



Modul 9: Adressauflösung

Unterlagen für Instruktoren

Einführung in Netzwerke v7.0
(ITN)



Was erwartet Sie in diesem Modul

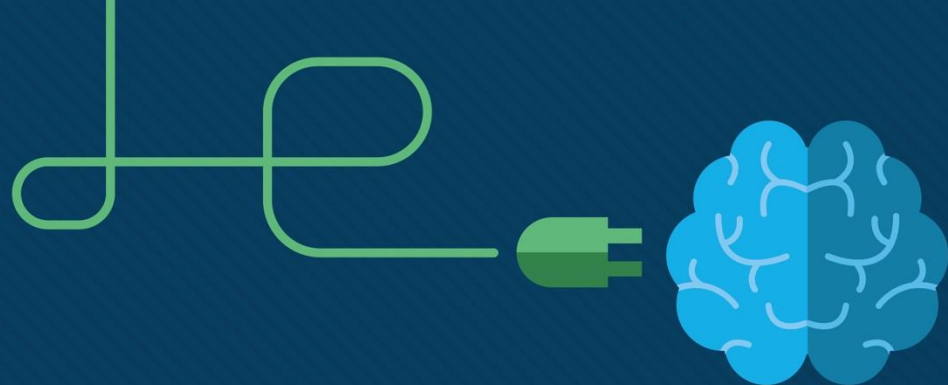
- Um das Lernen zu vereinfachen, sind folgende Funktionen der grafischen Bedienoberfläche in diesem Modul enthalten:

Funktion	Beschreibung
Animationen	Den Lernenden mit neuen Fertigkeiten und Konzepten in Kontakt zu bringen
Videos	Den Lernenden mit neuen Fertigkeiten und Konzepten in Kontakt zu bringen
Prüfen Sie Ihr Wissen	Mit Hilfe der interaktiven Quizzes beurteilen die Lernenden Ihr Wissen zu dem Thema.
Interaktive Aktivitäten	Die Vielfalt an Formaten hilft den Lernenden, ihr Wissen einzuschätzen.
Syntaxprüfer	Über kleinere Simulation wird die Konfiguration über Cisco command line Interface (CLI) erlernt.
Packet-Tracer (PT) Aktivitäten	Durch Simulations- und Entwurfsaufgaben entdecken und erwerben Sie neue Fähigkeiten, bereits erlernte werden gefestigt und erweitert.

Was erwartet Sie in diesem Modul (Inhalt)

- Um das Lernen zu vereinfachen sind folgende Funktionen der grafischen Bedienoberfläche in diesem Modul enthalten:

Funktion	Beschreibung
Praxisorientierte Übungen	Laborübungen sind für das Arbeiten an den Geräten vorgesehen.
Gruppenaktivitäten	Sie finden diese auf den Seiten mit den Hilfsmitteln für Instruktoren. Gruppenaktivitäten sollen das Lernen vereinfachen, Diskussionen fördern und Zusammenarbeit unterstützen.
Modulquizze	Selbstüberprüfung der erlernten Begrifflichkeiten und Fertigkeiten, die während der vielfachen Themen innerhalb des Moduls vorgestellt wurden.
Modulzusammenfassung	Kurze Wiederholung des Modulinhalts



Modul 9: Adressauflösung

Einführung in Netzwerke v7.0
(ITN)



Modulziele

Modultitel: Adressauflösung

Modulziel: Erläutern, wie ARP und ND die Kommunikation in einem Netzwerk ermöglichen.

Thema	Ziel
MAC und IP	Vergleichen der Rollen von MAC- und IP-Adresse.
ARP	Den Zweck von ARP beschreiben.
Neighbor Discovery	Beschreiben der Arbeitsweise von IPv6 Neighbor Discovery.

9.1 MAC und IP

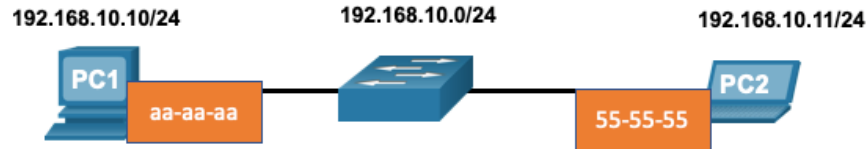
MAC und IP

Ziel im selben Netzwerk

Es gibt zwei elementare Adressen, die einem Gerät in einem Ethernet-LAN zugewiesen werden:

- **Schicht 2 Physische Adresse (die MAC-Adresse)** – Wird für die Kommunikation zwischen Netzkarten im selben Ethernet-Netzwerk verwendet.
- **Schicht 3 Logische Adresse (die IP-Adresse)** – Wird verwendet, um das Paket von Quellgerät zu Zielgerät zu senden.

Schicht-2-Adressen werden verwendet, um Frames von einer Netzwerkkarte an eine andere Netzwerkkarte im selben Netzwerk zu übertragen. Befindet sich die Ziel-IP-Adresse im selben Netzwerk, ist die Ziel-MAC-Adresse die MAC-Adresse des Zielgeräts.



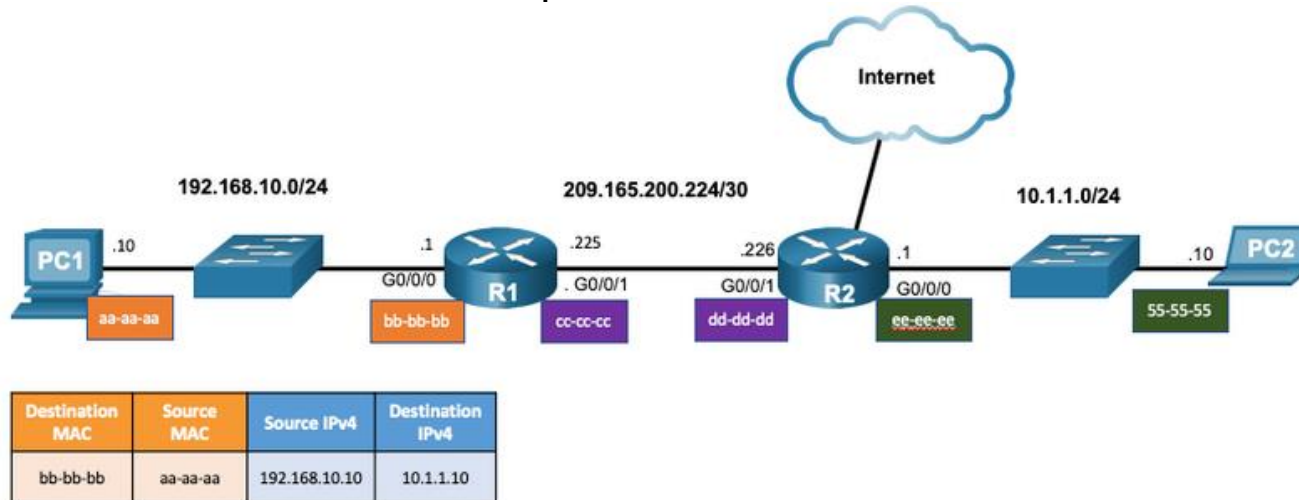
Destination MAC	Source MAC	Source IPv4	Destination IPv4
55-55-55	aa-aa-aa	192.168.10.10	192.168.10.11

MAC und IP

Ziel im Remote-Netzwerk

Wenn sich die Ziel-IP-Adresse in einem Remote-Netzwerk befindet, ist die Ziel-MAC-Adresse die MAC-Adresse des Standardgateways.

- ARP wird von IPv4 verwendet, um die IPv4-Adresse eines Geräts mit der MAC-Adresse der Geräte-NIC zu verknüpfen.
- ICMPv6 wird von IPv6 verwendet, um die IPv6-Adresse eines Geräts mit der MAC-Adresse der Geräte-NIC zu verknüpfen.



Packet Tracer – Identifizieren von MAC- und IP-Adressen

Mit diesem Packet Tracer schließen Sie die folgenden Ziele ab:

- Sammeln von PDU-Informationen für die lokale Netzwerkkommunikation
- Sammeln von PDU-Informationen für die Remote-Netzwerkkommunikation

9.2 ARP

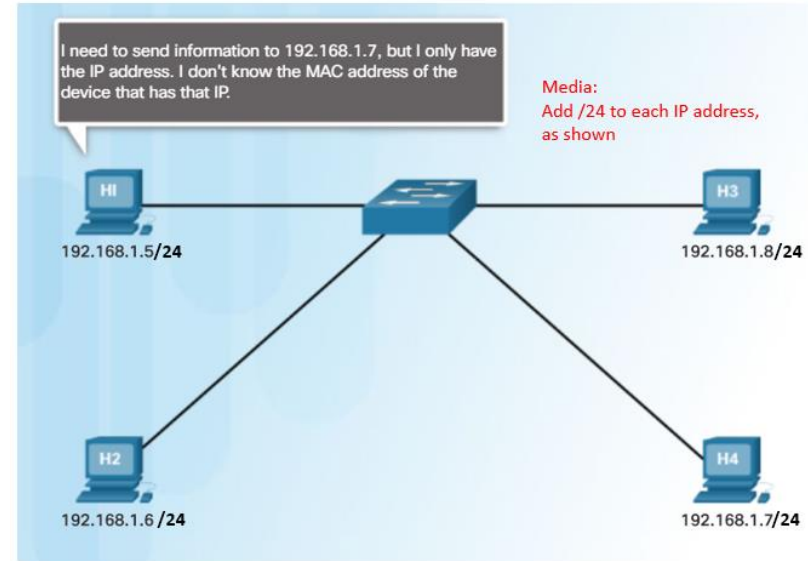
ARP

ARP Übersicht

Ein Gerät verwendet ARP, um die Ziel-MAC-Adresse eines lokalen Geräts zu ermitteln, wenn es seine IPv4-Adresse kennt.

ARP bietet zwei grundlegende Funktionen:

- Auflösung von IPv4-Adressen in MAC-Adressen
- Verwalten einer ARP-Tabelle von IPv4-zu-MAC-Adresszuordnungen



ARP

ARP Funktionsweise

Um einen Frame zu senden, sucht ein Gerät in seiner ARP-Tabelle nach der Ziel-IPv4-Adresse und der zugeordneten MAC-Adresse.

- Wenn sich die Ziel-IPv4-Adresse des Pakets im selben Netzwerk befindet, durchsucht das Gerät die ARP-Tabelle nach der Ziel-IPv4-Adresse.
- Befindet sich die Ziel-IPv4-Adresse des Pakets in einem anderen Netzwerk als die Quell-IPv4-Adresse, durchsucht das Gerät die ARP-Tabelle nach der IPv4-Adresse des Standardgateways.
- Wenn das Gerät die IPv4-Adresse sucht, wird die entsprechende MAC-Adresse als Ziel-MAC-Adresse im Frame verwendet.
- Wird kein Eintrag gefunden, sendet das Gerät einen ARP-Request.

ARP Video - ARP-Request

Dieses Video zeigt einen ARP-Request für eine MAC-Adresse.

ARP Video – ARP-Reply

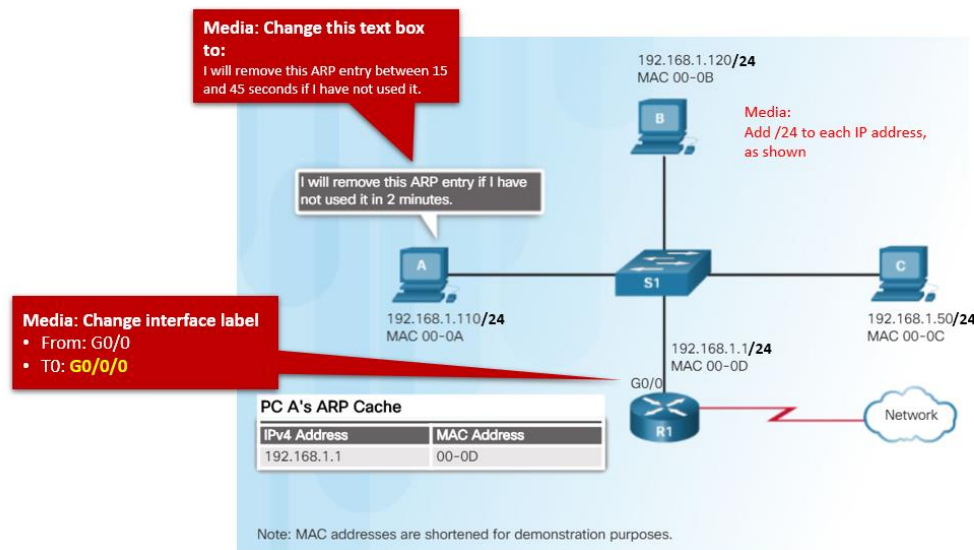
Dieses Video zeigt einen ARP-Reply als Antwort auf einen ARP-Request.

ARP Video – Welche Rolle spielt ARP bei Remote-Kommunikationen

Dieses Video erklärt, wie ein ARP-Request einem Host die MAC-Adresse des Standard-Gateways liefert.

Entfernen von Einträgen aus einer ARP-Tabelle

- Einträge in der ARP-Tabelle sind dort nicht dauerhaft gespeichert. Sie werden wieder entfernt, wenn der ARP-Cache-Timer nach einem bestimmten Zeitraum abgelaufen ist.
- Die Zeitspanne unterscheidet sich je nach Betriebssystem des Geräts.
- ARP-Tabelleneinträge können auch manuell vom Administrator entfernt werden.



ARP

ARP-Tabellen auf Netzwerkgeräten

- Der Befehl **show ip arp** zeigt die ARP-Tabelle auf einem Cisco-Router an.
- Der Befehl **arp -a** zeigt die ARP-Tabelle auf einem Windows 10 PC an.

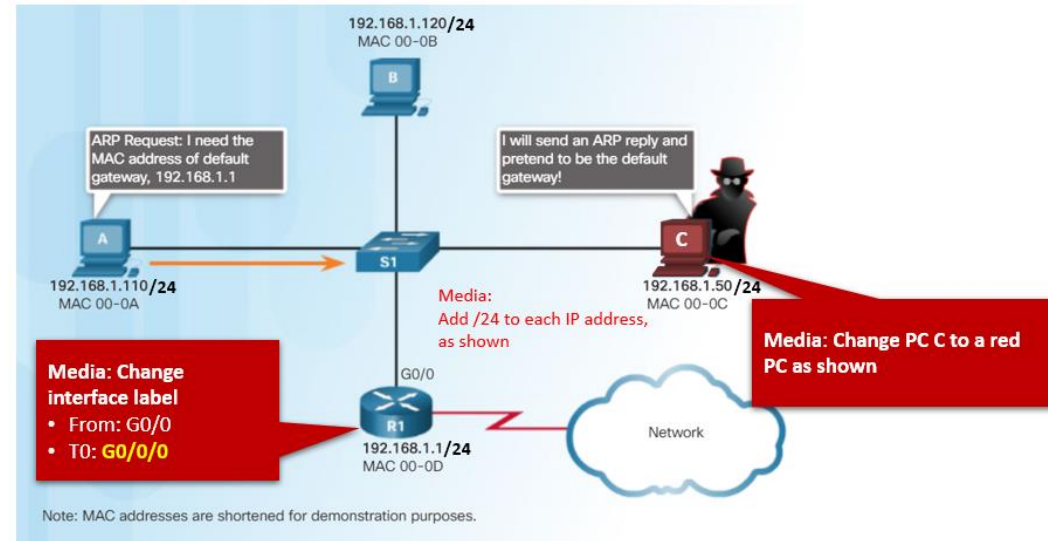
```
R1# show ip arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 192.168.10.1 - a0e0.af0d.e140 ARPA GigabitEthernet0/0/0
```

```
C:\Users\PC> arp -a

Interface: 192.168.1.124 --- 0x10
    Internet Address Physical Address Type
    192.168.1.1 c8-d7-19-cc-a0-86 dynamic
    192.168.1.101 08-3e-0c-f5-f7-77 dynamic
```

ARP Probleme — ARP-Broadcasting und ARP-Spoofing

- Ein ARP-Request wird von jedem Gerät im lokalen Netzwerk empfangen und verarbeitet.
- Übermäßig viele ARP-Requests können zu einer gewissen Leistungsminderung im Netzwerk führen.
- ARP-Replies können von einem Angreifer gefälscht werden, um einen ARP-Poisoning-Angriff durchzuführen.
- Unternehmensswitches verfügen über Techniken zur Abschwächung und Schutz vor ARP-Angriffen.



Packet-Tracer - Untersuchen der ARP-Tabelle

Mit diesem Packet Tracer schließen Sie die folgenden Ziele ab:

- Untersuchen einer ARP-Anfrage
- Untersuchen der MAC-Adresstabelle eines Switches
- Untersuchen des ARP-Prozesses bei Remote-Kommunikationen

9.3 Kupferverkabelung

IPv6 Neighbor Discovery

Video — IPv6-Neighbor Discovery

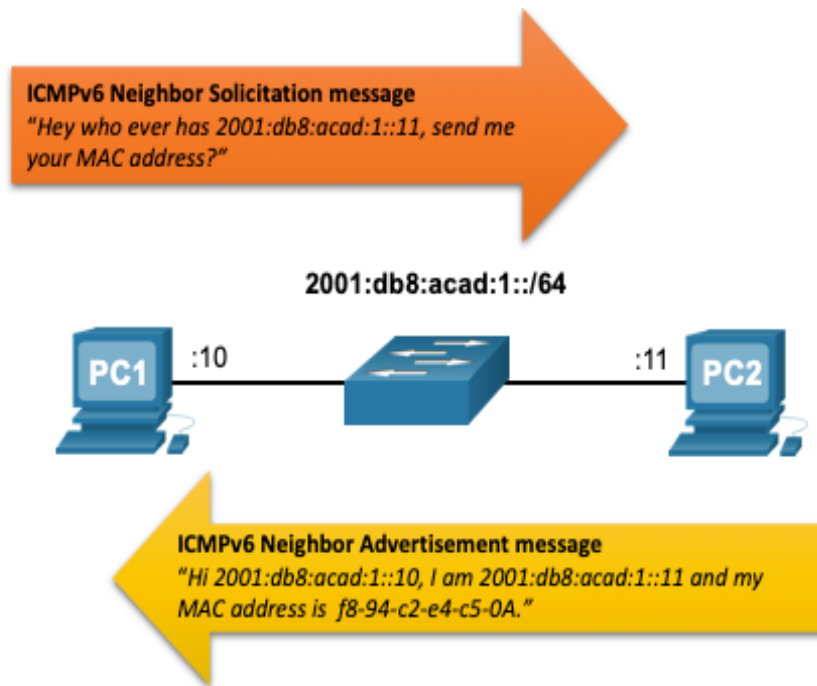
In diesem Video wird erläutert, wie IPv6 die Adressauflösung mittels ICMPv6-Neighbor-Solicitation- sowie Neighbor-Advertisement-Messages vornimmt.

IPv6-Neighbor-Discovery-Nachrichten

Das IPv6-Neighbor Discovery (ND) -Protokoll bietet:

- Adressauflösung
- IPv6-Routererkennung
- Umleitungsdienste
- ICMPv6 Neighbor Solicitation (NS) und Neighbor Advertisement (NA) - Nachrichten werden beim Nachrichtenaustausch zwischen IPv6-Geräten verwendet, wie z. B. für die Adressauflösung.
- ICMPv6 Router Solicitation- (RS) und Router Advertisement (RA)- Nachrichten werden beim Nachrichtenaustausch zwischen IPv6-Geräten und Routern verwendet.
- ICMPv6-Redirect-Nachrichten werden von Routern für die Auswahl eines besseren Next-Hops verwendet.

IPv6 Neighbor Discovery — Adressauflösung



- IPv6-Geräte verwenden ND, um die MAC-Adresse einer bekannten IPv6-Adresse aufzulösen.
- ICMPv6-Neighbor Solicitation-Nachrichten werden an spezielle Ethernet- und IPv6-Multicastadressen gesendet.

IPv6-Neighbor Discovery

Packet Tracer — IPv6-Neighbor Discovery

In dieser Packet Tracer Übung sind die folgenden Lernziele enthalten:

- Teil 1: IPv6 Neighbor Discovery lokales Netzwerk
- Teil 2: IPv6 Neighbor Discovery Remote-Netzwerk

9.4 Modul Praxis und Quiz

Was habe ich in diesem Modul gelernt?

- Die physischen Adressen auf Schicht 2 (Ethernet-MAC-Adressen) werden verwendet, um den Frame der Sicherungsschicht mit dem eingekapselten IP-Paket von einer Netzwerkkarte an eine andere Netzwerkkarte im selben Netzwerk zu übertragen.
- Wenn sich die Ziel-IP-Adresse im selben Netzwerk befindet, ist die Ziel-MAC-Adresse die MAC-Adresse des Zielgeräts.
- Wenn sich die Ziel-IP-Adresse (IPv4 oder IPv6) in einem Remote-Netzwerk befindet, ist die Ziel-MAC-Adresse die MAC-Adresse des Standardgateways des Hosts, also die MAC-Adresse der Router-Netzwerkkarte.
- Ein IPv4-Gerät verwendet ARP, um die Ziel-MAC-Adresse eines lokalen Geräts zu ermitteln, wenn es seine IPv4-Adresse kennt.
- ARP bietet zwei grundlegende Funktionen: das Auflösen von IPv4-Adressen in MAC-Adressen und das Verwalten einer Tabelle mit IPv4-zu-MAC-Adresszuordnungen.
- Sobald die ARP-Antwort empfangen wird, fügt das Gerät die IPv4-Adresse und die verknüpfte MAC-Adresse zur ARP-Tabelle hinzu.
- Ein ARP-Cache-Zeitgeber entfernt ARP-Einträge, die über eine bestimmte Zeit nicht mehr verwendet wurden.
- IPv6 verwendet kein ARP. Stattdessen wird das ND-Protokoll verwendet, um MAC-Adressen aufzulösen.
- Ein IPv6-Gerät verwendet ICMPv6 Neighbor Discovery, um die Ziel-MAC-Adresse eines lokalen Geräts zu ermitteln, wenn es seine IPv6-Adresse kennt.

