ZSL
Zentrum für Schulqualität
und Lehrerbildung
Baden-Württemberg

cisco
Networking
Academy

ICMP

Andreas Grupp
Andreas.Grupp@zsl-rstue.de

Carina Haag
haag.c@lanz.schule

Tobias Heine
tobias.heine@springer-schule.de

Uwe Thiessat
uwe.thiessat@gbs-sha.de

Worum geht es in diesem Modul?

- Stellen sie sich vor sie hätten ein verzweigtes Modelleisenbahnnetz mit mehreren Bahnhöfen! Der einmal gestartete Zug kann stets gesehen werden und im Fall eines Stops mit einem Blick auf die Bahn geortet werden.
- Diesen direkten Überblick gibt es in einem Datennetzwerk nicht. Hierfür müssen, und können, gewisse Werkzeuge oder Protokolle verwendet werden:
- ICMPv4 für IPv4 und
- ICMPv6 für IPv6

ICMP – Lernziele - Inhaltsübersicht

- ICMP Messages kennenlernen

  ICMPv4 und -v6 Messages

  Host Reachability

  Destination or Service Unreachable

  Time Exceeded

  ICMPv6 Messages

- Ping(**p**acket **i**nter**n**et **g**roper) und Traceroute Tests

  Ping – Test Connectivity zu Loopback, Default Gateway und Remote Host

  Traceroute – Test the Path

  PT – Ipv4 und Ipv6 Adressierung überprüfen

  PT – mit Ping und Traceroute die Netzwerkverbindungen testen

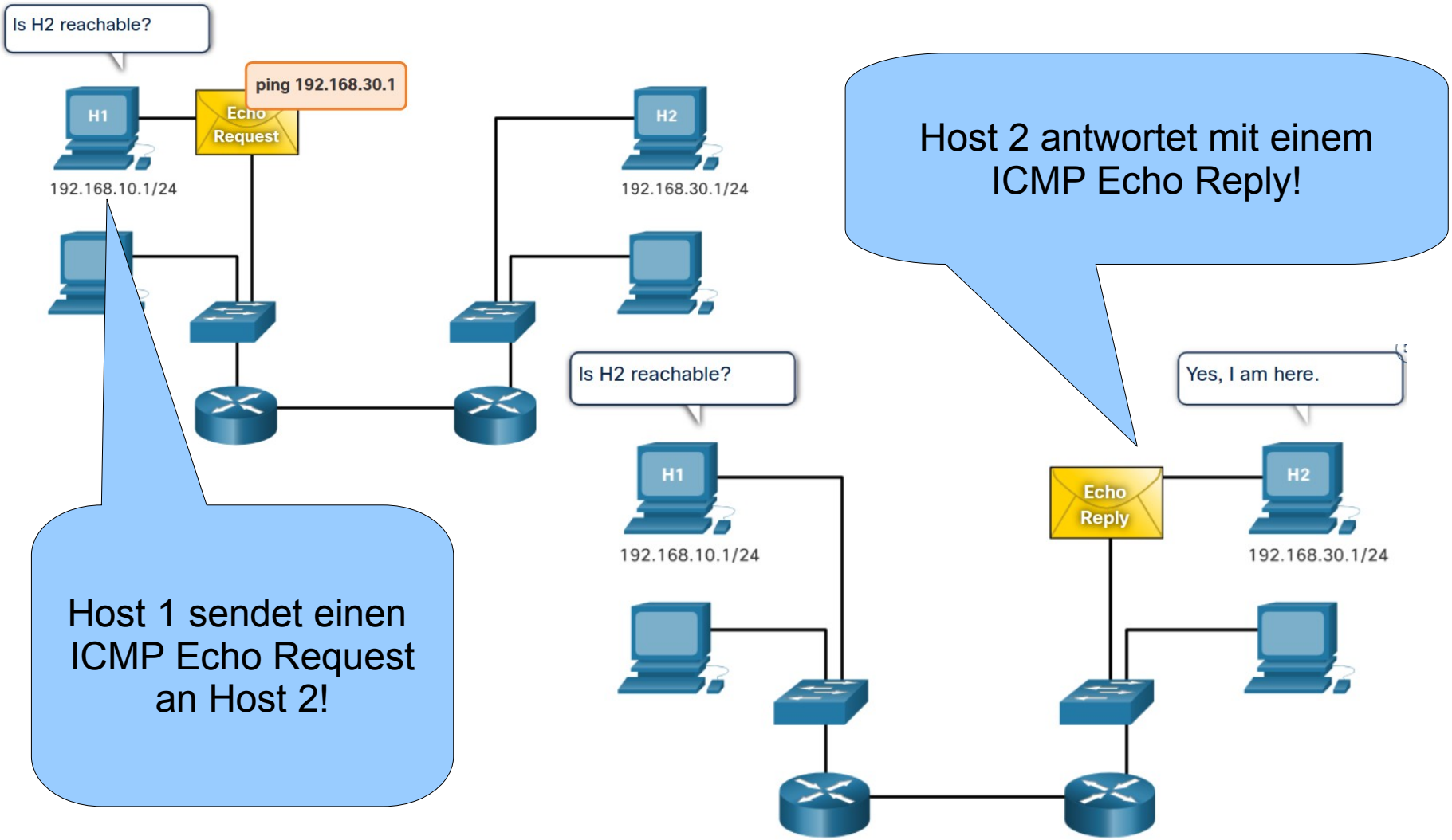
ICMPv4 und ICMPv6 Messages

Das Internet Control Message Protocol ist ein Service der TCP/IP suite um Fehlermeldungen und informelle Botschaften bei der Kommunikation mit anderen IP Geräten zu bieten.
Lediglich Rückmeldungen zu Fehlern bei der Ausführung von IP Paketen nicht aber Verlässlichkeit oder Fehlerkorrektur sind die Aufgabe dieser Messages.
Aus Sicherheitsgründen sind ICMP Messages oftmals verboten.

ICMP ist für beide Protokolle IPv4 und IPv6 verfügbar.
ICMPv4 für IPv4 und ICMPv6 für IPv6.
ICMPv6 unterstützt die selben Dienste wie ICMPv4, hat jedoch noch zusätzliche Funktionalitäten zu bieten.
In diesem Kurs bezieht sich der Begriff ICMP auf beide Versionen ICMPv4 und ICMPv6.
Beiden gemeinsam sind die in diesem Kurs besprochenen Messages:

- Host reachability
- Destination or Service Unreachable
- Time exceeded

Host Reachability - die grundlegende Ping-Funktion



Destination or Service Unreachable

Erhält ein Host oder Gateway ein IP-Paket, welches er nicht weiterleiten kann, dann kann er eine „ICMP Destination Unreachable“ Botschaft senden um der Paketquelle anzuzeigen, dass das Ziel oder der Service nicht erreichbar ist.
Diese Benachrichtigung enthält einen Code, warum das Paket nicht ausgeliefert werden konnte.

Einiger der Destination Unreachable Codes für ICMPv4 sind:

- 0 – Net unreachable
- 1 – Host unreachable
- 2 – Protocol unreachable
- 3 – Port unreachable

Achtung: ICMPv6 hat ähnliche, jedoch leicht unterschiedliche Codes

Einige der Destination Unreachable Codes für ICMPv6 sind:

- 0 – No route to destination
- 1 – Communication with destination ist administratively prohibited (Firewall etc.)
- 2 – Beyond scope of the source address
- 3 – Address unreachable
- 4 – Port unreachable

Time Exceeded

Erreicht ein Paket einen Router, so reduziert dieser den TTL – Wert um 1!

Eine ICMPv4 Time Exceeded Nachricht wird von Routern verwendet, um anzuzeigen, dass ein Paket nicht ausgeliefert werden kann, da das Time to Live (TTL) – Feld auf 0 gesetzt wurde.

Das Paket wird verworfen und eine Time Exceeded message wird an die Paketquelle gesendet.

Bei ICMPv6 wird ebenso verfahren. Anstatt eines TTL-Feldes wird bei IPv6 ein Hop Limit-Feld verwendet.

Hinweis: Time Exceeded messages werden vom tool **traceroute** verwendet!

ICMPv6 Messages

ICMPv6 bietet neue Möglichkeiten und Funktionalitäten welche in ICMPv4 nicht vorkommen. ICMPv6 messages sind in IPv6 verkapselt.
ICMPv6 beinhaltet vier neue Protokolle als Bestandteil des Neighbor Discovery Protocol (ND oder NDP).

Zwischen IPv6 Router und IPv6 Gerät werden folgende Protokolle verwendet:

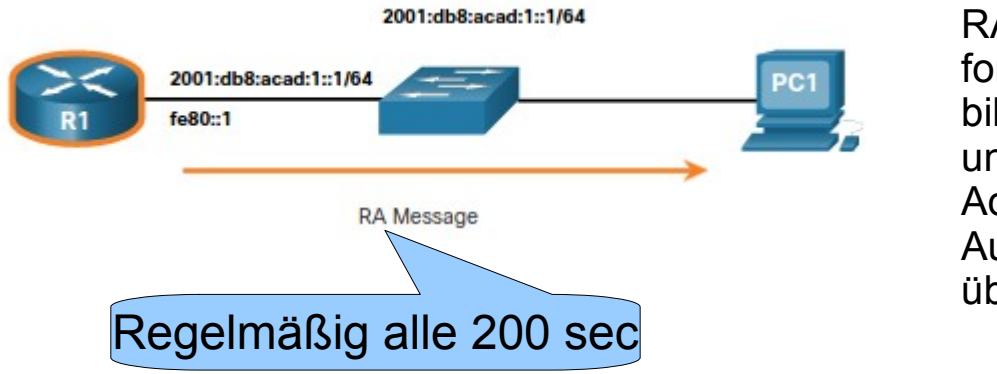
- Router Solicitation (RS) message
- Router Advertisement (RA) message

Zwischen zwei IPv6 Geräten werden folgende Protokolle verwendet:

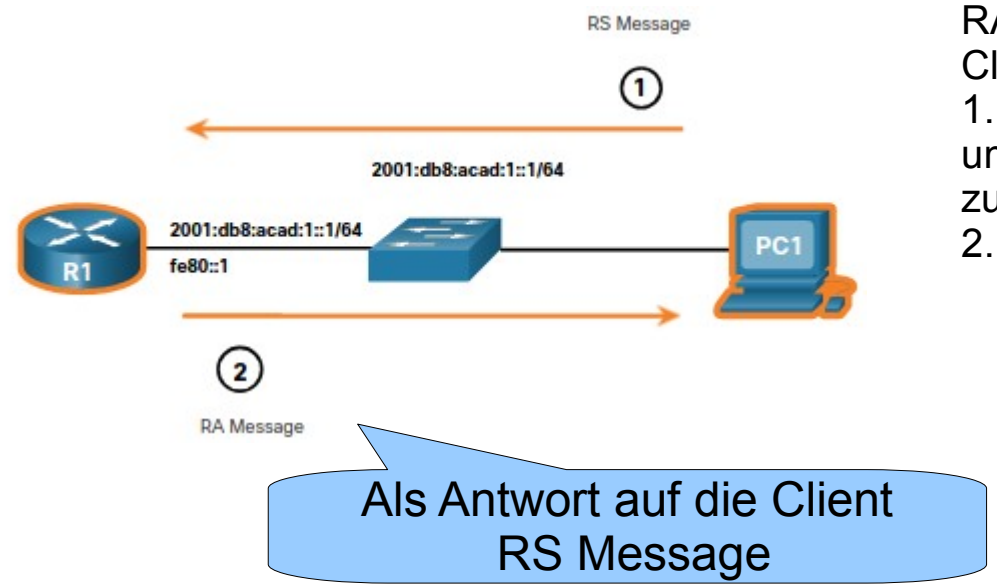
- Neighbor Solicitation (NS) message
- Neighbor Advertisement (NA) message

Hinweis: ICMPv6 ND beinhaltet ebenfalls die **redirect message** mit gleicher Funktion wie in ICMPv4.

Beispiele zu ICMPv6 Messages – Teil 1

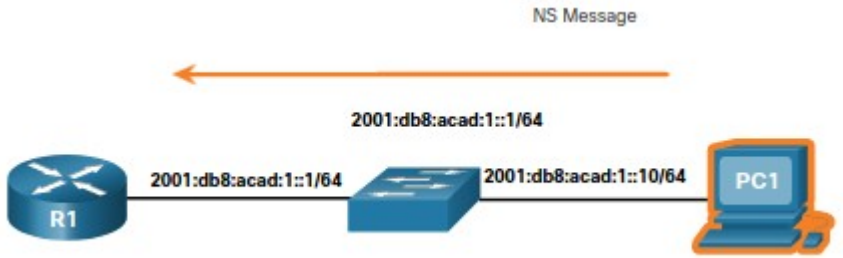


RA Message: „an alle IPv6 – Geräte: ich bin R1 und fordere euch auf mit SLAAC eine GU – Adresse zu bilden. Der Präfix hierfür ist 2001:db8:acad:1::/64 und euer Default Gateway soll meine Link Local Adresse FE80::1 sein.“
Auch DNS-Adresse und Domänenname können übermittelt werden.

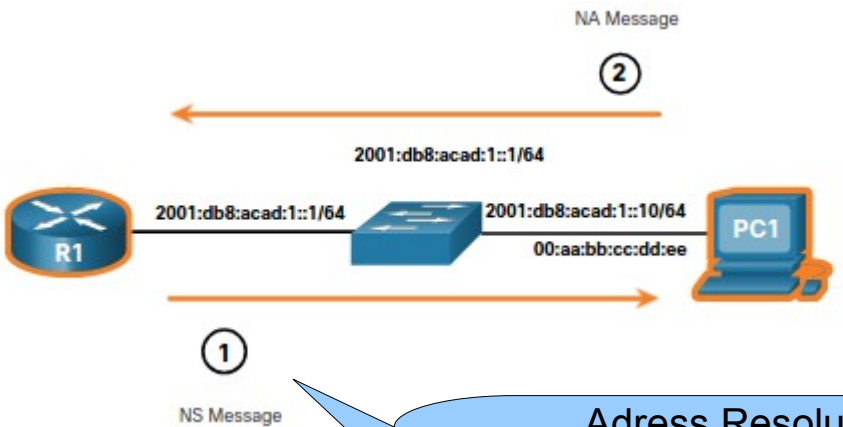


RA Message als Antwort auf eine RS Message des Clients.
1. Der Client, hier PC1, sendet die RS – Message, um einen IPv6 -Router zu ermitteln und um ein RA zu bitten.
2. Das Angebot, RA, ist identisch mit obigem RA.

Beispiele zu ICMPv6 Messages – Teil 2



PC1 sendet eine NS Message um die einzigartigkeit einer Adresse zu überprüfen:
„wer die IPv6 Adresse 2001:db8:acad:1::10 hat, sende mir seine MAC Adresse!“
→ DAD – die eigene IPv6 Adresse wird als Zieladresse in einer NS verschickt.



1. R1 sendet eine NS Message: „wer die IPv6 Adresse 2001:db8:acad:1::10 hat, sende mir seine MAC Adresse!“
2. PC1 antwortet mit einer NA Message: „ich habe die Adresse 2001:db8:acad:1::10 und meine MAC Adresse lautet 00:aa:bb:cc:dd:ee“

Adress Resolution,
um die MAC Adresse zu
einer bekannten IPv6 Adresse
zu erhalten. Vergleiche mit ARP

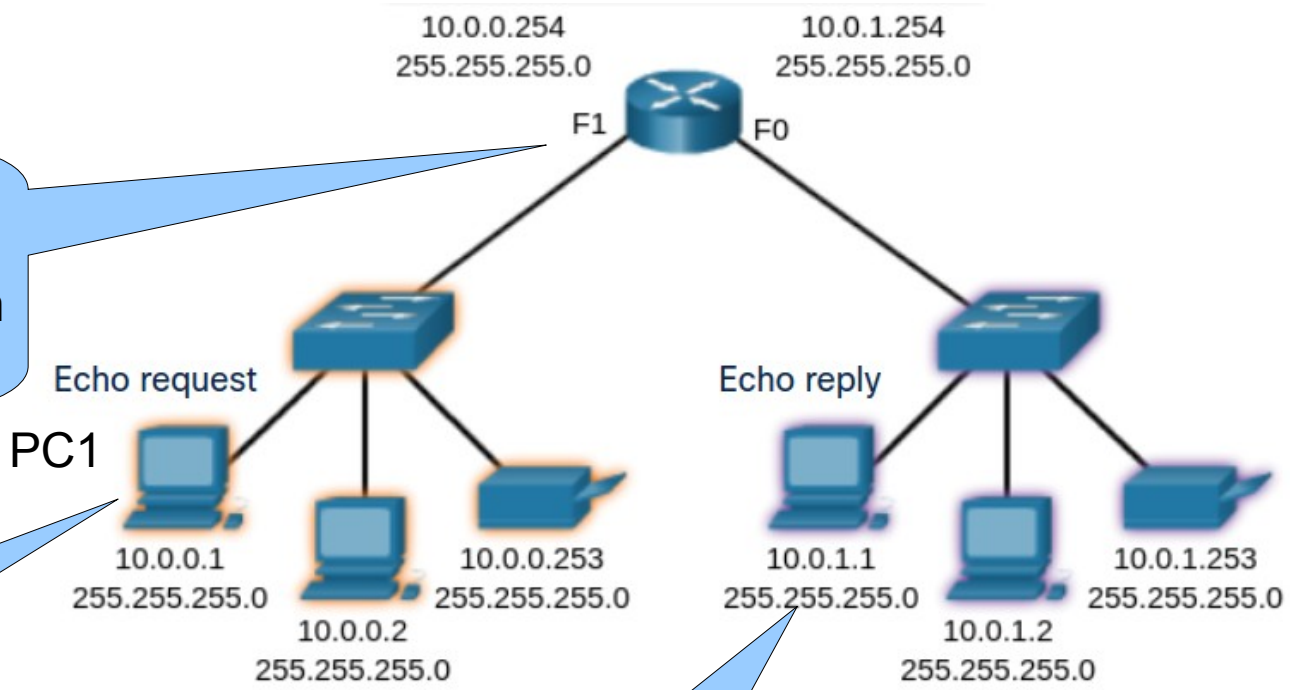
Ping in drei Bereichen

PC1>ping 10.0.0.254

Das Default Gateway von PC1 (Anfrage bleibt im eigenen Teilnetz)

PC1>ping 127.0.0.1
(::1 für IPv6)

Der TCP/IP Stack von PC1 wird so überprüft. (Anfrage Bleibt im eigenen Host)

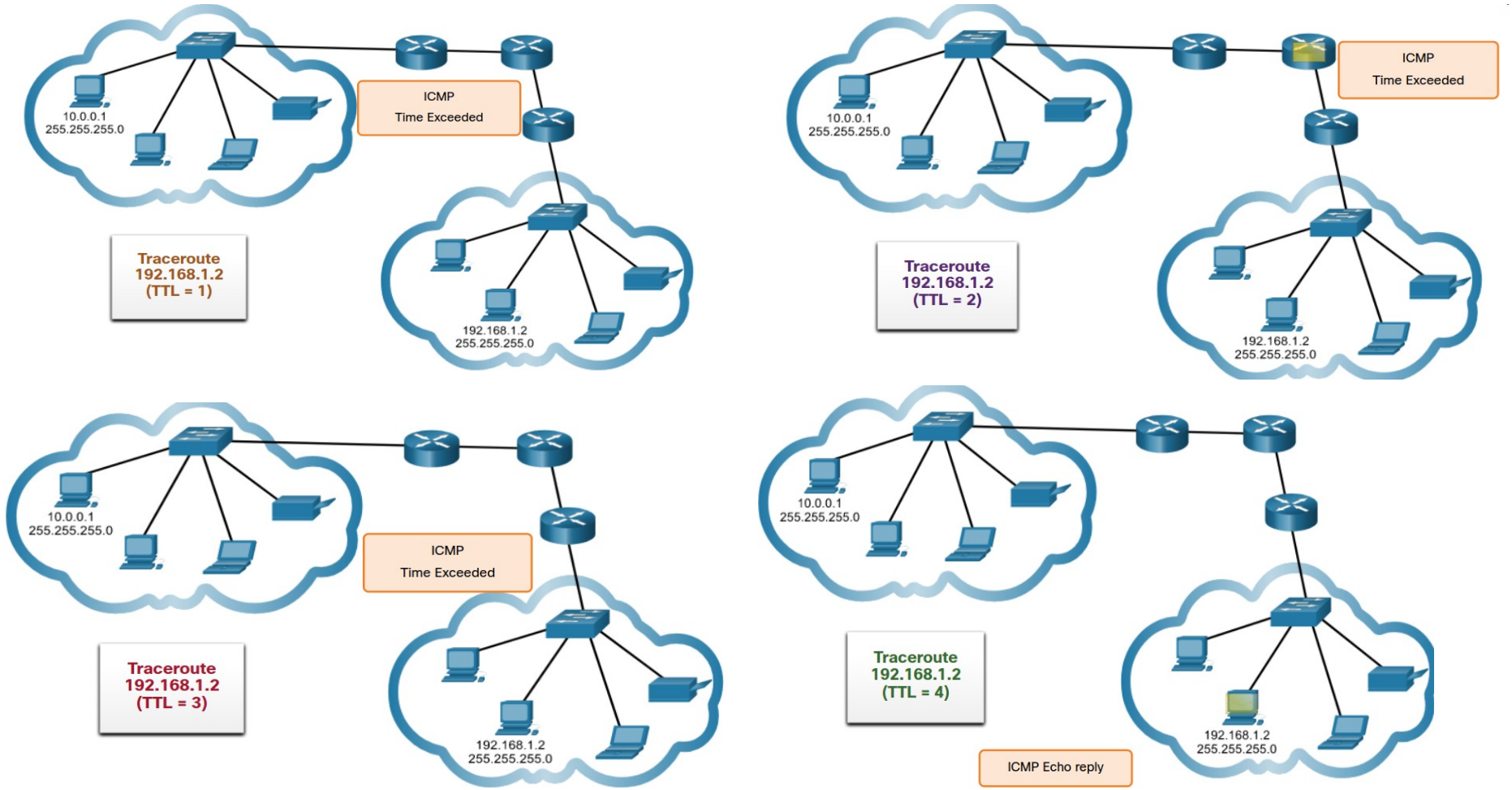


PC1>ping 10.0.1.1

Der entfernte Host wird angepingt. (Anfrage gelangt in ein Anderes Teilnetz)

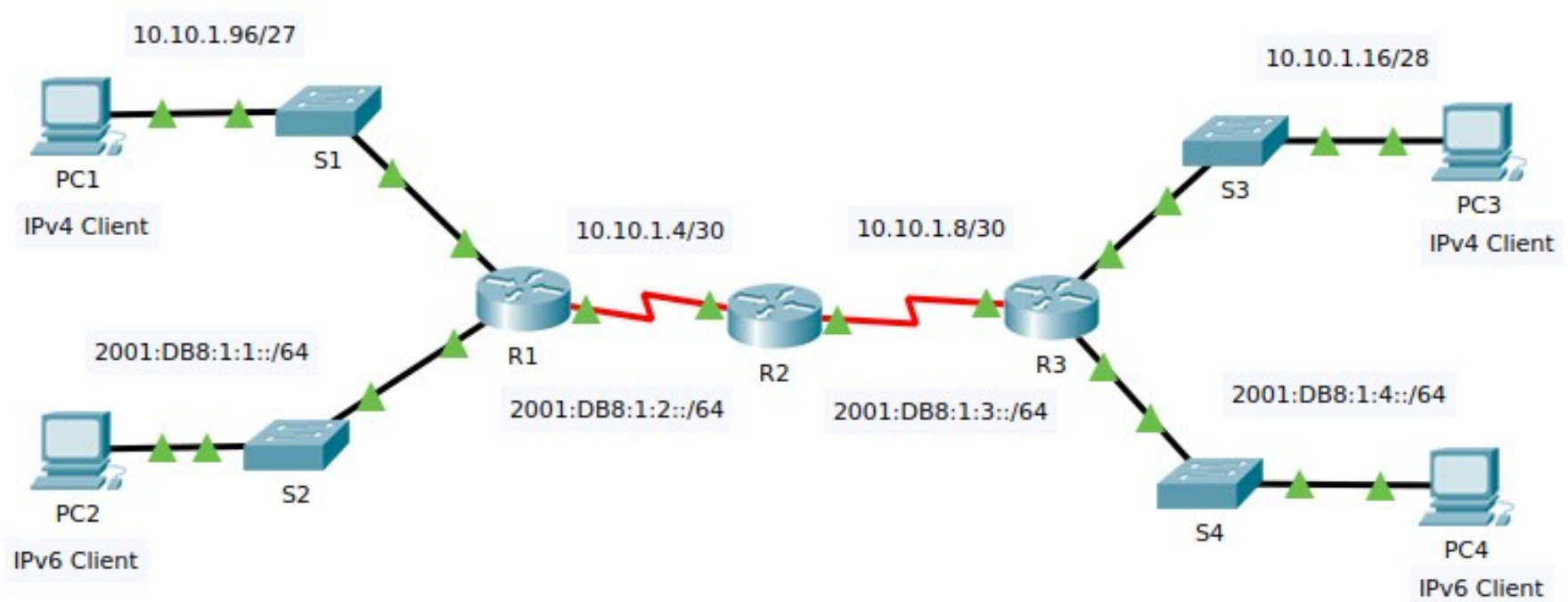
Traceroute – den Pfad zum Ziel ermitteln!

TTL bzw. Hop Limit werden beginnend mit 1 nacheinander um eins erhöht, solange bis das Ziel erreicht wurde.



Praxistips zu 13.2.7 – Ping und Traceroute zur Fehlersuche!

Diese Übung zeigt die Vorteile einer gezielten, planmäßigen Fehlersuche mit ping und traceroute. Bei noch größeren Netzen, (z.B. 10 und mehr Router), ist es notwendig, sehr strukturiert vorzugehen.
In kleinen Netzen können noch alle Konfigurationsdaten überblickt werden.



Modulabschluß

- PT – 13.2.6 Verify IPv4 and IPv6 Addressing
- PT – 13.2.7 Use Ping and Traceroute to Test Network Connectivity
- PT – 13.3.1 Use ICMP to Test and Correct Network Connectivity
- Lab – 13.3.2 Use Ping and Traceroute to Test Network Connectivity
- Modulquiz – 13.3.4

Fragen?