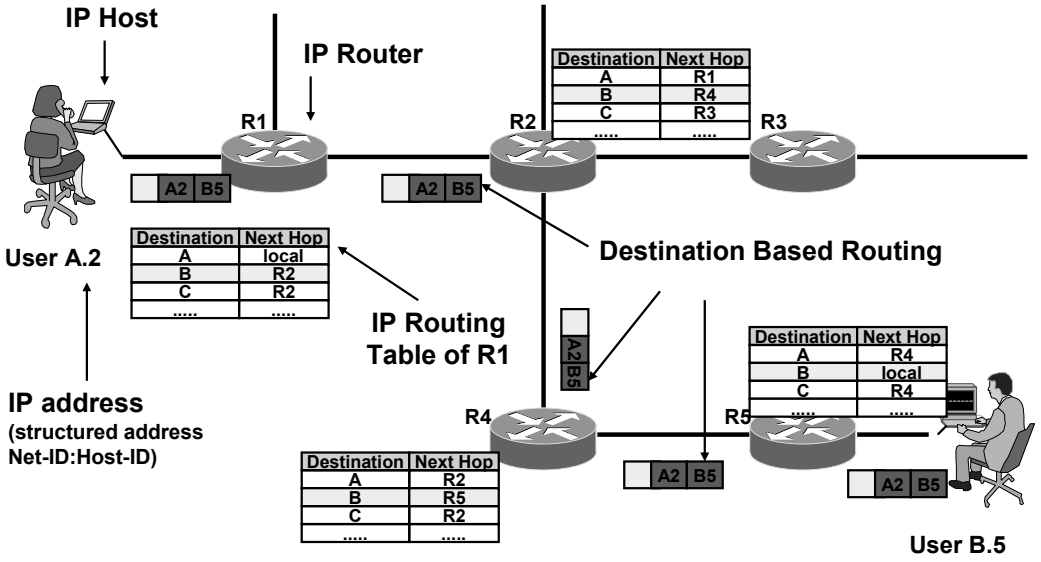
Address Resolution

ARP, RARP, Proxy ARP

Agenda

- IP Forwarding Principle
- Address Resolution Protocol (ARP)
  - IP Routing Basics
  - IP Forwarding and ARP
- RARP
- Proxy ARP
- ICMP
  - IP Forwarding and ICMP

IP Datagram Service



2005/03/11 3

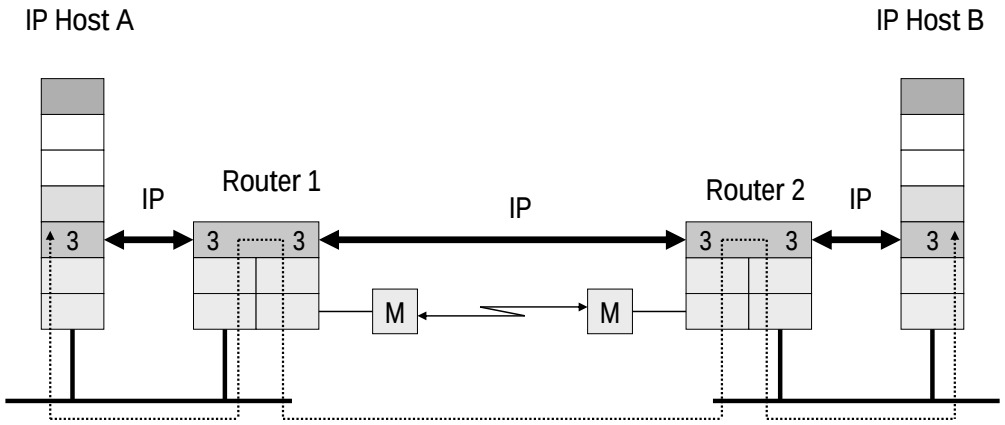
In the Datagram technology user A.2 sends out data packets destined for the user B.5. Each single datagram holds the information about sender and receiver address.

The datagram forwarding devices in our example routers hold a routing table in memory. In the routing table we find a correlation between the destination address of a data packet and the corresponding outgoing interface as well as the next hop router. So data packets are forwarded through the network on a hop by hop basis.

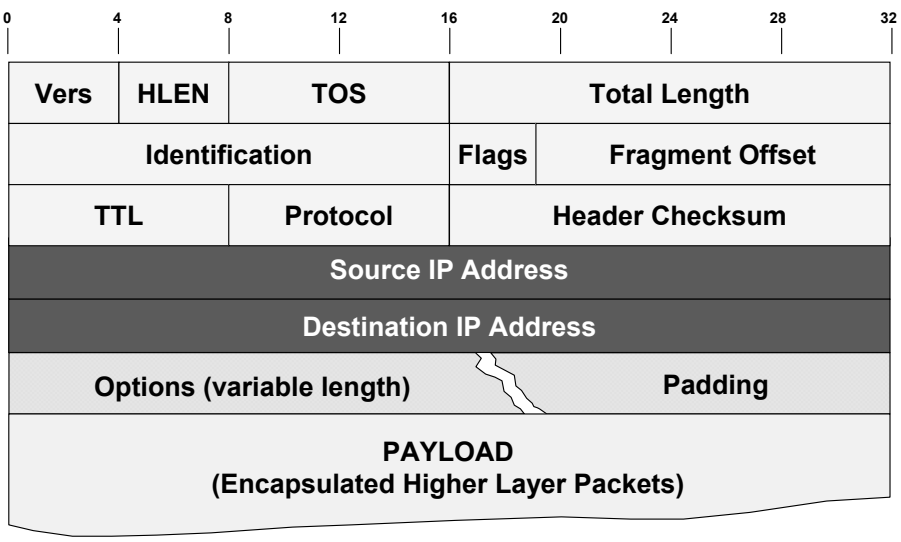
The routing tables can be set up either by manual configuration of the administrator or by the help of dynamic routing protocols like RIP, OSPF, IS-IS, etc. The use of dynamic routing protocols may lead to rerouting decisions in case of network failure and so packet overtaking may happen in these systems.

IP and OSI Network Layer 3

Layer 3 Protocol = IP
Layer 3 Routing Protocols = RIP, OSPF, EIGRP, BGP



The IP Header (Address Fields)



The IP header consists of the following fields:

Version (Vers): 4 Bits. This Header describe IP Version 4.

Header Length (HLEN): 4 Bits.

Type of Service (TOS): 8 Bits. TOS is a parameter, who describe the quality of transmission of the datagram through a particular network.

Total Length: 16 Bits. Is the length of the datagram including header and data.

Identifcation: 16 Bits. See Page 37.

Flags: 3 Bits. See Page 37.

Fragment Offset: 13 Bits. See Page 38.

Time to Live (TTL): 8 Bits. This field indicates the maximum time the datagram is allowed to remain in the system. The datagram must be destroyed, if the field contains the value zero.

Protocol: 8 Bits. Describe what protocol is used in the next level.

Header Checksum: 16 Bits. A Checksum for the Header only.

Source IP Address: 32 Bits.

Destination IP Address: 32 Bits.

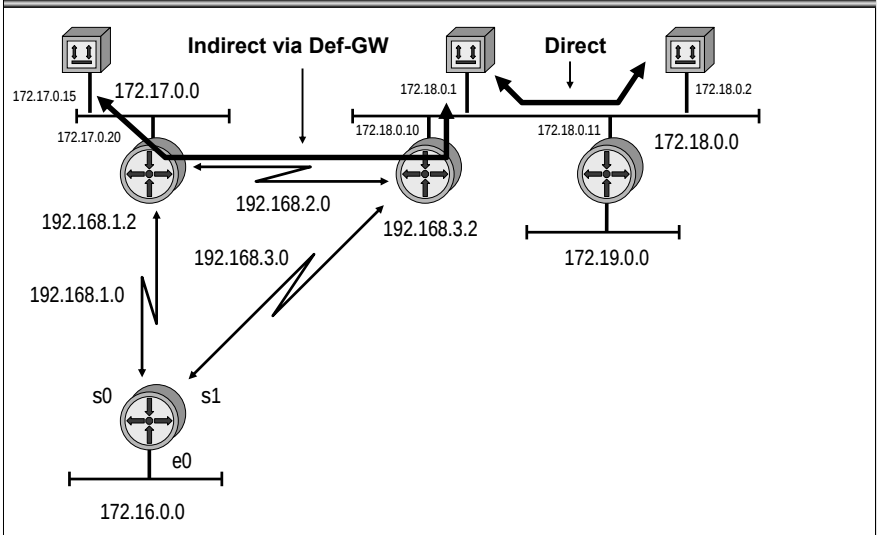
Options: Variable length. The Option field can be used for security or routing information's.

Padding: Variable length. Its only used that the Internet header ends on a 32 Bit boundary.

Routing Differences

- Routing = finding a path to a destination address
- Direct delivery performed by host
  - Destination network = local network
- Indirect delivery performed by router
  - Destination network ≠ local network
  - Packet is forwarded to default gateway

Direct versus Indirect Delivery



Why Adress Resolution?

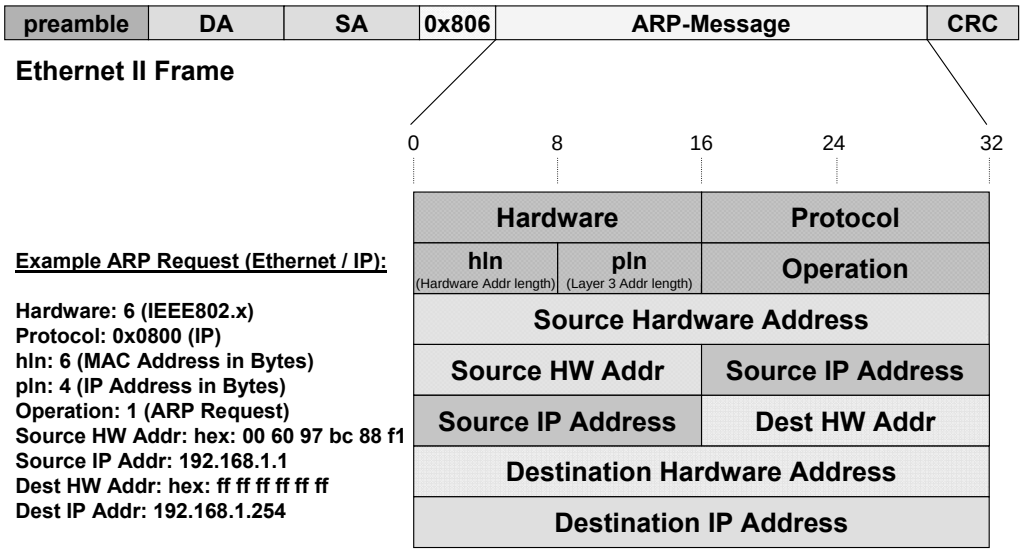
- On a multipoint network every station needs a layer-2 address
- When IP packets should be sent to a local destination the sender must first determine the corresponding layer-2 address
- The layer-2 address could be a MAC address, a DLCI (Frame-Relay) or similar
  - In this chapter we only focus on Ethernet

A multipoint network is also known as a shared medium. It could be a broadcast domain (like Ethernet) or not (like Frame-Relay or ATM).

Direct Delivery

- IP host checks if packet's destination network is identical with local network
  - By applying the configured subnet mask of the host's interface
- If destination network = local network then the L2 address of the destination is discovered using ARP
  - Remember: not necessary for point-to-point connections

ARP Format



ARP messages are carried within Ethernet II frames or SNAP encapsulation using type field 0x806.

Hardware: Defines the type of network hardware, e.g.:

1	Ethernet DIX
6	802.x-LAN
7	ARCNET
11	LocalTalk

Protocol: Identifies the layer 3 protocol (same values as for Ethertype, e.g. 0x800 for IP)

hln: Length of hardware address in bytes

pln: Length of layer 3 address in bytes

Operation

- 1 .... ARP Request
- 2 .... ARP Response
- 3 .... RARP Request
- 4 .... RARP Response

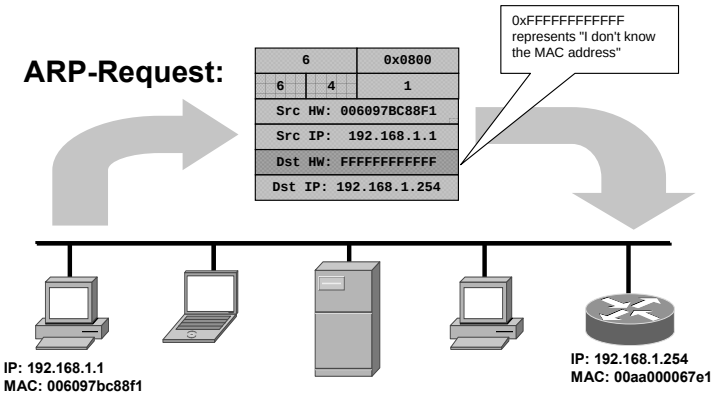
Addresses

- Hardware addresses: MAC addresses (src. and dest.).
- IP addresses: layer 3 addresses (src. and dest.).

ARP requ. / resp. are not forwarded by routers.

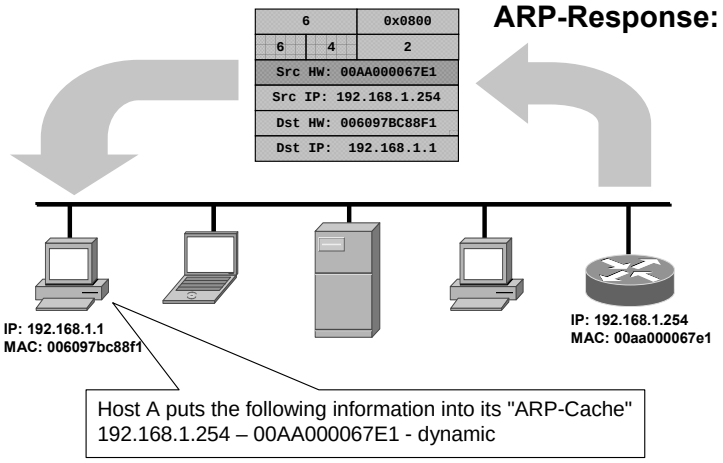
Direct Delivery

- **Sent as Broadcast**



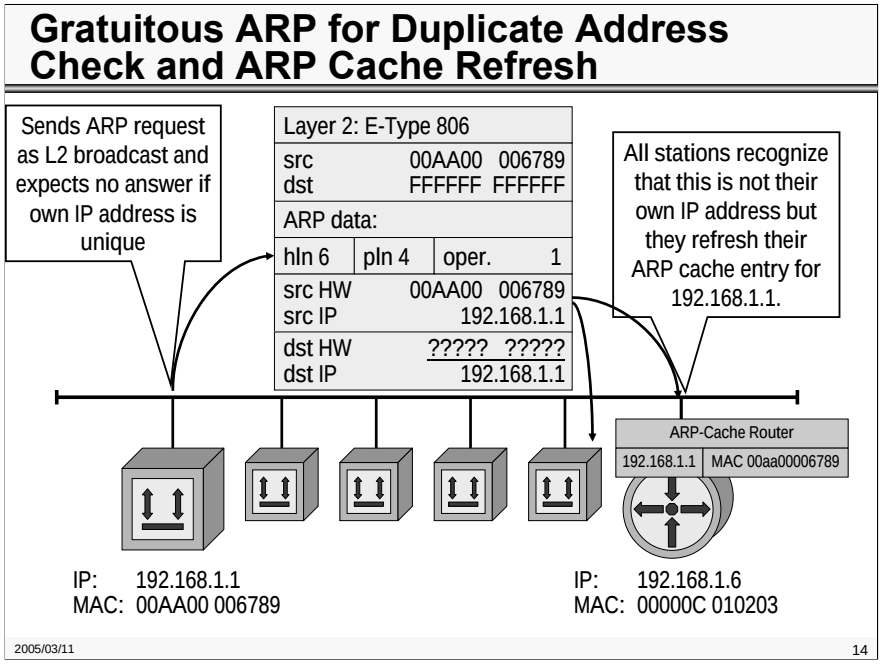
Direct Delivery

- **Response is unicast**



IP Host Facts

- Learned MAC addresses are stored in an ARP-cache
  - Aging timer: 20 minutes
- IP hosts have also routing tables !
  - But typically only a static route to the default gateway is entered
  - Default gateway for indirect delivery



gratuitous

Gratis, kostenlos, überflüssig, unnötig

Gratuitous ARP

Gratuitous ARP (engl. "gratis ARP") bezeichnet eine spezielle Verwendung von ARP. Dabei wird von einem Host ein ARP-Anforderungs-Broadcast gesendet, bei der er seine eigene IP-Adresse als Quell- und Ziel-IP-Adresse einträgt. Das kann zwei Zwecken dienen:

Normalerweise darf keine Antwort kommen, denn eine IP-Adresse muss in einem Netz eindeutig sein. Bekommt er trotzdem eine Antwort, ist das für den Administrator ein Hinweis darauf, dass ein Host nicht richtig konfiguriert ist.

Jeder Host aktualisiert seinen ARP-Cache. Das ist beispielsweise dann nützlich, wenn die Netzwerkkarte eines Rechners ausgetauscht wurde und die anderen Hosts über die neue MAC-Adresse informiert werden sollen. Gratuitous ARP geschieht deshalb normalerweise beim Booten eines Computers.

ARP Probleme

ARP ist für den Benutzer unsichtbar, so dass das Vorhandensein dieses Protokolls meist nur bemerkt wird, wenn seltene Fehler auftreten.

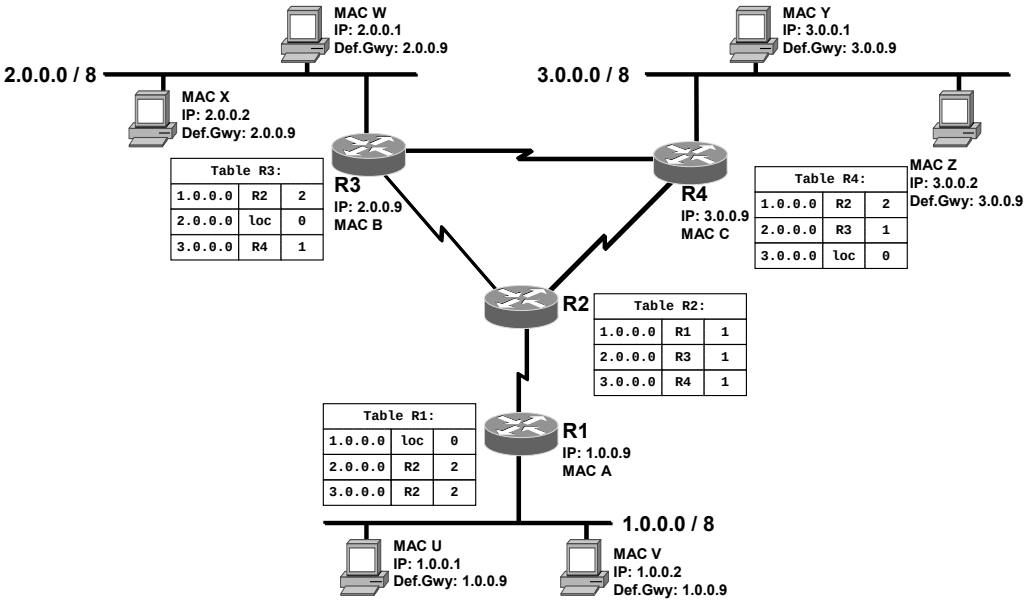
Die Länge der Gültigkeit eines ARP-Eintrags (normalerweise 20 Minuten) kann ein Problem darstellen, wenn falsche Einträge vorhanden sind. Solange ein fehlerhafter Eintrag existiert, kann mit dem betreffenden Host nicht kommuniziert werden. Die Fehlfunktion wird häufig nicht dem ARP-Protokoll zugeschrieben, sondern dem Netz oder einem Fehler in der Netzwerkimplementierung. Darüber hinaus ermöglicht nicht jedes Betriebssystem das Erzeugen eines korrigierten Eintrags oder einer Anforderung.

Gravierender ist das Eintragen von Daten in den ARP-Cache aus Paketen, für die keine Anforderung erzeugt wurde (blinder Glaube). Ein überlasteter Host, der eine alte IP-Adresse führt, antwortet mit großer Wahrscheinlichkeit als letzter auf eine ARP-Anforderung mit einer Antwort,

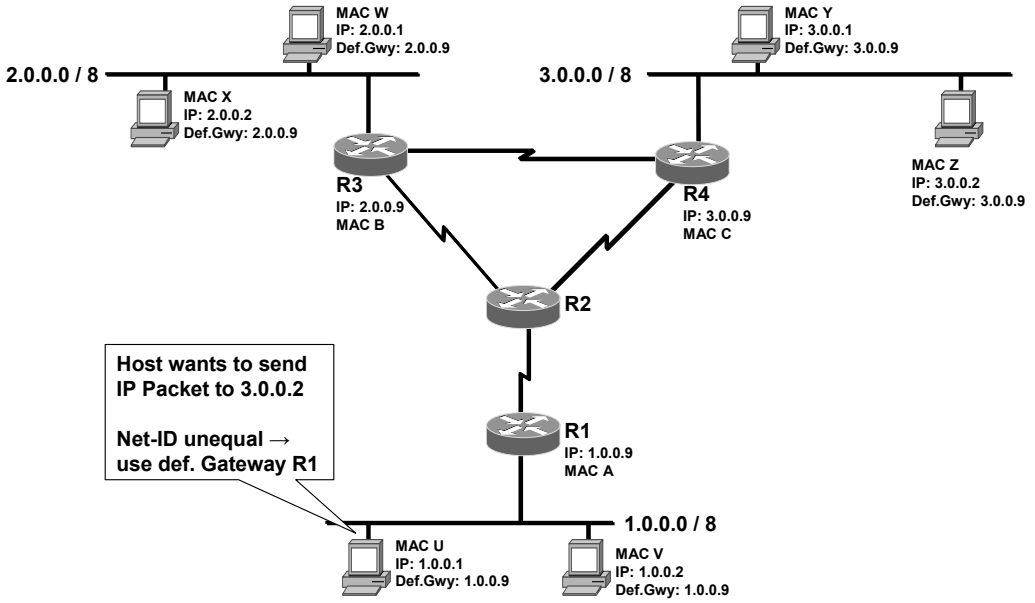
Using the Default Gateway

- Default gateway delivers packet in behalf of its host using a routing table
- Host must determine MAC address of default gateway using ARP
- IP datagram is handed over to default gateway

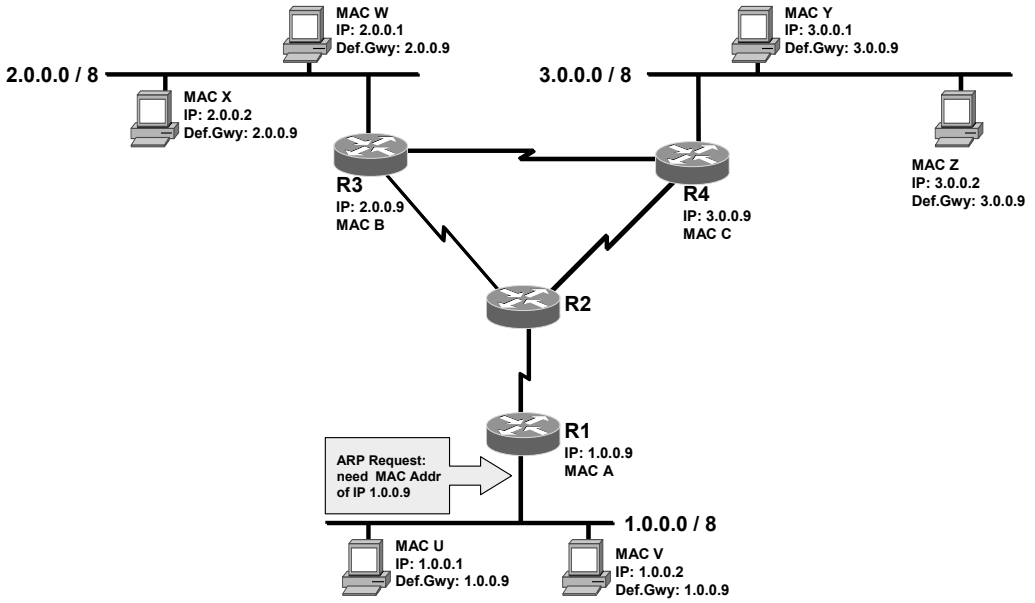
Indirect Delivery (1)



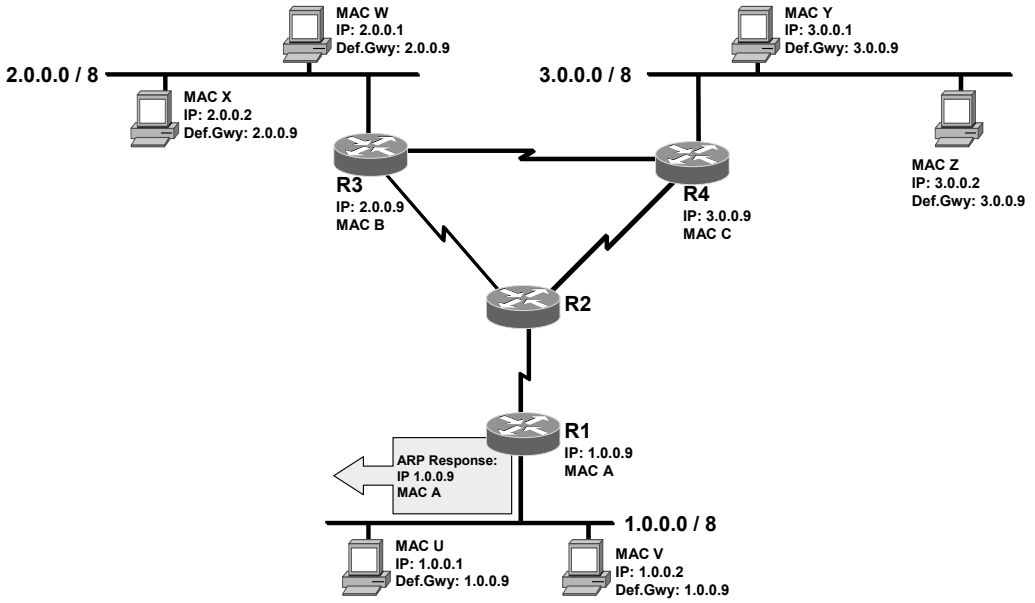
Indirect Delivery (2)



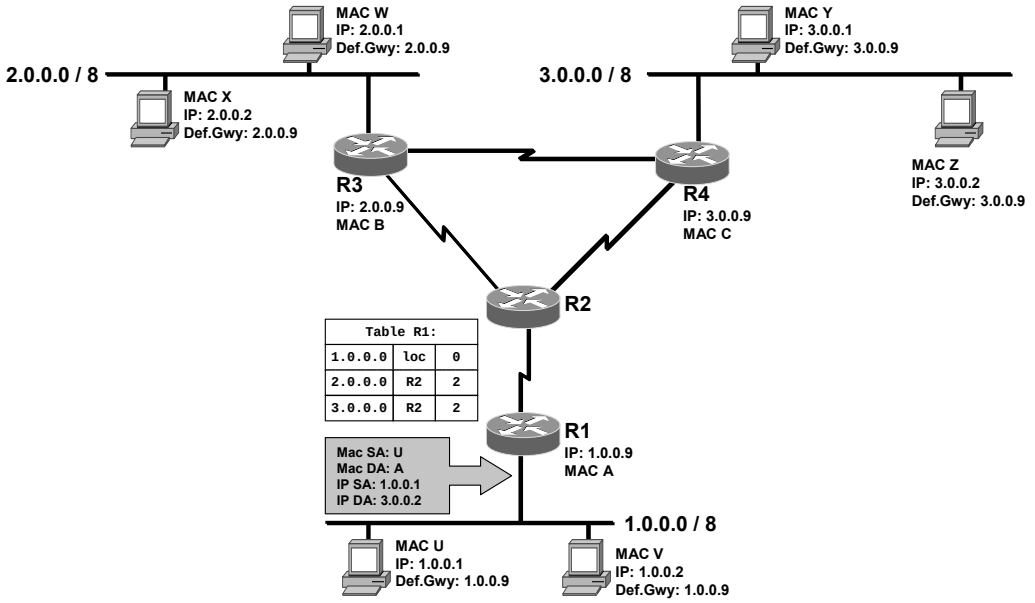
Indirect Delivery (3)



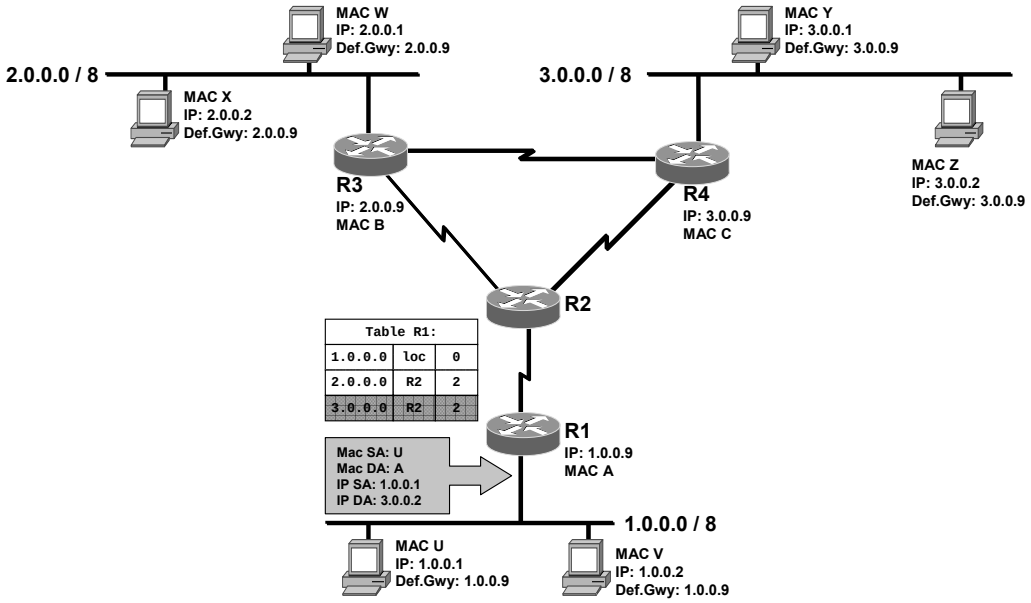
Indirect Delivery (4)



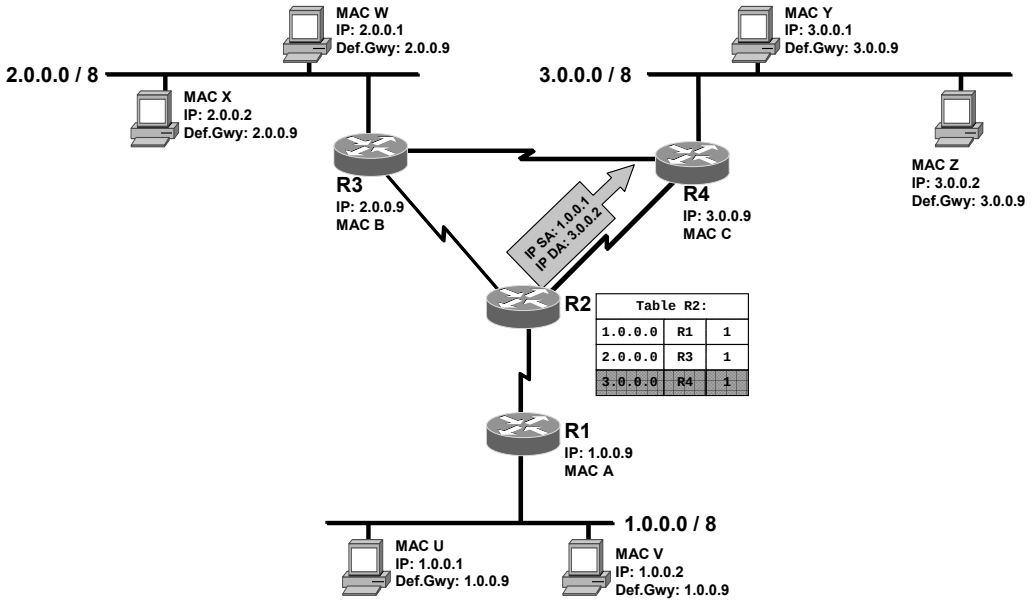
Indirect Delivery (5)



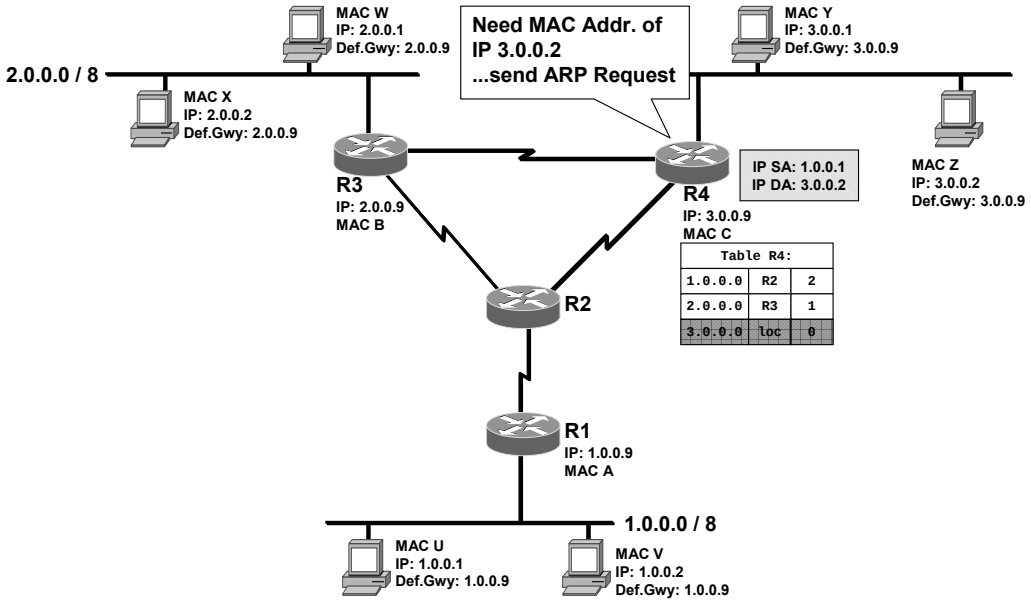
Indirect Delivery (6)



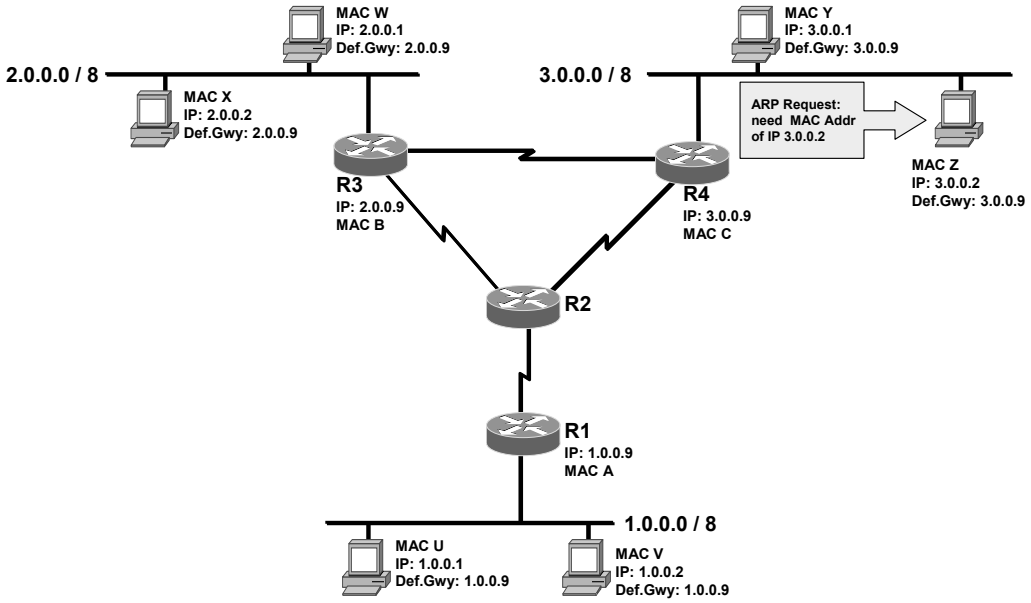
Indirect Delivery (7)



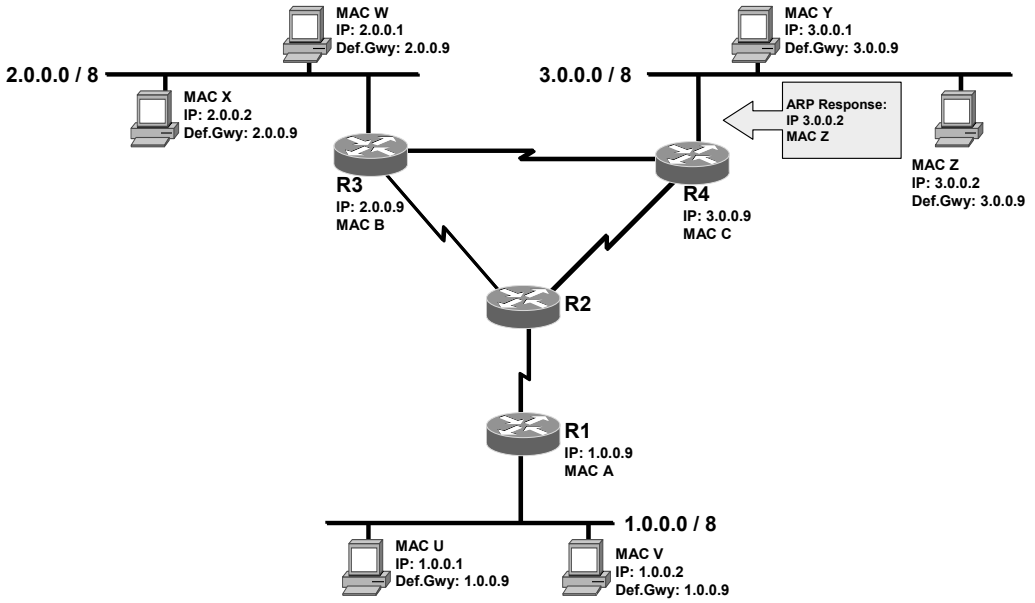
Indirect Delivery (8)



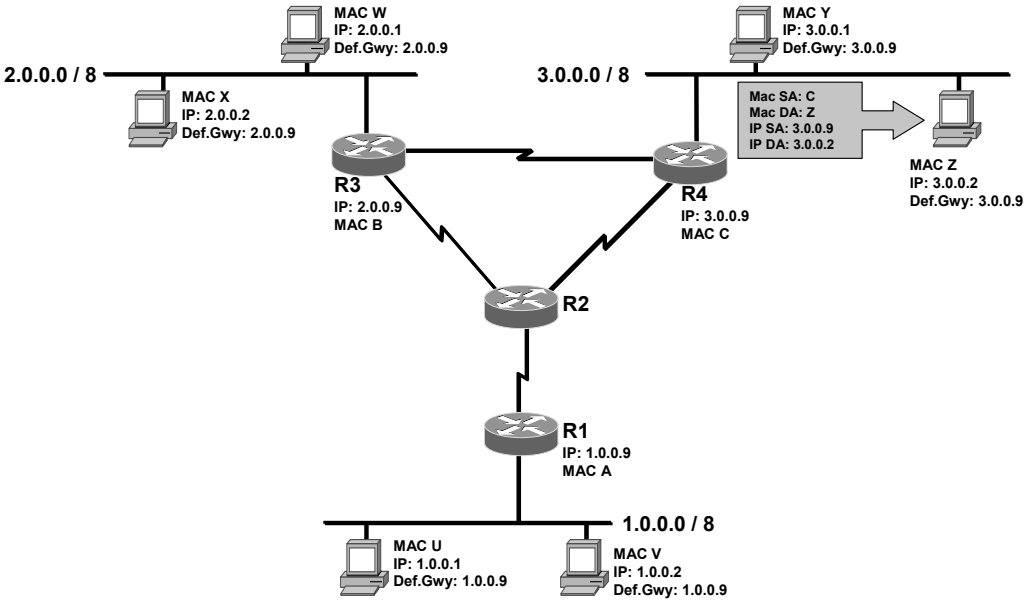
Indirect Delivery (9)



Indirect Delivery (10)



Indirect Delivery (END)



Reverse ARP

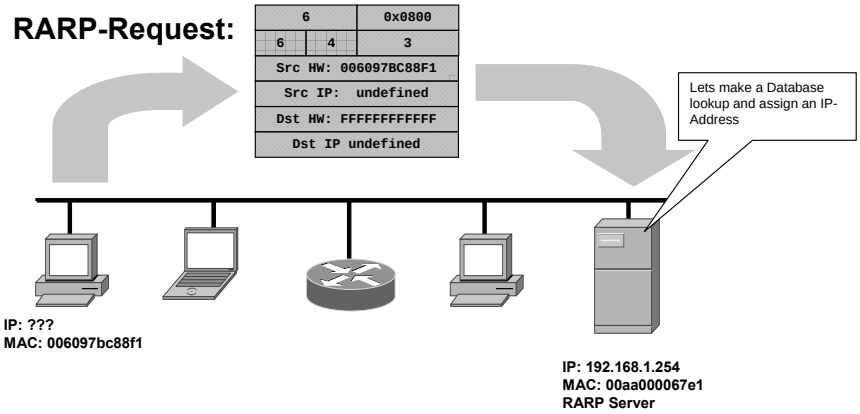
Reverse ARP (RARP)

- ARP assumes, that an IP station knows its IP address (stored in NVRAM, on hard disk, in config file etc.).
- Diskless Machines usually don't have such means so they must retrieve an IP address for network booting.
- RARP (Reverse ARP) provides IP addresses for unconfigured stations.
- RFC 903

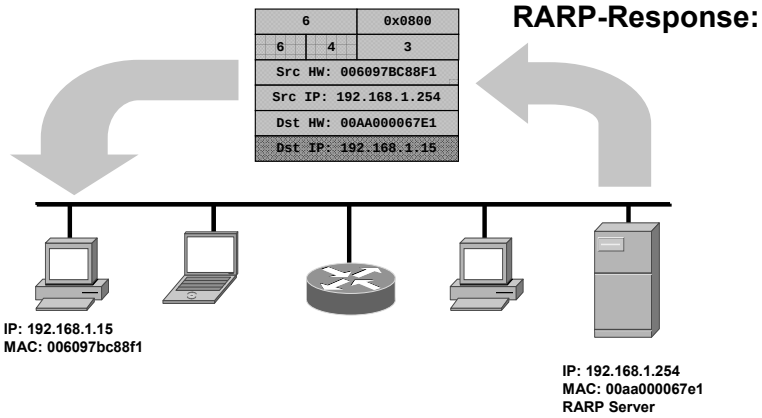
Reverse ARP (RARP)

- A station sends a RARP request broadcast.
- One station, the RARP server, looks up the IP address for that MAC address in a database and replies.
- Newer methods:
  - BOOTP
  - DHCP

Reverse ARP (RARP)



Reverse ARP (RARP)



Proxy ARP

"The ARP Hack"

Proxy ARP (1)

- Router connect only networks with different net-IDs
- Router with Proxy ARP enabled also connect networks with same Net-ID
  - Router replies on ARP request in behalf of station in other segment
  - Security or performance reasons
- "proxy" simply means *"instead of"*

As stated in RFC1027:

If hosts A and B are on different physical networks, host B will not receive the ARP broadcast request from host A and cannot respond to it. However, if the physical network of host A is connected by a gateway to the physical network of host B, the gateway will see the ARP request from host A. Assuming that subnet numbers are made to correspond to physical networks, the gateway can also tell that the request is for a host that is on a different physical network from the requesting host. The gateway can then respond for host B, saying that the network address for host B is that of the gateway itself. Host A will see this reply, cache it, and send future IP packets for host B to the gateway. The gateway will forward such packets to host B by the usual IP routing mechanisms. The gateway is acting as an agent for host B, which is why this technique is called "Proxy ARP"; we will refer to this as a transparent subnet gateway or ARP subnet gateway.

When host B replies to traffic from host A, the same algorithm happens in reverse: the gateway connected to the network of host B answers the request for the network address of host A, and host B then sends IP packets for host A to gateway. *The physical networks of host A and B need not be connected to the same gateway. All that is necessary is that the networks be reachable from the gateway.*

From the host point of view, there are no subnets, and their physical networks are simply one big IP network. If a host has an implementation of subnets, its network masks must be set to cover only the IP network number, excluding the subnet bits, for the system to work properly.

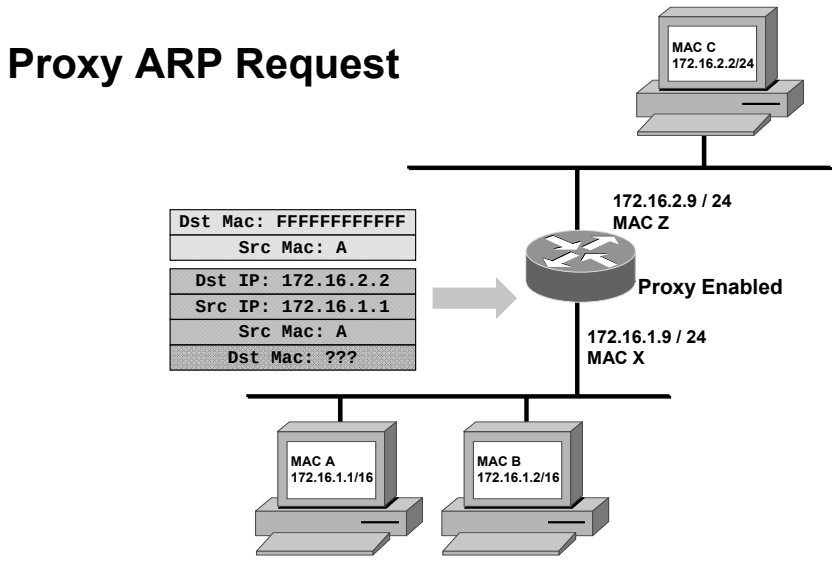
Proxy ARP (2)

- Using Proxy ARP on routers, hosts do not need default gateway or routing entries to reach other subnets
- Default router's address = own interface address
  - Force ARP for every destination address
- If the local router is configured for Proxy-ARP it replies with an ARP response claiming to be the destination host
  - Then accepts and forward the IP packet
  - Cisco routers have Proxy-ARP enabled by default

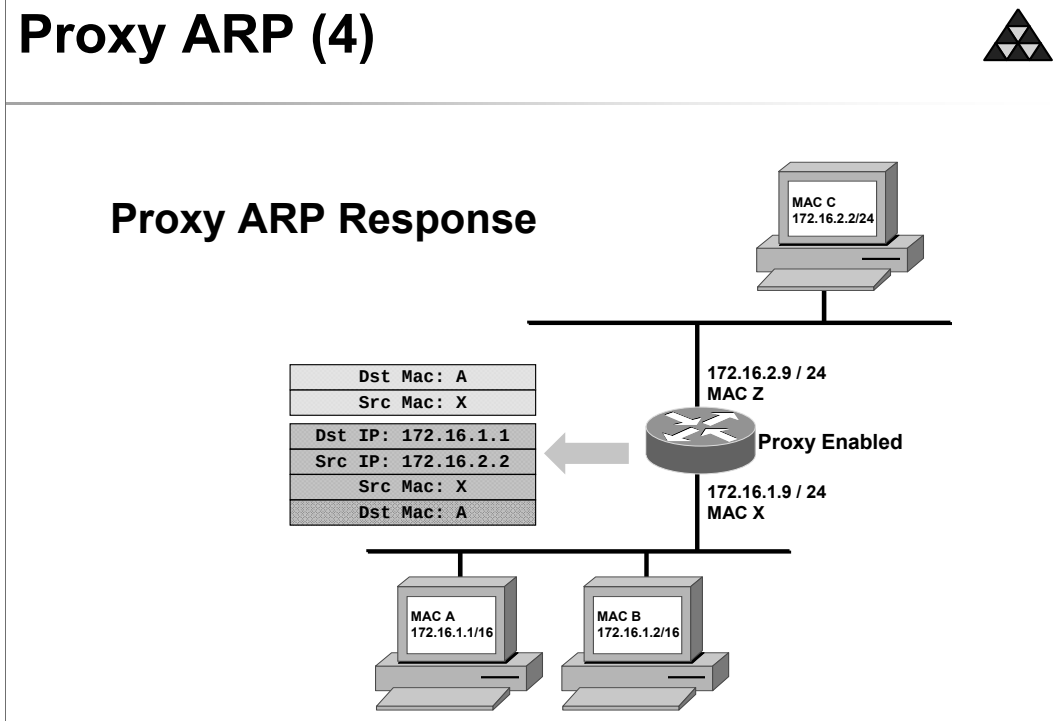
In the early days of the Internet not many vendors supported subnets. A method for hiding the existence of subnets from hosts

was highly desirable.

Proxy ARP (3)


Proxy ARP Request
MAC C
172.16.2.2/24
172.16.2.9 / 24
MAC Z
Dst Mac: FFFFFFFFFFFF
Src Mac: A
Dst IP: 172.16.2.2
Src IP: 172.16.1.1
Src Mac: A
Dst Mac: ???
Proxy Enabled
172.16.1.9 / 24
MAC X
MAC A
172.16.1.1/16
MAC B
172.16.1.2/16

Proxy ARP (4)


Proxy ARP Response
MAC C
172.16.2.2/24
Dst Mac: A
Src Mac: X
Dst IP: 172.16.1.1
Src IP: 172.16.2.2
Src Mac: X
Dst Mac: A
172.16.2.9 / 24
MAC Z
Proxy Enabled
172.16.1.9 / 24
MAC X
MAC A
172.16.1.1/16
MAC B
172.16.1.2/16

Rules (1)

- Originally Proxy ARP only allowed to hide subnets – *not networks* !
  - Proxy ARP GW should not be used to bypass normal GWs
- Multiple Proxy ARP GWs
  - Requesting host will use the first ARP response it receives
  - Simple load balancing service

Rules (2)

- **Proxy ARP GWs must not reply if the destination is reachable through the same interface**
  - **Either destination is in same segment**
  - **Or another Proxy ARP GW will reply, knowing a better route**

Another rule stated in RFC 1027:

An ARP request for a broadcast address must elicit no reply, regardless of the source address or physical networks involved. If the gateway were to respond with an ARP reply in this situation, it would be inviting the original source to send actual traffic to a broadcast address. This could result in the "Chernobyl effect" wherein every host on the network replies to such traffic, causing network "meltdown".

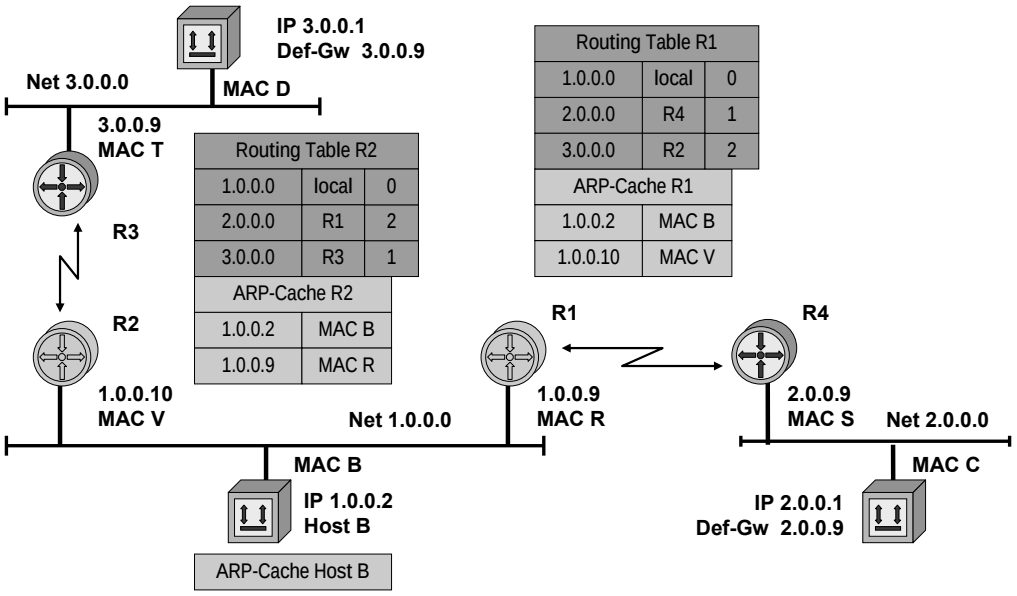
Disadvantages

- Much ARP traffic
  - Forwarded by bridges! (Broadcasts)
- Hosts need larger ARP caches
- Address spoofing possible
  - Station claims to be another station

Proxy ARP Usage Nowadays

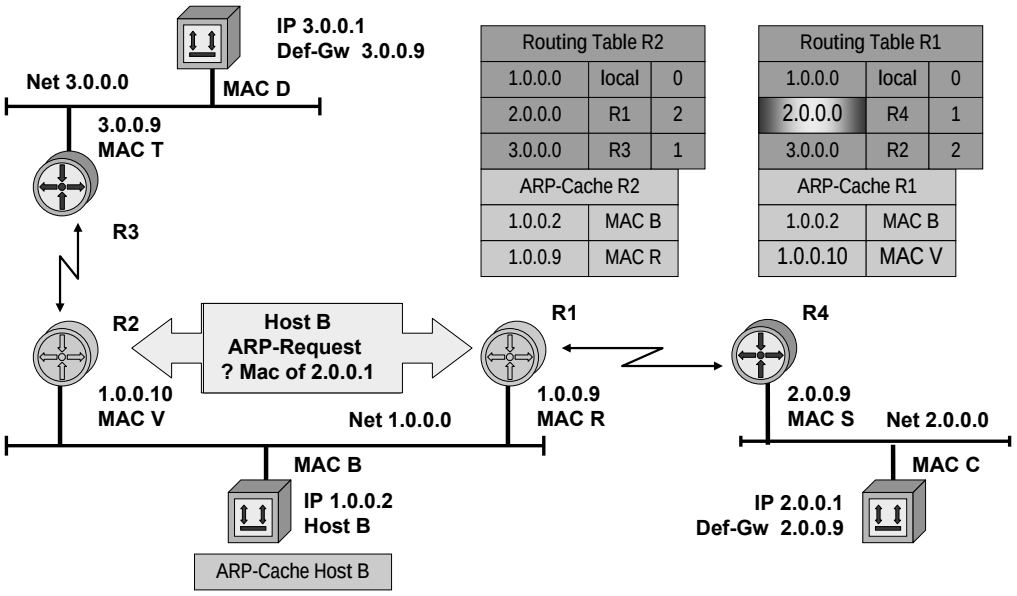
- **Proxy ARP is also be used if an IP host didn't know the address of the default gateway:**
  - In an IP host normally a static entry will tell the IP address of the router
    - if an IP datagram has to be sent to a non-local Net-ID, an ARP request will find the MAC address of the default gateway
  - With Proxy ARP extensions in the IP host and in the router
    - the MAC address of the router can be found without knowing the routers IP address
    - An ARP request will be sent for IP hosts with NET-IDs different from the local Net-ID and the router will respond
  - With Unix stations or Windows NT/XP:
    - proxy ARP extensions are triggered by setting the default gateway to the systems IP address itself

1.0.0.2 -> 3.0.0.1 / 2.0.0.1 with proxy ARP 1



R1 and R2 proxy ARP enabled; Host B sends ARP also for net-ID unequal own net-ID

1.0.0.2 -> 3.0.0.1 / 2.0.0.1 with proxy ARP 2



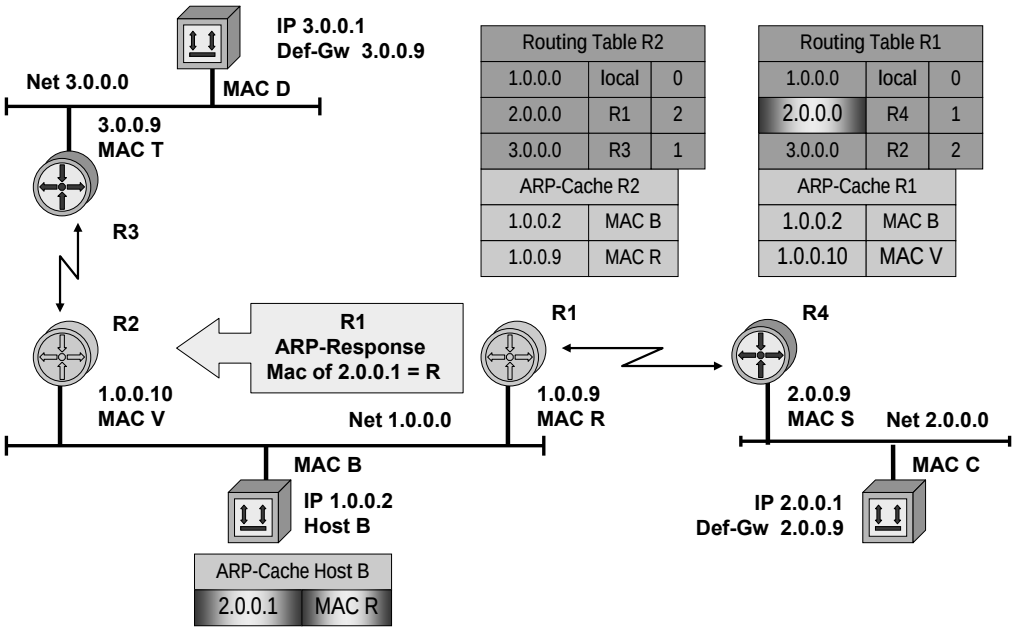
Routing Table R2		
1.0.0.0	local	0
2.0.0.0	R1	2
3.0.0.0	R3	1

ARP-Cache R2	
1.0.0.2	MAC B
1.0.0.9	MAC R

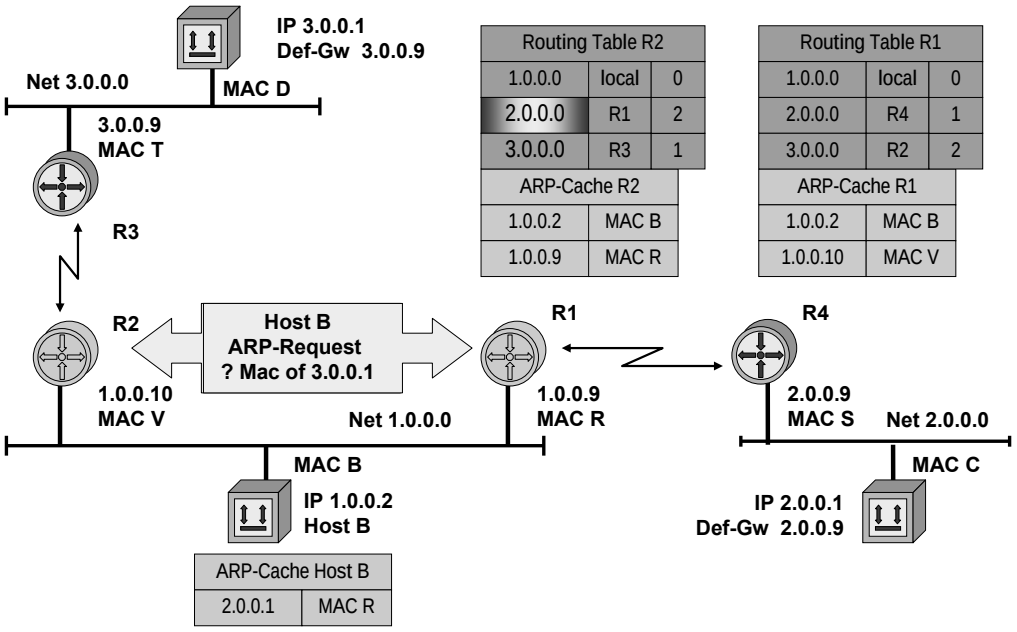
Routing Table R1		
1.0.0.0	local	0
2.0.0.0	R4	1
3.0.0.0	R2	2

ARP-Cache R1	
1.0.0.2	MAC B
1.0.0.10	MAC V

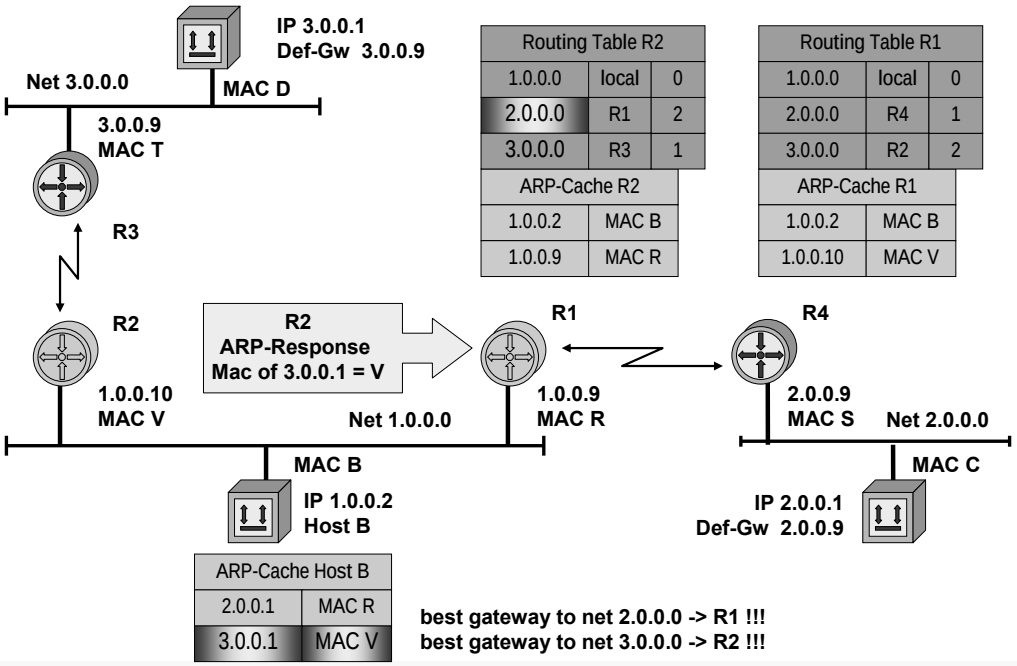
1.0.0.2 -> 3.0.0.1 / 2.0.0.1 with proxy ARP 3



1.0.0.2 -> 3.0.0.1 / 2.0.0.1 with proxy ARP 4



1.0.0.2 -> 3.0.0.1 / 2.0.0.1 with proxy ARP 5



ICMP

The Internet Control Message Protocol

- If network cannot deliver packets the sender must be informed somehow !
  - Reasons: no route, TTL expired, ...
- ICMP enhances network reliability and performance by carrying error and diagnostic messages
- ICMP must be supported by every IP station
  - Implementation differences!

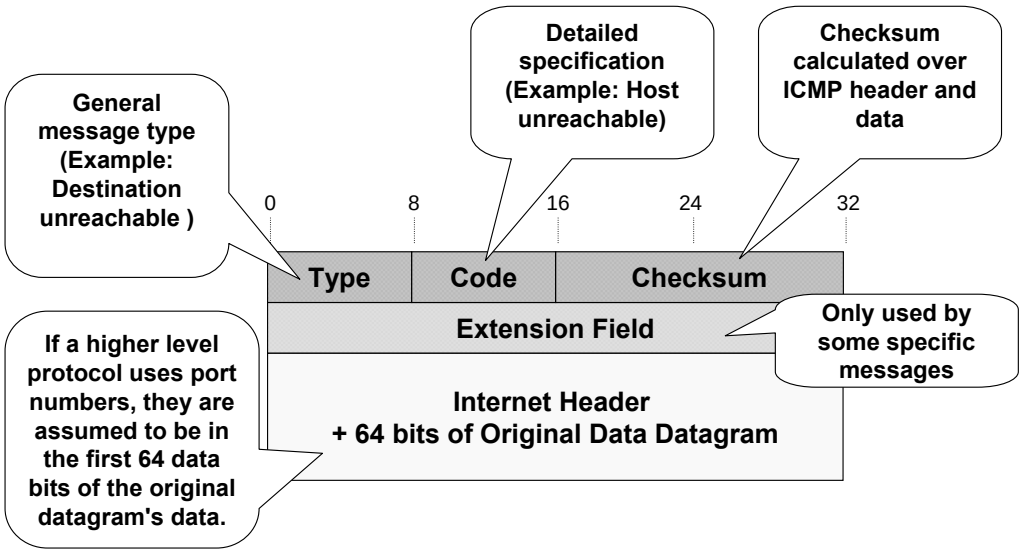
Simple Operation

- Any station (host or router) detecting transmission problems sends ICMP error message back to the originator
- ICMP gives feedback
- ICMP messages are carried within IP packets
  - Protocol field = 1
  - ICMP header and code in the IP data area

Important Rule

- If a IP packet carrying an ICMP message cannot be delivered
  - No additional ICMP error message is generated to avoid an ICMP avalanche
  - "ICMP must not invoke ICMP"
- Exception: PING command
  - Echo request and echo response
  - Microsoft's tracert expects "TTL expired" upon "Echo request"

ICMP Message Format



Type Field Values

(0) - Echo reply ("PING")
(3) - Destination Unreachable
(4) - Source Quench (decrease data rate of sender)
(5) - Redirect (use different router)
(8) - Echo Request ("PING")
(11) - Time Exceeded (TTL = 0 or reassembly timer expired)
(12) - Parameter Problem (IP header)
(13) - Time Stamp Request
(14) - Time Stamp Reply
(15/16) - Information Request/Reply (finding the Net-ID of the network; e.g. SLIP)
(17/18) - Address Mask Request/Reply

Example: Codes for Type 3

(0) - Network unreachable: no path to network known or network down; generated by intermediate or far-end router.

(1) - Host unreachable: Host-ID can't be resolved or host not responding; generated by far-end router.

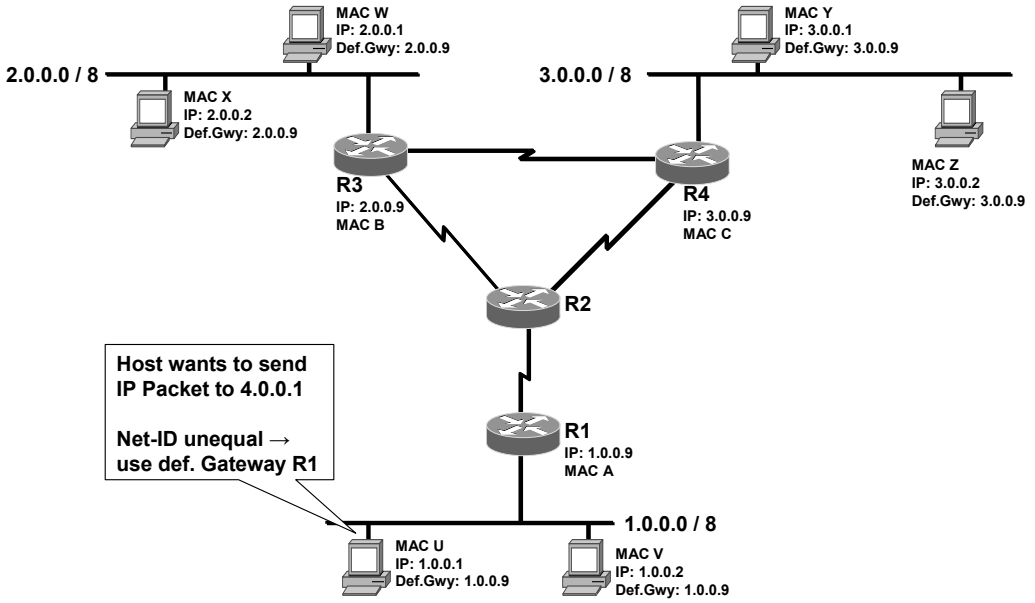
(2) - Protocol unreachable: protocol specified in IP header not available; generated by end system.

(3) - Port unreachable: port (service) specified in layer 4 not available; generated by end system.

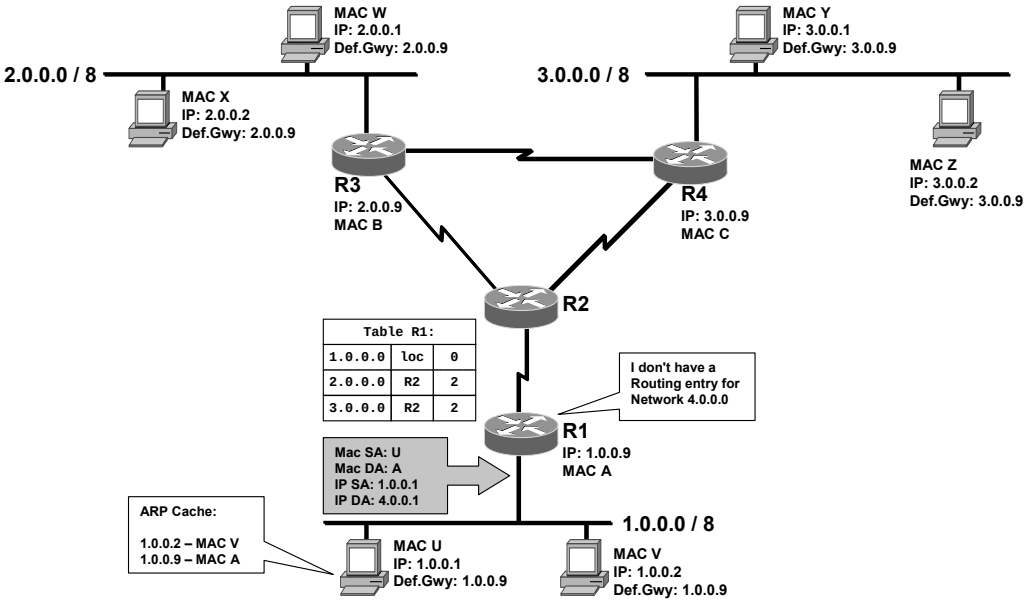
(4) - Fragmentation needed and do not fragment bit set: DF bit =1 but the packet is too big for the network (MTU); generated by router.

(5) - Source route failed: Path in IP Options couldn't be followed; generated by intermediate or far-end router.

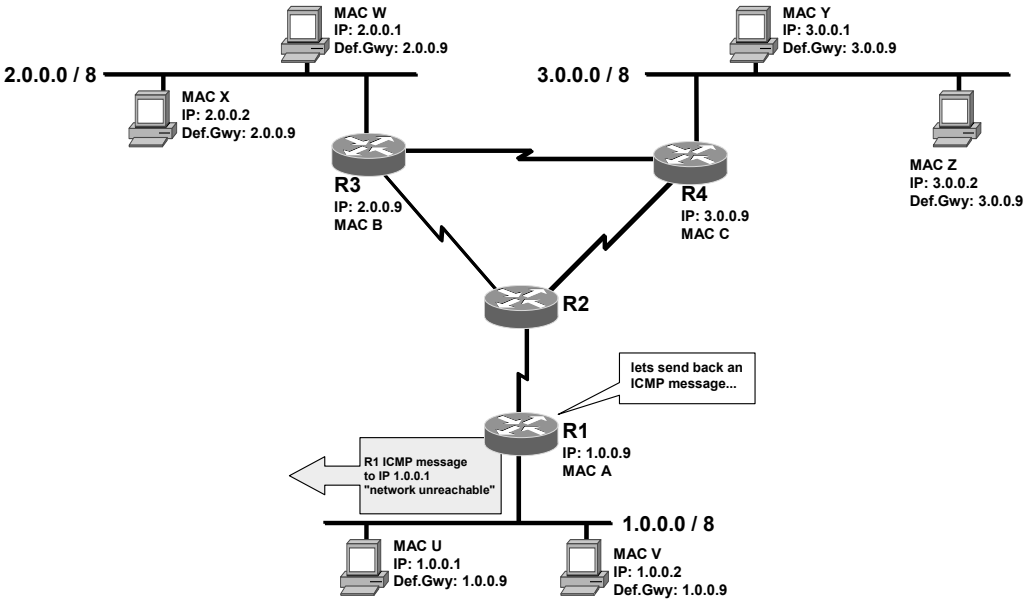
IP Forwarding und ICMP(1)



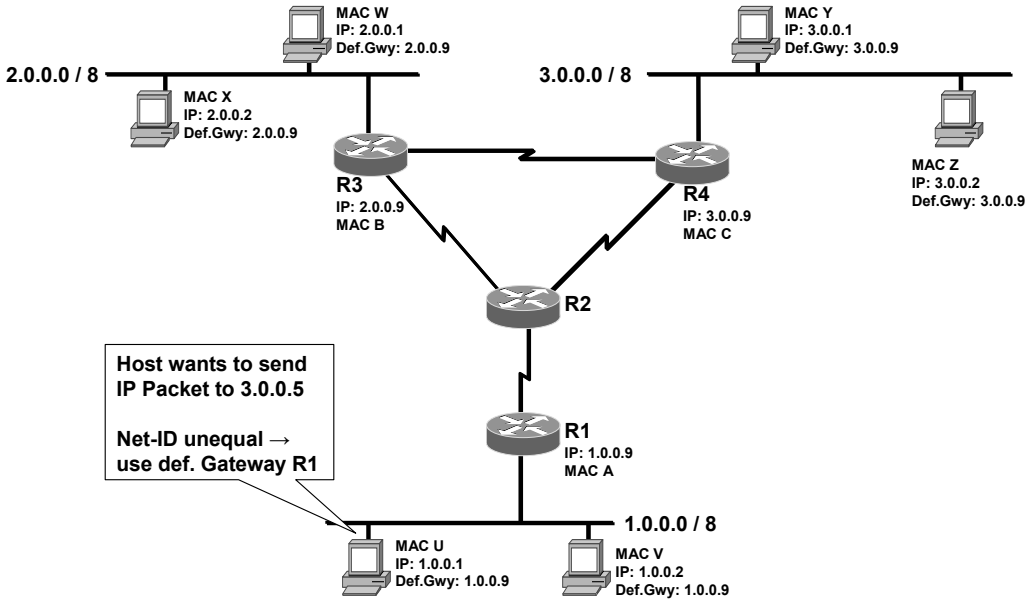
IP Forwarding und ICMP(1)



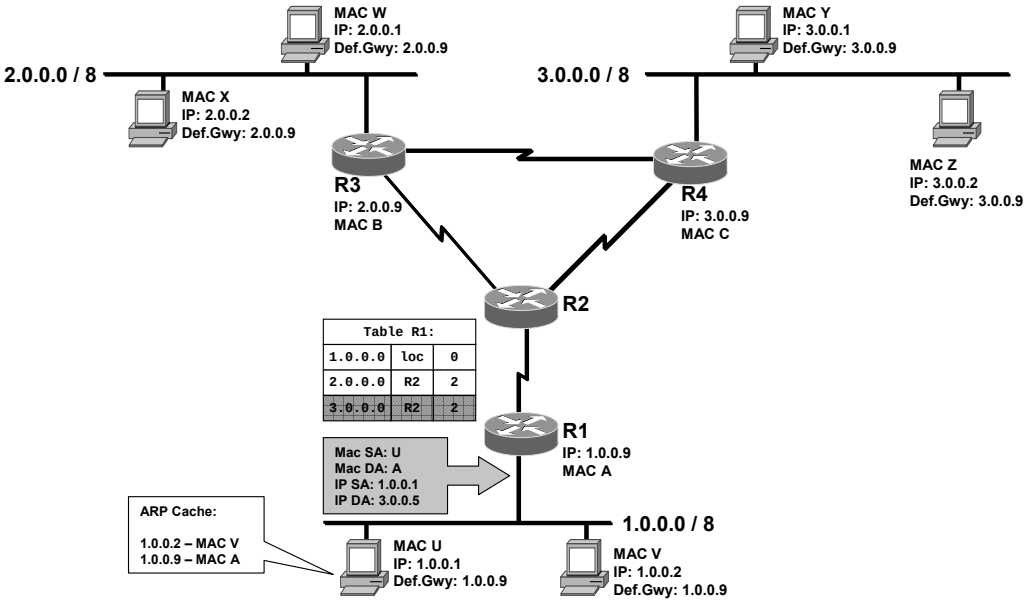
IP Forwarding und ICMP(1)



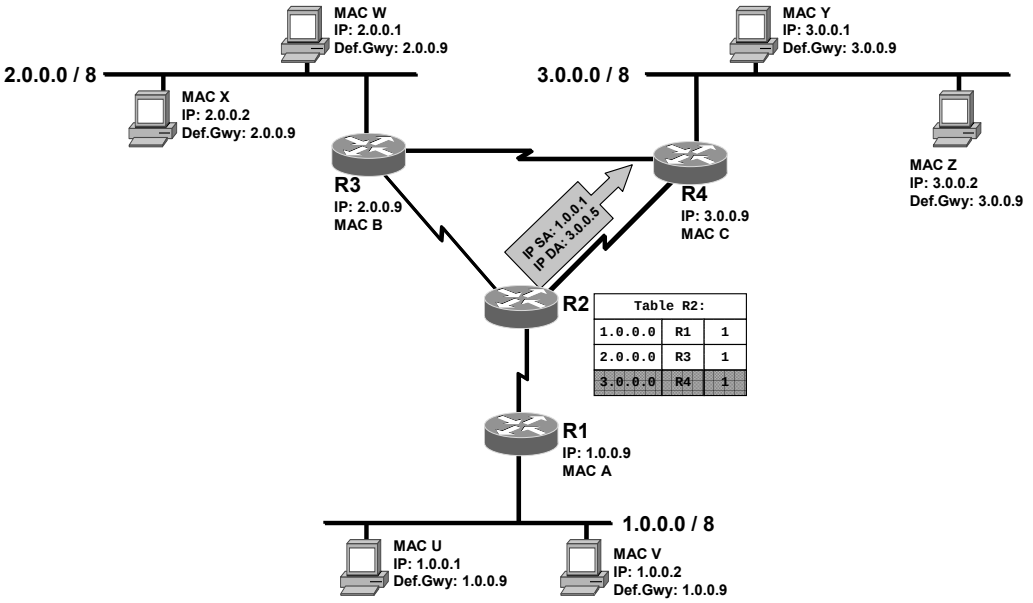
IP Forwarding und ICMP(2)



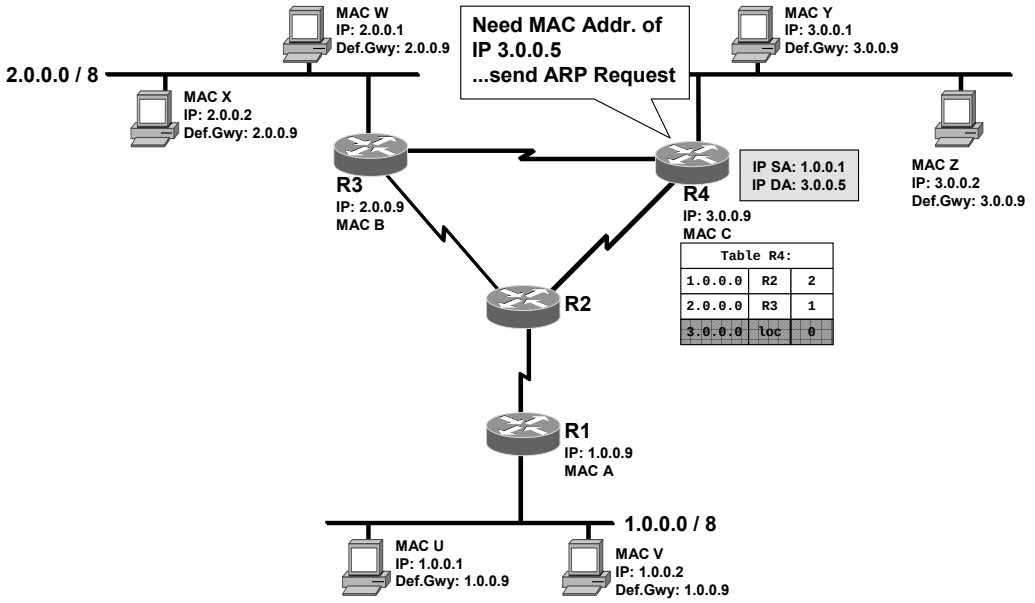
IP Forwarding und ICMP(2)



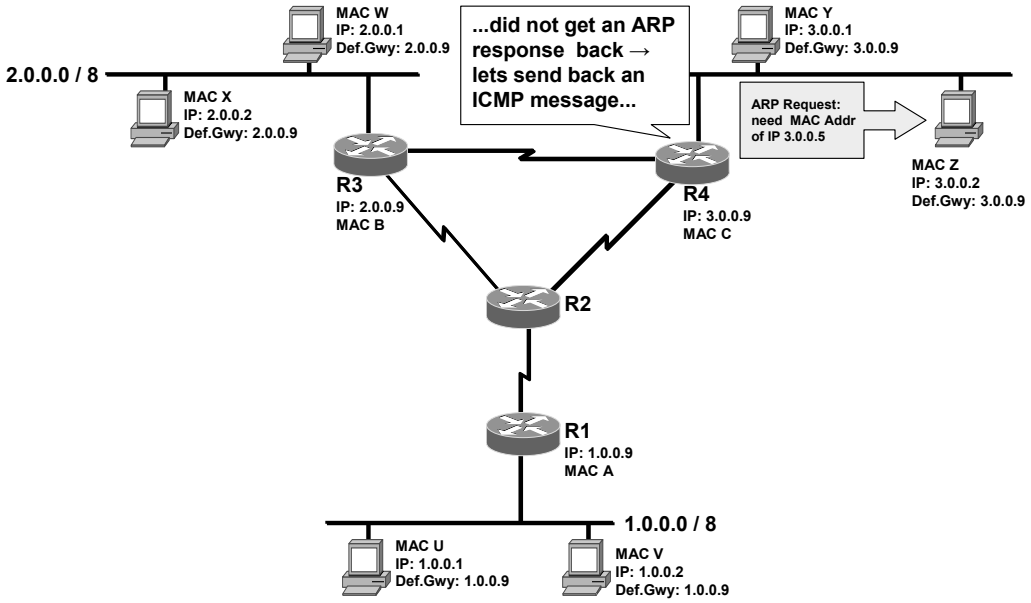
IP Forwarding und ICMP(2)



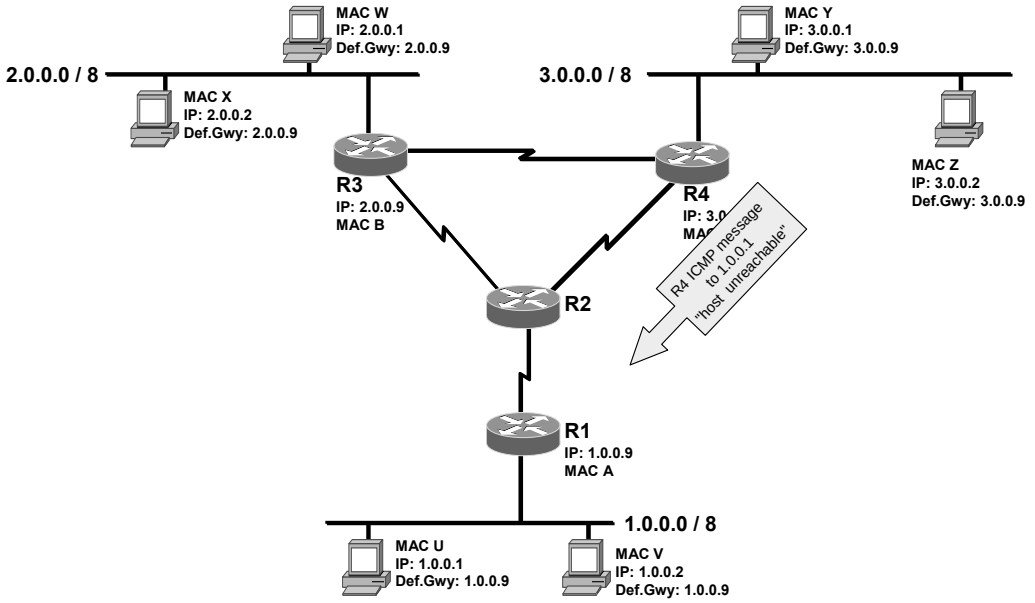
IP Forwarding und ICMP(2)



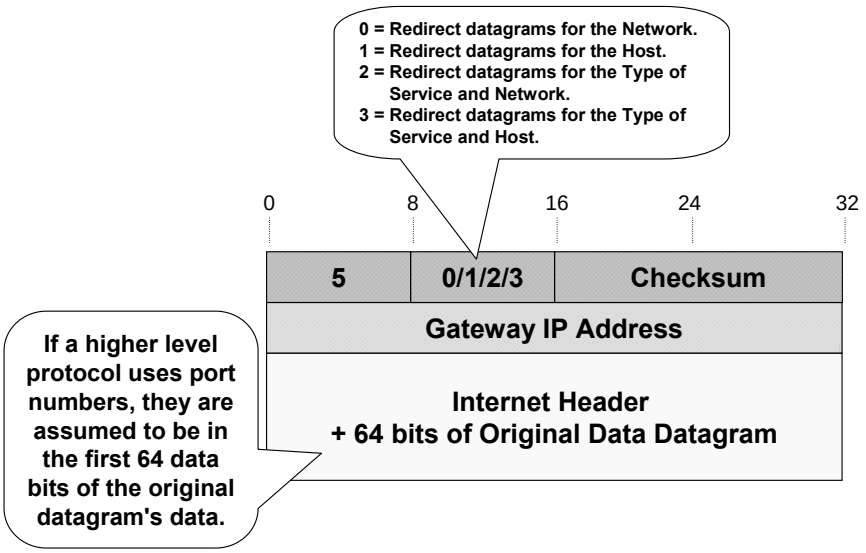
IP Forwarding und ICMP(2)



IP Forwarding und ICMP(2)



ICMP Redirect

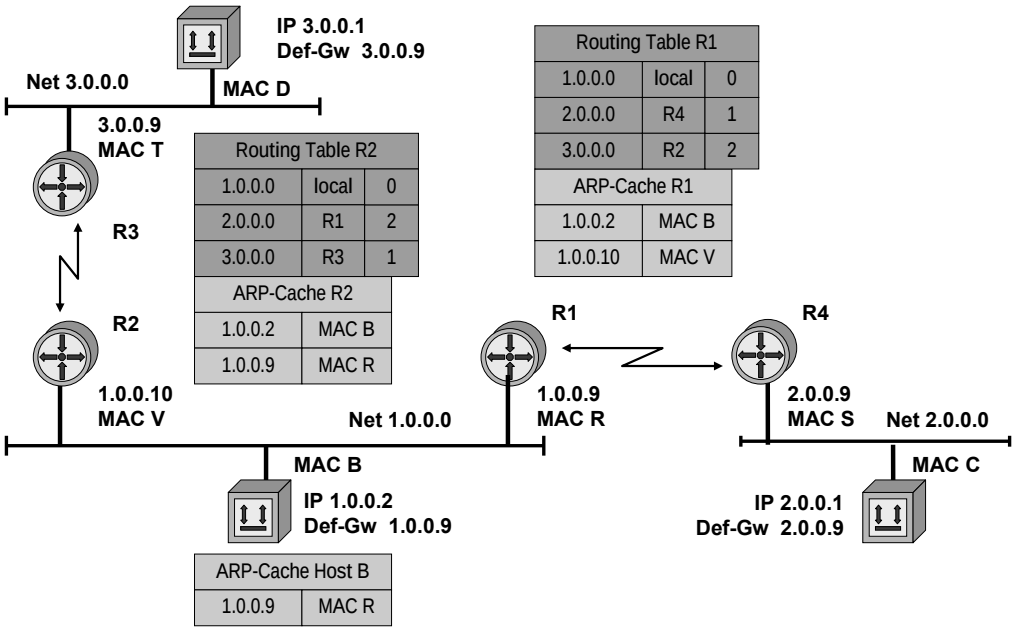


Rules

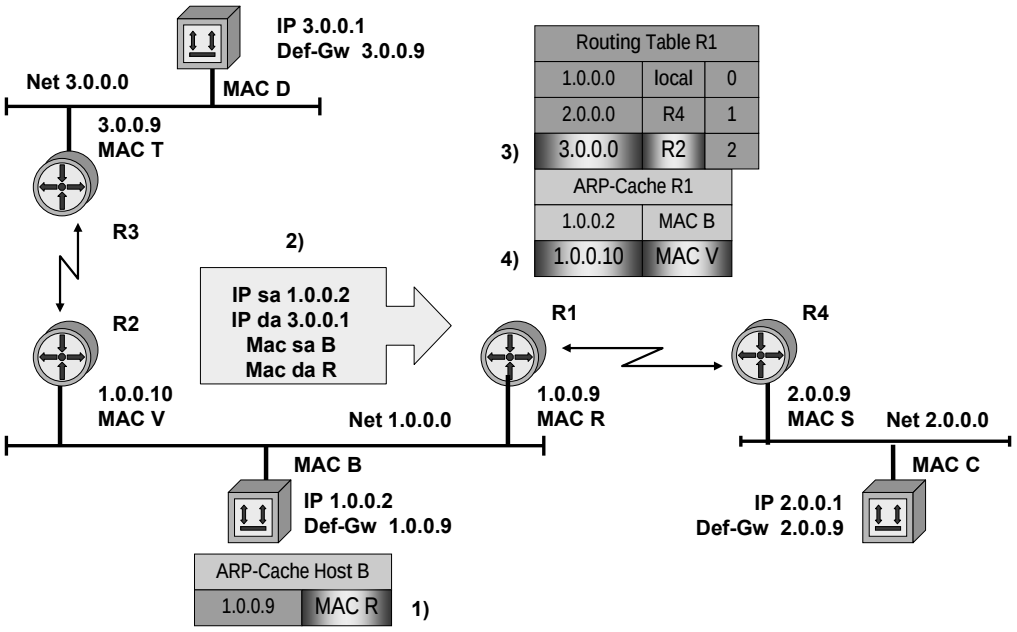
- The interface on which the packet comes into the router is the same interface on which the packet gets routed out
- The subnet/network of the source IP address is the same subnet/network of the next-hop IP address of the routed packet
- The datagram is not source-routed
- The kernel is configured to send redirects

By default, Cisco routers send ICMP redirects. It can be disabled by the interface subcommand "no ip redirects".

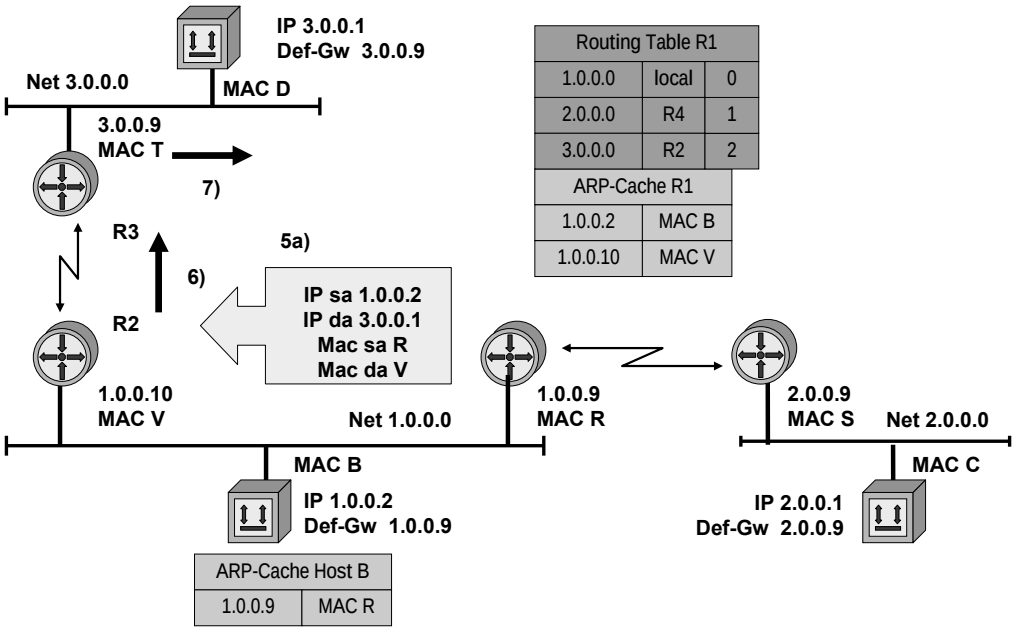
Delivery 1.0.0.2 -> 3.0.0.1



Delivery 1.0.0.2 -> 3.0.0.1



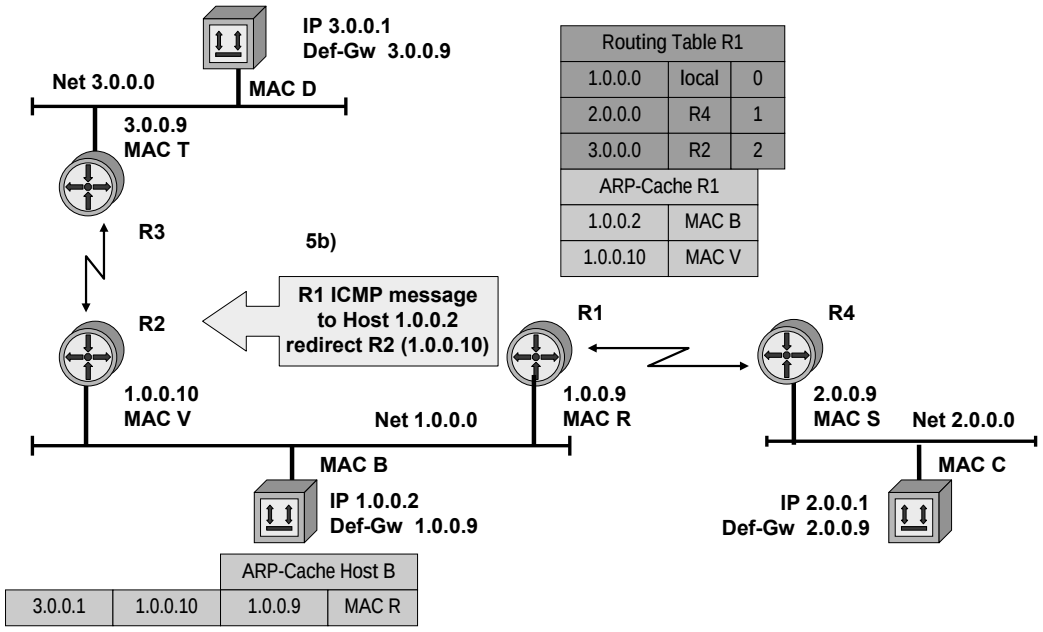
Delivery 1.0.0.2 -> 3.0.0.1



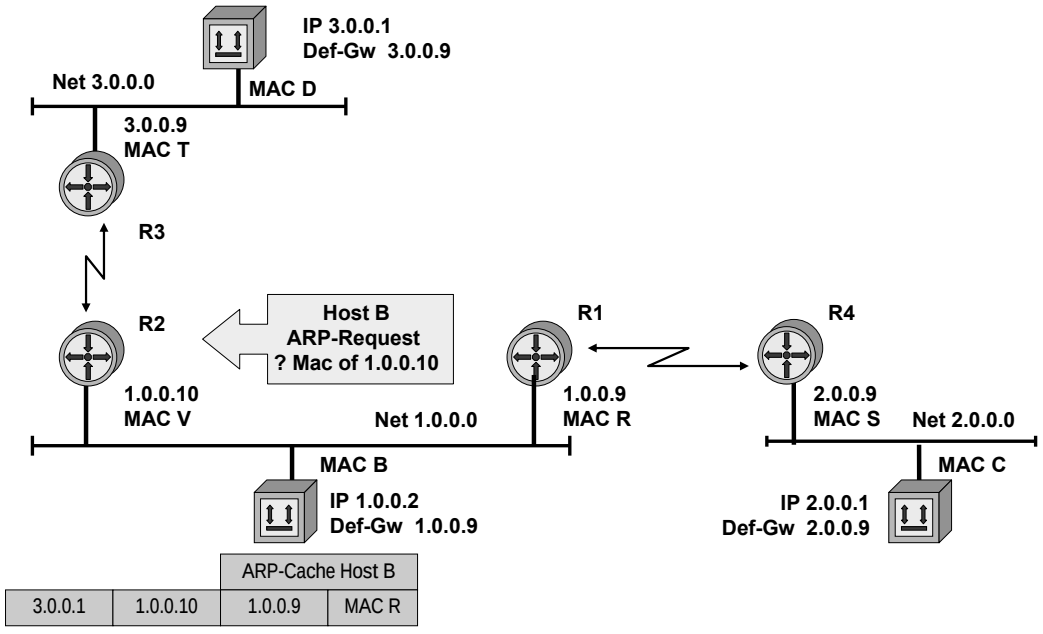
Routing Table R1		
1.0.0.0	local	0
2.0.0.0	R4	1
3.0.0.0	R2	2

ARP-Cache R1	
1.0.0.2	MAC B
1.0.0.10	MAC V

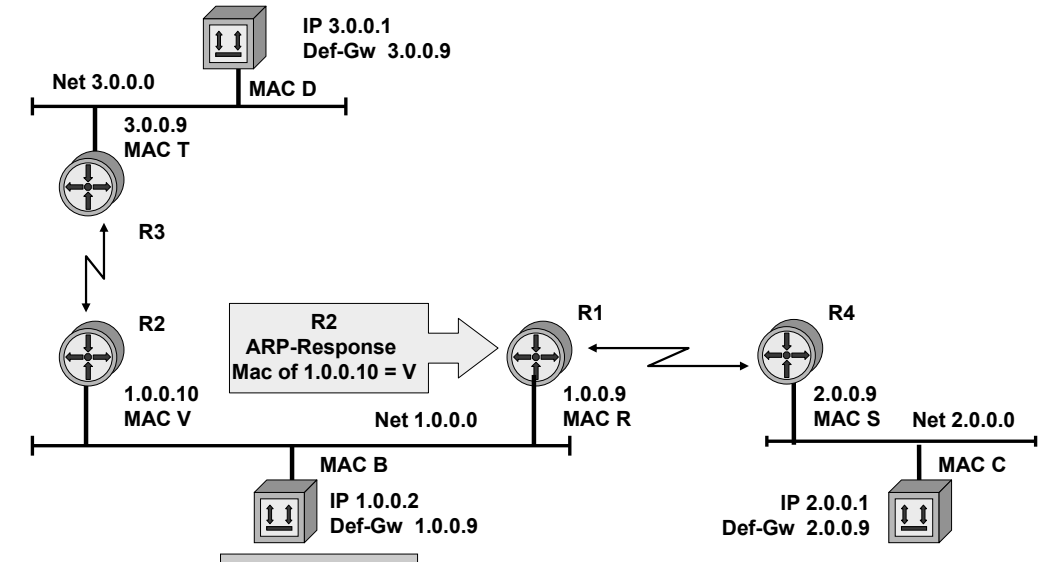
ICMP redirect



Delivery 1.0.0.2 -> 3.0.0.1

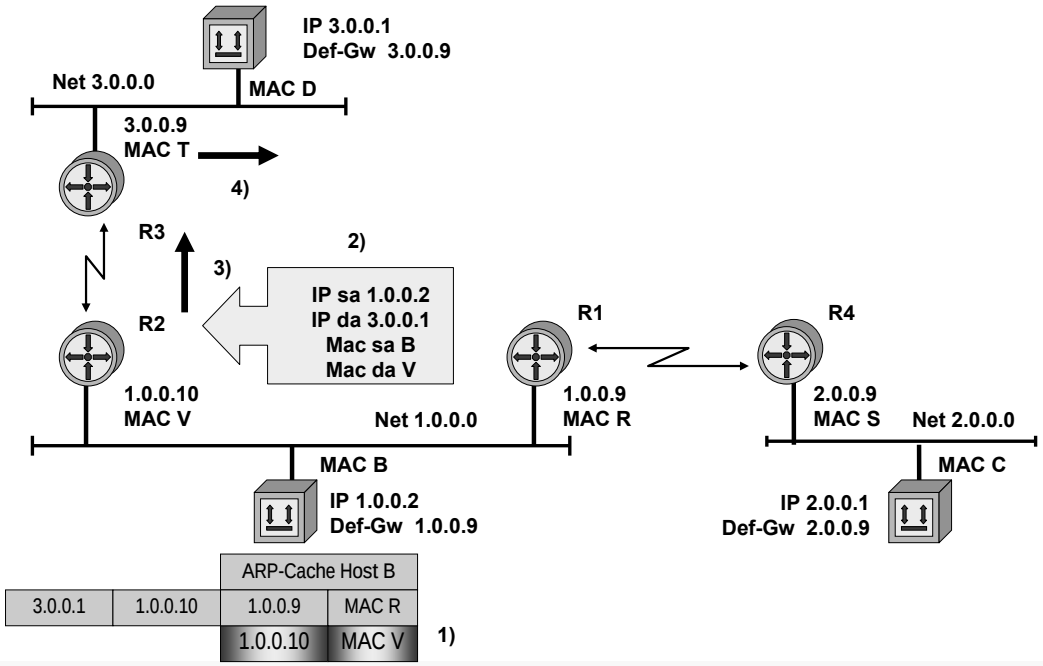


Delivery 1.0.0.2 -> 3.0.0.1

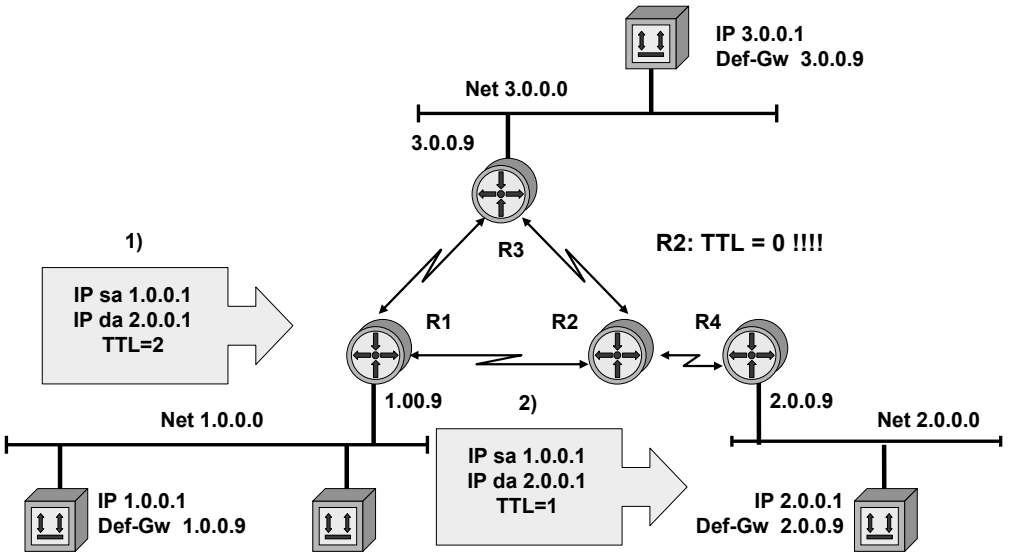


		ARP-Cache Host B	
3.0.0.1	1.0.0.10	1.0.0.9	MAC R
		1.0.0.10	MAC V

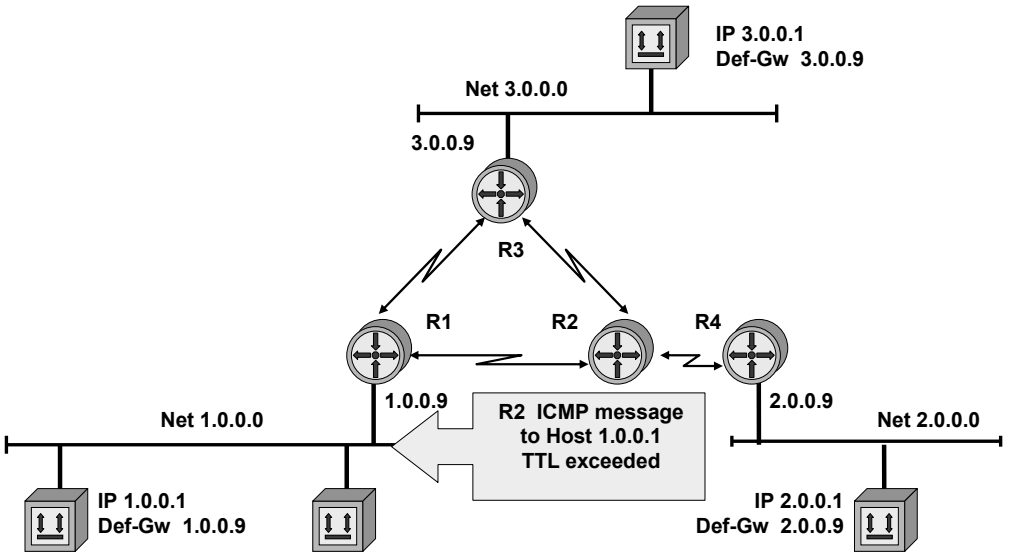
Next Packet 1.0.0.2 -> 3.0.0.1



Delivery 1.0.0.1 - > 2.0.0.1 (TTL=2)



ICMP TTL exceeded



Summary

- On Layer 3, IP-Addresses are used to route packets
  - On Layer 2 different addresses are used (e.g. MAC-Address)
  - Mapping/Resolution needed → ARP
- ARP is mostly dynamic (static entries are possible)
- The other way round: RARP (BootP, DHCP)
- ICMP is used to inform the originating IP-Host about what happend with its IP Packet
  - IP Stacks do not neccesarily listen to ICMP message
  - Could be one way to implement flow-control (ICMP - source quench)

Quiz

- Why is ARP not needed on serial lines?
- Why are ARP-Cache entries timeing out?
- Why should you use DHCP instead of RARP?
- What happens if a router discards an ICMP message?
- Ever heard of "Inverse ARP"?