

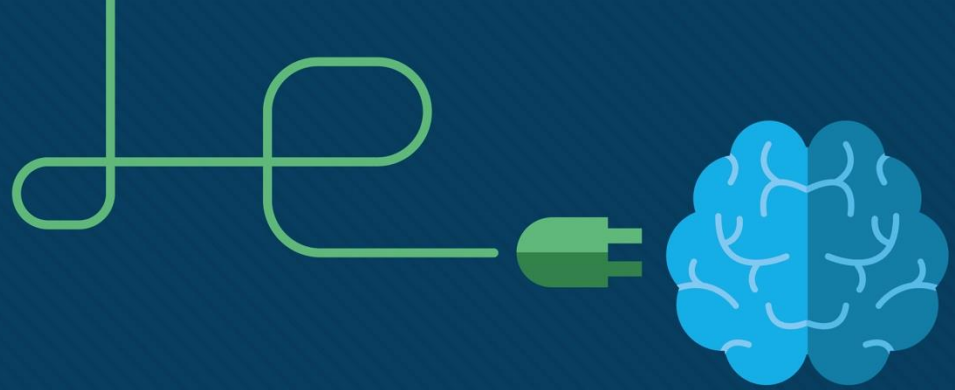


Modul 13: ICMP

Unterlagen für Instruktoren

Einführung in Netzwerke v7.0
(ITN)





Modul 13: ICMP

Einführung in Netzwerke v7.0
(ITN)



Modulziele

Modultitel: ICMP

Modulziel: Verwenden Sie verschiedene Tools, um die Netzwerkkonnektivität zu testen.

Thema	Ziel
ICMP-Nachrichten	Erläutern Sie, wie ICMP zum Testen der Netzwerkkonnektivität verwendet wird.
Ping und Traceroute Tests	Verwenden Sie Ping- und Traceroute-Dienstprogramme, um die Netzwerkkonnektivität zu testen.

13.1 ICMP-Nachrichten

ICMPv4- und ICMPv6-Nachrichten

- Internet Control Message Protocol (ICMP) gibt Rückmeldungen zu Problemen im Zusammenhang mit der Verarbeitung von IP-Paketen unter bestimmten Bedingungen.
- ICMPv4 ist das Nachrichtenprotokoll für IPv4. ICMPv6 ist das Messaging-Protokoll für IPv6 und enthält zusätzliche Funktionen.
- Die ICMP-Meldungen, die sowohl in ICMPv4 als auch ICMPv6 gemeinsam sind, umfassen:
 - Erreichbarkeit des Hosts
 - Ziel oder Dienst nicht erreichbar
 - Zeitüberschreitung

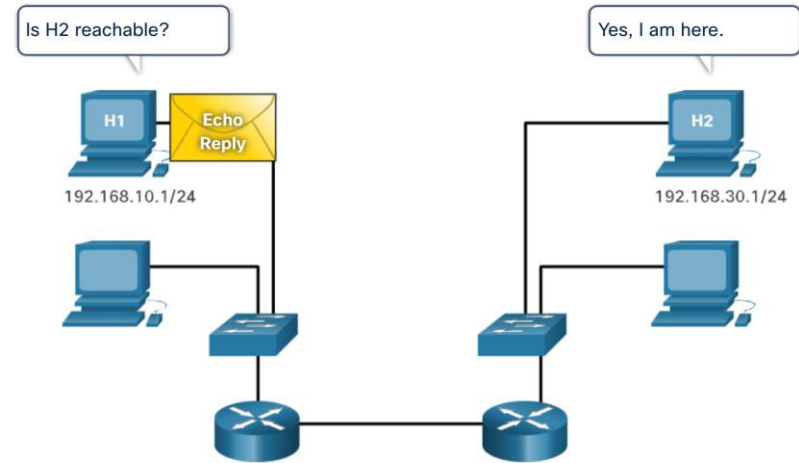
Hinweis: ICMPv4-Nachrichten sind nicht zwingend notwendig und werden oft aus Sicherheitsgründen in einem Netzwerk nicht zugelassen.

Host-Erreichbarkeit

ICMP Echo Nachricht kann verwendet werden, um die Erreichbarkeit eines Hosts in einem IP-Netzwerk zu testen.

Im Beispiel:

- Der lokale Rechner sendet eine ICMP-Echo-Anfrage an einen Host.
- Wenn der Host verfügbar ist, reagiert der Ziel-Host mit einer Echo-Antwort.



Destination or Service Unreachable

- Eine ICMP-Destination Unreachable Nachricht kann verwendet werden, um die Quelle zu benachrichtigen, dass ein Ziel oder Dienst nicht erreichbar ist.
- Die ICMP-Nachricht enthält einen Code, der angibt, warum das Paket nicht zugestellt werden konnte.

Einige Destination Unreachable Codes für ICMPv4 lauten wie folgt:

- 0 – Netzwerk nicht erreichbar
- 1 – Host nicht erreichbar
- 2 – Protokoll nicht erreichbar
- 3 – Port nicht erreichbar

Einige Destination Unreachable Codes für ICMPv6 lauten wie folgt:

- 0 - Keine Route zum Ziel
- 1 - Kommunikation mit dem Ziel ist administrativ verboten (z.B. Firewall)
- 2 — Über den Umfang der Quelladresse hinaus
- 3 - Adresse nicht erreichbar
- 4 – Port nicht erreichbar

Hinweis: ICMPv6 arbeitet mit ähnlichen, aber leicht unterschiedlichen Codes für Destination-Unreachable Nachrichten.

- ```
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-Nachrichten

ICMPv6 verfügt über neue Funktionen und verbesserte Funktionalität, die nicht in ICMPv4 gefunden werden, darunter sind vier neue Protokolle als Teil des Neighbor Discovery Protocol (ND oder NDP).

Benachrichtigungen zwischen einem IPv6-Router und einem IPv6-Gerät, einschließlich dynamischer Adresszuweisung, sind wie folgt:

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

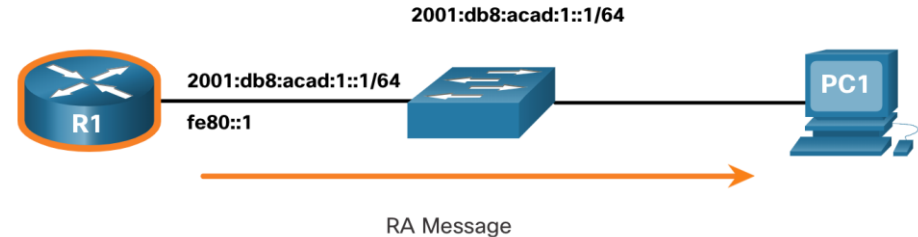
Benachrichtigungen zwischen IPv6-Geräten, einschließlich doppelter Adresserkennung und Adressauflösung sind wie folgt:

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

**Hinweis: ICMPv6 ND schließt auch die Umleitungsnachricht ein, die eine ähnliche Funktion wie die Umleitungsnachricht in ICMPv4 hat.**

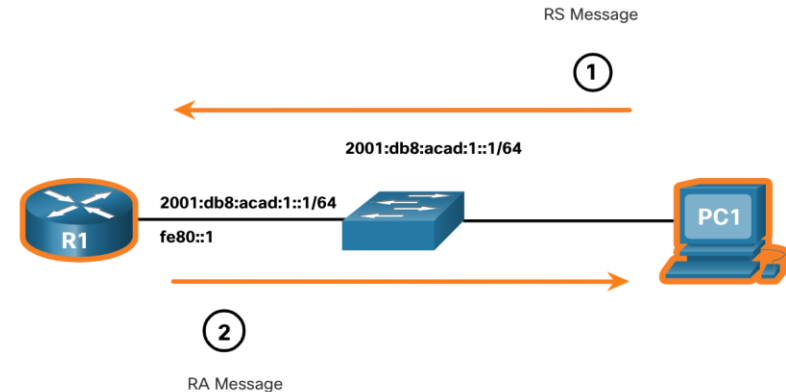
# ICMPv6-Nachrichten (Fortsetzung)

- RA-Nachrichten werden alle 200 Sekunden von IPv6-fähigen Routern gesendet, um Adressierungsinformationen an IPv6-fähige Hosts bereitzustellen.
- RA-Nachricht kann Adressierungsinformationen für den Host enthalten, z. B. das Präfix, die Präfixlänge, die DNS-Adresse und den Domännennamen.
- Ein Host, der SLAAC nutzt, legt für sein Standardgateway die Link-Local-Adresse des Routers fest, der die RA gesendet hat.



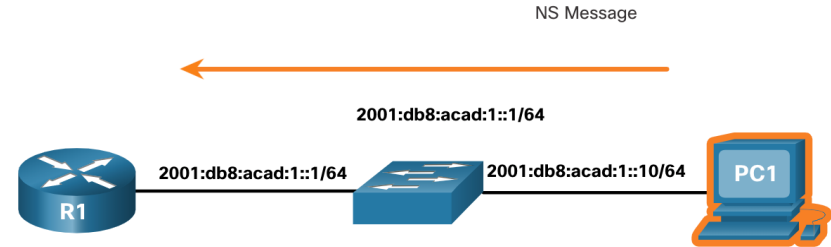
# ICMPv6-Nachrichten (Fortsetzung)

- Ein IPv6-fähiger Router sendet auch eine RA-Nachricht als Antwort auf eine RS-Nachricht.
- In der Abbildung sendet PC1 eine RS-Nachricht, um zu ermitteln, wie die IPv6-Adressinformationen dynamisch empfangen werden.
  - R1 antwortet mit einer RA-Nachricht an den RS.
  - PC1 sendet eine RS-Nachricht: „Hi, ich wurde gerade hochgefahren. Gibt es einen IPv6-Router im Netzwerk? Ich muss wissen, wie ich meine IPv6-Adressinformationen dynamisch erhalten kann.“
  - R1 antwortet mit einer RA-Nachricht. „Hallo an alle IPv6-fähigen Geräte. Ich bin R1 und Sie können SLAAC verwenden, um eine IPv6-globale Unicastadresse zu erstellen. Das Präfix ist 2001:db8:acad:1::/64. Übrigens verwenden Sie meine link-lokale Adresse fe80::1 als Standard-Gateway.“



# ICMPv6-Nachrichten (Fortsetzung)

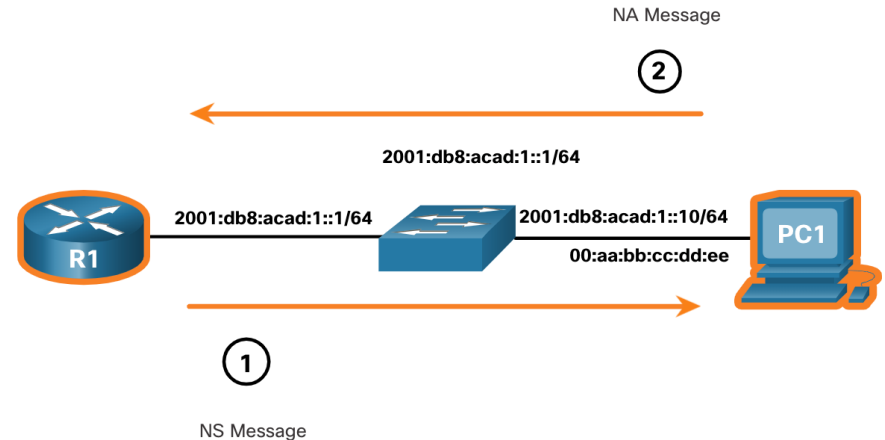
- Ein Gerät, dem eine globale IPv6-Unicast- oder Link-Local-Unicastadresse zugewiesen ist, kann Duplicate Address Detection (DAD) durchführen, um sicherzustellen, dass die IPv6-Adresse eindeutig ist.
- Um die Eindeutigkeit einer Adresse zu überprüfen, sendet das Gerät eine NS-Nachricht mit eigener IPv6-Adresse als Ziel-IPv6-Adresse.
- Wenn ein anderes Gerät im Netzwerk diese Adresse hat, antwortet es mit einer NA-Nachricht, die das sendende Gerät informiert, dass die Adresse verwendet wird.



**Hinweis: DAD ist nicht erforderlich, allerdings empfiehlt RFC 4861 die Durchführung von DAD für Unicast-Adressen.**

# ICMPv6-Nachrichten (Fortsetzung)

- Um die MAC-Adresse für das Ziel herauszufinden, sendet das Gerät eine NS-Nachricht an die Solicited-Node-Adresse.
- Die Nachricht enthält die bekannte (Ziel-) IPv6-Adresse. Das Gerät, das genau diese IPv6-Adresse hat, antwortet mit einer NA-Nachricht, die die Ethernet-MAC-Adresse des Geräts enthält.
- In der Abbildung sendet R1 eine NS-Nachricht an 2001:db8:acad:1::10 und fragt nach seiner MAC-Adresse.



# 13.2 Ping- und Traceroute-Tests

# Ping — Test Konnektivität

- Der Befehl **ping** ist ein IPv4- und IPv6-Testdienstprogramm, das ICMP-Echoanforderungs- und Echo-Antwortmeldungen zum Testen der Konnektivität zwischen Hosts verwendet und eine Zusammenfassung der Erfolgsquote und die durchschnittliche Round-Trip-Zeit zum Ziel enthält.
- Wenn innerhalb des Zeitlimits keine Antwort eingeht, gibt das Ping-Dienstprogramm eine Nachricht aus, dass keine Antwort empfangen wurde.
- Es ist üblich, dass der erste Ping einen Timeout hat, wenn die Adressauflösung (ARP oder ND) durchgeführt werden muss, bevor die ICMP-Echo-Anfrage gesendet wird.

```
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
```

```
R1#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:
```

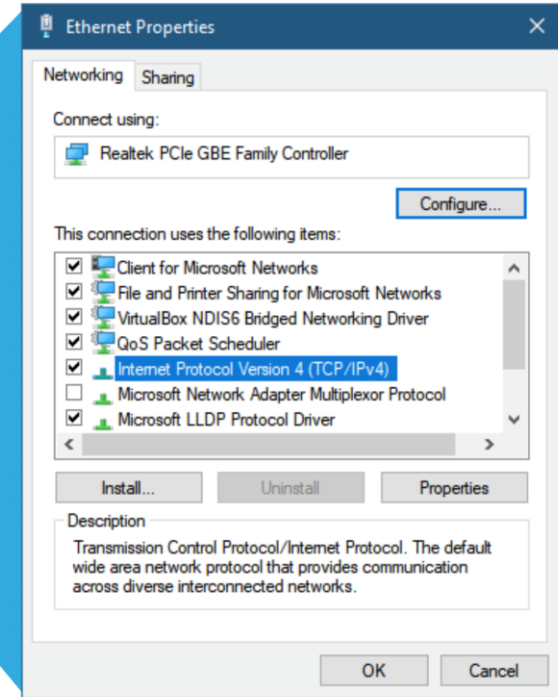
```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

# Ping an die Loopbackadresse

Ping kann verwendet werden, um die interne Konfiguration von IPv4 oder IPv6 auf dem lokalen Host zu testen. Um diesen Test durchzuführen, senden wir einen **ping** an die lokale Loopback-Adresse 127.0.0.1 für IPv4 (::1 für IPv6).

- Eine Antwort von 127.0.0.1 für IPv4 oder ::1 für IPv6 gibt an, dass das IP ordnungsgemäß auf dem Host installiert ist.
- Eine Fehlermeldung ist ein Hinweis darauf, dass TCP/IP auf dem Host nicht betriebsbereit ist.



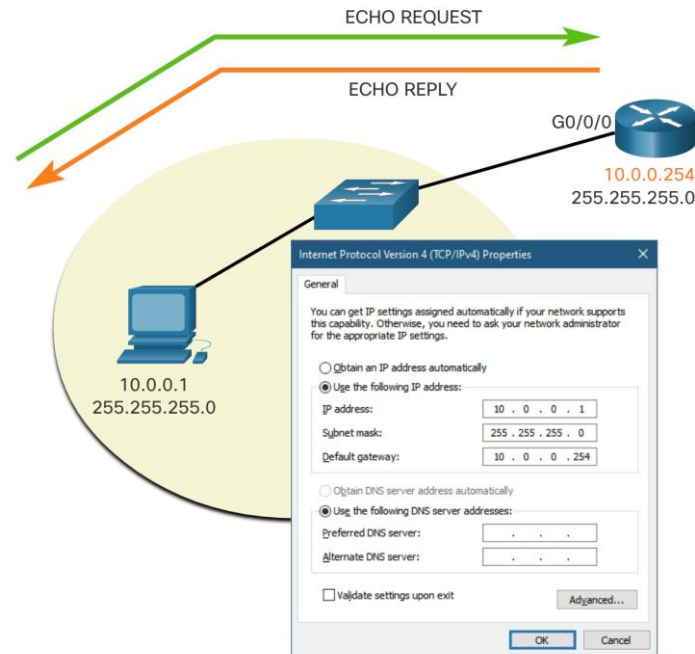


# Standard-Gateway-Ping

Sie können den **ping**-Befehl auch verwenden, um die Kommunikation eines Hosts auf dem lokalen Netzwerk zu testen.

Die Standard-Gateway-Adresse wird am häufigsten verwendet, da der Router normalerweise immer funktionsfähig ist.

- Ein erfolgreicher **ping** an das Standardgateway zeigt, dass die Host- und die Router-Schnittstelle, die als Standardgateway dient, im lokalen Netzwerk arbeiten.
- Wenn die Standardgateway-Adresse nicht reagiert, kann ein **ping** an die IP-Adresse eines anderen Hosts im lokalen Netzwerk gesendet werden, von dem bekannt ist, dass er aktiv ist.

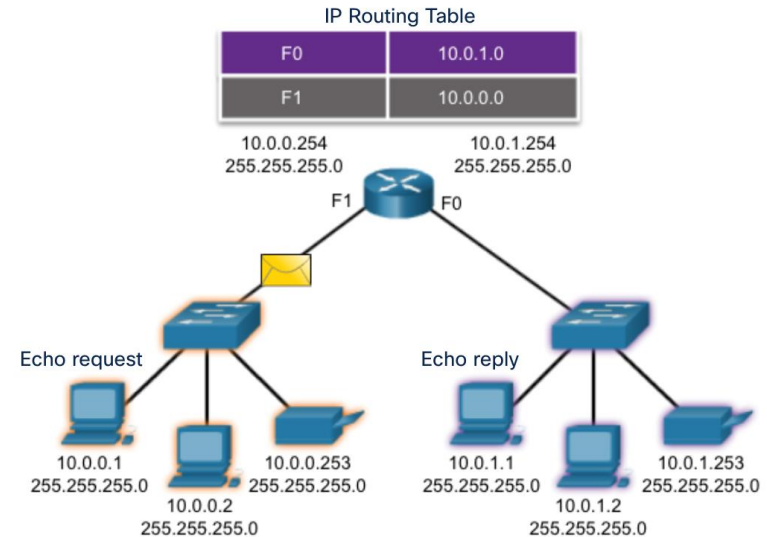


# Ping an einen Remote-Host

Ping kann auch verwendet werden, um die Kommunikation eines lokalen Hosts über ein Internetwork zu testen.

Ein lokaler Host kann einen Host in einem Remote-Netzwerk anpingen. Ein erfolgreicher **ping** über das Netzwerk bestätigt die Kommunikation im lokalen Netzwerk.

**Hinweis:** Viele Netzwerkadministratoren beschränken oder verbieten die Übertragung von ICMP-Nachrichten im Unternehmensnetzwerk; daher kann das Fehlen einer **ping** -Antwort auch durch Sicherheitsbeschränkungen verursacht werden.



# Traceroute — Testen Sie den Pfad

- Traceroute (**tracert**) ist ein Dienstprogramm, das verwendet wird, um den Weg zwischen zwei Hosts zu testen und eine Liste der Hops zu erstellen, die auf diesem Pfad erfolgreich erreicht wurden.
- Traceroute bietet eine Laufzeit für jeden Hop im Netzwerkpfad und gibt an, falls ein Hop nicht antwortet. Ein Sternchen (\*) wird verwendet, um eine verlorenes oder unbeantwortetes Paket zu kennzeichnen.
- Diese Informationen können verwendet werden, um einen problematischen Router im Pfad zu finden oder können darauf hinweisen, dass der Router so konfiguriert ist, dass er nicht antwortet.

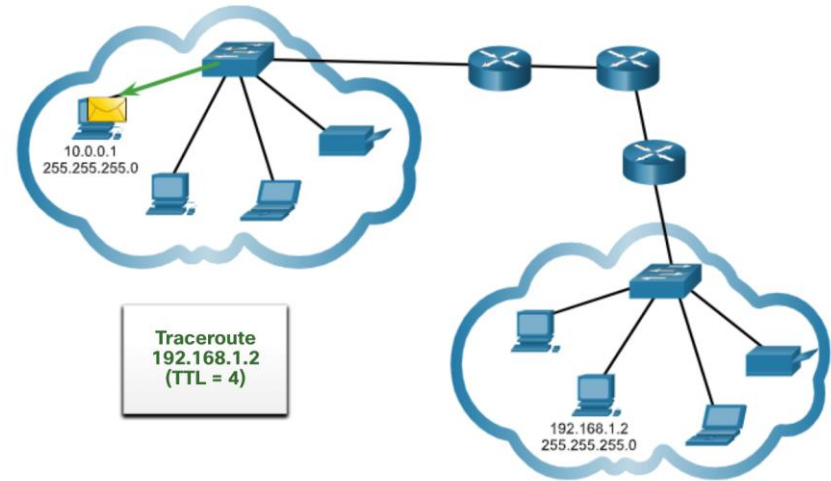
```
R1#traceroute 192.168.40.2
Type escape sequence to abort.
Tracing the route to 192.168.40.2

 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
```

**Hinweis:** Traceroute nutzt eine Funktion des IPv4-TTL-Felds und des IPv6-Hop-Limit-Felds im Layer 3-Header, zusammen mit der ICMP-Nachricht „Zeit überschritten“.

# Traceroute — Testen Sie den Pfad (Fortsetzung)

- Die erste Folge, die von Traceroute gesendet wird, hat den Wert 1 im TTL-Feld. Dies veranlasst TTL, das Senden am ersten Router abubrechen. Dieser Router antwortet dann mit einer ICMPv4-Zeitüberschreitungsnachricht.
- Traceroute erhöht dann schrittweise das TTL-Feld (2, 3, 4 ...) für jede weitere Nachricht. Auf diese Weise erhält Traceroute die Adresse aller weiteren Hops im weiteren Netzwerkpfad.
- Das TTL-Feld wird kontinuierlich erhöht, bis das Ziel erreicht ist. Es kann auch bis zu einem vorgegebenen Höchstwert schrittweise erhöht werden.



# Packet Tracer – Überprüfung der IPv4 und IPv6 Adressierung

In dieser Paket-Tracer-Übung werden Sie Folgendes tun:

- Vervollständigen der Adressierungstabelle
- Testen der Netzwerkverbindungen mit Ping
- Ermittlung des Pfads durch Verfolgung der Route

# Packet Tracer — Verwenden Sie Ping und Traceroute zum Testen der Netzwerkkonnektivität

In dieser Paket-Tracer-Übung werden Sie Folgendes tun:

- Testen und Wiederherstellen einer IPv4-Verbindung
- Testen und Wiederherstellen einer IPv6-Verbindung

# 13.3 Modul Praxis und Quiz

# Paket-Tracer — Verwenden Sie ICMP zum Testen und Korrigieren der Netzwerkkonnektivität

In dieser Paket-Tracer-Übung werden Sie Folgendes tun:

- Verwenden Sie ICMP, um Verbindungsprobleme zu finden.
- Konfigurieren Sie Netzwerkgeräte, um Verbindungsprobleme zu beheben.



# Testen der Netzwerkkonnektivität mithilfe von Ping und Traceroute

Mit dieser Übung können Sie die folgenden Lernziele erreichen:

- Einrichten und Konfigurieren des Netzwerks
- Teil 2: Verwenden des Befehls „ping“ für grundlegende Netzwerkprüfungen
- Verwenden der Befehle „tracert“ und „traceroute“ für grundlegende Netzwerkprüfungen
- Fehlersuche in der Topologie

# Was habe ich in diesem Modul gelernt?

- Zweck dieser Nachrichten ist es, Rückmeldungen über Probleme bei der Verarbeitung von IP-Paketen unter bestimmten Bedingungen zu liefern.
- Die ICMP-Meldungen, die sowohl ICMPv4 als auch ICMPv6 gemeinsam haben, sind Erreichbarkeit des Hosts, Zielort oder Dienst unerreichbar und Zeit überschritten.
- Die Nachrichten zwischen einem IPv6-Router und einem IPv6-Gerät einschließlich dynamischer Adresszuweisung beinhalten RS und RA. Die Meldungen zwischen IPv6-Geräten umfassen die Umleitung (ähnlich wie IPv4), NS und NA.
- Ping (von IPv4 und IPv6 verwendet) verwendet ICMP-Echoanforderungs- und Echo-Antwornachrichten, um die Konnektivität zwischen Hosts zu Überprüfen.
- Ping kann verwendet werden, um die interne Konfiguration von IPv4 oder IPv6 auf dem lokalen Host zu testen.
- Traceroute (tracert) erzeugt eine Liste der Hops, die auf dem Pfad erfolgreich erfasst wurden.

