

(Reverse) Address Resolution Protocol ([R]ARP)

Von: Tobias Tekath

Inhalt

- ARP
 - Verwendung
 - Protokoll
 - ARP-Paket
 - ARP-spoofing
- RARP
 - Verwendung
 - Protokoll
- NDP
- Einordnung OSI/TCP-IP

ARP – Adress Resolution Protocol

- RFC 826 vom November 1982 von David C. Plummer

Das Protokoll soll im lokalen Netzwerk zu einer bekannten logischen Adresse die entsprechende physikalische Adresse herausfinden

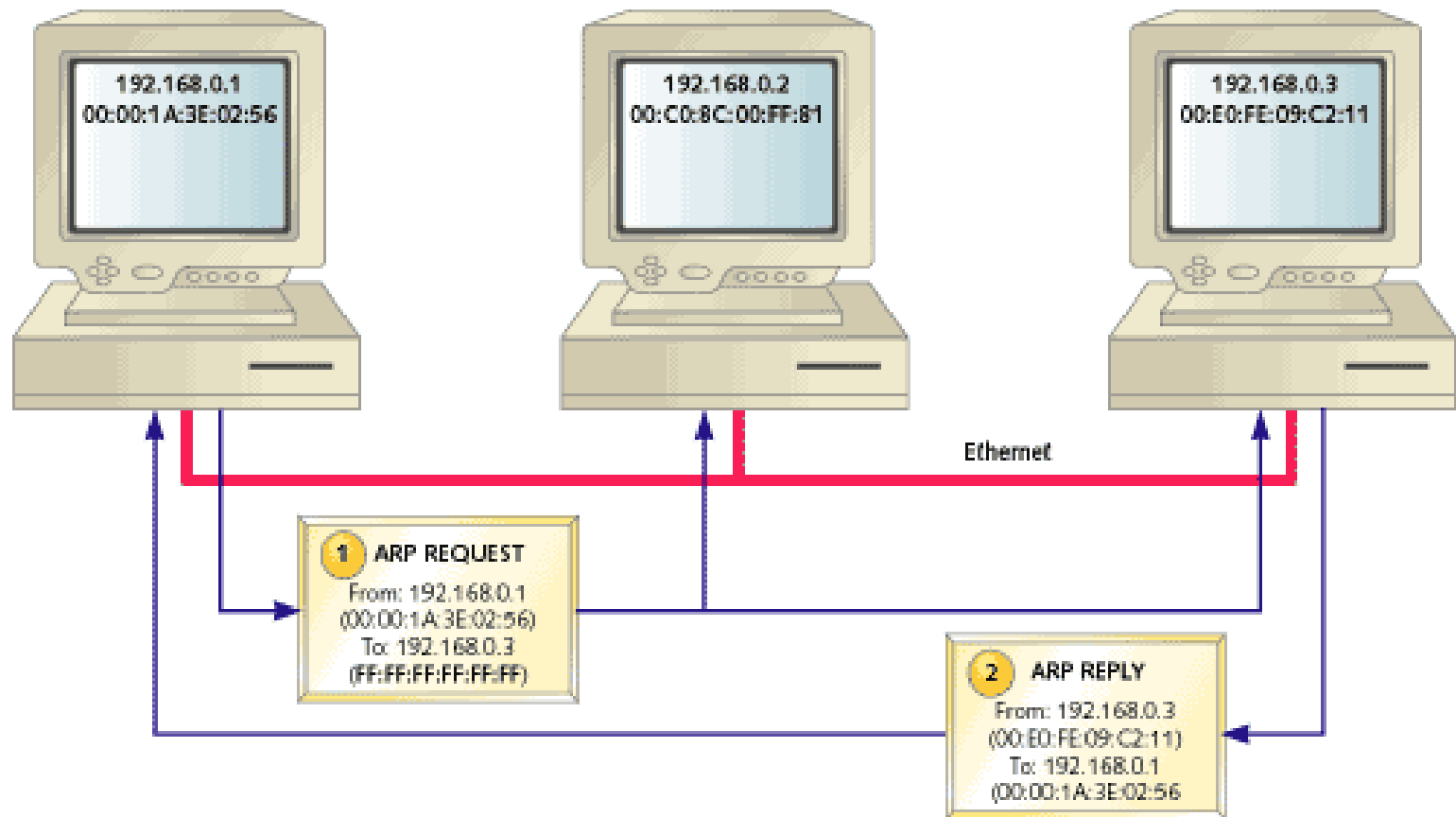
Verwendung

- Hauptsächlich für IPv4 –Netzwerke (logische Adresse) in Verbindung mit MAC-Adressen (physikalischen Adresse)
- Bei IPv6 wird ARP durch das Neighbor Discovery Protocol (NDP) ersetzt
 - Ein Computer möchte eine Nachricht an eine IP-Adresse im lokalen Netzwerk schicken, kennt aber die zugehörige MAC-Adresse nicht

Exkurs: MAC-Adresse

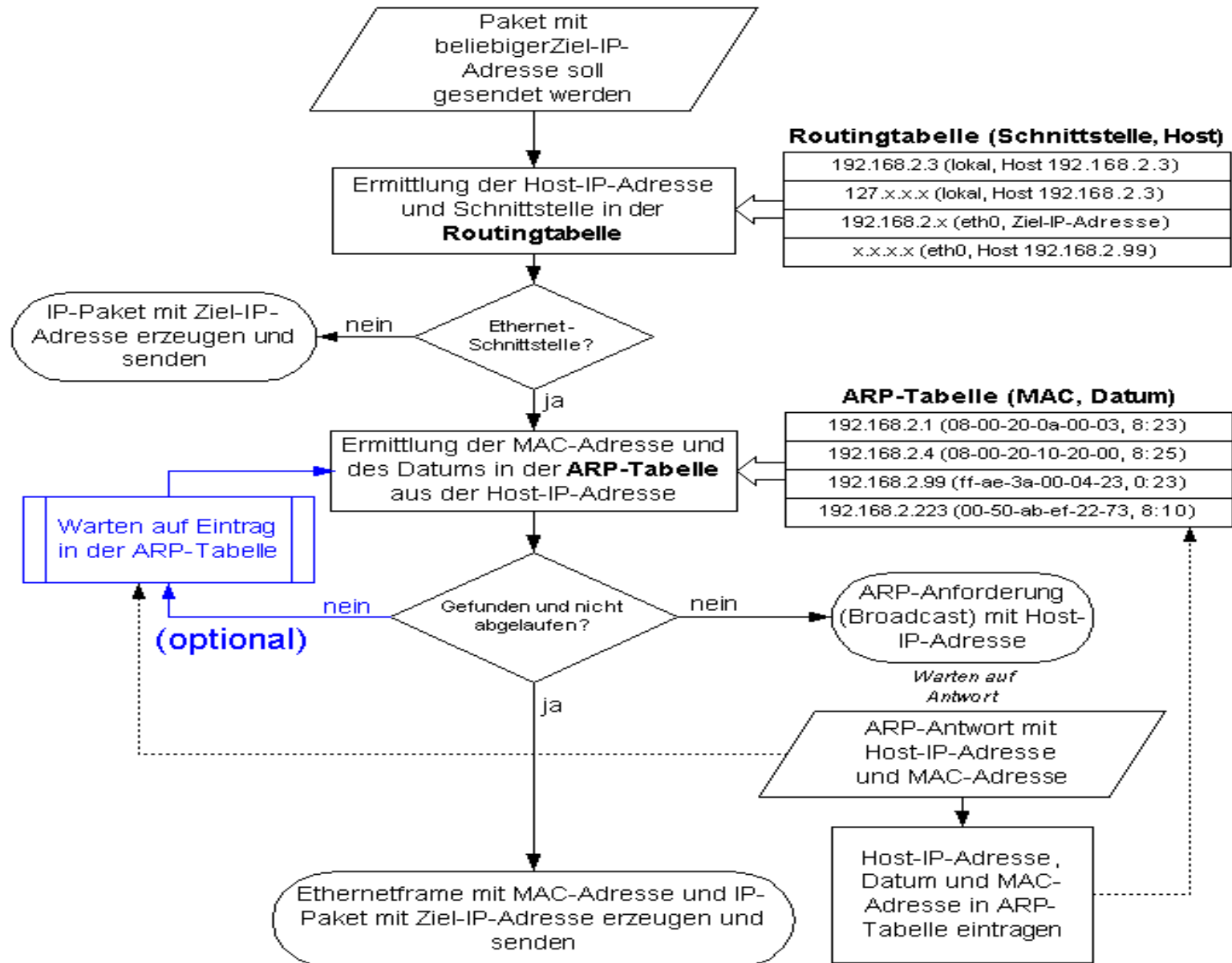
- MAC: media access control
- (weltweit) Eindeutiger Identifikator für netzwerkfähige Geräte
- Vom Hersteller in die Netzwerkkarte eingetragen (z.B. im Read-Only Memory)
- Kann aber von fast jedem Betriebssystem geändert werden
- 48 Bit, z.B.: 01:23:45:67:89:ab

ARP-Protokoll



<http://www.barrgroup.com/images/articles/ARPRequestReply.gif> vom 26.10.14

ARP-Protokoll



ARP-Paket

- Hardware type (HTYPE) (Ethernet = 1)
- Protocol type (PTYPE) (IPv4 = 0x0800)
- Hardware length (HLEN) (6)
- Protocol length (PLEN) (4)
- Operation (1=request, 2=reply)
- Sender hardware address (SHA)
- Sender protocol address (SPA)
- Target hardware address (THA)
- Target protocol address (TPA)

ARP-Cache

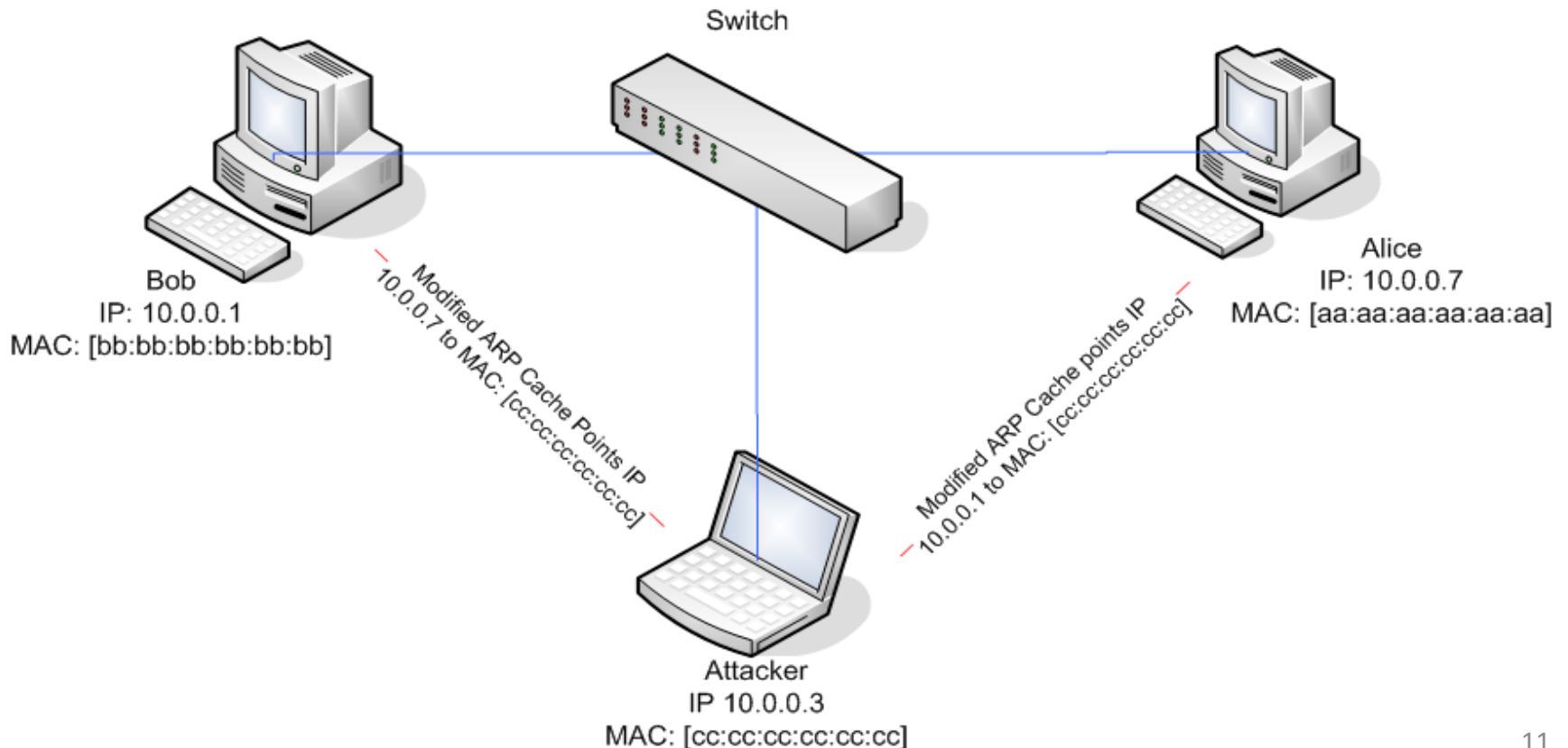
- Erhaltene Antworten werden für bestimmte Zeit zwischengespeichert
- Manuell auch statische Einträge möglich
- ARP-Einträge anzeigen: `arp -a` (Win/Unix)
- Aktualisierung des Caches bei jeder Anfrage, wenn IP/MAC bereits im Cache

Spezielle ARP-Pakete

- ARP probe
 - Nach RFC5227 muss vor Nutzung von IP ein Probe-Request erfolgen
 - Absender IP 0.0.0.0 -> Empfänger IP *zugewiesene IP*
 - Verhinderung von IPv4 Adresskonflikten
- Gratuitous Arp („unaufgefordertes“ ARP)
 - Quell IP = Ziel IP
 - Aktualisierung der ARP-Cache

ARP-spoofing

- Gefälschte ARP-Pakete um Datenverkehr zwischen Teilnehmern umzuleiten



RARP – Reverse Address Resolution Protocol

- RFC 903 vom Juni 1984 von Finlayson, Mann, Mogul, Theimer

Das Protokoll soll im lokalen Netzwerk zu einer bekannten physischen Adresse die entsprechende lokale Adresse herausfinden

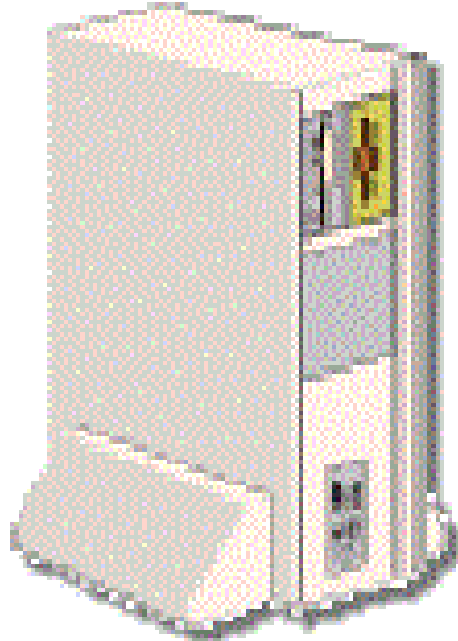
- Quasi die Gegenfunktion zu ARP

RARP-Verwendung

- Ein Computer möchte im lokalen Netzwerk seine eigene IP-Adresse herausfinden
 - RARP-Request mit eigener MAC-Adresse
- Ein Computer soll eine TCP/IP-Verbindung aufbauen, hat aber keine IP-Adresse
 - RARP-Request mit eigener MAC-Adresse an RARP-Server

RARP-Protokoll

IP-Adresse unbekannt
MAC-Adresse bekannt

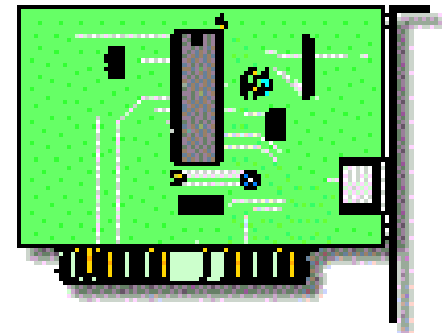


RARP Server

RARP Request
MAC-Adresse



RARP Reply
IP-Adresse



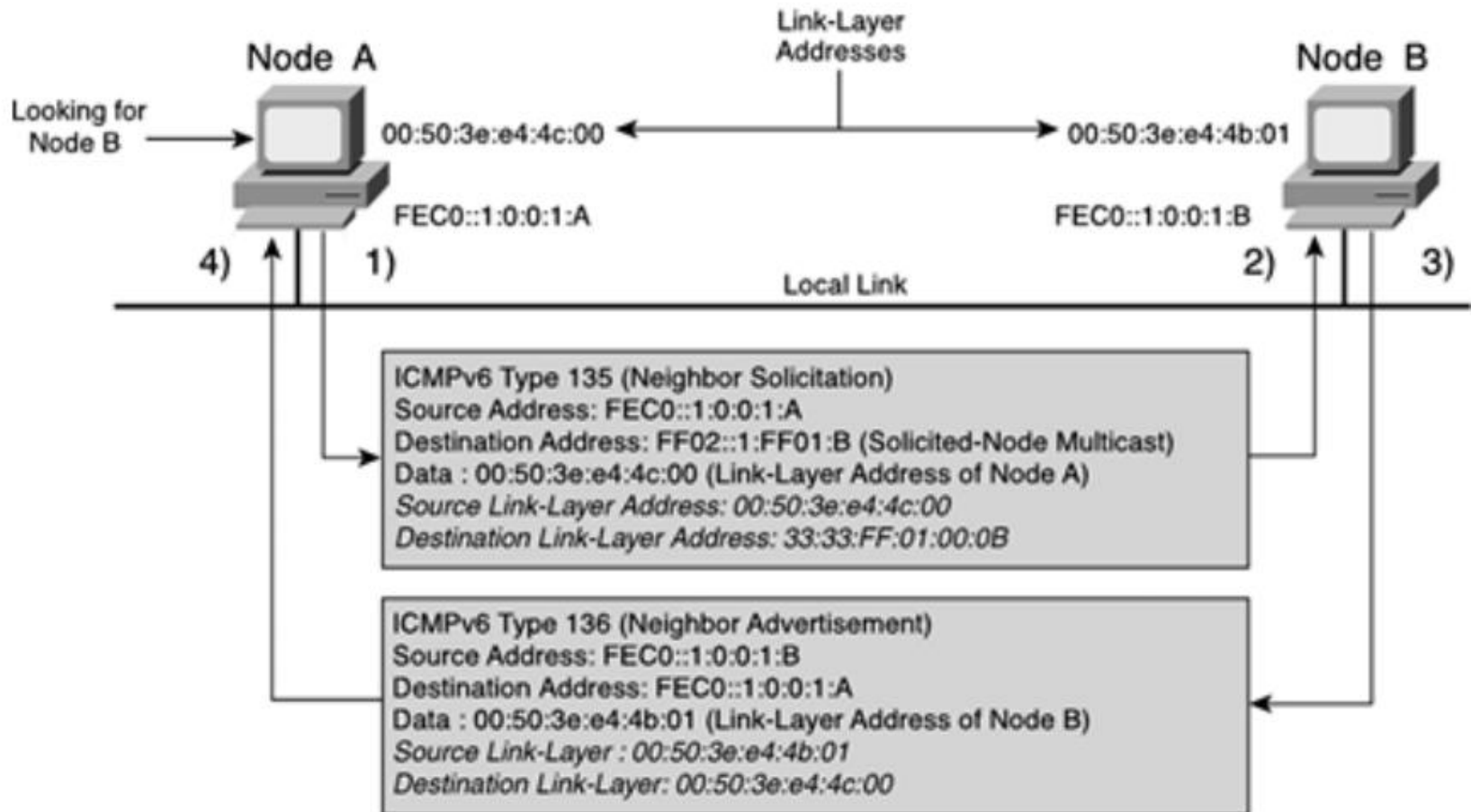
NDP – Neighbor Discovery Protocol

- RFC 4861 von der Network Working Group im September 2007
- Eine Internet Protocol Suite für IPv6
- Ersetzt verschiedene IPv4 Protokolle in einem
 - ARP
 - Internet Control Message Protocol (ICMP)
 - Router Discovery
 - Router Redirect

ICMPv6 Pakete

- Router Solicitation (Type 133)
 - Aufforderung an alle Router sich zu melden
- Router Advertisement (Type 134)
 - Router bestätigen Anwesenheit im Netzwerk
- Neighbor Solicitation (Type 135)
- Neighbor Advertisement (Type 136)
- Redirect (Type 137)
 - Router verweist auf besseren Hop

NDP Adressauflösung



Einordnung OSI/TCP-IP

OSI-Schicht	TCP/IP-Schicht	Beispiel
Anwendungen (7)	Anwendungen	HTTP, UDS, FTP, SMTP, POP, Telnet, OPC UA
Darstellung (6)		
Sitzung (5)		
		SOCKS
Transport (4)	Transport	TCP, UDP, SCTP
Vermittlung (3)	Internet	IP (IPv4, IPv6), ICMP (über IP)
Sicherung (2)	Netzzugang	↓ ARP/RARP ↑
Bitübertragung (1)		Ethernet, Token Bus, Token Ring, FDDI, IPoAC

Quellen

- <http://tools.ietf.org/html/rfc826>
- <http://tools.ietf.org/html/rfc903>
- <http://tools.ietf.org/html/rfc4861>
- <http://tools.ietf.org/html/rfc2461>
- <http://www.lug-erding.de/vortrag/ng.html#ARP>
- http://en.wikipedia.org/wiki/Address_Resolution_Protocol
- http://de.wikipedia.org/wiki/Neighbor_Discovery_Protocol

Vielen Dank für eure
Aufmerksamkeit!