

Grundlagen der Informationstechnik

Übung 03 - IP Layer

Technische Universität Carolo-Wilhelmina zu Braunschweig
Institut für Datentechnik und Kommunikationsnetze (IDA)
Abteilung Kommunikationsnetze



Ein Unternehmen benötigt von einem Provider 1000 Host-Adressen. Dieser verwendet CIDR um einen geeigneten zusammenhängenden Adressbereich bereitzustellen. Zeigen Sie diesen Adressbereich und die Netzmaske, falls der Adressbereich bei 194.168.56.0 beginnen soll.

- Netzwerk-Präfixe variabler Länge ersetzen ursprünglich feste Bereiche (Klasse A - 8 Bit, Klasse B – 16 Bit, Klasse C – 24 Bit)
 - Beispiel 1: **194.168.56.0 / 24**
 - Der Netzwerk - Präfix hat eine Länge von 24 Bit (früher Klasse C Netz)
 - Beispiel 2: **194.168.56.0 / 22**
 - Der Präfix hat eine Länge von 22 Bit
 - Die ersten 22 Bit der IP - Adresse kennzeichnen das Netzwerk

11000010 10101000 00111000 00000000 ↔ 194.168.56.0
/22 10 Bit Hostanteil

Konsequenz:

- IP- Adressbereiche können in variablen Blockgrößen vergeben werden
- Länge des Netzwerk-Präfixes muss mit IP - Adresse angegeben werden
- Anmerkung: CIDR wurde im Zusammenhang mit dem Border Gateway Routing Protokoll (BGP) eingeführt

- Unternehmen benötigt 1000 Host-Adressen
- Hierfür ist ein Adress-Block der Größe $2^{10} - 2 = 1022$ erforderlich
 - Es werden 10 Bit für den Host-Teil der IP - Adresse benötigt

Adressen: **11000010.10101000.001110** 00.00000001 \Leftrightarrow 194.168.56.1

11000010.10101000.001110 11.11111110 \Leftrightarrow 194.168.59.254

Maske: **11111111.11111111.111111** 00.00000000 \Leftrightarrow **255.255.252.0**

Präfix : **11000010.10101000.001110** 00.00000000 \Leftrightarrow **194.168.56.0 / 22**
 |----- network-prefix -----|

- Netzwerk-Adresse ist 194.168.56.0 / 22, Präfix-Länge ist 22 Bit
- Host Adress-Bereich ist 194.168.56.1 - 194.168.59.254

A2) Longest Prefix Matching



Ein Router besitzt die unten gezeigte Weiterleitungstabelle. Eine gegebene IP-Adresse verknüpft der Router mit den in der Weiterleitungstabelle gegebenen Netzmasken und wählt den nächsten Hop mit dem korrespondierenden Netzwerk-Präfix aus. Sind mehrere Netzwerk-Präfixe gültig, wird der gewählt, bei dem die meisten Bits übereinstimmen (Longest-Prefix-Matching). Führen sie die IP-Vermittlung für folgende IP-Zieladressen durch:

Netz-Präfix	Netz-Maske	Nächster Hop
128.96.170.0	255.255.254.0 /23	Interface 0
128.96.168.0	255.255.252.0 /22	Interface 1
128.96.166.0	255.255.254.0 /23	R2
128.96.164.0	255.255.252.0 /22	R3
default		R4


- a) 128.96.171.92
- b) 128.96.167.151
- c) 128.96.163.151
- d) 128.96.165.121

Netzwerkmasken	Byte 1	Byte 2	128	64	32	16	8	4	2	1	Byte 4
255.255.254.0	11111111.	11111111.	1	1	1	1	1	1	1	0	.00000000
255.255.252.0	11111111.	11111111.	1	1	1	1	1	1	0	0	.00000000
Netz-Präfixe											
128.96.170.0	128.	96.	1	0	1	0	1	0	1	0	.0
128.96.168.0	128.	96.	1	0	1	0	1	0	0	0	.0
128.96.166.0	128.	96.	1	0	1	0	0	1	1	0	.0
128.96.164.0	128.	96.	1	0	1	0	0	1	0	0	.0
IP-Adressen											
a) 128.96.171.92	128.	96.	1	0	1	0	1	0	1	1	.92
b) 128.96.167.151	128.	96.	1	0	1	0	0	1	1	1	.151
c) 128.96.163.151	128.	96.	1	0	1	0	0	0	1	1	.151
d) 128.96.165.121	128.	96.	1	0	1	0	0	1	0	1	.121

2a)

a) 128.96.171.92

IP ^ Netzmaske	Byte1	Byte2	128	64	32	16	8	4	2	1	Byte 4	Netz-Präfix	Näch. Hop
128.96.171.92 ^ 255.255.254.0	128.	96.	1	0	1	0	1	0	1	0	.0	128.96.170.0	IF 0
128.96.171.92 ^ 255.255.252.0	128.	96.	1	0	1	0	1	0	0	0	.0	128.96.168.0	



Netz-Präfix	Netz-Maske	Nächster Hop
128.96.170.0	255.255.254.0 /23	Interface 0
128.96.168.0	255.255.252.0 /22	Interface 1
128.96.166.0	255.255.254.0 /23	R2
128.96.164.0	255.255.252.0 /22	R3
default		R4

2b)

b) 128.96.167.151

IP ^ Netzmaske	Byte1	Byte2	128	64	32	16	8	4	2	1	Byte 4	Netz-Präfix	Näch. Hop
128.96.167.151 ^ 255.255.254.0	128.	96.	1	0	1	0	0	1	1	0	.0	128.96.166.0	R2
128.96.167.151 ^ 255.255.252.0	128.	96.	1	0	1	0	0	1	0	0	.0	128.96.164.0	

Netz-Präfix	Netz-Maske	Nächster Hop
128.96.170.0	255.255.254.0 /23	Interface 0
128.96.168.0	255.255.252.0 /22	Interface 1
→ 128.96.166.0	255.255.254.0 /23	R2
128.96.164.0	255.255.252.0 /22	R3
default		R4

2c)

c) 128.96.163.151


IP ^ Netzmaske	Byte1	Byte2	128	64	32	16	8	4	2	1	Byte 4	Netz-Präfix	Näch. Hop
128.96.163.151 ^ 255.255.254.0	128.	96.	1	0	1	0	0	0	1	0	.0	128.96.162.0	R4 (default)
128.96.163.151 ^ 255.255.252.0	128.	96.	1	0	1	0	0	0	0	0	.0	128.96.160.0	R4 (default)

Netz-Präfix	Netz-Maske	Nächster Hop
128.96.170.0	255.255.254.0 /23	Interface 0
128.96.168.0	255.255.252.0 /22	Interface 1
128.96.166.0	255.255.254.0 /23	R2
128.96.164.0	255.255.252.0 /22	R3
→ default		R4

2d)

d) 128.96.165.121

IP ^ Netzmaske	Byte1	Byte2	128	64	32	16	8	4	2	1	Byte 4	Netz-Präfix	Näch. Hop
128.96.165.121 ^ 255.255.254.0	128.	96.	1	0	1	0	0	1	0	0	.0	128.96.164.0	R3
128.96.165.121 ^ 255.255.252.0	128.	96.	1	0	1	0	0	1	0	0	.0	128.96.164.0	R3

Netz-Präfix	Netz-Maske	Nächster Hop
128.96.170.0	255.255.254.0 /23	Interface 0
128.96.168.0	255.255.252.0 /22	Interface 1
128.96.166.0	255.255.254.0 /23	R2
 128.96.164.0	255.255.252.0 /22	R3
default		R4

Ein Host A sendet einem Host B alle 20 ms ein Datagramm, welches ein TCP-Segment der Größe 40 Bytes enthält. Wenn Host B das Datagramm erhält, wie weiß das Network-Layer in Host B, dass die Payload an TCP weitergeleitet werden muss und nicht an UDP? Wie groß ist der Overhead auf dem Network-Layer?

- TCP Overhead 20 Bytes
- 8-Bit Protokoll Feld enthält Protokollnummer zur Identifikation des Transportschichtprotokolls

0	4	8	16	19	31
Version	Header- Length	DS	ECN	Total-Length (in bytes)	
16 Bit - Identification			Flags	13-Bit-Fragment offset	
Time-to-live (TTL)		Protocol		Header - checksum	
32-Bit – IP – source address					
32-Bit – IP – destination address					
Options (0 to 40 bytes)					
Payload					

Ein TCP-Segment inklusive des TCP-Headers ist 2436 Byte lang und soll mittels des IP-Protokolls über 2 Netzwerke zum Ziel-Host vermittelt werden. Es wird angenommen, dass der IP-Header keine Optionen enthält.

- a) Das erste Netzwerk besitzt eine MTU = 1188 Byte, das zweite eine MTU = 576 Byte. Geben Sie die Größen und den Offset aller Fragmente in den beiden Netzen an. Zeigen Sie die Defragmentierung im Ziel-Host.
- b) Mittels einer path-MTU Discovery-Prozedur erfährt der Quell-Host, dass die path-MTU 576 Byte beträgt. Geben Sie die Größen und Anzahl der Fragmente für diesen Fall an.
- c) Warum wird der Fragment-Offset in Vielfachen von 8 Byte angegeben

- a) Das erste Netzwerk besitzt eine MTU = 1188 Byte, das zweite eine MTU = 576 Byte. Geben Sie die Größen und den Offset aller Fragmente in den beiden Netzen an. Zeigen Sie die Defragmentierung im Ziel-Host.

Nutzdaten von 2436 Byte werden in N Fragmente aufgeteilt

Netz 1:

MTU1 = 1188 Byte

→ 1188 Byte – 20 Byte IP-Header = 1168 Byte für Nutzdaten je
Fragment

Offset: $1168 / 8 = 146$

→ maximale Nutzdatenlänge Vielfaches von 8

- a) Das erste Netzwerk besitzt eine MTU = 1188 Byte, das zweite eine MTU = 576 Byte. Geben Sie die Größen und den Offset aller Fragmente in den beiden Netzen an. Zeigen Sie die Defragmentierung im Ziel-Host.

Fragmente im Netz1			Fragmente im Netz2		
Nutzdaten	Offset	Fragmentlänge	Nutzdaten	Offset	Fragmentlänge
1168 Byte	0	1188 Byte			
1168 Byte	$1168/8=146$	1188 Byte			
100 Byte	$2336/8=292$	120 Byte			

- a) Das erste Netzwerk besitzt eine MTU = 1188 Byte, das zweite eine MTU = 576 Byte. Geben Sie die Größen und den Offset aller Fragmente in den beiden Netzen an. Zeigen Sie die Defragmentierung im Ziel-Host.

Netz 2:

MTU2 = 576 Byte

→ 576 Byte – 20 Byte IP-Header = 556 Byte für Nutzdaten je
Fragment

Offset: $556 / 8 = 69,5$

→ maximale Nutzdatenlänge nicht Vielfaches von 8

→ maximal $8 * 69 = 552$ Byte Nutzdaten in den Fragmenten 1,...,N-1

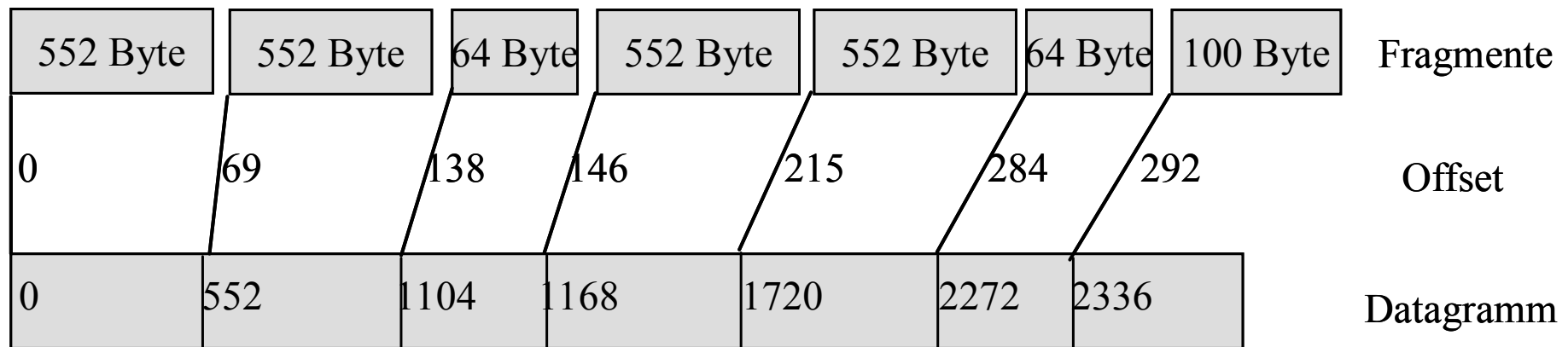
→ maximal 556 Byte im letzten Fragment

- a) Das erste Netzwerk besitzt eine MTU = 1188 Byte, das zweite eine MTU = 576 Byte. Geben Sie die Größen und den Offset aller Fragmente in den beiden Netzen an. Zeigen Sie die Defragmentierung im Ziel-Host.

Fragmente im Netz1			Fragmente im Netz2		
Nutzdaten	Offset	Fragmentlänge	Nutzdaten	Offset	Fragmentlänge
1168 Byte	0	1188 Byte	552 Byte	0	572 Byte
			552 Byte	$522/8 = 69$	572 Byte
			64 Byte	$1104/8 = 138$	84 Byte
1168 Byte	$1168/8 = 146$	1188 Byte	552 Byte	$1168/8 = 146$	572 Byte
			552 Byte	215	572 Byte
			64 Byte	284	84 Byte
100 Byte	$2336/8 = 292$	120 Byte	100 Byte	292	120 Byte

- a) Das erste Netzwerk besitzt eine MTU = 1188 Byte, das zweite eine MTU = 576 Byte. Geben Sie die Größen und den Offset aller Fragmente in den beiden Netzen an. Zeigen Sie die Defragmentierung im Ziel-Host.

Defragmentierung im Ziel-Host:



- b) Mittels einer path-MTU Discovery Prozedur erfährt der Quell-Host, dass die path-MTU 576 Byte beträgt. Geben Sie die Größen und Anzahl der Fragmente für diesen Fall an.

Path-MTU = 576 Byte

→ maximal $8 * 69 = 522$ Byte Nutzdaten pro Fragment

→ $2436 \text{ Byte} = 4 * 522 \text{ Byte} + 228 \text{ Byte}$

→ Anzahl der Fragmente: 5

- c) Warum wird der Fragment-Offset in Vielfachen von 8 Byte angegeben?

Maximale Länge der Nutzdaten eines Datagramms:

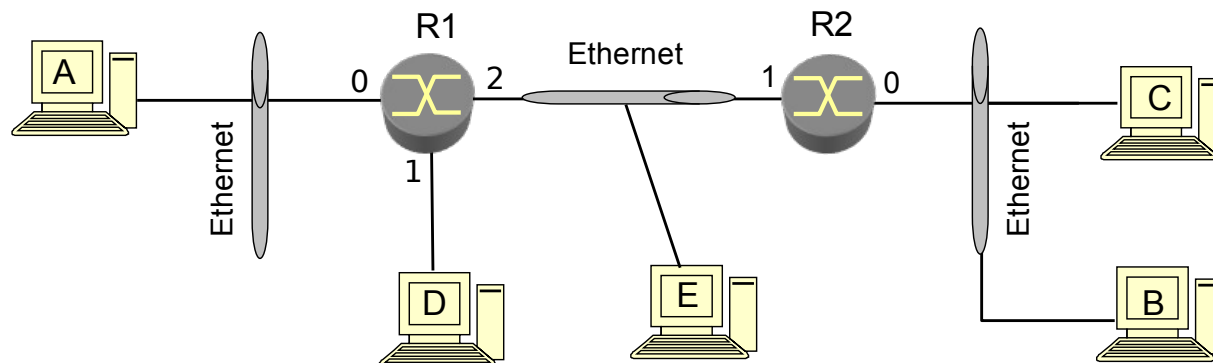
$$(2^{16} - 1) \text{ Byte} - 20 \text{ Byte Header} = (65535 - 20) \text{ Byte} = 65515 \text{ Byte}$$

Offset-Feld hat 13 Bit:

$$\begin{aligned} \rightarrow \text{maximaler Wert des Offsets ist: } (2^{13} - 1) * 8 \text{ Byte} &= 8191 * 8 \text{ Byte} \\ &= 65528 \text{ Byte} \end{aligned}$$

Da der Offset ein Vielfaches von 8 Byte darstellt, lässt sich mit einem 13 Bit Feld der Offset für ein Datagramm maximaler Länge angeben, falls dieses in Fragmente zerlegt wird.

Der gezeigte Netzausschnitt umfasst 2 Router und 5 Hosts (PCs), die über Ethernet-Segmente (R1, R2, sowie Hosts A, B, C und E) oder direkt (Host D) gekoppelt sind.



Die Adresszuordnung auf der Ethernet-Layer (MAC Adressen) und der Network-Layer (IP-Adressen) zeigen die folgenden Tabellen.

Router 1		
IF	MAC Adresse	IP-Adresse
0	00.1c.58.bb.4c.d7	194.168.59.4
1	00.1c.58.bb.4c.d8	194.168.6.27
2	00.1c.58.bb.4c.d9	194.168.70.9

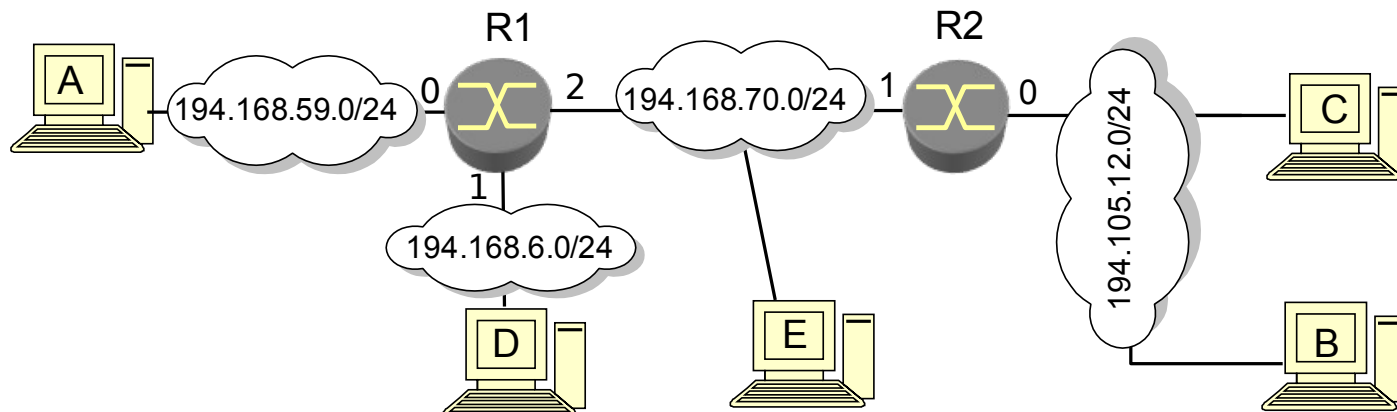
Router 2		
IF	MAC Adresse	IP-Adresse
0	00.1d.46.f1.dd.b0	194.105.12.250
1	00.1d.46.f1.dd.b1	194.168.70.72

Host	MAC Adresse	IP-Adresse
A	00.1f.58.de.a1.c1	194.168.59.1
B	00.1f.58.de.a2.c2	194.105.12.2
C	00.1f.58.bb.a3.c3	194.105.12.1
D	00.1f.58.bb.a4.c4	194.168.6.1
E	00.1f.58.bb.a5.c5	194.168.70.1

Die logische Darstellung der IP-Netzwerkstruktur auf der Network-Layer und die Forwarding Tabellen in den Routern und in Host A zeigt das folgende Diagramm.

Forwarding Table in Router 1		
Prefix	next Router	IF
194.168.59.0/24	direct	0
194.168.6.0/24	direct	1
194.168.70.0/24	direct	2
194.105.12.0/24	194.168.70.72	2
default	194.168.70.72	2

Forwarding Table in Router 2		
Prefix	next Router	IF
194.105.12.0/24	direct	0
194.168.70.0/24	direct	1
194.168.6.0/24	194.168.70.9	1
194.168.59.0/24	194.168.70.9	1
default	194.168.70.9	0



Forwarding Table in Host A		
Prefix	next Router	IF
194.168.59.0/24	direct	0
default	194.168.59.4	0

Die Layer 2 Informationen einiger Netzelemente ist in folgenden ARP-Tabellen dargestellt.

ARP - Cache im Router 1	
IP-Adresse	L2 MAC Adresse
194.168.59.1	00.1f.58.de.a1.c1
194.168.6.1	00.1f.58.bb.a4.c4
194.168.70.72	00.1d.46.f1.dd.b1

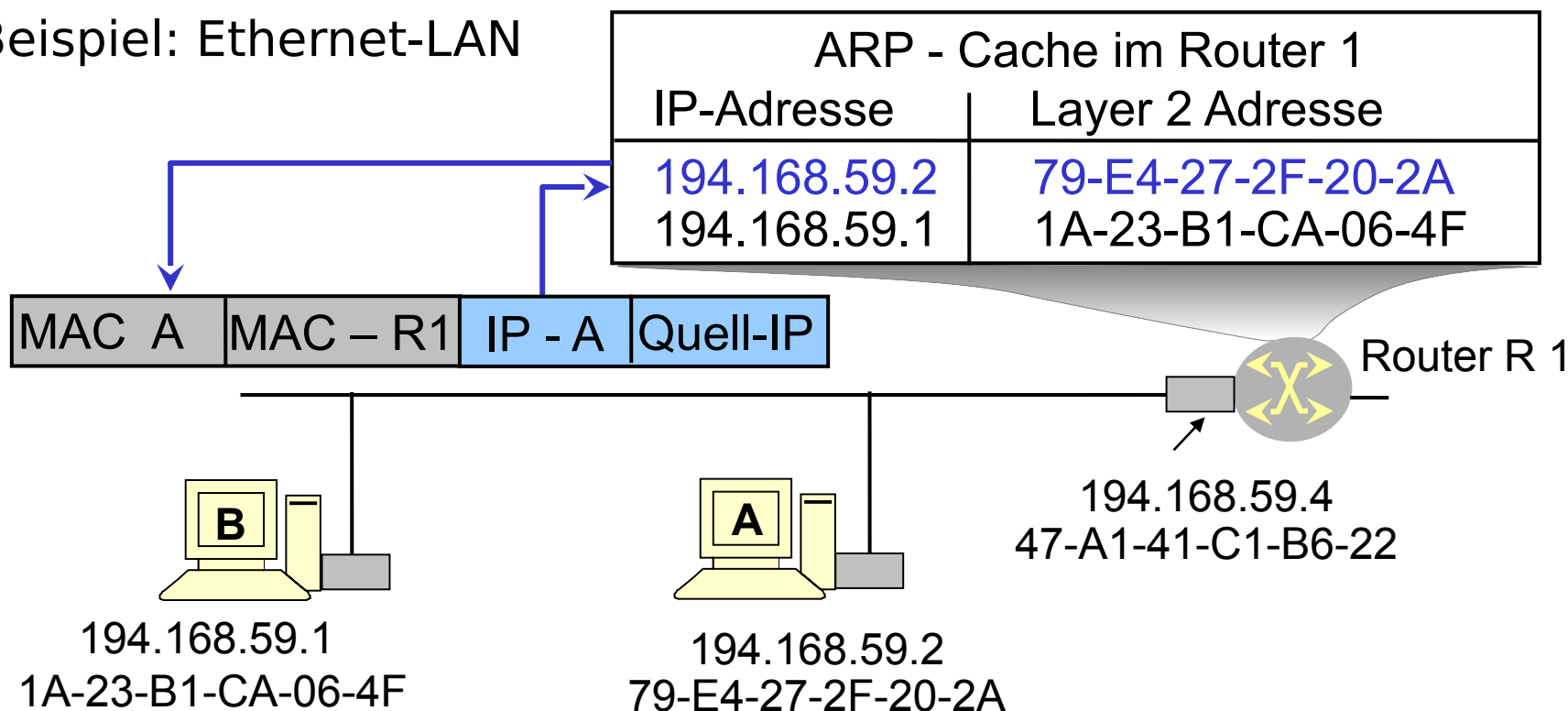
ARP - Cache im Router 2	
IP-Adresse	L2 MAC Adresse
194.168.70.9	00.1c.58.bb.4c.d9
194.168.70.1	00.1f.58.bb.a5.c5
194.105.12.1	00.1f.58.de.a3.c3

ARP - Cache im Host A	
IP-Adresse	L2 MAC Adresse
194.168.59.4	00.1c.58.bb.4c.d7

Es soll ein Datagramm von Host A zum Zielhost B gesendet werden. Zeigen und erläutern Sie das abschnittsweise Forwarding der Datagramme unter Angabe der Ethernet-MAC- und der IP-Datagramm-Header.

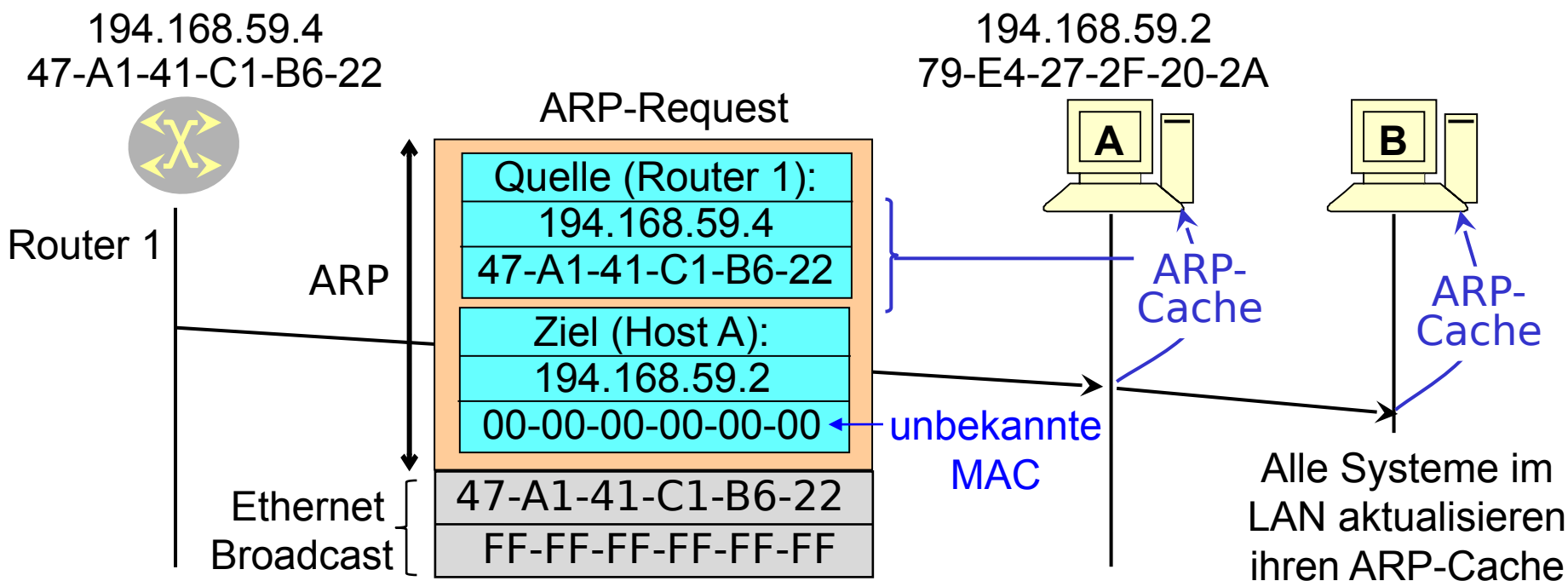
- Der ARP – Cache (Adressumsetztabelle) liefert die Zuordnung
IP-Adresse => Layer-2 Hardware-Adresse
 - ARP - Cache wird automatisch durch das ARP - Protokoll erstellt
 - Einträge werden nach einem Zeitintervall gelöscht

- Beispiel: Ethernet-LAN

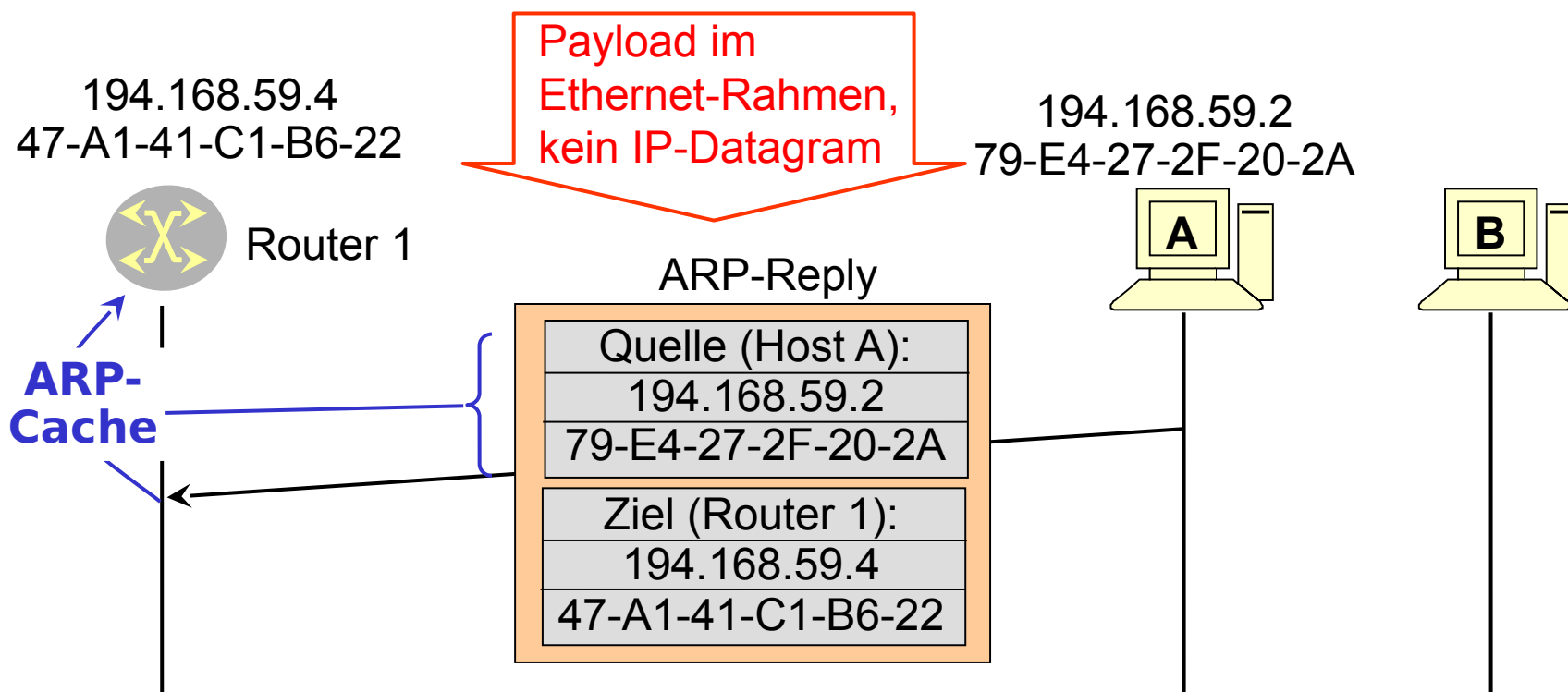


Problem: MAC Adresse von Host A nicht im ARP - Cache vorhanden

- Router 1 sendet *ARP-Request* per LAN- Broadcast an alle LAN- Systeme
„Wie lautet die HW-Adresse von Host A“
- Host A erkennt seine eigene IP-Adresse im *ARP-Request*
 - Quelle IP-Adresse => Quelle HW-Adresse* in ARP – Cache Host A



- Host A schickt dem Router 1 ein *ARP-Reply*
 - Dieses enthält seine IP und Layer 2 Hardware– Adresse
- Router 1 kopiert aus dem *ARP-Reply* die Zuordnung
 - *Quelle IP-Adresse => Quelle HW-Adresse* in ARP – Cache Router 1



Datagramm von **Host A** (194.168.59.1) zum Zielhost B (194.105.12.2)

I) Zielnetzwerk in FT ermitteln

194.105.12.2/24 \Leftrightarrow 194.105.12.0 \rightarrow kein Match

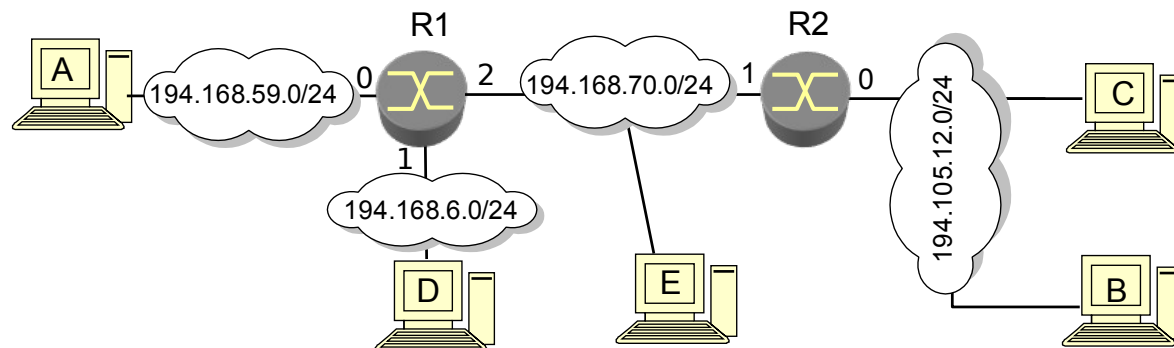
\rightarrow Default Eintrag wählen

GW 194.168.59.4 über Interface 0

Prefix	next Router	IF
194.168.59.0/24	direct	0
default	194.168.59.4	0

Prefix	next Router	IF
194.168.59.0/24	direct	0
194.168.6.0/24	direct	1
194.168.70.0/24	direct	2
194.105.12.0/24	194.168.70.72	2
default	194.168.70.72	2

Prefix	next Router	IF
194.105.12.0/24	direct	0
194.168.70.0/24	direct	1
194.168.6.0/24	194.168.70.9	1
194.168.59.0/24	194.168.70.9	1
default	194.168.70.9	0



Prefix	next Router	IF
194.168.59.0/24	direct	0
default	194.168.59.4	0

Datagramm von **Host A** (194.168.59.1) zum Zielhost B (194.105.12.2)

I) Zielnetzwerk in FT ermitteln

194.105.12.2/24 \Leftrightarrow 194.105.12.0 \rightarrow kein Match

\rightarrow Default Eintrag wählen

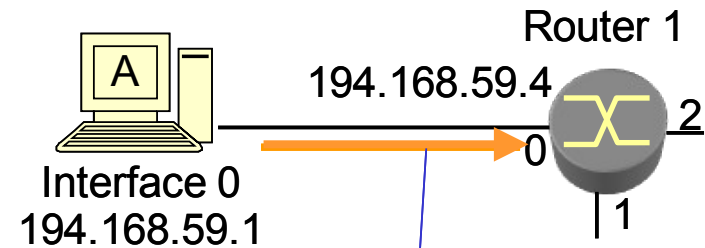
GW 194.168.59.4 über Interface 0

Forwarding Table (FT) in Host A		
Prefix	next Router	IF
194.168.59.0/24	direct	0
\rightarrow default	\rightarrow 194.168.59.4	0

II) Layer 2 Adresse (MAC) von GW (R1) ermitteln

- Eintrag in ARP-Tabelle für GW-IP verwenden

ARP - Cache im Host A	
IP-Adresse	L2 MAC Adresse
\rightarrow 194.168.59.4	00.1c.58.bb.4c.d7



Ziel-MAC	00.1c.58.bb.4c.d7
Quell-MAC	00.1f.58.de.a1.c1
Ziel-IP	194.105.12.2
Quell-IP	194.168.59.1
data	

III) Datagramm über Data-Link Layer an R1

- Layer 2 Ziel-Adresse (MAC) von R1 / IF0
- MAC-Quell-Adresse von Host A
- Ziel-IP-Adresse von Host B
- Quell-IP-Adresse von Host A

Host	MAC Adresse	IP-Adresse
\rightarrow A	00.1f.58.de.a1.c1	194.168.59.1

Datagramm von Host A mit Ziel 194.105.12.2 ist im **Router 1**

I) Zielnetzwerk in FT ermitteln

194.105.12.2/24 \Leftrightarrow 194.105.12.0 \rightarrow Match

GW 194.168.70.72 über Interface 2

Prefix	next Router	IF
194.168.59.0/24	direct	0
194.168.6.0/24	direct	1
194.168.70.0/24	direct	2
194.105.12.0/24	194.168.70.72	2
default	194.168.70.72	2

II) MAC Adresse von GW (R2) ermitteln

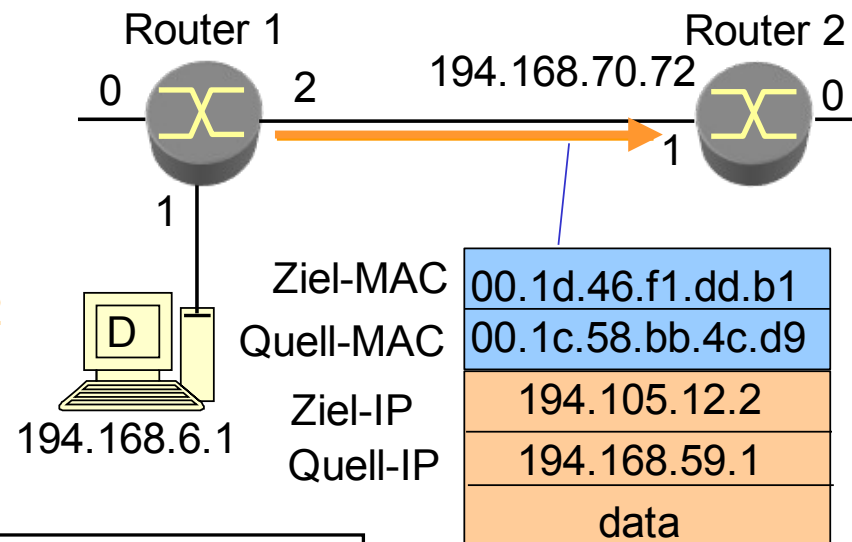
- Eintrag in ARP-Tabelle für GW-IP verwenden

IP-Adresse	L2 MAC Adresse
194.168.59.1	00.1f.58.de.a1.c1
194.168.6.1	00.1f.58.bb.a4.c4
194.168.70.72	00.1d.46.f1.dd.b1



III) Datagramm über Layer 2 von R1 an R2 senden.

- MAC-Ziel-Adresse von R2 / IF1
- MAC-Quell-Adresse von R1 / IF2
- IP-Ziel-Adresse von Host B



IF	MAC Adresse	IP-Adresse
2	00.1c.58.bb.4c.d9	194.168.70.9



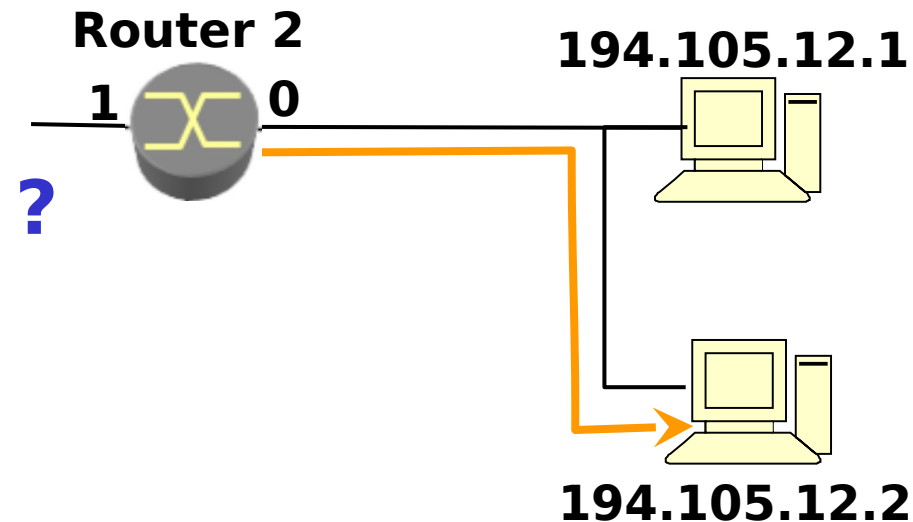
Datagramm von Host A mit Ziel 194.105.12.2 ist im **Router 2**

1) Zielnetzwerk in FT ermitteln

194.105.12.2/24 \Leftrightarrow 194.105.12.0 \rightarrow Match
angeschlossenes LAN über Interface 0

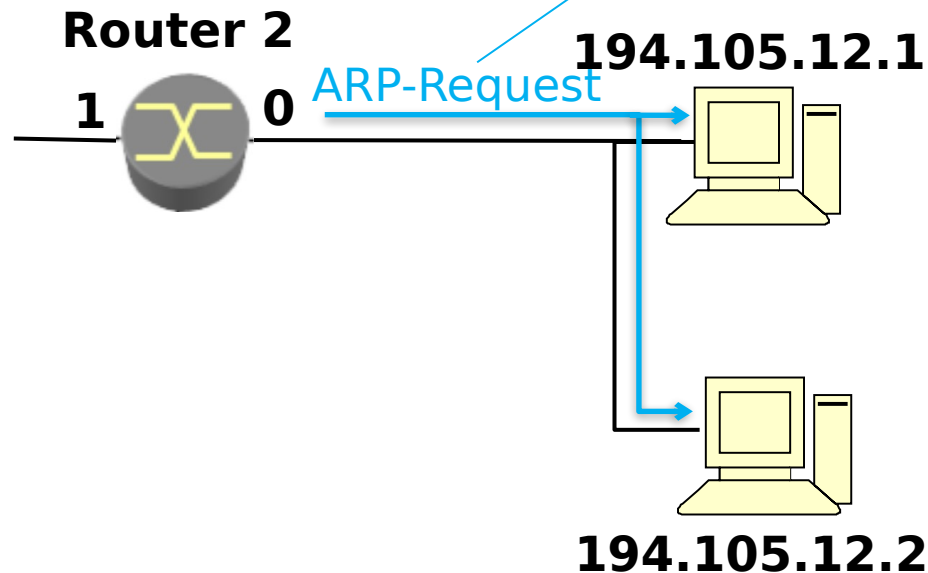
Forwarding Table in Router 2		
Prefix	next Router	IF
194.105.12.0/24	direct	0
194.168.70.0/24	direct	1
194.168.6.0/24	194.168.70.9	1
194.168.59.0/24	194.168.70.9	1
default	194.168.70.9	0

ARP - Cache im Router 2	
IP-Adresse	L2 MAC Adresse
194.168.70.9	00.1c.58.bb.4c.d9
194.168.70.1	00.1f.58.bb.a5.c5
194.105.12.1	00.1f.58.de.a3.c3



II) MAC Adresse von Ziel-IP ermitteln

- Kein Eintrag in ARP-Tab. für Ziel-IP vorhanden
- Zuordnung Ziel-IP <-> MAC mittels **ARP Protokoll** ermitteln

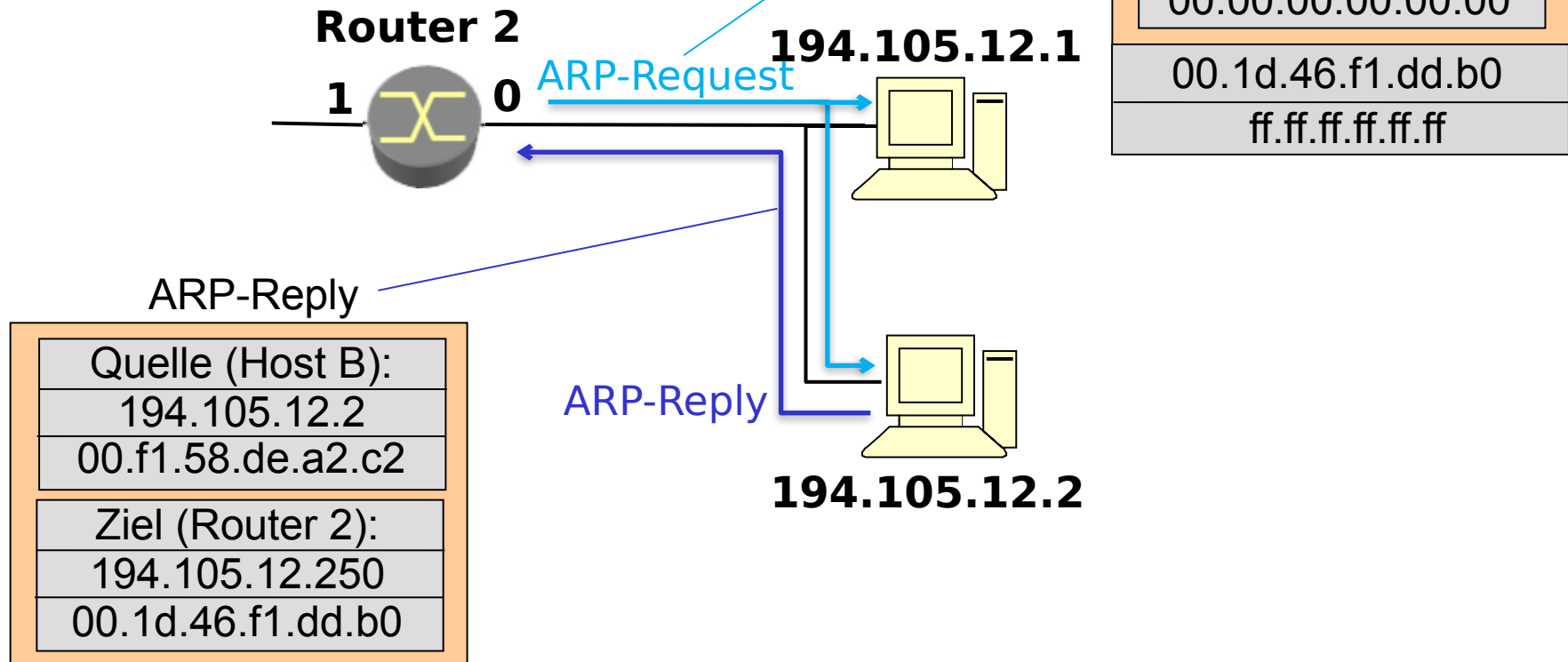


ARP-Request

Quelle (Router 2):
194.105.12.250
00.1d.46.f1.dd.b0
Ziel (Host B):
194.105.12.2
00.00.00.00.00.00
00.1d.46.f1.dd.b0
ff.ff.ff.ff.ff.ff

II) MAC Adresse von Ziel-IP ermitteln

- Kein Eintrag in ARP-Tab. für Ziel-IP vorhanden
- Zuordnung Ziel-IP <-> MAC mittels **ARP Protokoll** ermitteln



Datagramm von Host A mit Ziel 194.105.12.2 ist im **Router 2**

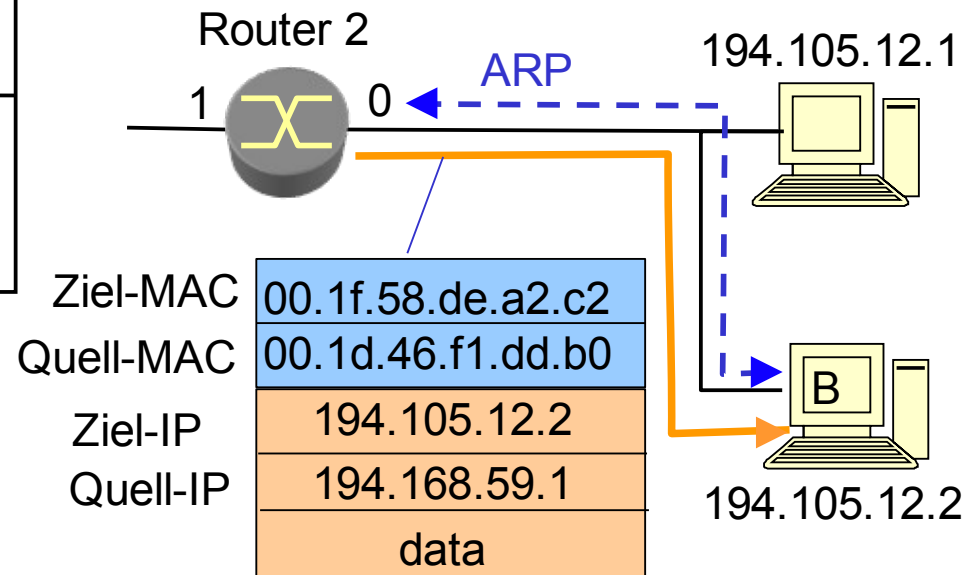
I) Zielnetzwerk in FT ermitteln

194.105.12.2/24 \Leftrightarrow 194.105.12.0 \rightarrow Match
angeschlossenes LAN über Interface 0

Forwarding Table in Router 2		
Prefix	next Router	IF
194.105.12.0/24	direct	0
194.168.70.0/24	direct	1
194.168.6.0/24	194.168.70.9	1
194.168.59.0/24	194.168.70.9	1
default	194.168.70.9	0

ARP - Cache im Router 2	
IP-Adresse	L2 MAC Adresse
194.168.70.9	00.1c.58.bb.4c.d9
194.168.70.1	00.1f.58.bb.a5.c5
194.105.12.1	00.1f.58.de.a3.c3
194.105.12.2	00.1f.58.de.a2.c2

ARP



III) Datagramm über Layer 2 von R2 an Host B senden.

- MAC-Ziel-Adresse von Host B
- MAC-Quell-Adresse von R2 / IF0
- IP-Ziel-Adresse von Host B