ARP

ADDRESS RESOLUTION PROTOCOL

Thomas Schön
Albert-Ludwigs-Universität Freiburg

Address Resolution Protocol

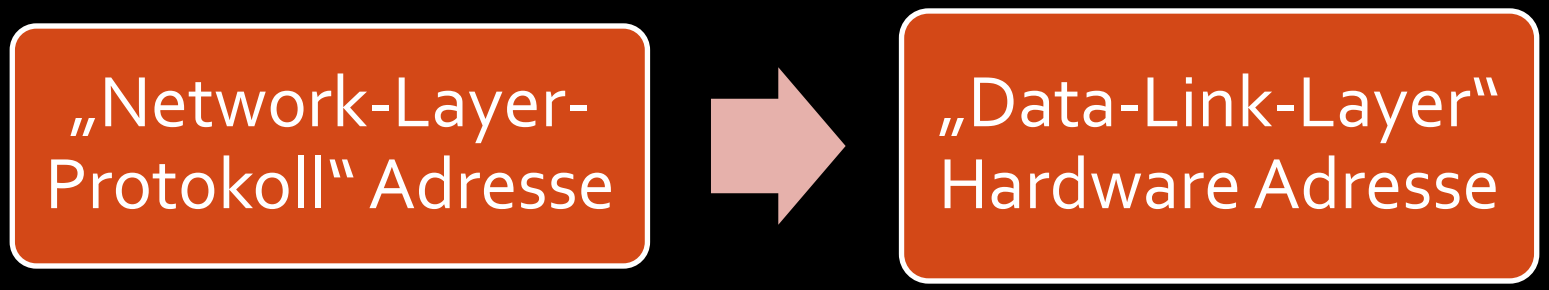
1) Funktionsweise
   a) Der ARP Cache
   b) Paketformat
2) Spezielle Formen
   a) Proxy ARP
   b) Gratuitous ARP
   c) Reverse ARP (RARP)
3) Sicherheit
   a) MAC-Spoofing
   b) ARP-Spoofing
   c) ARP-Cache-Poisoning

Address Resolution Protocol

1) Funktionsweise
   a) Der ARP Cache
   b) Paketformat
2) Spezielle Formen
   a) Proxy ARP
   b) Gratuitous ARP
   c) Reverse ARP (RARP)
3) Sicherheit
   a) MAC-Spoofing
   b) ARP-Spoofing
   c) ARP-Cache-Poisoning

Funktionsweise

- Netzwerkprotokoll



- Gehört zum Data Link Layer des ISO/OSI Referenzmodells
- Spezifiziert in RFC 826

Funktionsweise

- Kommunikation zwischen Hosts im Ethernet nur möglich, wenn die MAC-Adressen bekannt sind
- Higher Level Protokolle wie IP benutzen andere Adressierungen
- Warum nicht direkt MAC verwenden?

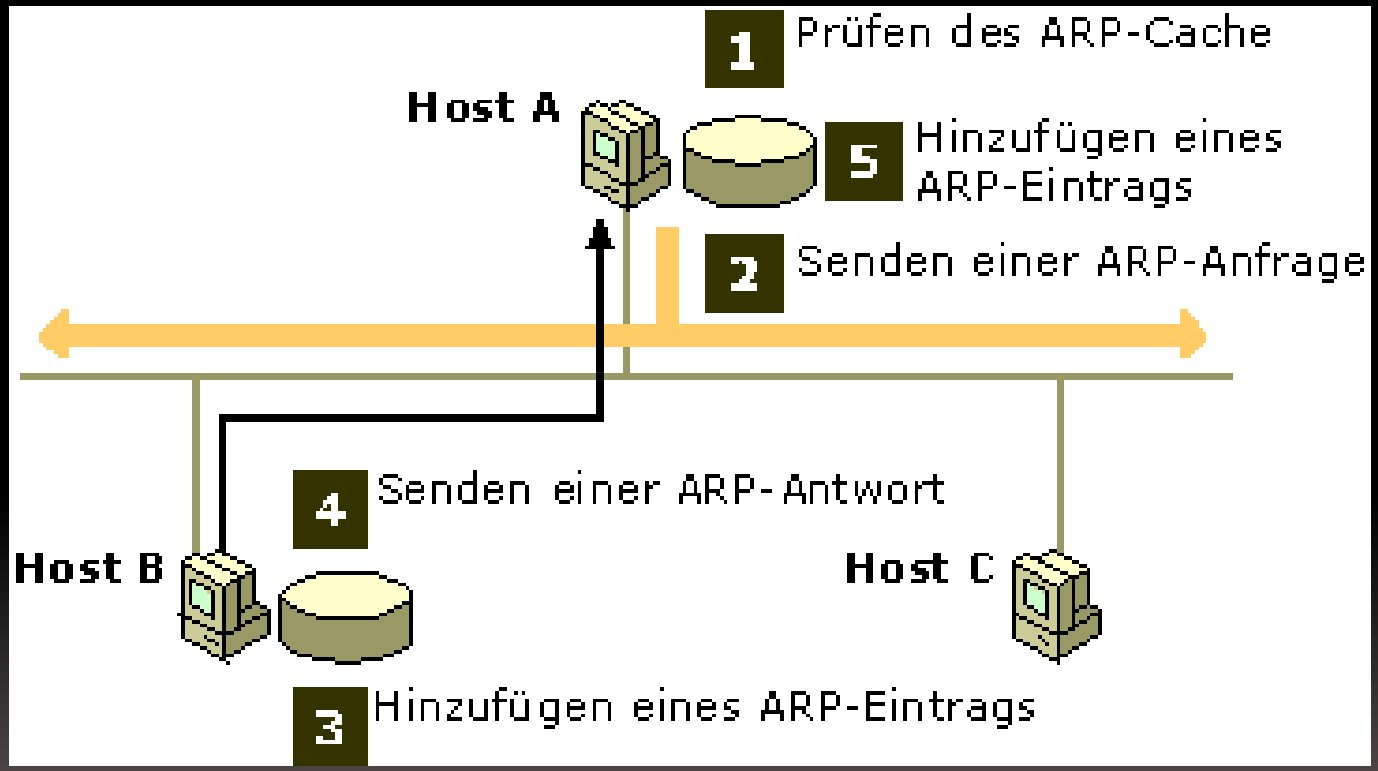
  MAC-Adresse: 6 Bytes  IP-Adresse: 4 Bytes

  TCP/IP unterstützt Routing / Subnetzte usw.

  IP-Adressen können dynamisch vergeben werden

Funktionsweise

Host A möchte Daten an Host B senden:



Microsoft Technet

Der ARP Cache

- Vermeiden von unnötigem Traffic (ARP Broadcast)
- Einträge sind mit Timer versehen (meist 5-20 min)
- Einträge werden bei Empfang von Request- oder Reply-Paketen aktualisiert
- Auch statische Einträge sind möglich

Paketformat

ARP-Paket für IPv4:

Bit 0-7	Bit 8-15	Bit 16-23	Bit 24-31
Hardwareadresstyp (1)		Protokolladresstyp (0x0800) / (0x86DD)	
Hardwareadress-größe (6)	Protokolladress-größe (4) / (16)	Operation 1: ARP-Request / 2: ARP-Reply	
Quell-MAC-Adresse			
Quell-MAC-Adresse		Quell-IP-Adresse	
Quell-IP-Adresse		Ziel-MAC-Adresse	
Ziel-MAC-Adresse			
ZIEL-IP-Adresse			

Address Resolution Protocol

1) Funktionsweise
   a) Der ARP Cache
   b) Paketformat
2) Spezielle Formen
   a) Proxy ARP
   b) Gratuitous ARP
   c) Reverse ARP (RARP)
3) Sicherheit
   a) MAC-Spoofing
   b) ARP-Spoofing
   c) ARP-Cache-Poisoning

Proxy ARP

- Router kann ARP-Requests beantworten
- Verbindung zu Hosts außerhalb des eigenen Netzes möglich
- ARP-Reply gibt die MAC-Adresse des Routers zurück
- ARP Cache weist eventuell mehrere IP-zu-MAC-Zuordnungen auf
- Kann auch Hinweis auf ARP Spoofing sein!!!

Gratuitous ARP

- Zu deutsch: "unaufgefordertes ARP"
- Host sendet ARP-Request mit eigener IP als Quell- und Zieladresse
  - Kann Hinweis auf fehlerhafte Konfiguration sein (wenn ein Reply zurückkommt)
  - Bekanntmachen der MAC-Adresse, z.B. bei Tausch des Netzwerkadapters
  - Ausfallsicherheit bei Servern:
    - Fällt der Hauptserver aus, kann der Ersatzserver so die IP auf seine MAC umleiten

Reverse ARP (RARP)

- Funktioniert genau umgekehrt zu ARP
- Anhand der MAC-Adresse lässt sich die eigene IP ermitteln
- Setzt einen RARP Server voraus
  - Für jedes Subnetz einen
  - Muss manuell gepflegt werden
  - Host erhält nur eigene IP, keine weiteren Informationen (z.B. Gateway)
- Host sendet ein RARP-Request
- RARP Server antwortet mit einem RARP-Reply

Reverse ARP (RARP)

Bit 0-7	Bit 8-15	Bit 16-23	Bit 24-31
Hardwareadresstyp (1)		Protokolladresstyp (0x0800)	
Hardwareadress-größe (6)	Protokolladress-größe (4)	Operation 3: RARP-Request / 4: RARP-Reply	
Quell-MAC-Adresse			
Quell-MAC-Adresse		Quell-IP-Adresse	
Quell-IP-Adresse		Ziel-MAC-Adresse	
Ziel-MAC-Adresse			
ZIEL-IP-Adresse			

Address Resolution Protocol

1) Funktionsweise
   a) Der ARP Cache
   b) Paketformat
2) Spezielle Formen
   a) Proxy ARP
   b) Gratuitous ARP
   c) Reverse ARP (RARP)
3) Sicherheit
   a) MAC-Spoofing
   b) ARP-Spoofing
   c) ARP-Cache-Poisoning

MAC-Spoofing

- Kein direktes Problem von ARP
- MAC-Adressen können gefälscht werden
- Szenario: WLAN
  - Nicht verschlüsseltes WLAN mit MAC-Filter
  - Eindringling kann MAC eines autorisierten Benutzers ermitteln
  - Er konfiguriert seinen Netzwerkadapter mit MAC, IP, Subnetzmaske, Gateway des Benutzers
  - Kann sich nun ins WLAN verbinden
  - Problem bei gleichzeitiger Anwesenheit von Angreifer und Benutzer
  - Jedoch kann er sich bei Abwesenheit des Benutzers problemlos verbinden und Schaden anrichten (z.B. MAC-Filter abschalten)

ARP-Spoofing

- Meist: Man-In-The-Middle-Angriff
- Datenverkehr zwischen zwei Hosts wird abgehört
- Durch gezieltes Senden gefälschter ARP-Pakete wird der Verkehr umgeleitet:
  - Host A möchte mit Host B kommunizieren
  - Angreifer sendet gezielt ARP-Replies, um im Cache von Host A seine MAC unter der IP von Host B zu speichern
  - Bei Host B analog
  - Nun müssen nur noch die Pakete an den richtigen Empfänger weitergeleitet werden.
  - Software, die dies automatisch erledigt, ist kostenlos für alle gängigen Betriebssysteme zu erhalten

ARP-Cache-Poisoning

- "Spezialfall" von ARP-Spoofing
- Ändern des ARP Cache mehrerer Hosts
- Vielfältige Möglichkeiten:
  - Eigenen PC als Gateway eintragen
  - Netzwerkverkehr total umleiten
  - Verkehr zu bestimmten Hosts kann auf eigenen PC umgeleitet werden
- Schwierig, Abwehrmaßnahmen zu entwickeln.

Vielen Dank!

FRAGEN?