

Übung 5

Tutorübung zu Grundlagen: Rechnernetze und Verteilte Systeme (Gruppen MI-T7 / DO-T5 SS 2015)

Michael Schwarz

Technische Universität München
Fakultät für Informatik

20.05.2015 / 21.05.2015

Addressierung auf Layer 3 (IP) erfolgt mithilfe der IP-Adresse,
für die Level darunter verwende ich aber für die Next-Hop
Adressierung die MAC-Adresse

Adressauflösung [5]

- ▶ Host1 will eine Nachricht an Host2 senden
- ▶ Die IP-Adresse von Host2 (192.168.1.2) sei ihm bereits bekannt
- ▶ Wie erhält Host1 die zugehörige MAC-Adresse?

c8:2a:14:4f:dc:02
192.168.1.1



Host1

04:0c:ce:e2:c8:2e
192.168.1.2



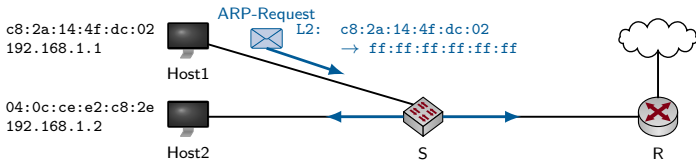
Address Resolution Protocol (ARP)

1. Host1 sendet einen ARP Request: „Who has 192.168.1.2? Tell 192.168.1.1“
2. Host2 antwort mit einem ARP Reply: „192.168.1.2 is at 04:0c:ce:e2:c8:2e“

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0 B	Hardware Type																Protocol Type															
4 B	Hardware Addr. Length								Protocol Addr. Length								Operation															
8 B	Sender Hardware Address (first 32 bit)																															
12 B	Sender Hardware Address (last 16 bit)																Sender Protocol Address (first 16 bit)															
16 B	Sender Protocol Address (last 16 bit)																Target Hardware Address (first 16 bit)															
20 B	Target Hardware Address (last 32 bit)																															
24 B	Target Protocol Address																															

Abbildung: ARP-Paket für IPv4 über Ethernet

Beispiel:



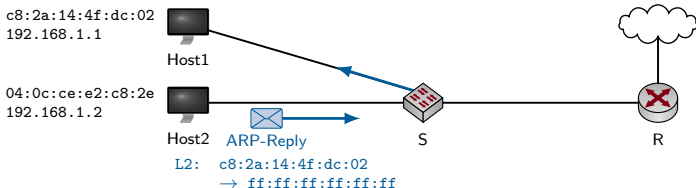
Hinweis: L2: xx:xx:xx:xx:xx:xx → yy:yy:yy:yy:yy:yy stellt Absender- und Ziel-MAC auf Schicht 2 dar.

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0 B	0x0001 (Ethernet)												0x0800 (IPv4)																			
4 B	0x06				0x04				0x0001 (Request)																							
8 B	0xc82a144f																															
12 B	0xdc02 (Sender Hardware Address)												0xc0a8																			
16 B	0x0101 (Sender Protocol Address)												0x0000																			
20 B	0x00000000 (Target Hardware Address)																															
24 B	0xc0a80102 (Target Protocol Address)																															

(a) ARP Request

- Der ARP-Request wird an die MAC-Broadcastadresse ff:ff:ff:ff:ff:ff geschickt, weswegen der Switch S den Rahmen an alle angeschlossenen Hosts weiterleitet.

Beispiel:



Hinweis: L2: xx:xx:xx:xx:xx:xx → yy:yy:yy:yy:yy:yy stellt Absender- und Ziel-MAC auf Schicht 2 dar.

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0 B	0x0001 (Ethernet)												0x0800 (IPv4)																			
4 B	0x06						0x04						0x0001 (Request)																			
8 B	0xc82a144f																															
12 B	0xdc02 (Sender Hardware Address)															0xc0a8																
16 B	0x0101 (Sender Protocol Address)															0x0000																
20 B	0x00000000 (Target Hardware Address)																															
24 B	0xc0a80102 (Target Protocol Address)																															

(c) ARP Request

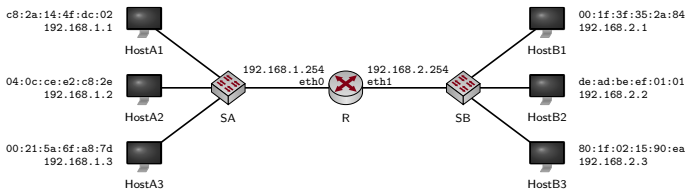
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0 B	0x0001 (Ethernet)												0x0800 (IPv4)																			
4 B	0x06						0x04						0x0002 (Reply)																			
8 B	0x040ccee2															0xc0a8																
12 B	0xc82e															0xc0a8																
16 B	0x0102															0xc82a																
20 B	0x144f4c02																															
24 B	0xc0a80101																															

(d) ARP Reply

- ▶ Der ARP-Request wird an die MAC-Broadcastadresse ff:ff:ff:ff:ff:ff geschickt, weswegen der Switch S den Rahmen an alle angeschlossenen Hosts weiterleitet.
- ▶ Der ARP-Reply wird als MAC-Unicast versendet (adressiert an Host1).
- ▶ Die Rollen Sender / Target sind zwischen Request und Reply vertauscht (vgl. Inhalte der grünen und roten Felder).

Was ist nun, wenn das Ziel **nicht** im selben Netz liegt (z. B. HostA1 an HostB2)?

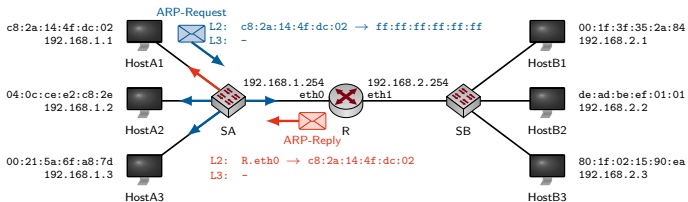
- ▶ Jeder Host sollte ein **Default Gateway** kennen, an das er alle Pakete schickt, deren Zieladressen nicht im eigenen Netz liegen.
- ▶ Die Zugehörigkeit einer Adresse zum jeweiligen Netz erkennt ein Host durch Vergleich der eigenen Adresse mit der Zieladresse.
- ▶ Im Moment gehen wir noch davon aus, dass die ersten 3 Oktette einer IP-Adresse das Netz identifizieren
⇒ 192.168.1.1 und 192.168.2.2 liegen in unterschiedlichen Netzen.



1. HostA1 erkennt, dass 192.168.2.2 nicht im eigenen Netz liegt. Sein Default-Gateway ist 192.168.1.254.

Was ist nun, wenn das Ziel **nicht** im selben Netz liegt (z. B. HostA1 an HostB2)?

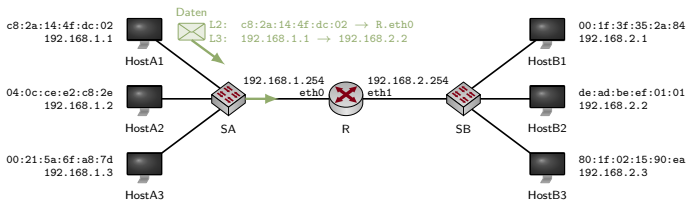
- ▶ Jeder Host sollte ein **Default Gateway** kennen, an das er alle Pakete schickt, deren Zieladressen nicht im eigenen Netz liegen.
- ▶ Die Zugehörigkeit einer Adresse zum jeweiligen Netz erkennt ein Host durch Vergleich der eigenen Adresse mit der Zieladresse.
- ▶ Im Moment gehen wir noch davon aus, dass die ersten 3 Oktette einer IP-Adresse das Netz identifizieren
⇒ 192.168.1.1 und 192.168.2.2 liegen in unterschiedlichen Netzen.



1. HostA1 erkennt, dass 192.168.2.2 nicht im eigenen Netz liegt. Sein Default-Gateway ist 192.168.1.254.
2. HostA1 löst die MAC-Adresse zu 192.168.1.254 auf.

Was ist nun, wenn das Ziel **nicht** im selben Netz liegt (z. B. HostA1 an HostB2)?

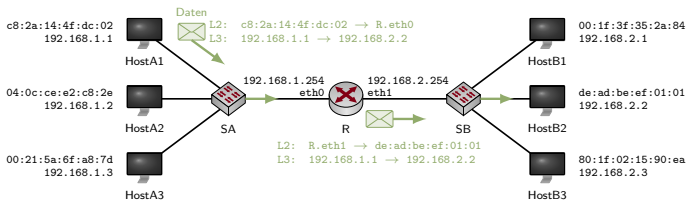
- ▶ Jeder Host sollte ein **Default Gateway** kennen, an das er alle Pakete schickt, deren Zieladressen nicht im eigenen Netz liegen.
- ▶ Die Zugehörigkeit einer Adresse zum jeweiligen Netz erkennt ein Host durch Vergleich der eigenen Adresse mit der Zieladresse.
- ▶ Im Moment gehen wir noch davon aus, dass die ersten 3 Oktette einer IP-Adresse das Netz identifizieren
⇒ 192.168.1.1 und 192.168.2.2 liegen in unterschiedlichen Netzen.



1. HostA1 erkennt, dass 192.168.2.2 nicht im eigenen Netz liegt. Sein Default-Gateway ist 192.168.1.254.
2. HostA1 löst die MAC-Adresse zu 192.168.1.254 auf.
3. HostA1 sendet das Datenpaket an R: Dabei adressiert er R mittels der eben bestimmten MAC-Adresse (Schicht 2). Als Ziel-IP-Adresse (Schicht 3) verwendet er die IP-Adresse von HostB2.

Was ist nun, wenn das Ziel **nicht** im selben Netz liegt (z. B. HostA1 an HostB2)?

- ▶ Jeder Host sollte ein **Default Gateway** kennen, an das er alle Pakete schickt, deren Zieladressen nicht im eigenen Netz liegen.
- ▶ Die Zugehörigkeit einer Adresse zum jeweiligen Netz erkennt ein Host durch Vergleich der eigenen Adresse mit der Zieladresse.
- ▶ Im Moment gehen wir noch davon aus, dass die ersten 3 Oktette einer IP-Adresse das Netz identifizieren
⇒ 192.168.1.1 und 192.168.2.2 liegen in unterschiedlichen Netzen.



1. HostA1 erkennt, dass 192.168.2.2 nicht im eigenen Netz liegt. Sein Default-Gateway ist 192.168.1.254.
2. HostA1 löst die MAC-Adresse zu 192.168.1.254 auf.
3. HostA1 sendet das Datenpaket an R: Dabei adressiert er R mittels der eben bestimmten MAC-Adresse (Schicht 2). Als Ziel-IP-Adresse (Schicht 3) verwendet er die IP-Adresse von HostB2.
4. R akzeptiert das Paket, bestimmt das ausgehende Interface und leitet das Paket weiter an HostB2. Dabei adressiert R wiederum HostB2 anhand seiner MAC-Adresse (erfordert ggf. einen weiteren ARP-Schritt).

Merke:

- ▶ MAC-Adressen dienen zur Adressierung **innerhalb** eines (Direktverbindungs-)Netzes und werden beim Routing verändert.
- ▶ IP-Adressen dienen der End-zu-End-Adressierung **zwischen** mehreren (Direktverbindungs-)Netzen und werden beim Routing nicht verändert.

Anmerkungen

- ▶ Das Ergebnis einer Adressauflösung wird i. d. R. im **ARP-Cache** eines Hosts zwischengespeichert, um nicht bei jedem zu versendenden Paket erneut eine Adressauflösung durchführen zu müssen.
- ▶ Die Einträge im ARP-Cache altern und werden nach einer vom Betriebssystem festgelegten Zeit invalidiert (5-10 Minuten).
- ▶ Den Inhalt des ARP-Caches kann man sich unter Linux, OS X und Windows mittels des Befehls `arp -a` anzeigen lassen.
- ▶ ARP-Replies können auch als MAC-Broadcast verschickt werden, so dass alle Hosts innerhalb einer Broadcast-Domain den Reply erhalten. Abhängig vom Betriebssystem werden derartige „unaufgeforderten ARP-Replies“ (engl. **unsolicited ARP replies**) häufig ebenfalls im ARP-Cache gespeichert.

Fragen: Was würde passieren, wenn ...

- ▶ zwei Hosts innerhalb derselben Broadcast-Domain identische MAC-Adressen aber unterschiedliche IP-Adressen haben?
- ▶ ein Host absichtlich auf ARP-Requests antwortet, die nicht an ihn gerichtet waren?
- ▶ ein Host unsinnige ARP-Replies via MAC-Broadcasts verschickt?

Subnetting (Classless Routing)

Bereits 1993 wurde mit **CIDR**³ ein Verfahren zur Unterteilung von IP-Netzen eingeführt:

- ▶ Zusätzlich zur IP-Adresse erhält ein Interface eine ebenfalls 32 Bit lange **Subnetzmaske**
- ▶ Die Subnetzmaske unterteilt die IP-Adresse in einen **Netzanteil** und einen **Hostanteil**
- ▶ Eine logische 1 in der Subnetzmaske bedeutet Netzanteil, eine logische 0 Hostanteil
- ▶ UND-Verknüpfung von IP-Adresse und Subnetzmaske ergibt die Netzadresse
- ▶ Die übliche Klassenzugehörigkeit hat damit nur noch im Sprachgebrauch eine Bedeutung

Beispiel 1:

IP-Adresse	11000000 . 10101000 . 00000000 . 10110010	192.168.0.178
Subnetz Maske	11111111 . 11111111 . 11111111 . 00000000	255.255.255.0
Netzadresse	11000000 . 10101000 . 00000000 . 00000000	192.168.0.0
Broadcastadresse	11000000 . 10101000 . 00000000 . 11111111	192.168.0.255

- ▶ 24 Bit Netzanteil, 8 Bit Hostanteil $\Rightarrow 2^8 = 256$ Adressen
- ▶ Netzadresse: 192.168.0.0
- ▶ Broadcastadresse: 192.168.0.255
- ▶ Nutzbare Adressen für Hosts: $2^8 - 2 = 254$

³Classless Inter-Domain Routing

Subnetting (Classless Routing)

Bereits 1993 wurde mit **CIDR**³ ein Verfahren zur Unterteilung von IP-Netzen eingeführt:

- ▶ Zusätzlich zur IP-Adresse erhält ein Interface eine ebenfalls 32 Bit lange **Subnetzmaske**
- ▶ Die Subnetzmaske unterteilt die IP-Adresse in einen **Netzanteil** und einen **Hostanteil**
- ▶ Eine logische 1 in der Subnetzmaske bedeutet Netzanteil, eine logische 0 Hostanteil
- ▶ UND-Verknüpfung von IP-Adresse und Subnetzmaske ergibt die Netzadresse
- ▶ Die übliche Klassenzugehörigkeit hat damit nur noch im Sprachgebrauch eine Bedeutung

Beispiel 2:

IP-Adresse	11000000 . 10101000 . 00000000 . 10110010	192.168.0.178
Subnetz Maske	11111111 . 11111111 . 11111111 . 10000000	255.255.255.128
Netzadresse	11000000 . 10101000 . 00000000 . 10000000	192.168.0.128
Broadcastadresse	11000000 . 10101000 . 00000000 . 11111111	192.168.0.255

- ▶ 25 Bit Netzanteil, 7 Bit Hostanteil $\Rightarrow 2^7 = 128$ Adressen
- ▶ Netzadresse: 192.168.0.128
- ▶ Broadcastadresse: 192.168.0.255
- ▶ Nutzbare Adressen für Hosts: $2^7 - 2 = 126$

³Classless Inter-Domain Routing

Subnetting (Classless Routing)

Bereits 1993 wurde mit **CIDR**³ ein Verfahren zur Unterteilung von IP-Netzen eingeführt:

- ▶ Zusätzlich zur IP-Adresse erhält ein Interface eine ebenfalls 32 Bit lange **Subnetzmaske**
- ▶ Die Subnetzmaske unterteilt die IP-Adresse in einen **Netzanteil** und einen **Hostanteil**
- ▶ Eine logische 1 in der Subnetzmaske bedeutet Netzanteil, eine logische 0 Hostanteil
- ▶ UND-Verknüpfung von IP-Adresse und Subnetzmaske ergibt die Netzadresse
- ▶ Die übliche Klassenzugehörigkeit hat damit nur noch im Sprachgebrauch eine Bedeutung

Beispiel 3:

IP-Adresse	11000000 . 10101000 . 00000000 . 10110010	192.168.0.178
Subnetz Maske	11111111 . 11111111 . 11111111 . 11000000	255.255.255.192
Netzadresse	11000000 . 10101000 . 00000000 . 10000000	192.168.0.128
Broadcastadresse	11000000 . 10101000 . 00000000 . 10111111	192.168.0.191

- ▶ 26 Bit Netzanteil, 6 Bit Hostanteil $\Rightarrow 2^6 = 64$ Adressen
- ▶ Netzadresse: 192.168.0.128
- ▶ Broadcastadresse: 192.168.0.191
- ▶ Nutzbare Adressen für Hosts: $2^6 - 2 = 62$

³Classless Inter-Domain Routing

Supernetting

Dasselbe Prinzip funktioniert auch in die andere Richtung:

- ▶ Zusammenfassung mehrerer **zusammenhängender** kleinerer Netze zu einem größeren Netz
- ▶ Wird häufig von Routern angewendet, um die Anzahl der Einträge in der Routingtabelle zu reduzieren

Beispiel:

IP-Adresse	11000000 . 10101000 . 00000000 . 10110010	192.168.0.178
Subnetz Maske	11111111 . 11111111 . 11111110 . 00000000	255.255.254.0
Netzadresse	11000000 . 10101000 . 00000000 . 00000000	192.168.0.0
Broadcastadresse	11000000 . 10101000 . 00000001 . 11111111	192.168.1.255

- ▶ 23 Bit Netzanteil, 9 Bit Hostanteil $\Rightarrow 2^9 = 512$ Adressen
- ▶ Netzadresse: 192.168.0.0
- ▶ Broadcastadresse: 192.168.1.255
- ▶ Nutzbare Adressen für Hosts: $2^9 - 2 = 510$

Präfixschreibweise:

Anstelle die Subnetzmaske auszuschreiben, wird häufig nur die Länge des Netzanteils (Anzahl führender Einsen in der Subnetzmaske) angegeben, z. B. 192.168.0.0/23.

Frage: Können die beiden Netze 192.168.1.0/24 und 192.168.2.0/24 zu einem größeren Netz zusammengefasst werden?

Frage: Können die beiden Netze 192.168.1.0/24 und 192.168.2.0/24 zu einem größeren Netz zusammengefasst werden?

Antwort: Nein, denn es gibt keine passende Subnetzmaske:

- ▶ 192.168.0.0/23 enthält die Netze 192.168.{0,1}.0/24
- ▶ 192.168.2.0/23 enthält die Netze 192.168.{2,3}.0/24
- ▶ 192.168.1.0/23 ist **keine gültige** Netzadresse, denn UND-Verknüpfung der Adresse 192.168.1.0 mit der Subnetzmaske 255.255.254.0 ergibt 192.168.0.0 als Netzadresse!
⇒ 192.168.1.0 ist eine Hostadresse im Netz 192.168.0.0/23.

Frage: Können die beiden Netze 192.168.1.0/24 und 192.168.2.0/24 zu einem größeren Netz zusammengefasst werden?

Antwort: Nein, denn es gibt keine passende Subnetzmaske:

- ▶ 192.168.0.0/23 enthält die Netze 192.168.{0,1}.0/24
- ▶ 192.168.2.0/23 enthält die Netze 192.168.{2,3}.0/24
- ▶ 192.168.1.0/23 ist **keine gültige** Netzadresse, denn UND-Verknüpfung der Adresse 192.168.1.0 mit der Subnetzmaske 255.255.254.0 ergibt 192.168.0.0 als Netzadresse!
⇒ 192.168.1.0 ist eine Hostadresse im Netz 192.168.0.0/23.

Frage: Können die beiden Netze 192.168.0.0/24 und 192.168.2.0/24 zu einem größeren Netz zusammengefasst werden?

Frage: Können die beiden Netze 192.168.1.0/24 und 192.168.2.0/24 zu einem größeren Netz zusammengefasst werden?

Antwort: Nein, denn es gibt keine passende Subnetzmaske:

- ▶ 192.168.0.0/23 enthält die Netze 192.168.{0,1}.0/24
 - ▶ 192.168.2.0/23 enthält die Netze 192.168.{2,3}.0/24
 - ▶ 192.168.1.0/23 ist **keine gültige** Netzadresse, denn UND-Verknüpfung der Adresse 192.168.1.0 mit der Subnetzmaske 255.255.254.0 ergibt 192.168.0.0 als Netzadresse!
⇒ 192.168.1.0 ist eine Hostadresse im Netz 192.168.0.0/23.
-

Frage: Können die beiden Netze 192.168.0.0/24 und 192.168.2.0/24 zu einem größeren Netz zusammengefasst werden?

Antwort: Nein, denn die beiden Netze sind nicht benachbart:

- ▶ Das Netz 192.168.0.0/22 würde zwar beide Subnetze enthalten, zusätzlich aber auch die beiden Netze 192.168.{1,3}.0/24.

Frage: Können die beiden Netze 192.168.1.0/24 und 192.168.2.0/24 zu einem größeren Netz zusammengefasst werden?

Antwort: Nein, denn es gibt keine passende Subnetzmaske:

- ▶ 192.168.0.0/23 enthält die Netze 192.168.{0,1}.0/24
 - ▶ 192.168.2.0/23 enthält die Netze 192.168.{2,3}.0/24
 - ▶ 192.168.1.0/23 ist **keine gültige** Netzadresse, denn UND-Verknüpfung der Adresse 192.168.1.0 mit der Subnetzmaske 255.255.254.0 ergibt 192.168.0.0 als Netzadresse!
⇒ 192.168.1.0 ist eine Hostadresse im Netz 192.168.0.0/23.
-

Frage: Können die beiden Netze 192.168.0.0/24 und 192.168.2.0/24 zu einem größeren Netz zusammengefasst werden?

Antwort: Nein, denn die beiden Netze sind nicht benachbart:

- ▶ Das Netz 192.168.0.0/22 würde zwar beide Subnetze enthalten, zusätzlich aber auch die beiden Netze 192.168.{1,3}.0/24.
-

Frage: Können die vier Netze 192.168.{4,5,6,7}.0/24 zu einem größeren Netz zusammengefasst werden?

Frage: Können die beiden Netze 192.168.1.0/24 und 192.168.2.0/24 zu einem größeren Netz zusammengefasst werden?

Antwort: Nein, denn es gibt keine passende Subnetzmaske:

- ▶ 192.168.0.0/23 enthält die Netze 192.168.{0,1}.0/24
 - ▶ 192.168.2.0/23 enthält die Netze 192.168.{2,3}.0/24
 - ▶ 192.168.1.0/23 ist **keine gültige** Netzadresse, denn UND-Verknüpfung der Adresse 192.168.1.0 mit der Subnetzmaske 255.255.254.0 ergibt 192.168.0.0 als Netzadresse!
⇒ 192.168.1.0 ist eine Hostadresse im Netz 192.168.0.0/23.
-

Frage: Können die beiden Netze 192.168.0.0/24 und 192.168.2.0/24 zu einem größeren Netz zusammengefasst werden?

Antwort: Nein, denn die beiden Netze sind nicht benachbart:

- ▶ Das Netz 192.168.0.0/22 würde zwar beide Subnetze enthalten, zusätzlich aber auch die beiden Netze 192.168.{1,3}.0/24.
-

Frage: Können die vier Netze 192.168.{4,5,6,7}.0/24 zu einem größeren Netz zusammengefasst werden?

Antwort: Ja, das Netz 192.168.4.0/22 umfasst genau diese vier Netze.