

Address Resolution

ARP, RARP, Proxy ARP

Agenda



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



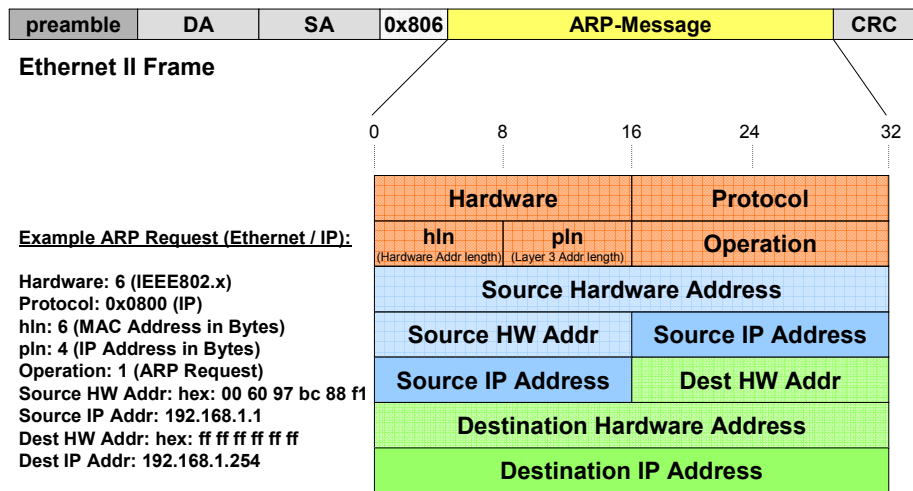
Address Resolution Protocol

Why ARP?



- 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

ARP Format



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 Delivery

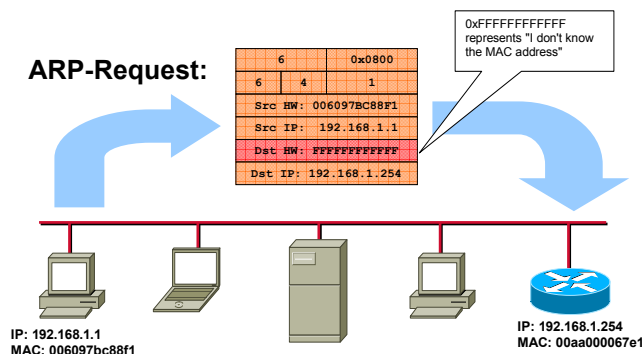


- IP host checks if packet's destination network is identical with local network
 - ♦ By applying the configured subnet mask of the host's interface
- If destination network = local network then the L2 address of the destination is discovered using ARP
 - ♦ Remember: not necessary for point-to-point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

Direct Delivery



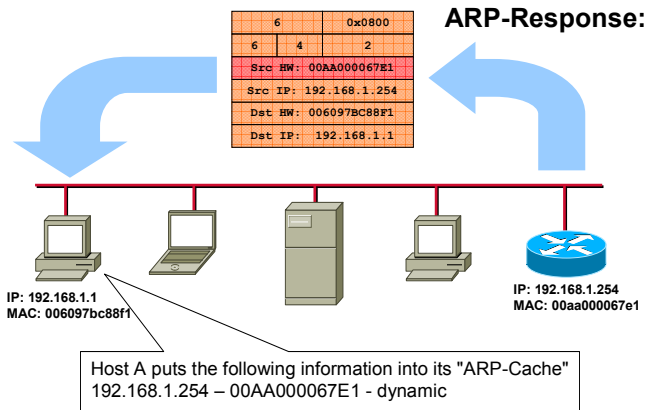
- Sent as Broadcast



Direct Delivery



- Response is unicast



IP Host Facts



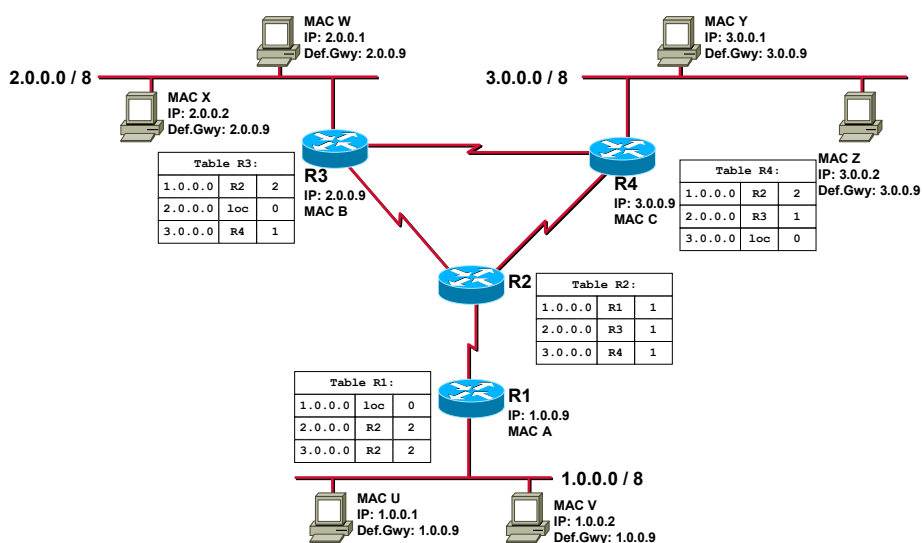
- Learned MAC addresses are stored in an **ARP-cache**
 - ♦ Aging timer: **20 minutes**
- IP hosts have also routing tables !
 - ♦ But typically only a static route to the default gateway is entered
 - ♦ Default gateway for indirect delivery

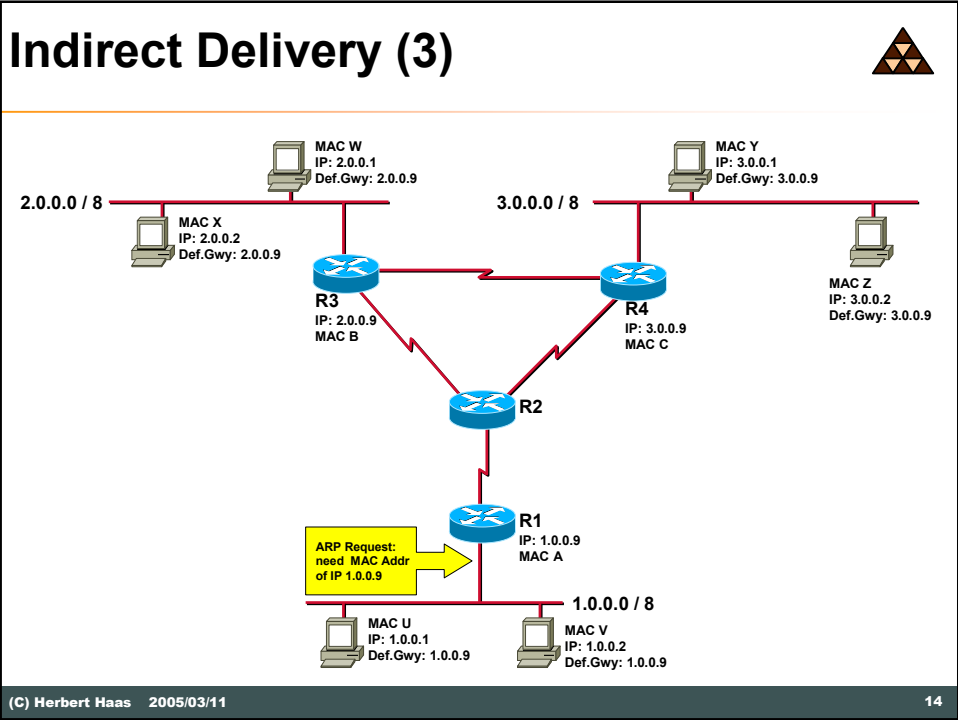
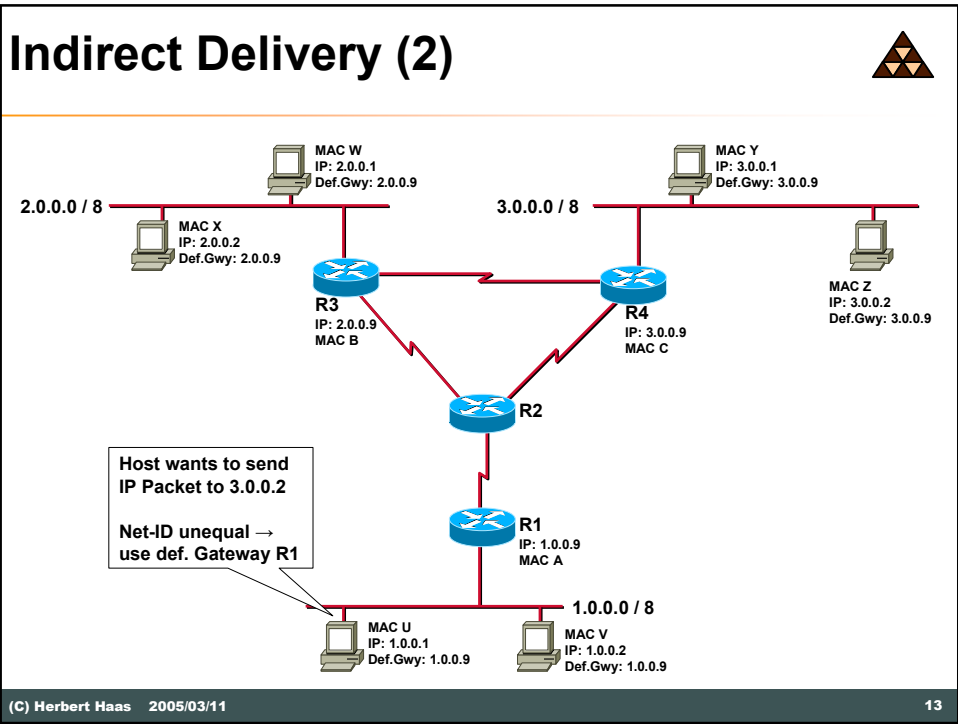
Using the Default Gateway

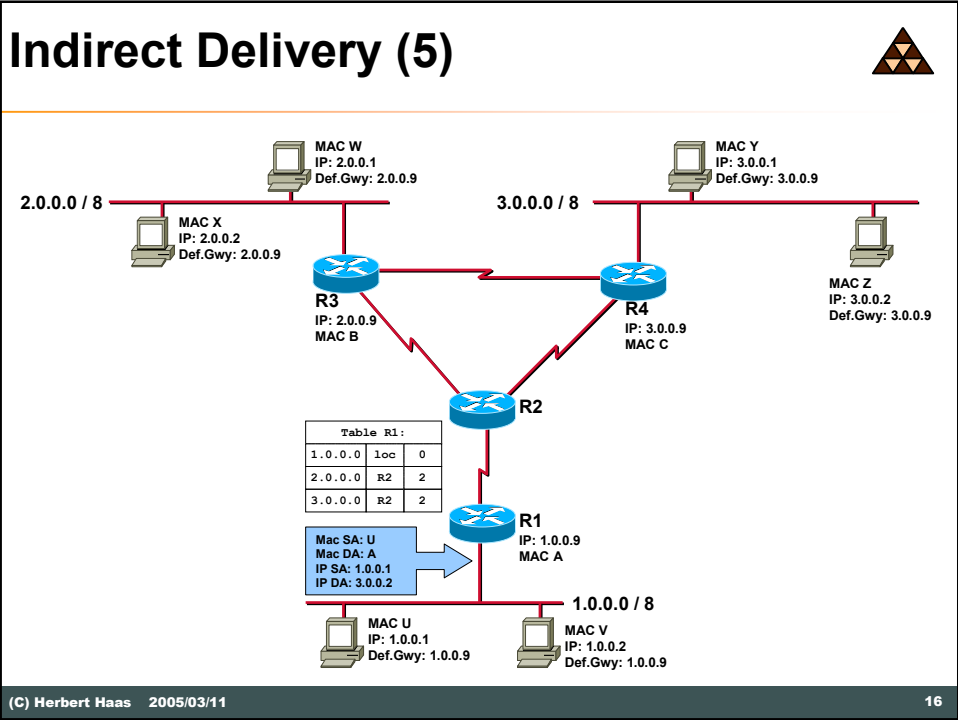
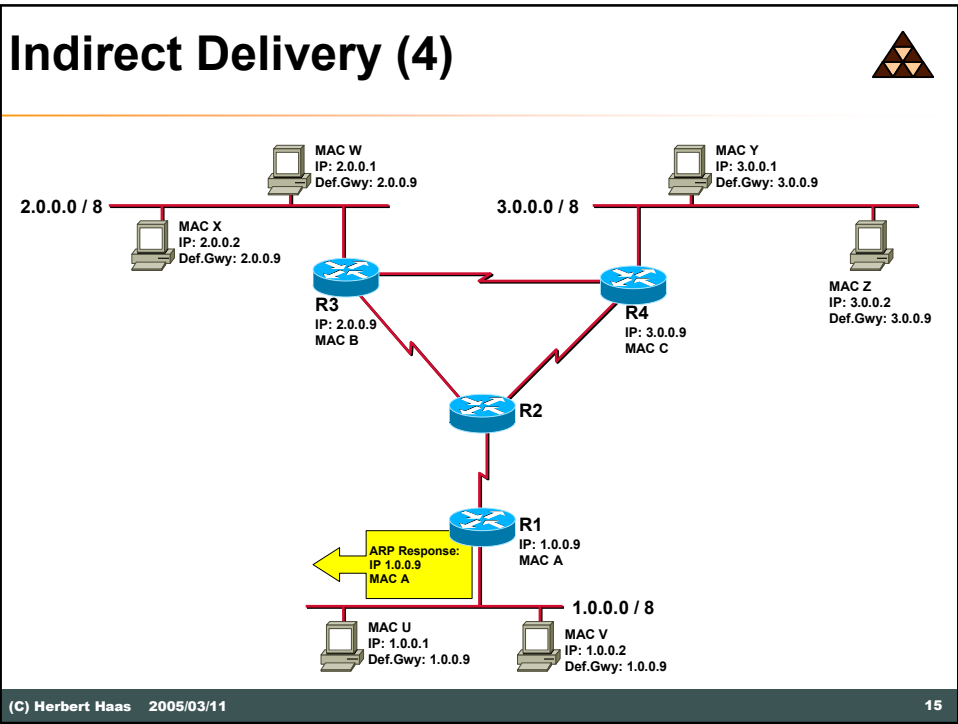


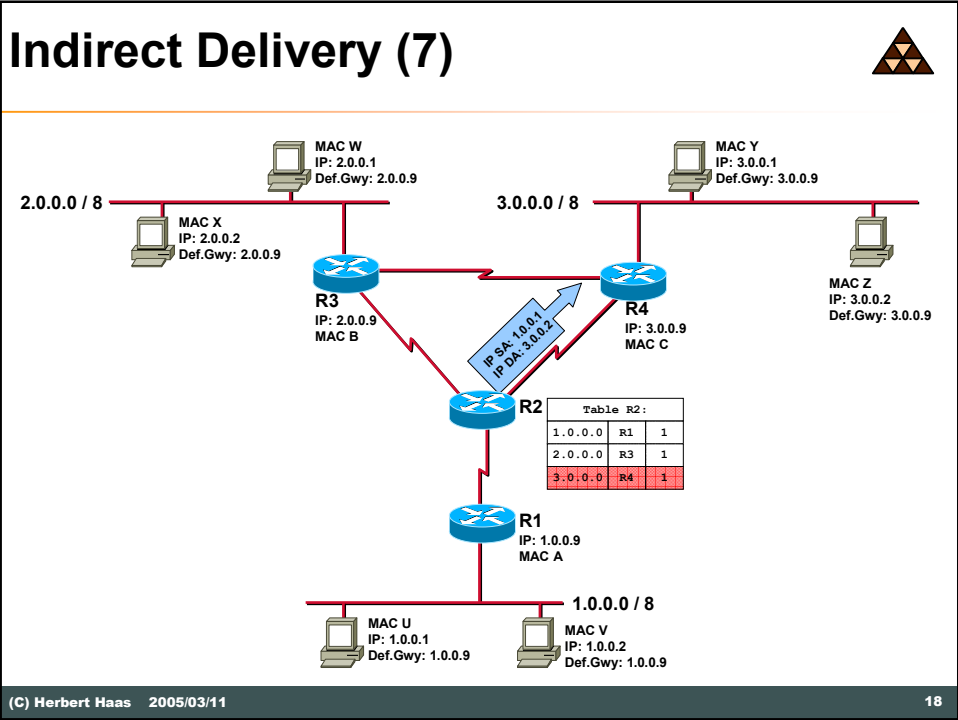
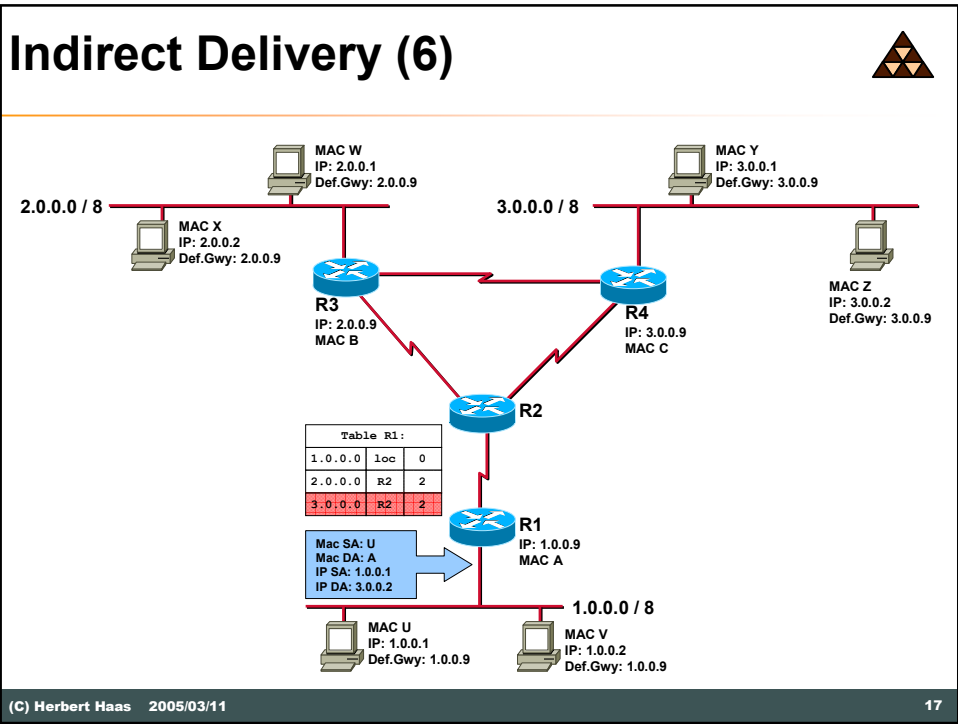
- Default gateway delivers packet in behalf of its host using a routing table
- Host must determine MAC address of default gateway using ARP
- IP datagram is handed over to default gateway

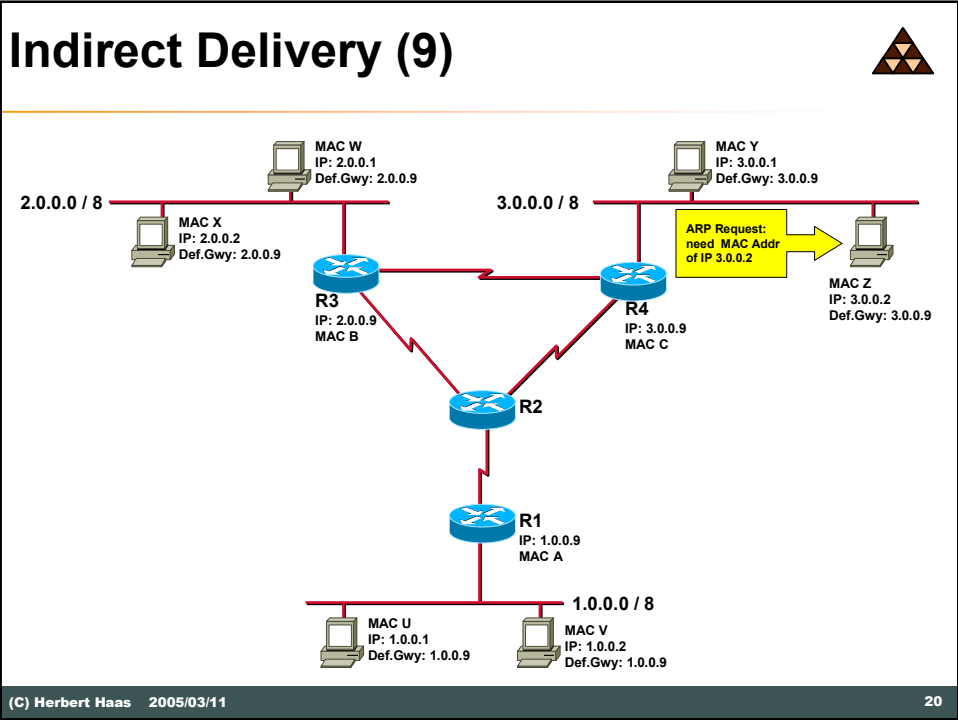
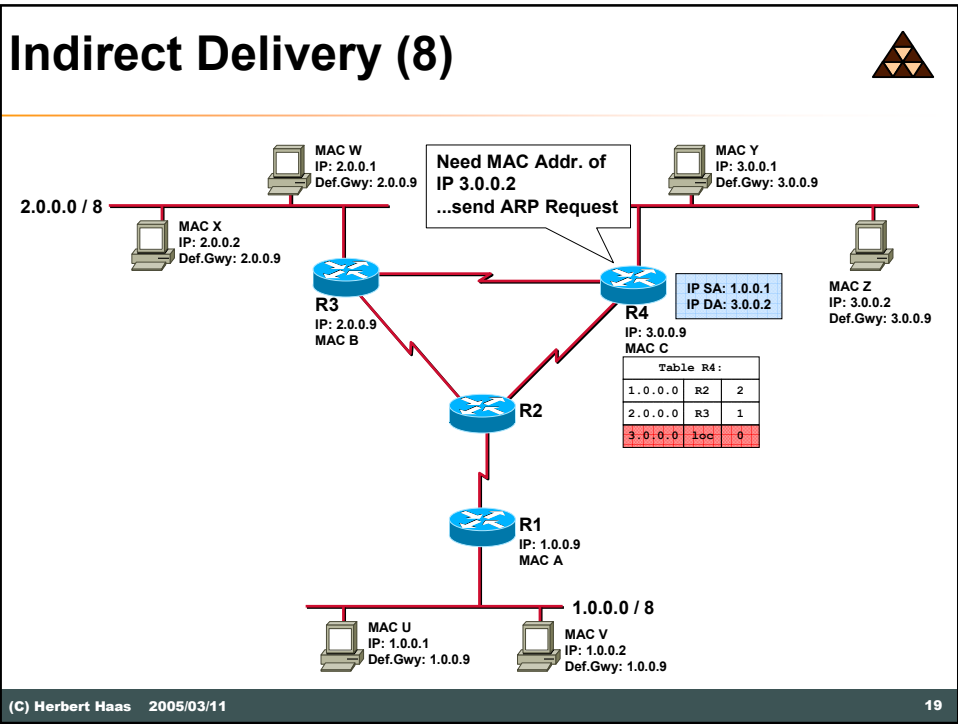
Indirect Delivery (1)



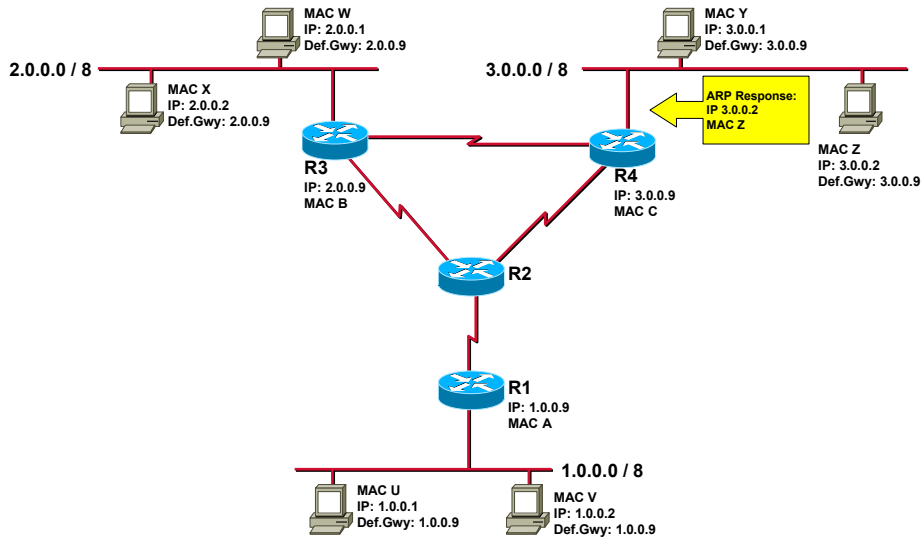




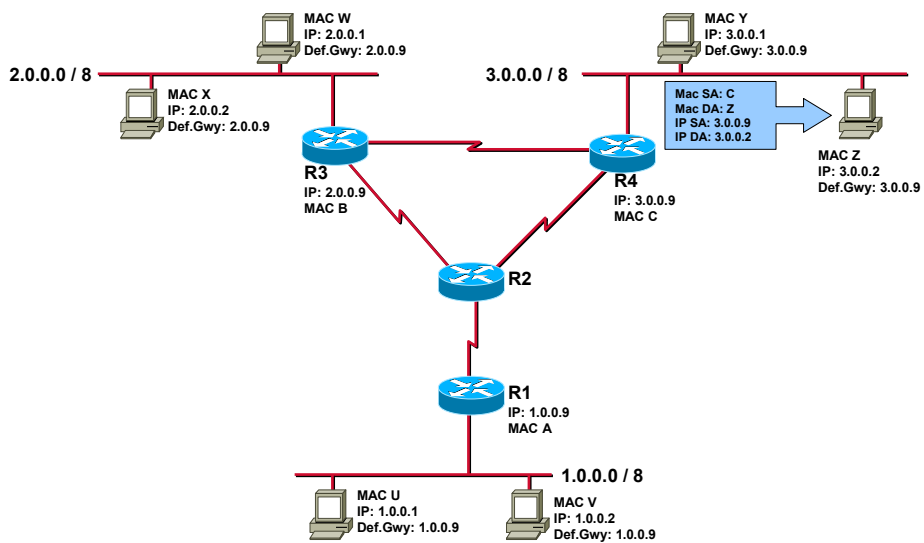




Indirect Delivery (10)



Indirect Delivery (END)





Reverse ARP

Reverse ARP (RARP)



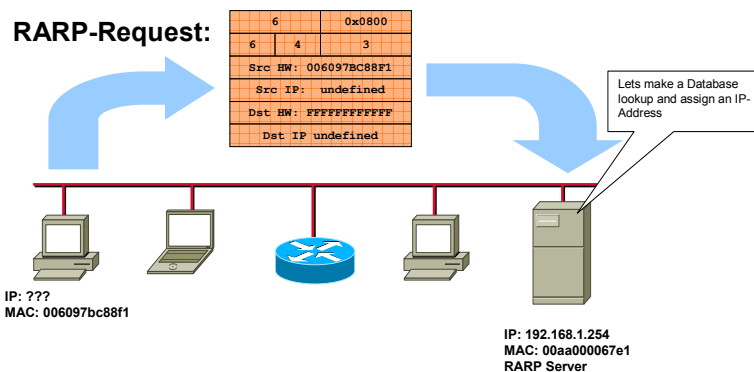
- ARP assumes, that an IP station knows its IP address (stored in NVRAM, on hard disk, in config file etc.).
- Diskless Machines usually don't have such means so they must retrieve an IP address for network booting.
- RARP (Reverse ARP) provides IP addresses for unconfigured stations.
- RFC 903

Reverse ARP (RARP)

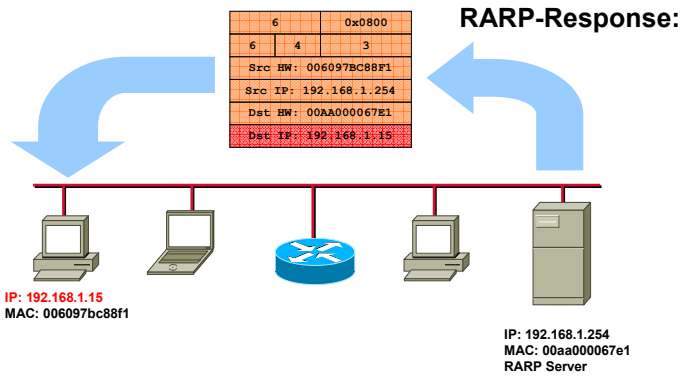


- A station sends a RARP request broadcast.
- One station, the RARP server, looks up the IP address for that MAC address in a database and replies.
- Newer methods:
 - ◆ BOOTP
 - ◆ DHCP

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”*

Proxy ARP (2)

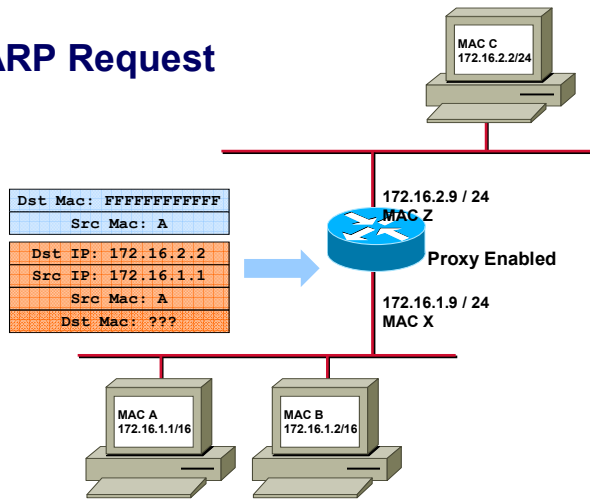


- Using Proxy ARP on routers, hosts do not need default gateway or routing entries to reach other subnets
- Default router's address = own interface address
 - ◆ Force ARP for every destination address
- If the local router is configured for Proxy-ARP it replies with an ARP response claiming to be the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

Proxy ARP (3)



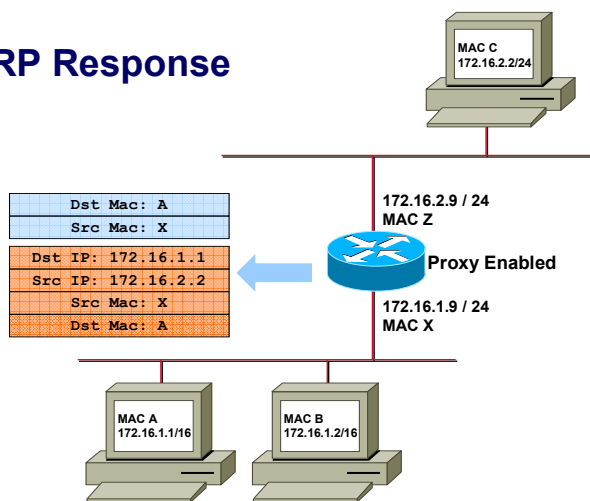
Proxy ARP Request



Proxy ARP (4)



Proxy ARP Response



Rules (1)



- **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

Disadvantages



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

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



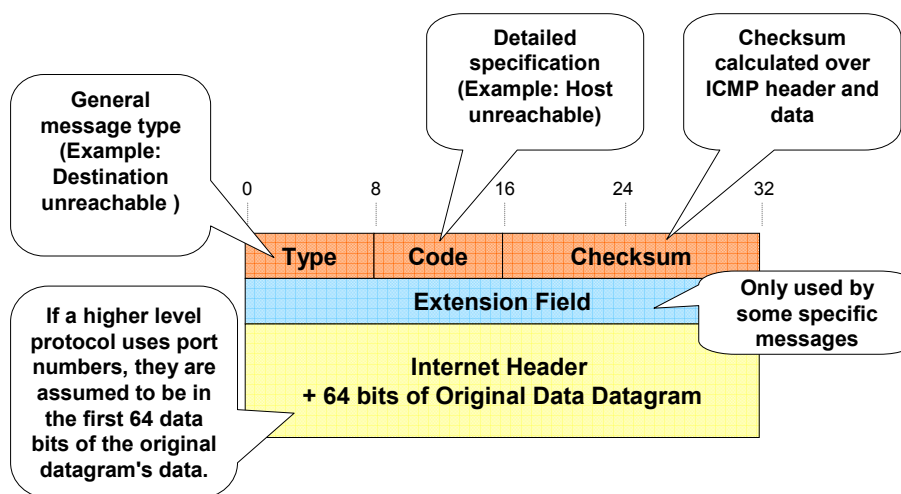
- Any station (host or router) detecting transmission problems sends ICMP error message back to the originator
- **ICMP gives feedback**
- ICMP messages are carried within IP packets
 - ◆ Protocol field = 1
 - ◆ ICMP header and code in the IP data area

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

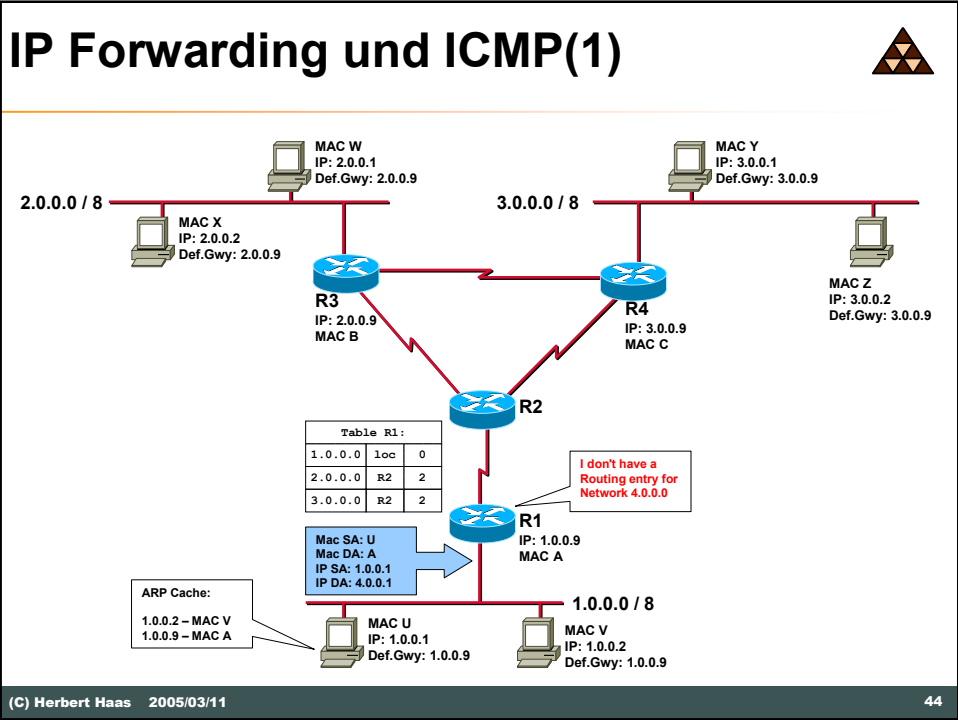
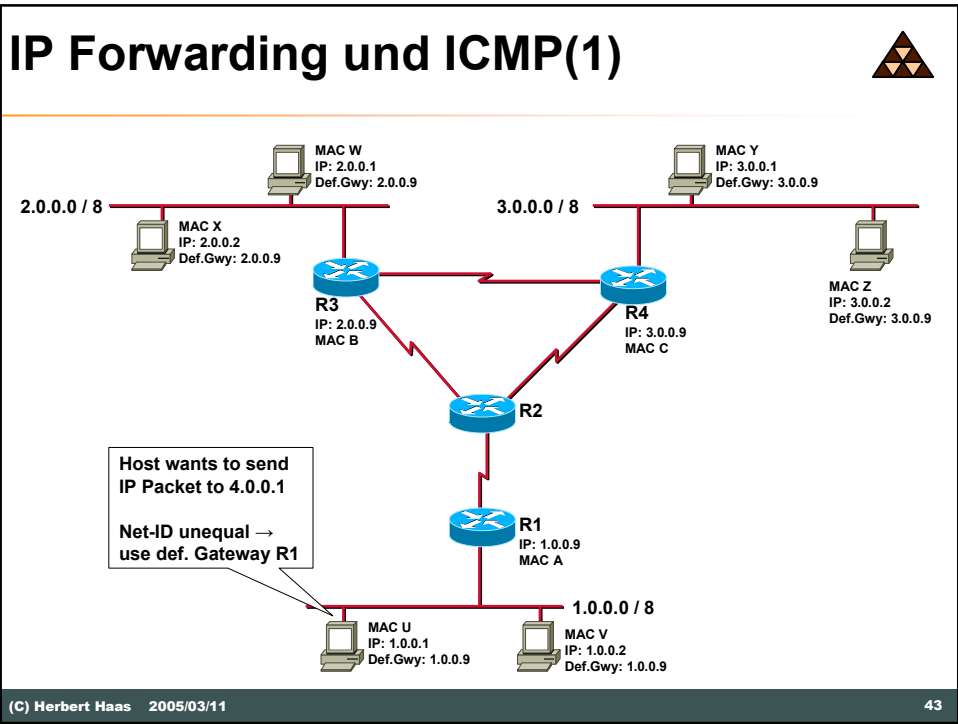


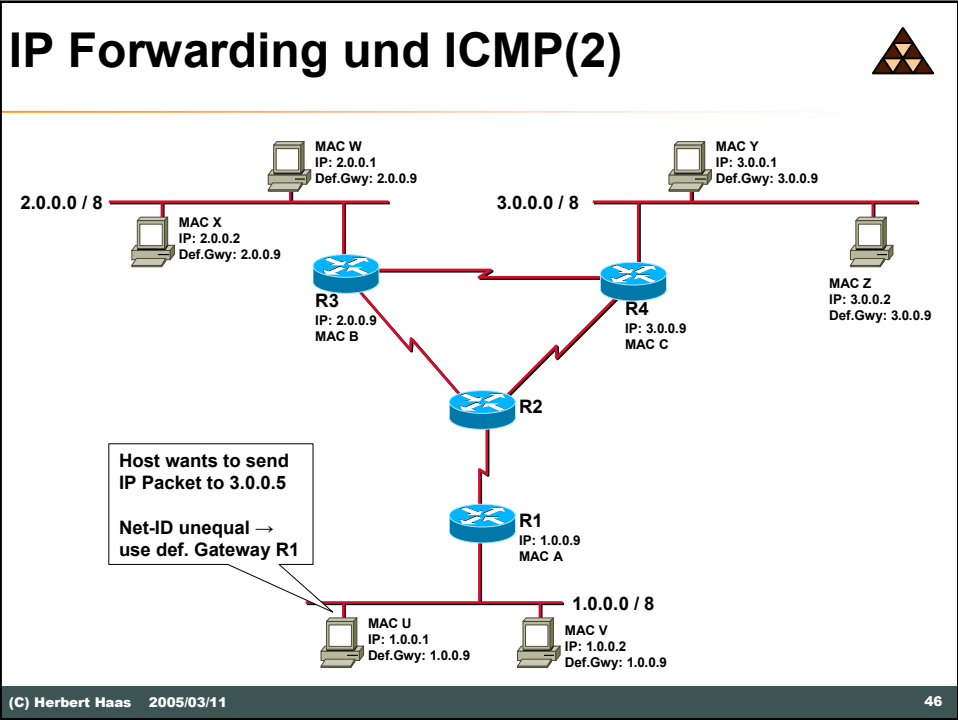
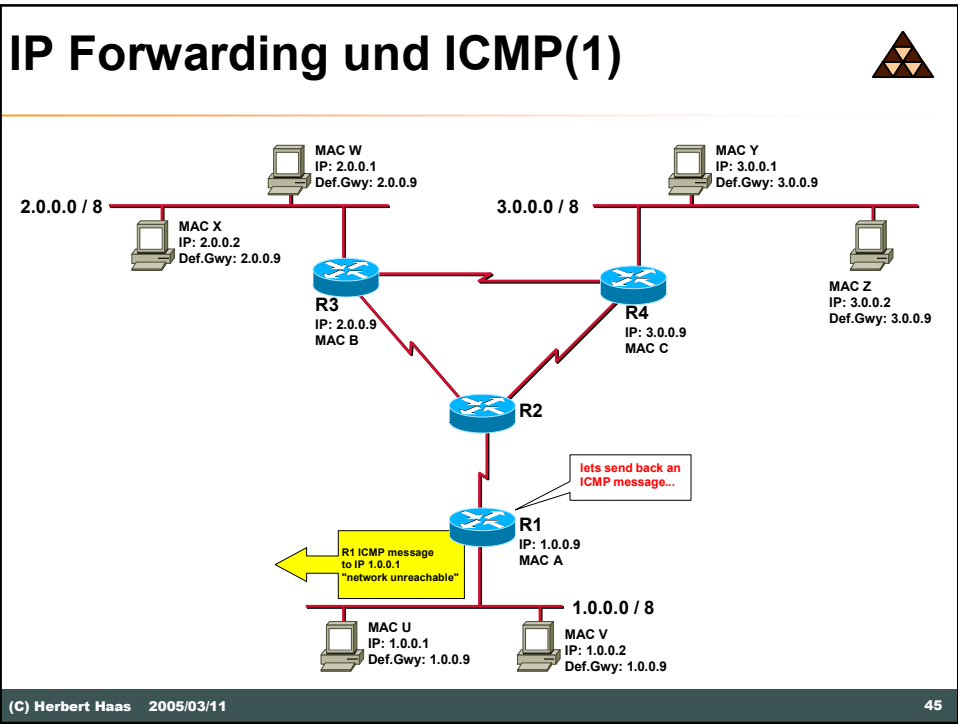
- (0)** - Echo reply ("PING")
- (3)** - Destination Unreachable
- (4)** - Source Quench (decrease data rate of sender)
- (5)** - Redirect (use different router)
- (8)** - Echo Request ("PING")
- (11)** - Time Exceeded (TTL = 0 or reassembly timer expired)
- (12)** - Parameter Problem (IP header)
- (13)** - 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

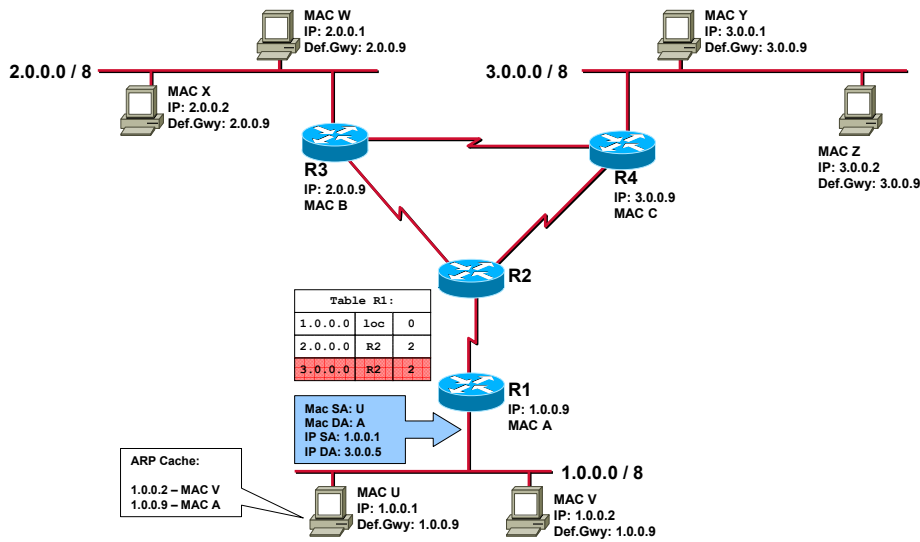


- (0)** - Network unreachable: no path to network known or network down; generated by intermediate or far-end router.
- (1)** - Host unreachable: Host-ID can't be resolved or host not responding; generated by far-end router.
- (2)** - Protocol unreachable: protocol specified in IP header not available; 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.

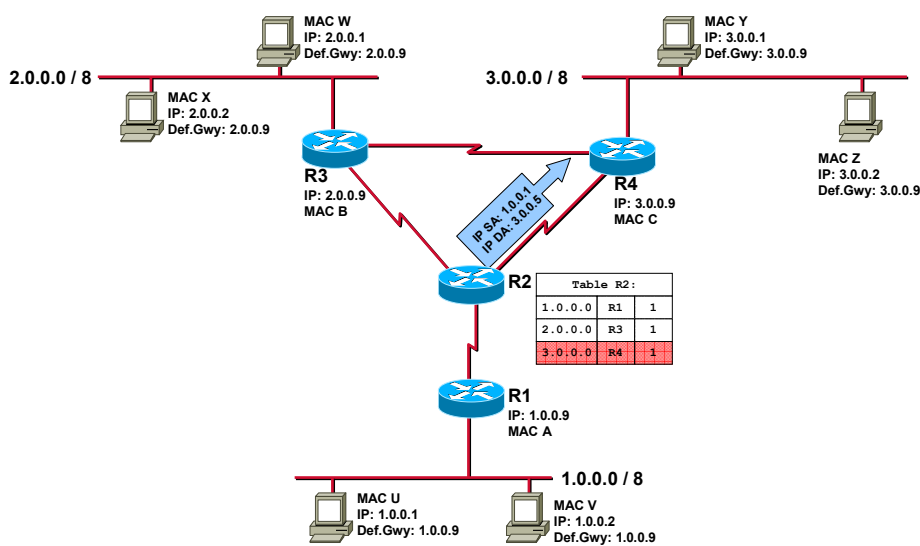




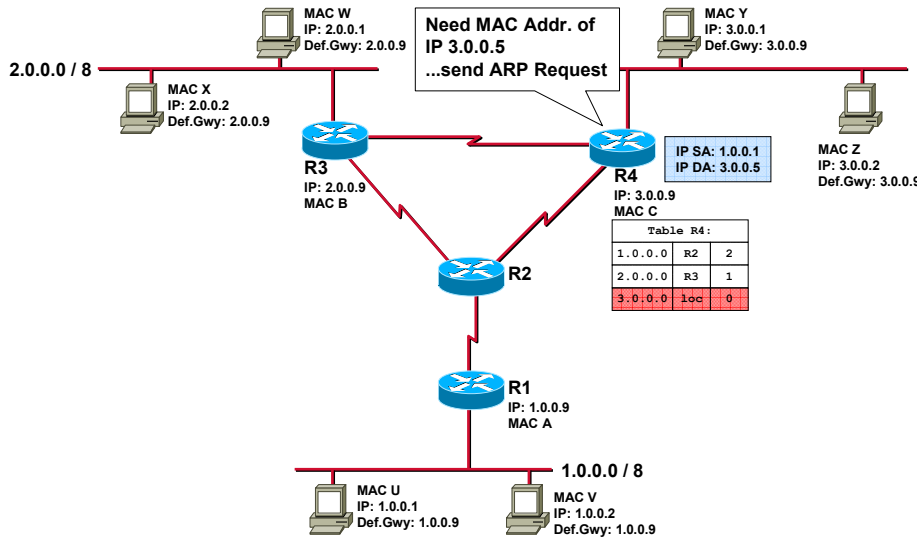
IP Forwarding und ICMP(2)



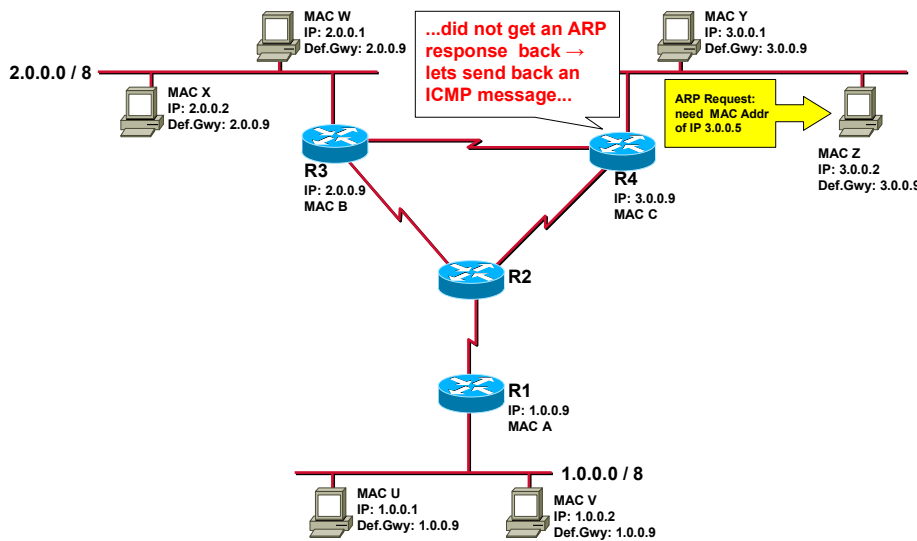
IP Forwarding und ICMP(2)



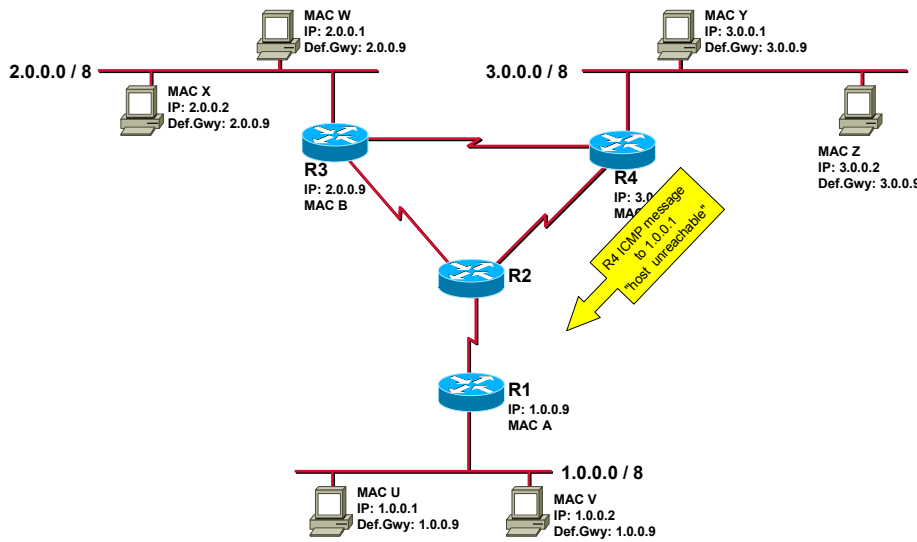
IP Forwarding und ICMP(2)



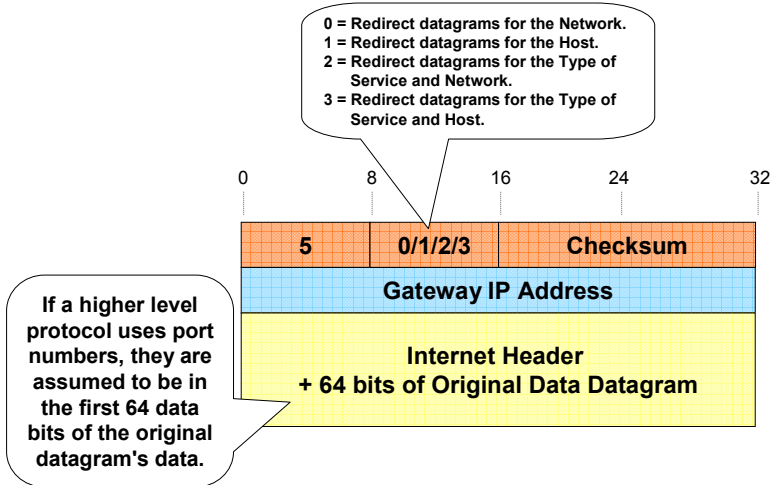
IP Forwarding und ICMP(2)



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

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 happened with its IP Packet
 - ♦ IP Stacks do not necessarily 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 timing out?**
- **Why should you use DHCP instead of RARP?**
- **What happens if a router discards an ICMP message?**
- **Ever heard of "Inverse ARP"?**

Hints



- **Q1: Point to point connection (no shared media)**
- **Q2: With infinite ARP-cache entries – changing IP-Addresses could be a problem**
- **Q3: More flexible – many things can be assigned (Subnet Mask(!), Def.Gwy,DNS-Srv ...)**
- **Q4: Router will NOT produce a new ICMP message (The Internet would be down in minutes if router would create new ICMP messages for every lost one)**
- **Q5: Used together with Frame Relay**