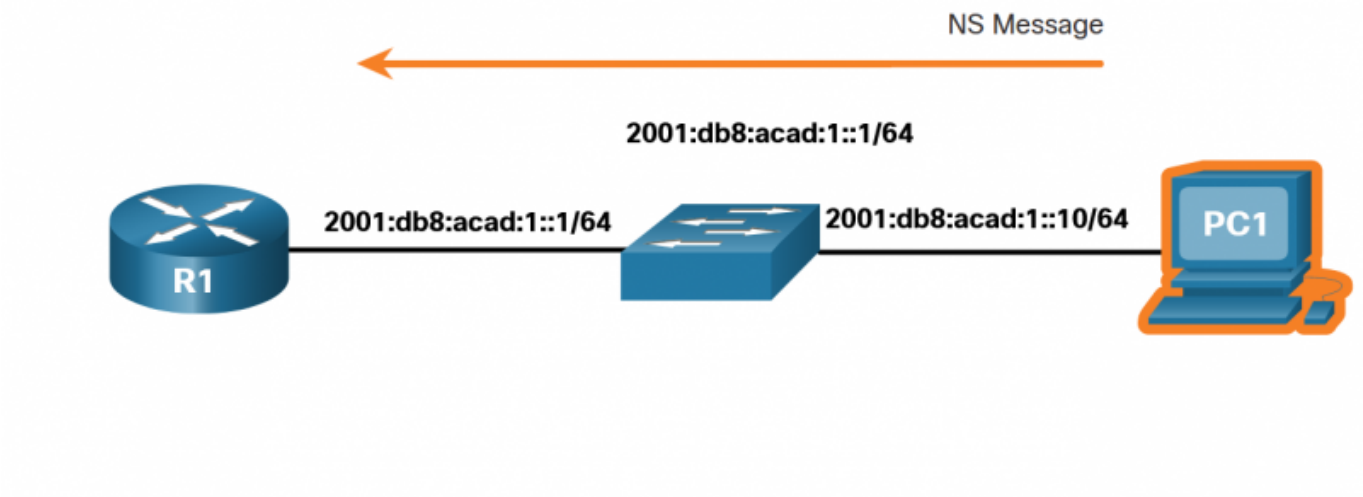
Az ICMPv6 Szomszéd Felderítő Protokoll (Neighbor Discovery Protocol) két további üzenettípust tartalmaz: szomszéd keresés (Neighbor Solicitation) és szomszéd hirdetés (Neighbor Advertisement).

A Neighbor Solicitation és a Neighbor Advertisement üzeneteket az alábbiakra használják:

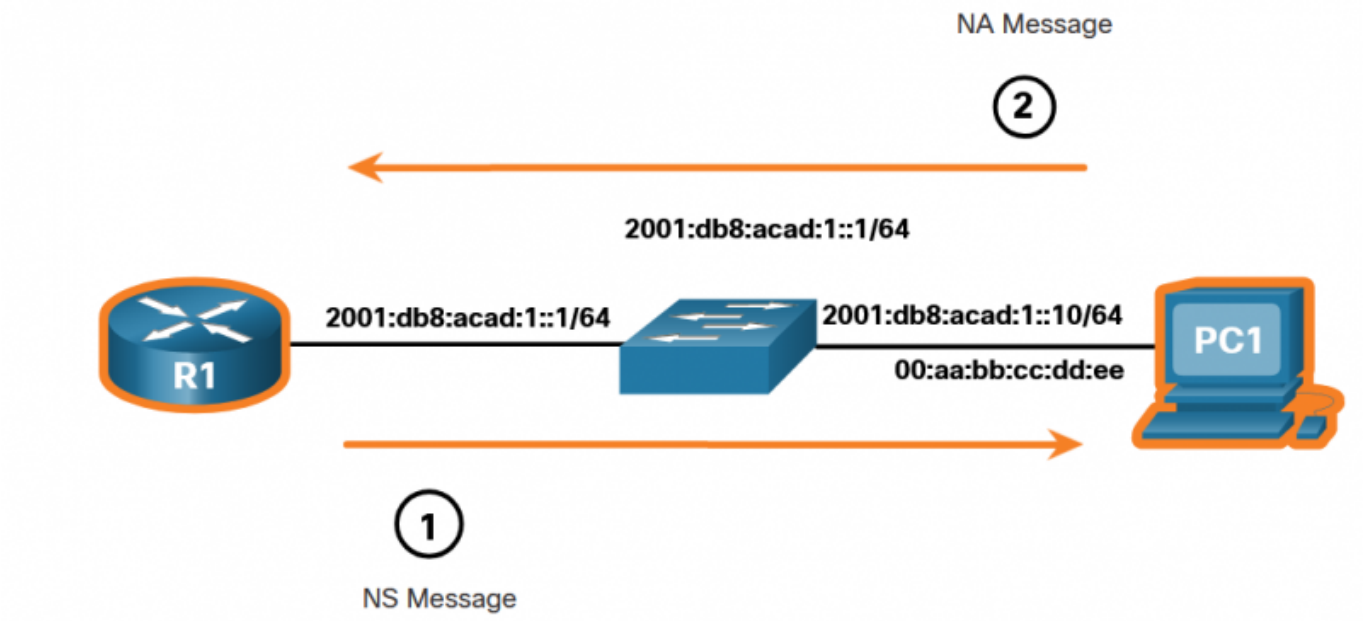
- **Címfeloldás**
- **Duplikált Cím Felderítés (Duplicate Address Detection, DAD)**

Címfeloldás

Címfeloldásra akkor van szükség, ha a LAN egy eszköze ismeri a cél egyedi IPv6-címét, de nem tudja a hozzá tartozó Ethernet MAC-címet. A cél MAC-címének meghatározásához az eszköz egy NS üzenetet küld a keresett csomópont címére. Ez az üzenet az ismert (cél) IPv6-címet fogja tartalmazni. Az eszköz, amelynek a címe megegyezik a cél IPv6-címmel, egy NA üzenettel fog válaszolni, amely a saját Ethernet MAC-címét tartalmazza.



PC1 sends an NS message to check the uniqueness of an address, "Will whoever has the IPv6 address 2001:db8:acad:1::10, send me your MAC address?"



1. R1 sends an address resolution NS message. "Will whoever has the IPv6 address 2001:db8:acad:1::10, send me your MAC address?"
2. PC1 replies with an NA message. "I'm 2001:db8:acad:1::10 and my MAC address is 00:aa:bb:cc:dd:ee."

Duplikált Cím Felderítés

Amikor egy eszköz globális egyedi vagy link-local egyedi címhez jut, egy DAD művelet elvégzése javasolt a számára, hogy megbizonyosodjon a címének egyediségéről. A cím egyediségét úgy ellenőrzi, hogy egy NS üzenetet küld ki a saját IPv6-címével, mint célcímmel. Ha a hálózat más eszköze is birtokolja ugyanezt a címet, egy NA üzenettel fog válaszolni. Ez az NA üzenet jelzi a küldőnek, hogy a cím használatban van. Ha egy bizonyos ideig nem érkezik vissza NA üzenet, akkor az egyedi cím valóban egyedi és használható.

Megjegyzés: A DAD művelet elvégzése nem kötelező, de az RFC 4861 ajánlja az egyedi címekre történő végrehajtását.

Ping - A helyi protokollkészlet tesztelése

A ping egy olyan tesztelési segédprogram, amely ICMP visszhang kérés és visszhang válasz üzeneteket használ az állomások közti kapcsolatok ellenőrzésére. A ping IPv4 és IPv6 állomások esetén is működik.

A hálózat egy másik állomásával úgy ellenőrizhetjük a kapcsolatot, hogy egy visszhang kérés üzenetet küldünk neki a ping paranccsal. Ha a megadott című állomás megkapja a visszhang kérést, egy visszhangkérés válasz (vagy visszhang válasz) üzenettel fog válaszolni. A visszhang válasz fogadásakor a ping kiírja a kérés elküldése és a válasz megérkezése közt eltelt időt. Ebből következtethetünk a hálózat teljesítményére is.

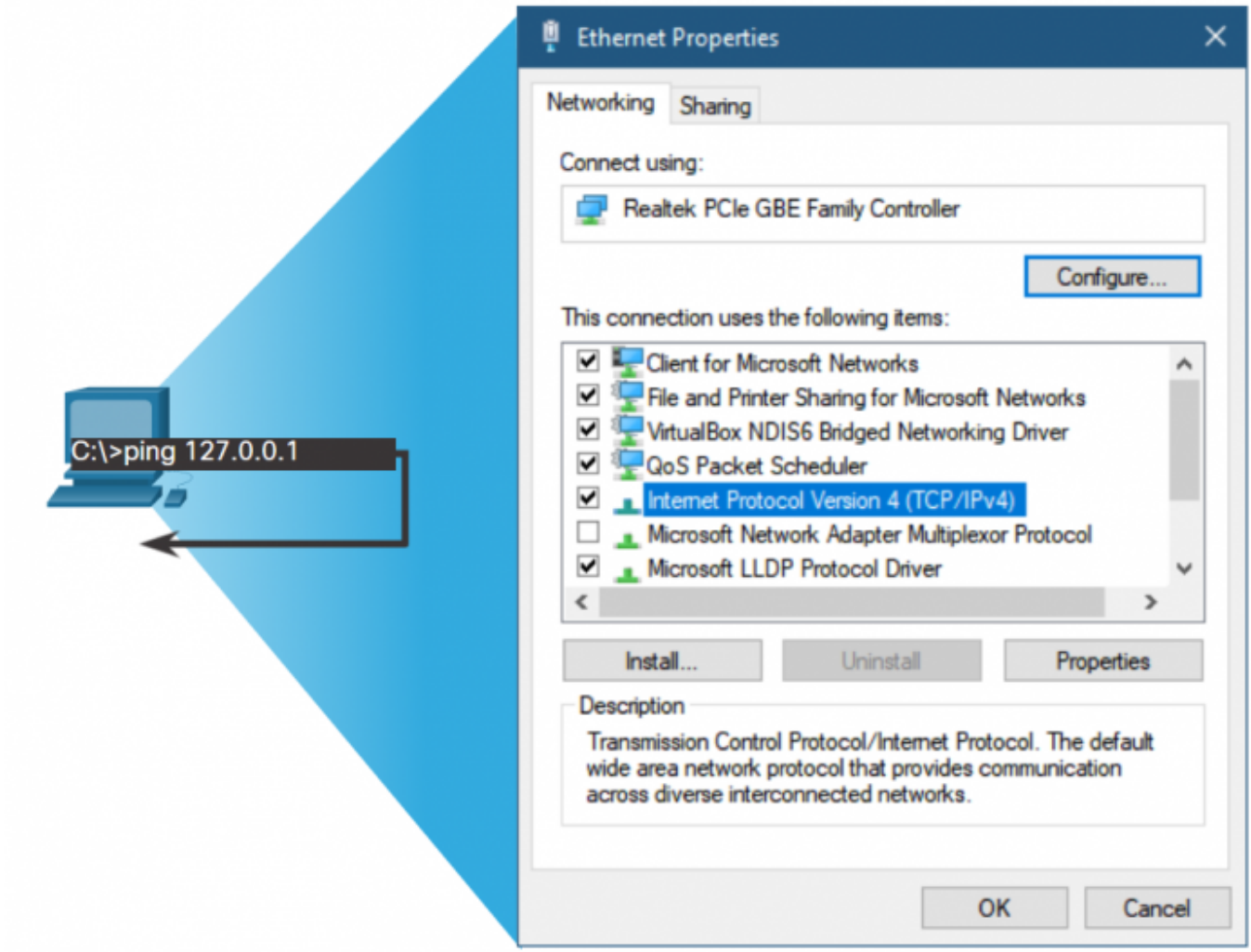
A ping a válaszra csak egy bizonyos ideig vár. Ha az adott időn belül nem érkezik válasz, a ping egy üzenetben közli, hogy nem érkezett válasz. Ez általában valamilyen probléma jele, de jelentheti azt is, hogy a hálózatban valamilyen biztonsági beállítás blokkolja a ping üzeneteit.

Az összes kérés elküldése után a ping segédprogram egy összegzést is ad, amelyben kiírja a sikerességi arányt valamint a céltól mért oda-vissza terjedési idő átlagát.

A helyi loopback pingelése

A ping néhány speciális tesztelési és ellenőrzési célra is használható. Az egyik ilyen eset, amikor a helyi gép IPv4- vagy IPv6-konfigurációját ellenőrizzük. Ezt a helyi loopback cím pingelésével végezhetjük el, ami IPv4 esetén 127.0.0.1 (és ::1 IPv6-nál). Az ábrán egy IPv4 loopback tesztelése látható.

Ha választ kapunk a 127.0.0.1- ről (IPv4) vagy a ::1-ről (IPv6), akkor az állomáson megfelelően van telepítve az IP protokoll . A választ a hálózati réteg adja. Ez a válasz azonban nem azt jelenti, hogy a címek, maszkok vagy átjárók helyesen vannak beállítva. Az alsóbb rétegek állapotáról sem kapunk információt. Egyszerűen csak a hálózati rétegig teszteli az IP-t. Ha hibaüzenetet kapunk, az azt jelenti, hogy a TCP/IP nem megfelelően működik az állomáson.



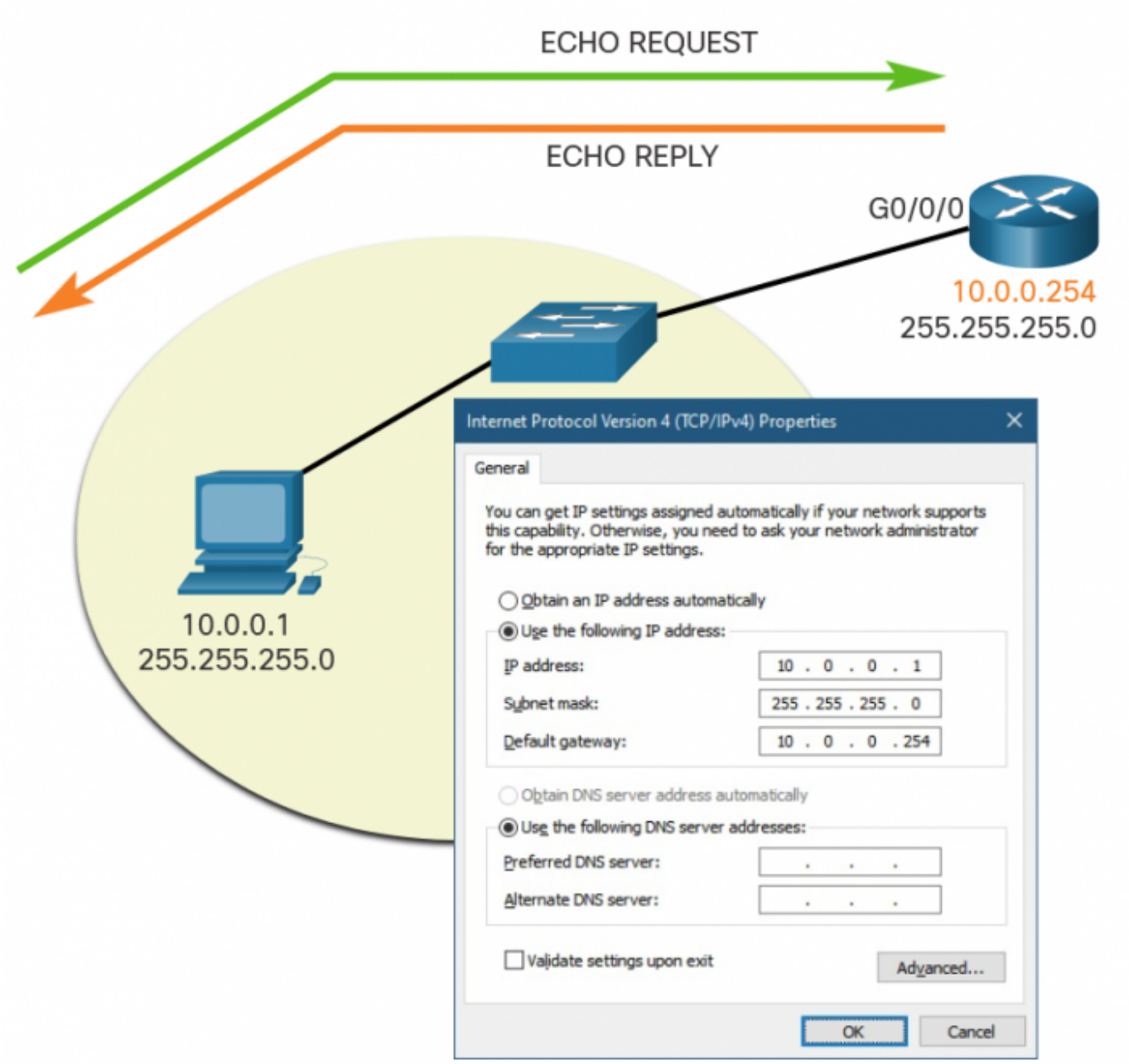
Ping - A helyi hálózattal való kapcsolat tesztelése

A ping az állomás helyi hálózattal való kommunikációjának ellenőrzésére is használható. Ezt legtöbbször úgy végezzük el, hogy megpingeljük az állomás átjárójának IP-címét. Az átjáró sikeres pingelése azt jelenti, hogy az állomás és a forgalomirányító átjáró funkciót betöltő hálózati interfésze egyaránt képes kommunikálni a helyi hálózaton.

Azért az átjáró címét használjuk leggyakrabban, mert a forgalomirányítónak normális esetben működnie kell. Ha az átjáró nem válaszol, megpróbálhatjuk egy másik, működőnek sejtett állomás IP-címét pingelni a helyi hálózaton belül.

Ha az átjáró, vagy egy másik állomás válaszol, biztosak lehetünk benne, hogy az állomásunk képes kommunikálni a helyi hálózaton. Ha az átjáró nem, de egy másik állomás válaszol, ez az átjáróként funkcionáló forgalomirányító problémáját jelezheti.

Az egyik lehetőség az, hogy az állomáson helytelen átjáró cím van beállítva. Egy másik lehetőség pedig, hogy a forgalomirányító interfész teljesen működőképes, viszont biztonsági szabályokat állítottak be rajta, amelyek megakadályozzák a ping kérések feldolgozását vagy megválaszolását.



Ping - Távoli eszközhöz vezető kapcsolat tesztelése

A ping arra is jó, hogy egy helyi állomás távoli hálózatok irányába történő kommunikációját teszteljük. A helyi állomás megpingel egy távoli hálózaton üzemelő IPv4 állomást, amint az ábrán is látható.

```
C:\> ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=125
Reply from 192.168.1.1: bytes=32 time<1ms TTL=125
Reply from 192.168.1.1: bytes=32 time<1ms TTL=125
Reply from 192.168.1.1: bytes=32 time<1ms TTL=125

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
R1# ping 12.0.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
```

Ha a ping sikeres, a köztes hálózat nagy részének működését igazoltuk. A sikeres ping megerősíti a helyi hálózat, az átjáróként használt forgalomirányító, minden egyéb köztünk levő forgalomirányító és a távoli állomás hálózatának működését.

Továbbá a távoli állomás működését is leellenőriztük. Ha a távoli gép nem tudna kommunikálni a saját hálózatán kívülre, válaszolni sem tudott volna.

Megjegyzés: Sok hálózati rendszergazda korlátozza vagy tiltja az ICMP üzenetek belépését a vállalat hálózatába, emiatt lehet, hogy a válasz a biztonsági korlátozások miatt nem érkezik meg.

Traceroute - Útvonal tesztelése

A ping két állomás közti kapcsolat tesztelésére való, de a köztes eszközökről semmilyen információval nem tud szolgálni. A traceroute (tracert) olyan segédprogram, amely listát ad az útvonal sikeres ugrásairól is. Ez a lista fontos ellenőrzési és hibakeresési információkat tartalmazhat. Ha az adat eléri a célját, a nyomkövetés felsorolja az állomások közti útvonalon érintett forgalomirányítókat. Ha az adat elakad valamelyik ugrásnál, az utolsóként választ adó forgalomirányító címe fontos információ lehet a probléma vagy biztonsági korlátozás helyére vonatkozóan.

Körülfordulási idő (Round Trip Time, RTT)

A traceroute megmutatja az útvonal minden ugrásának körülfordulási idejét és jelzi, ha valamelyik közbülső eszköz nem válaszol. A körülfordulási idő az az idő, ami alatt a csomag eléri a cél állomást, majd a válasz visszaér. Csillag (*) jelzi az elveszett, vagy megválaszolatlan csomagot.

Ezeket az információkat az útvonalon lévő problémás forgalomirányító megtalálásához használhatjuk. Ha a program kimenetében egy bizonyos ugrásnál magas válaszidőket vagy adatvesztést látunk, az annak a jele, hogy a forgalomirányító vagy a kapcsolatai leterheltek.

IPv4 élettartam (Time-to-Live, TTL) és IPv6 ugrás korlát (Hop Limit)

A traceroute az IPv4 TTL és az IPv6 ugrás korlát harmadik rétegbeli fejléc mezőjét használja az ICMP időtúllépés üzenetével együtt.

Az animáció lejátszásával megnézhetjük hogyan használja a traceroute TTL-t.

A traceroute által kiküldött első üzenetsorozat TTL értéke 1 lesz. Emiatt az első forgalomirányítónál a csomag TTL értéke lejár, időtúllépést eredményez. A forgalomirányító erre egy ICMPv4 üzenettel

válaszol. A traceroute ebből tudta meg az első ugrás címét.

A traceroute ezután fokozatosan növeli a TTL mező értékét (2, 3, 4…) üzenetsorozatonként. Így sorban megkapja az útvonal minden ugrását, ahogy a csomag egyre tovább jut az úton. A TTL mezőt addig növeli, amíg a célt vagy a meghatározott maximum értéket el nem éri.

Ha elértük a végső célt, az állomás az ICMP időtúllépés üzenet helyett ICMP port nem elérhető vagy ICMP visszhangkérés válasz üzenetet küld.

```
 C:\> tracert 11.1.0.1
The output from the command:


   Tracing route to 11.1.0.1 over a maximum of 30 hops
   ------------------------------------------------
   1      2 ms       3 ms       2 ms      157.54.48.1
   2     75 ms      83 ms      88 ms      11.1.0.67
   3     73 ms      79 ms      93 ms      11.1.0.1

   Trace complete.
```

```
R1# traceroute 172.16.0.2
Type escape sequence to abort.
Tracing the route to 172.16.0.2
1 10.0.0.1 0 msec 0 msec 0 msec
2 192.168.5.2 0 msec 0 msec 0 msec
3 172.16.0.2 0 msec 0 msec 0 msec
```