# IP Technology

Introduction, IP Protocol Details

IP Addressing and IP Forwarding

ARP, ICMP, PPP, HSRP, VRRP

# Agenda

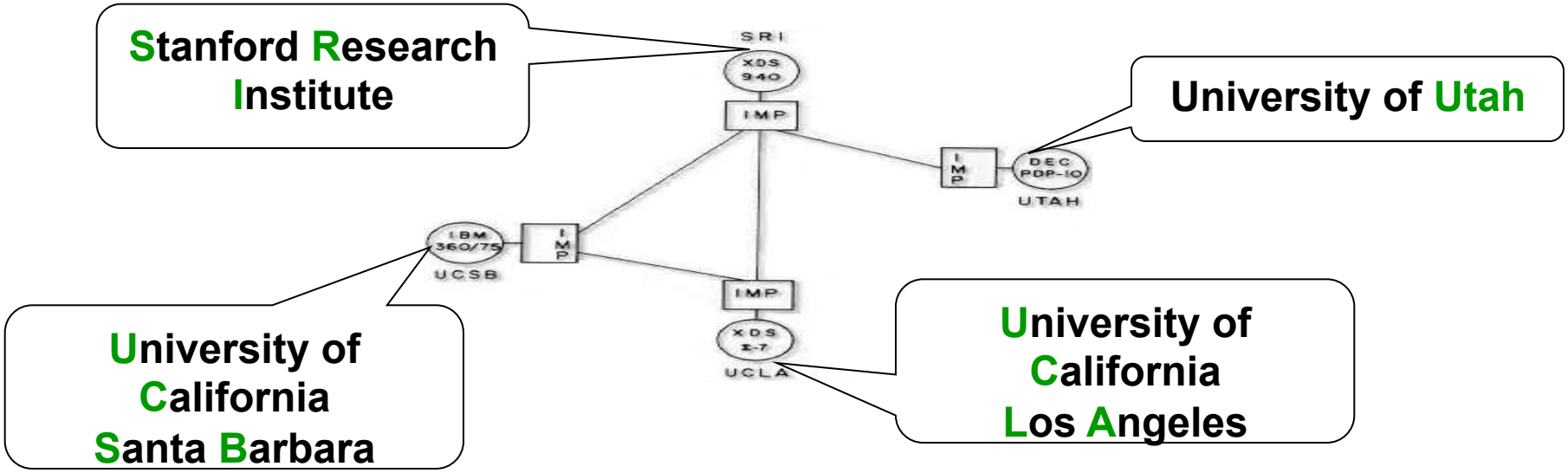
- **Introduction**
  - Short History of the Internet (not part of the exam!)
  - Basic Principles
- **IP**
  - IP Protocol
  - IP QoS
  - Addressing
  - Classful versus Classless (not part of the exam!)
- **IP Forwarding**
  - Principles
  - ARP
  - ICMP
  - PPP
- **First Hop Redundancy**
  - Proxy ARP, IDRP
  - HSRP
  - VRRP (not part of the exam!)

# Before Arpanet

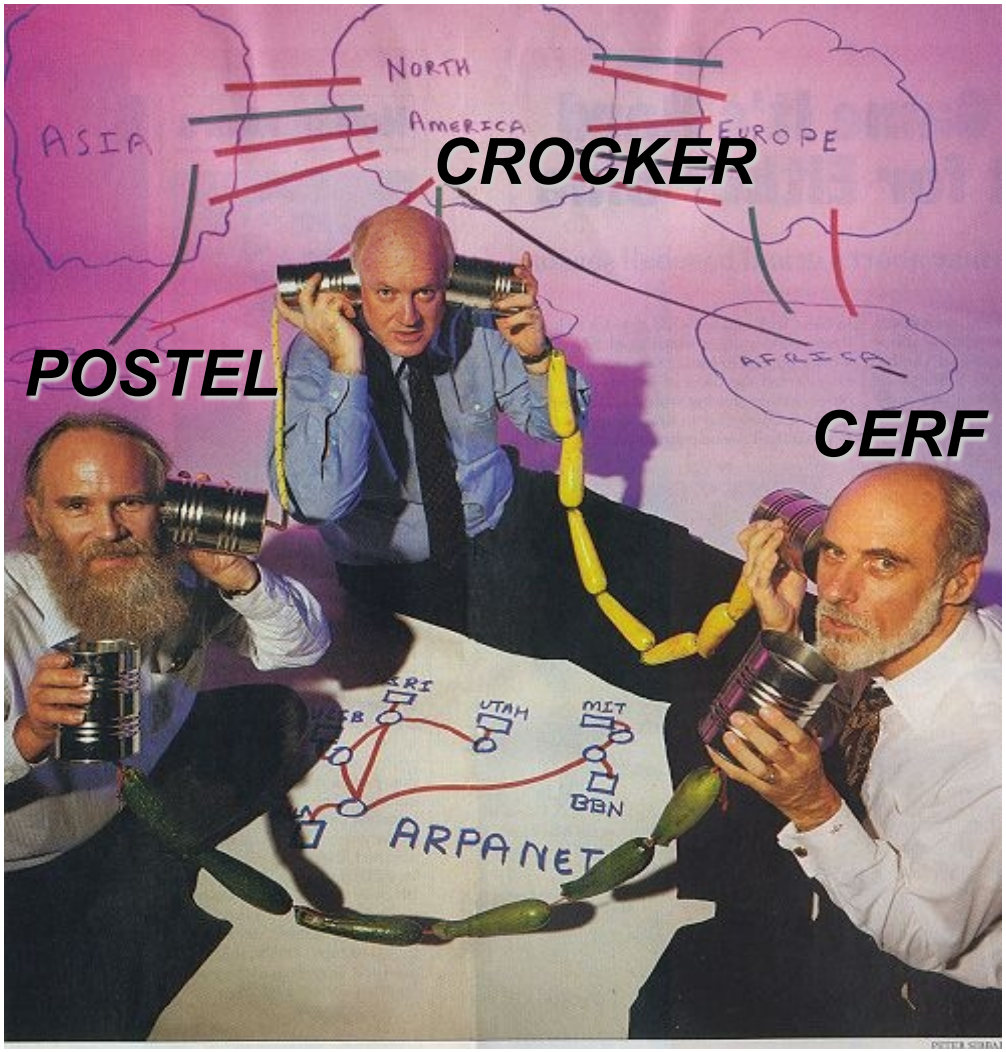
- 1957 - USSR launches Sputnik
- 1958 - US Congress Funds the Advanced Research Projects Agency (ARPA) for Space and Computer Research
- 1958 - ARPA Placed Under DOD
- 1958 - Space Research is Spun off to Separate Organization, NASA
- 1958 - ARPANET Design Discussions Started

# Birth Of The Arpanet

- Birth of the Arpanet: 1. Sept. 1969
- Predecessors of "Routers":
  Interface Message Processors (IMPs)
- First packet-switched network
- Connected UCLA, SRI, UCSB, UTAH



# Birth Of The Arpanet



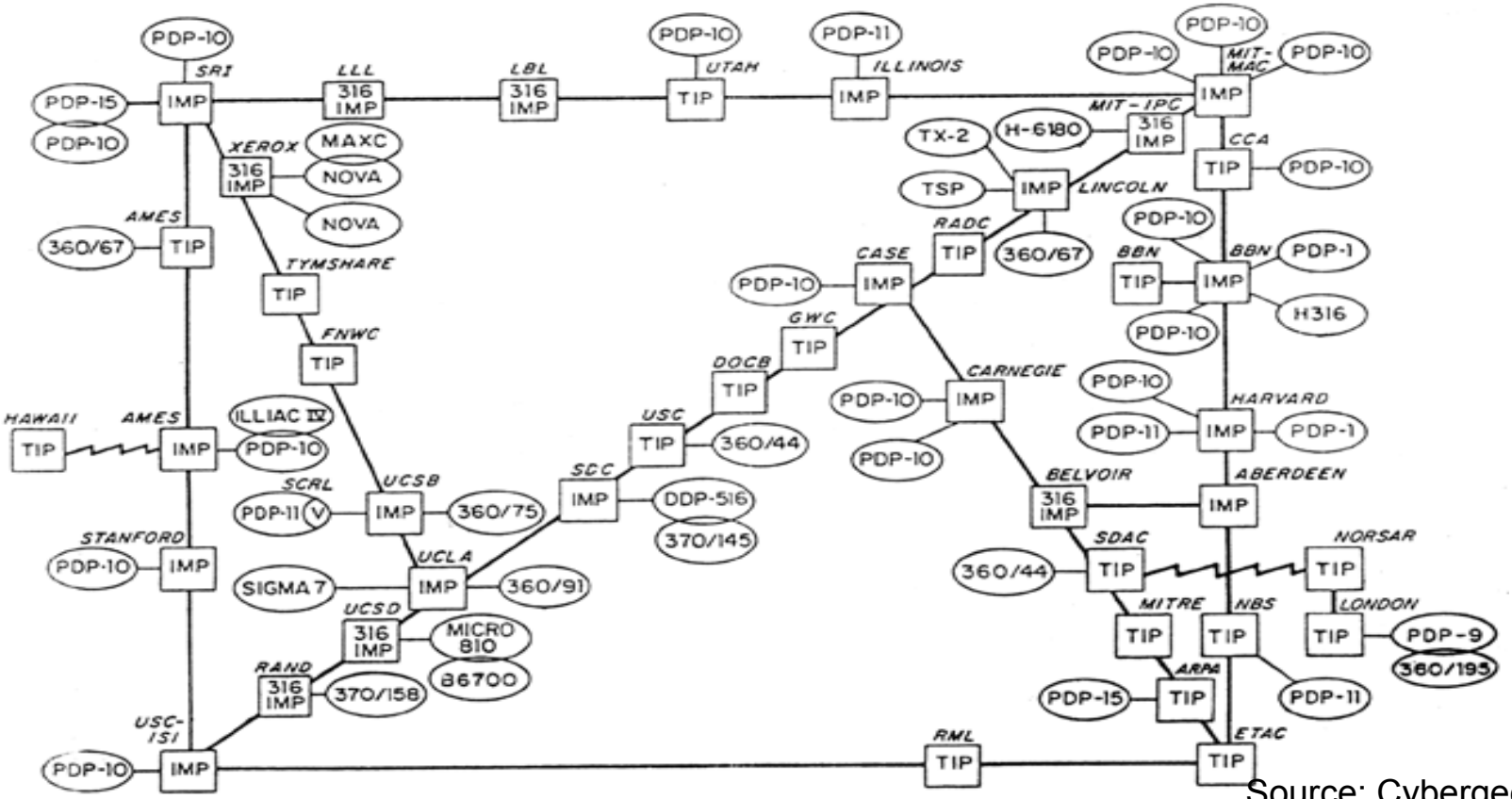

Newsweek, Aug 8,1994

# Birth Of The Arpanet

- **1970 - Arpanet use the Network Control Protocol (NCP)**
- **1971 - Arpanet connects 15 sites including universities and research organizations**
  - Birth of TELNET and FTP
- **1972 - Ray Tomlinson created first email program**
  - ALOHAnet connected to the Arpanet

# Birth Of The Arpanet

- 1973 - Arpanet comprises 35+ hosts

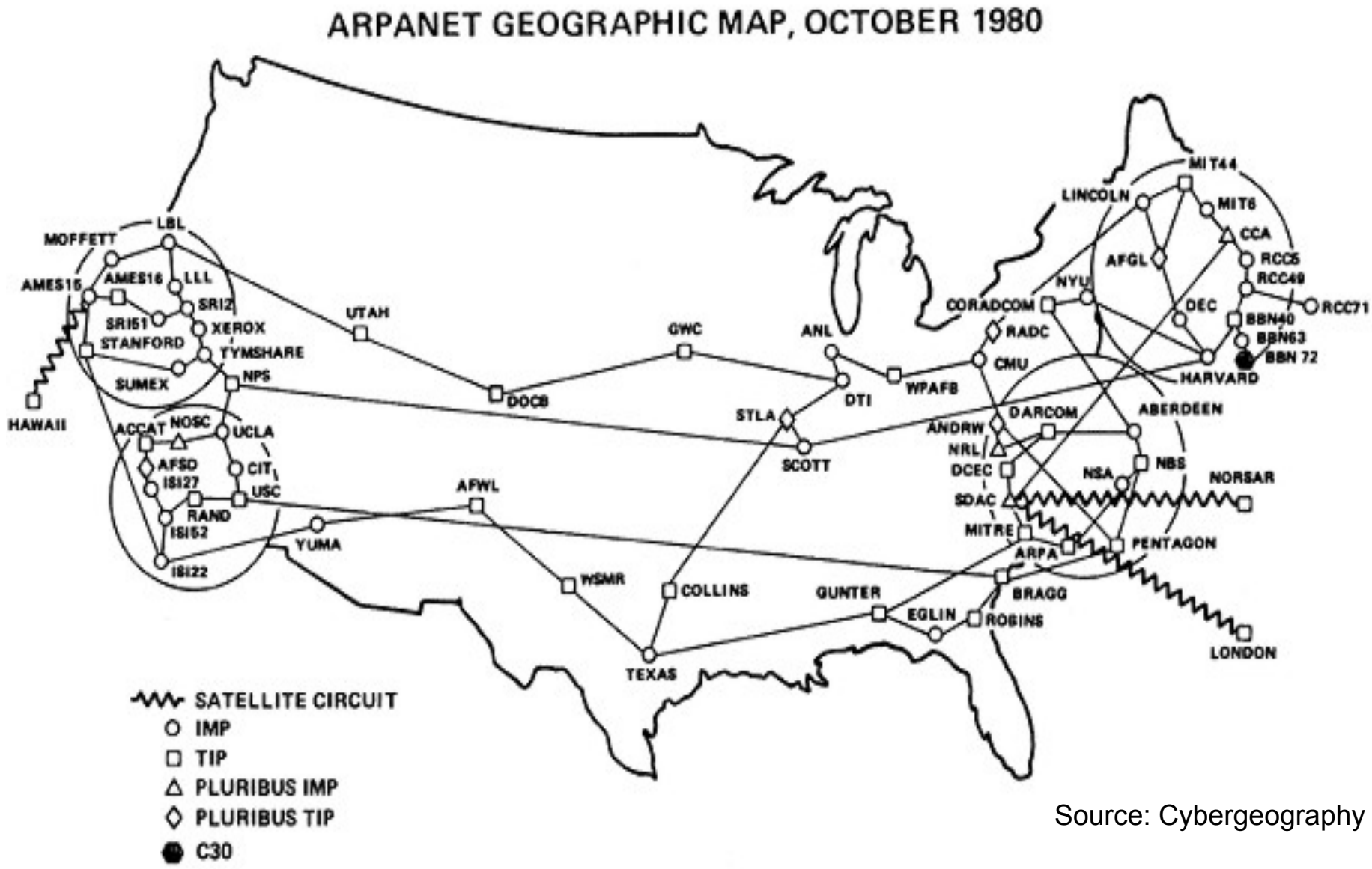



Source: Cybergeography

# The Arpanet Problem - Birth of TCP/IP and the Internet

- **Arpanet communicate with NCP but other networks use different protocols**
- **1974 - Transmission Control Protocol (TCP) specification published**
- **TCP enabled the expansion from the Arpanet to a worldwide Internet !**
- **The Winner: TCP/IP**
- **1978 - TCP Split into TCP and IP**
- **1983 - Arpanet converts to TCP/IP**
  - UNIX (v4.2 BSD) released with TCP/IP
  - DARPA switched from Arpanet architecture to Internet architecture with TCP/IP as base protocols

# Getting Bigger And Bigger




Source: Cybergeography

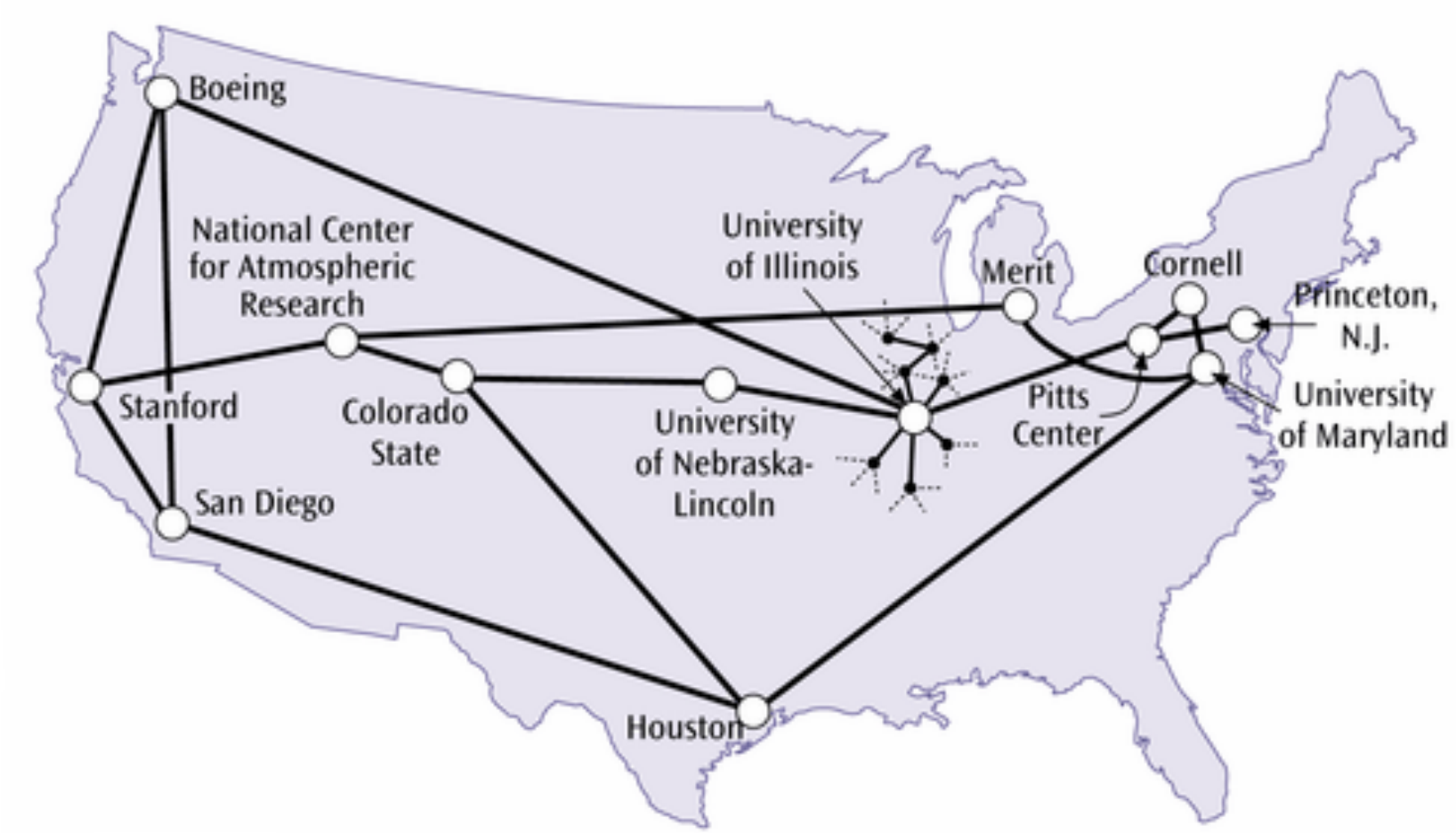
# Development Going On

- 1983 - Arpanet Splits into Arpanet and MILNET
- 1983 - Internet Activities Board (IAB)
- 1984 - Domain Name System (DNS)
- 1985 - Symbolics.com first registered domain.

# NSFNET Backbone

- **National Science Foundation (NFS) creates the NSFNET Backbone 1986**
- **It connects Cornell, Princeton, UC-SD, Pitt and UI-UC with 56k Lines**
- **Dramatic growth of hosts**
  - 1986: February 2000, November 5000.
- **Backbone is upgraded to T1 (1.544Mb/s) - 1988**

# NSFNET Backbone




Source: Cybergeography

# The Internet

- **1989 - Number of hosts: 100,000 !**
  - Reseaux IP Europeens (RIPE) founded
- **1990 - Arpanet Decommissioned, Now officially called "Internet“**
- **1990 - First Internet provider, “The World” comes online**

# The Internet

- 1991 - World Wide Web (WWW) Created by Tim Berners-Lee at CERN, http://www.cern.ch/
- 1991 - Backbone is upgraded to T3 (44.736Mbps)
- 1992 - Internet Society (ISOC) is chartered
- 1992 - Number of hosts: 1,000,000

# The Internet

- 1992 - Term: “Surfing the Internet” coined by Jean Armour Polly
- 1993 - Mosaic introduced first graphical Web browser
- 1993 - WWW is 0.1% of NSFNET Traffic

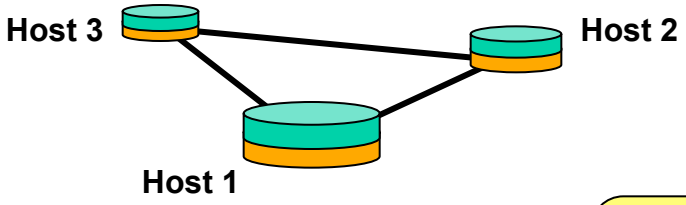
# Network Access Points

- **1993 - NSF specifies creations of Network Access Points (NAPs)**
  - Privatize the Internet – Replace Government funded
  - NSFNET backbone with (many) commercial Internet backbones
  - Central points to Interconnect Commercial Internet Backbones
  - Allow anyone to access the Internet via Internet
  - Service Providers (ISPs) – Connected to Backbones
- **1994 - Four NAPs Created**
  - San Francisco, Chicago, Washington D.C., New Jersey
- **1995 - NSFNET Backbone is decommissioned**

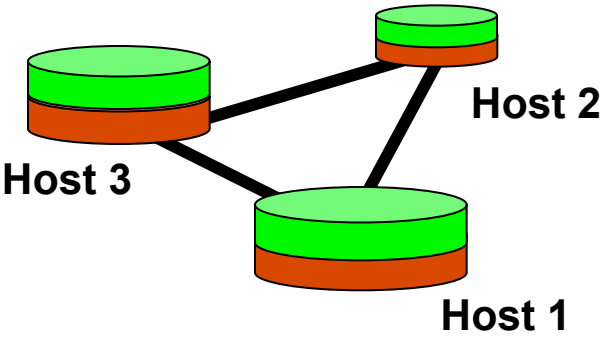
# Agenda

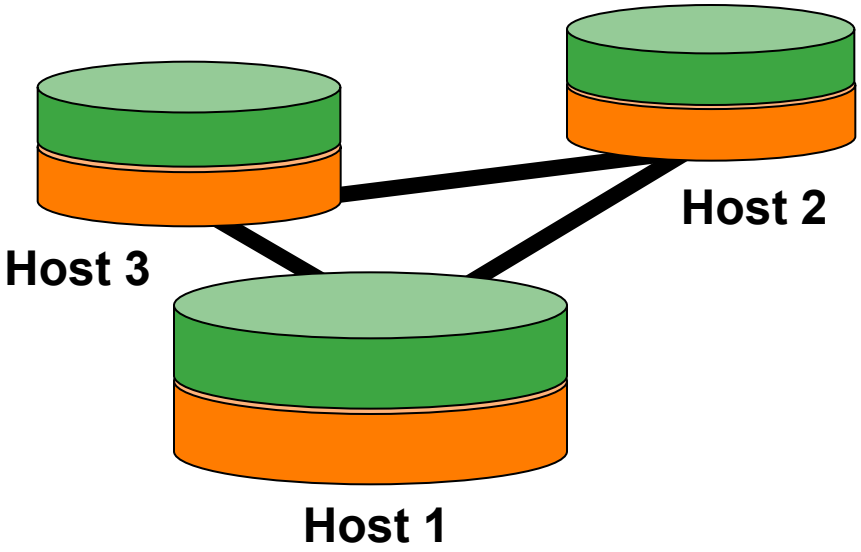
- **Introduction**
  - Short History of the Internet (not part of the exam!)
  - Basic Principles
- **IP**
  - IP Protocol
  - IP QoS
  - Addressing
  - Classful versus Classless (not part of the exam!)
- **IP Forwarding**
  - Principles
  - ARP
  - ICMP
  - PPP
- **First Hop Redundancy**
  - Proxy ARP, IDRP
  - HSRP
  - VRRP (not part of the exam!)

# Need of an Inter-Net Protocol (1)



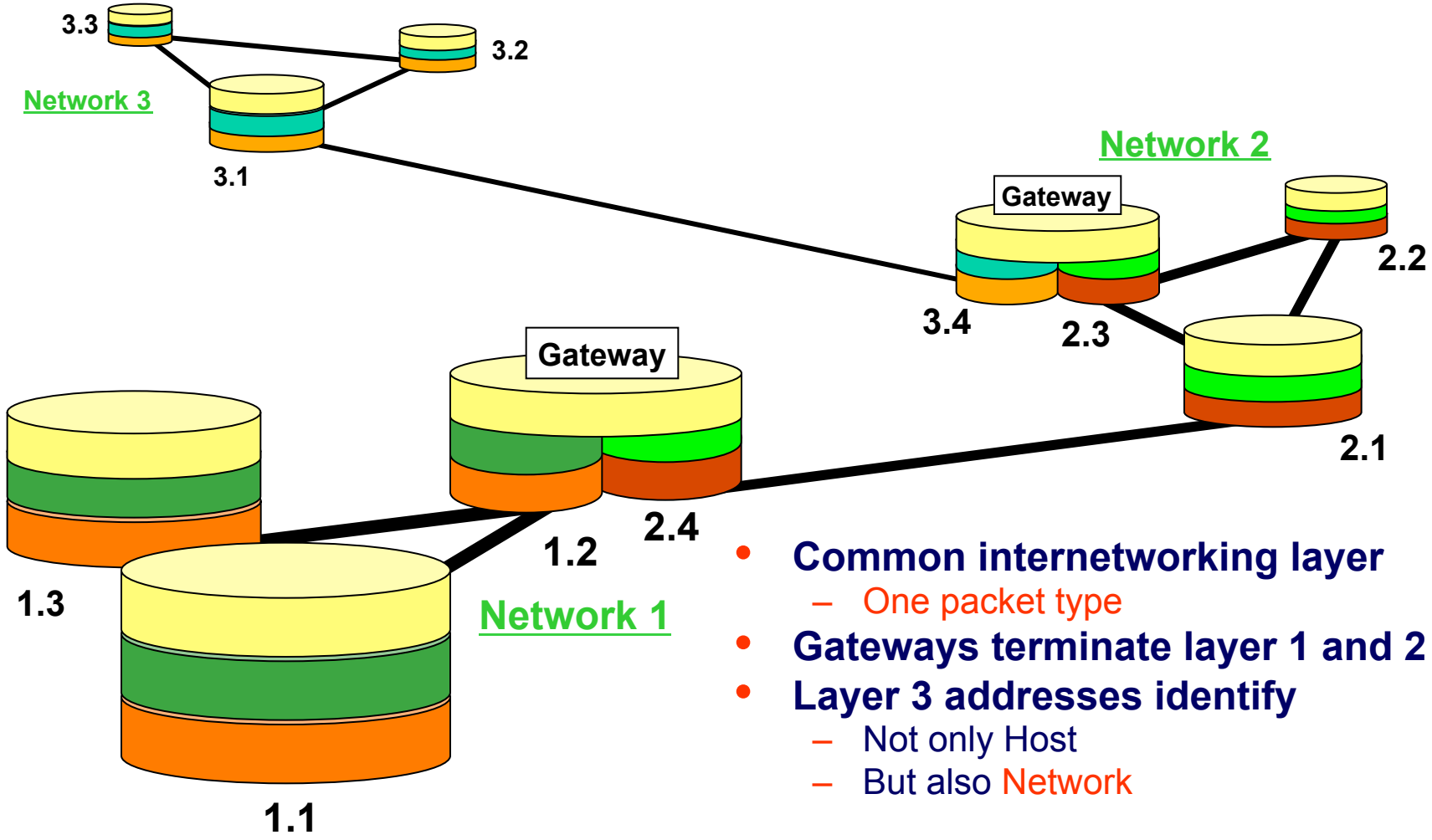

**No interconnection possible !!!**




- **Different Data-Link Layer**
  - Different frames
  - Different protocol handling
- **Different Physical Layer**
  - Different hardware
  - Different signals

# Need of an Inter-Net Protocol (2)

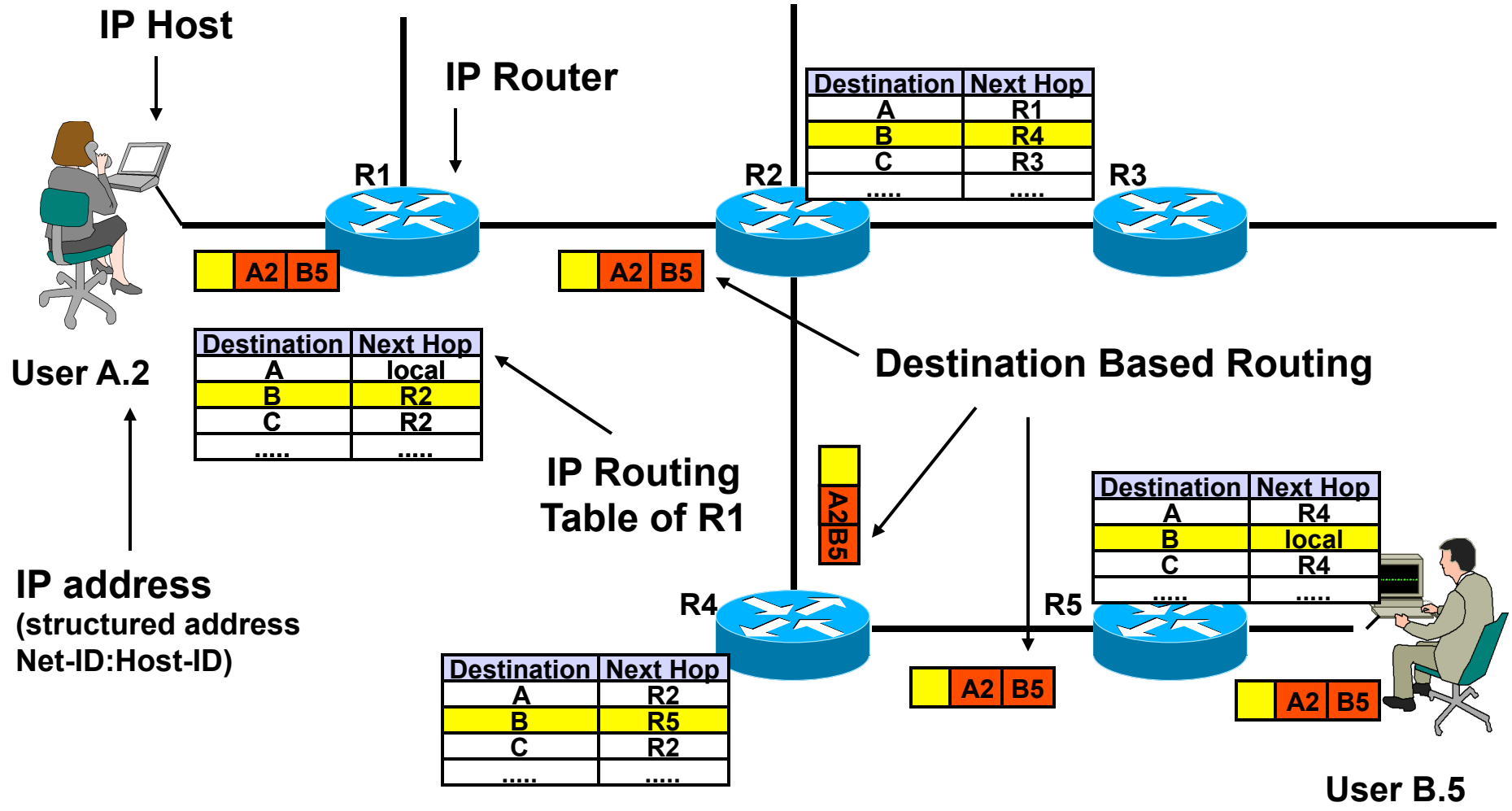



- **Common internetworking layer**
  - One packet type
- **Gateways terminate layer 1 and 2**
- **Layer 3 addresses identify**
  - Not only Host
  - But also Network

# IP Technology

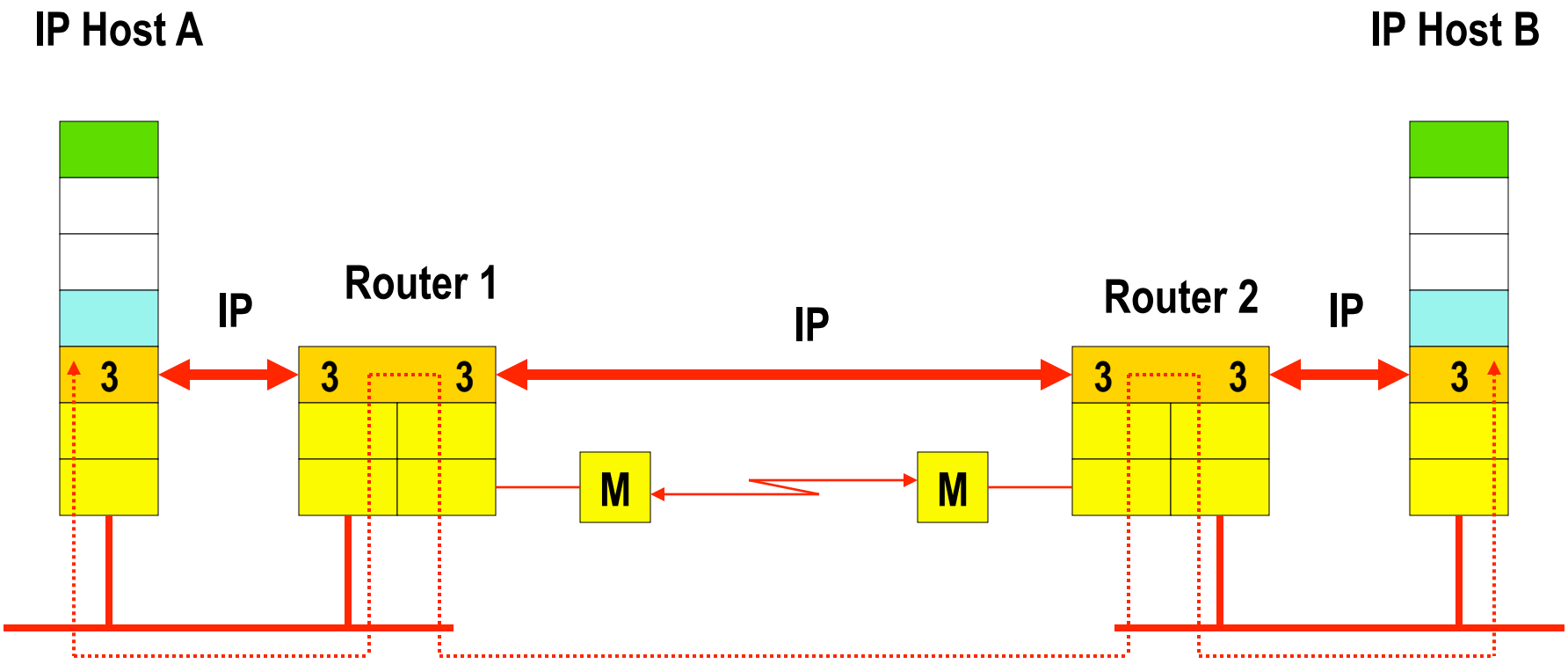
- **IP (Internet Protocol)**
  - Packet switching technology
    - Packet switch is called router or gateway (IETF terminology)
    - End system is called IP host
    - Structured layer 3 address (IP address)
- **Datagram service**
  - Connectionless
    - Datagrams are sent without establishing a connection in advance
  - Best effort delivery
    - Datagrams may be discarded due to transmission errors or network congestion

# IP Datagram Service



# IP and OSI Network Layer 3

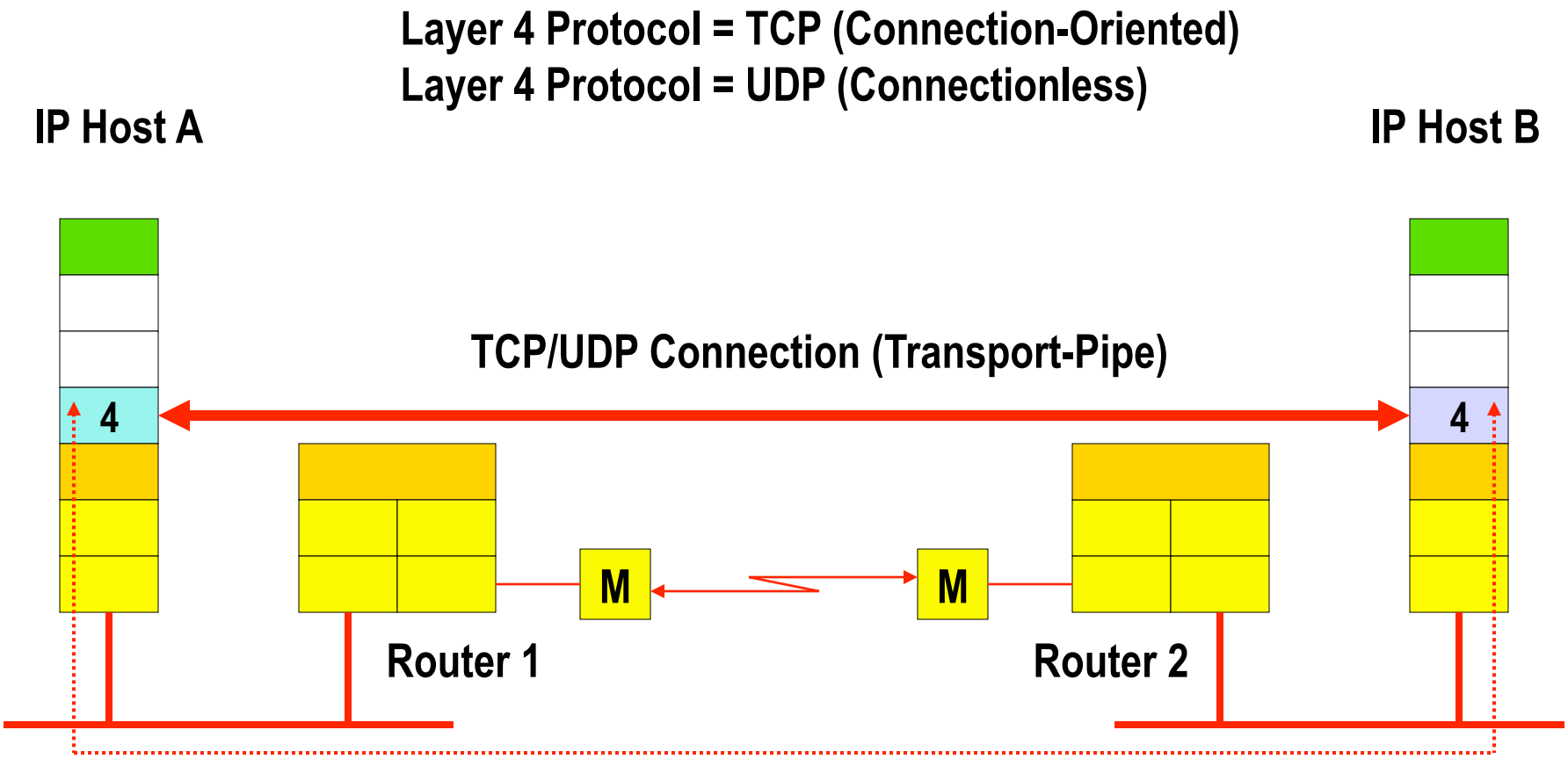
Layer 3 Protocol = IP
Layer 3 Routing Protocols = RIP, OSPF, EIGRP, BGP



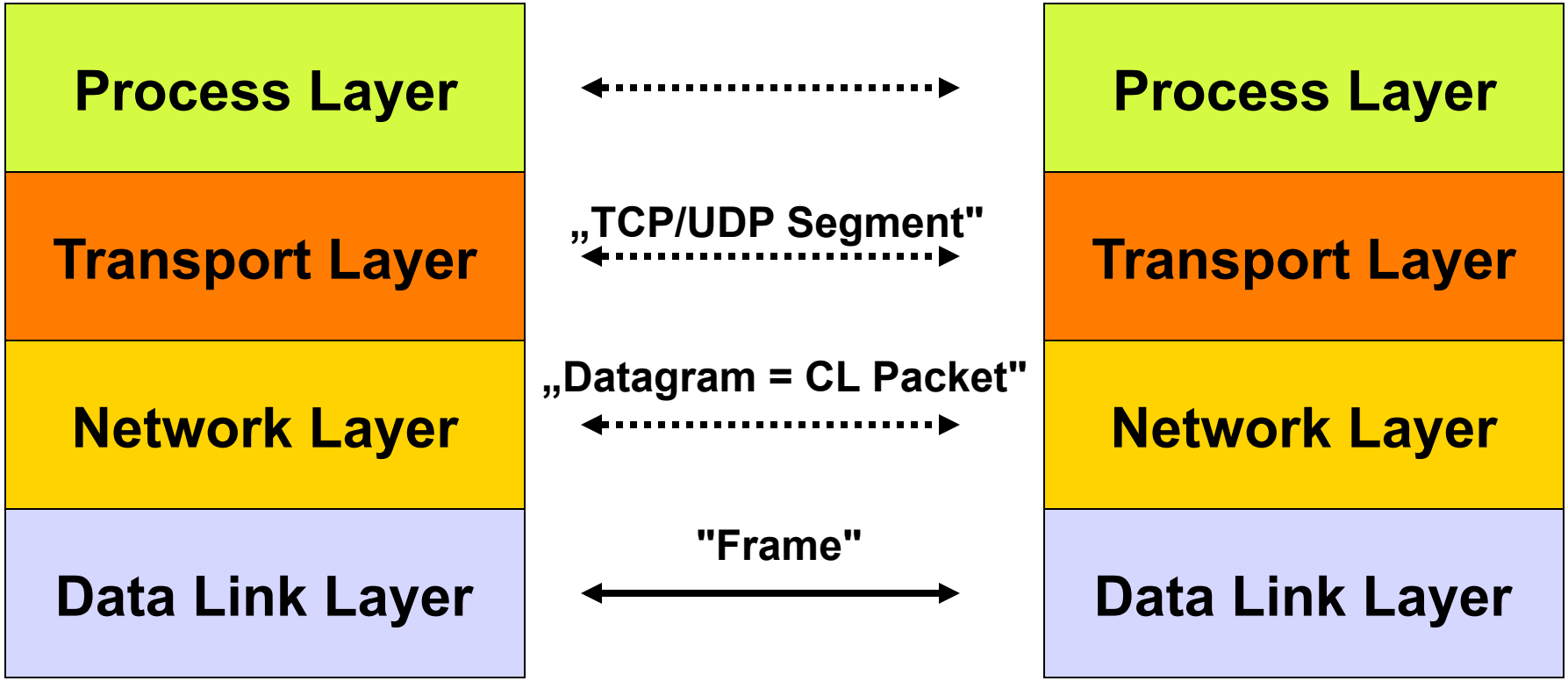
# TCP Technology

- **Shared responsibility between network and end systems**
  - Routers responsible for delivering datagrams to remote networks based on structured IP address
  - IP hosts responsible for end-to-end control
- **End to end control**
  - Is implemented in upper layers of IP hosts
  - TCP (Transmission Control Protocol)
    - Connection oriented
    - Sequencing, windowing
    - Error recovery by retransmission
    - Flow control between end systems

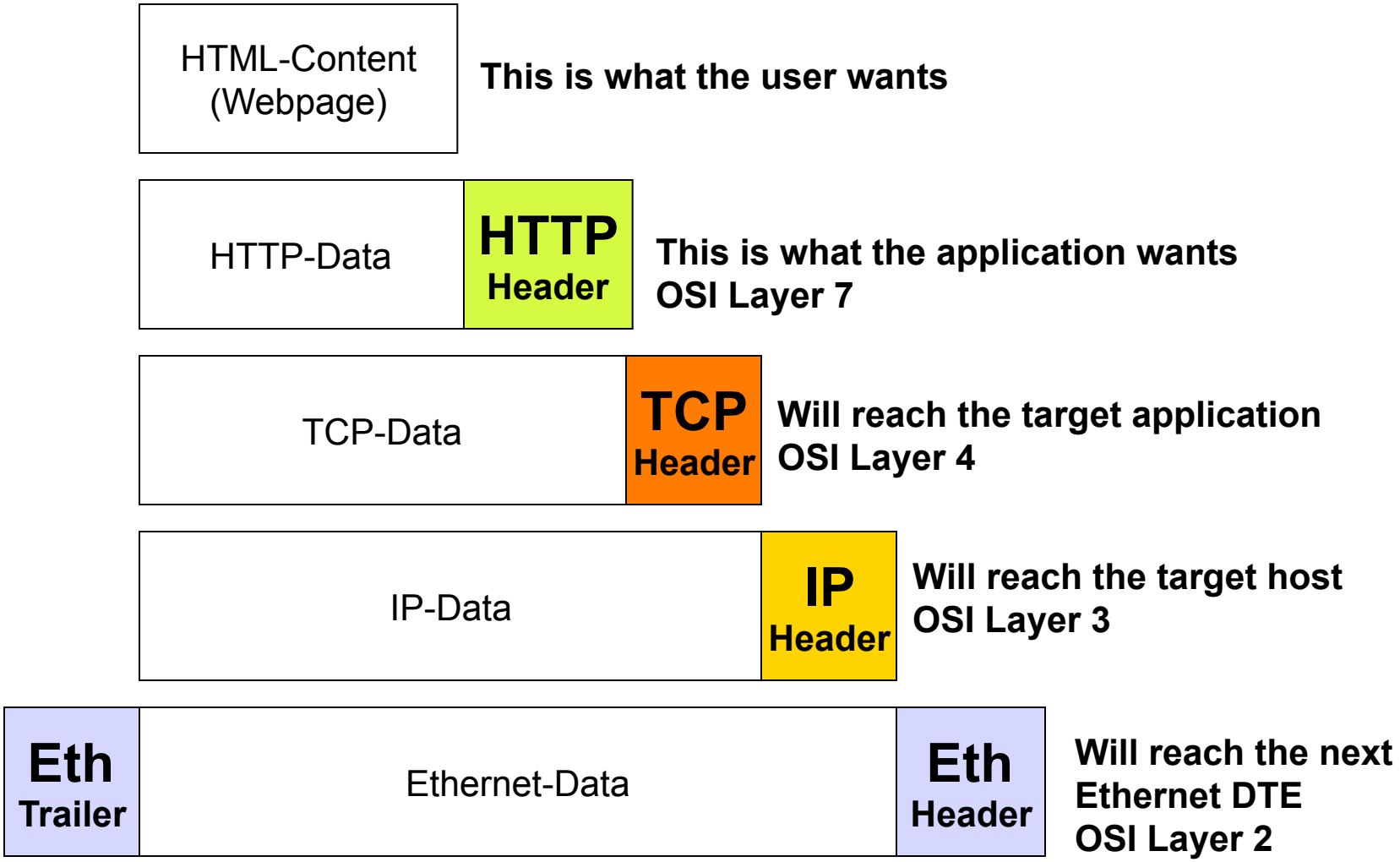
# TCP/UDP and OSI Transport Layer 4



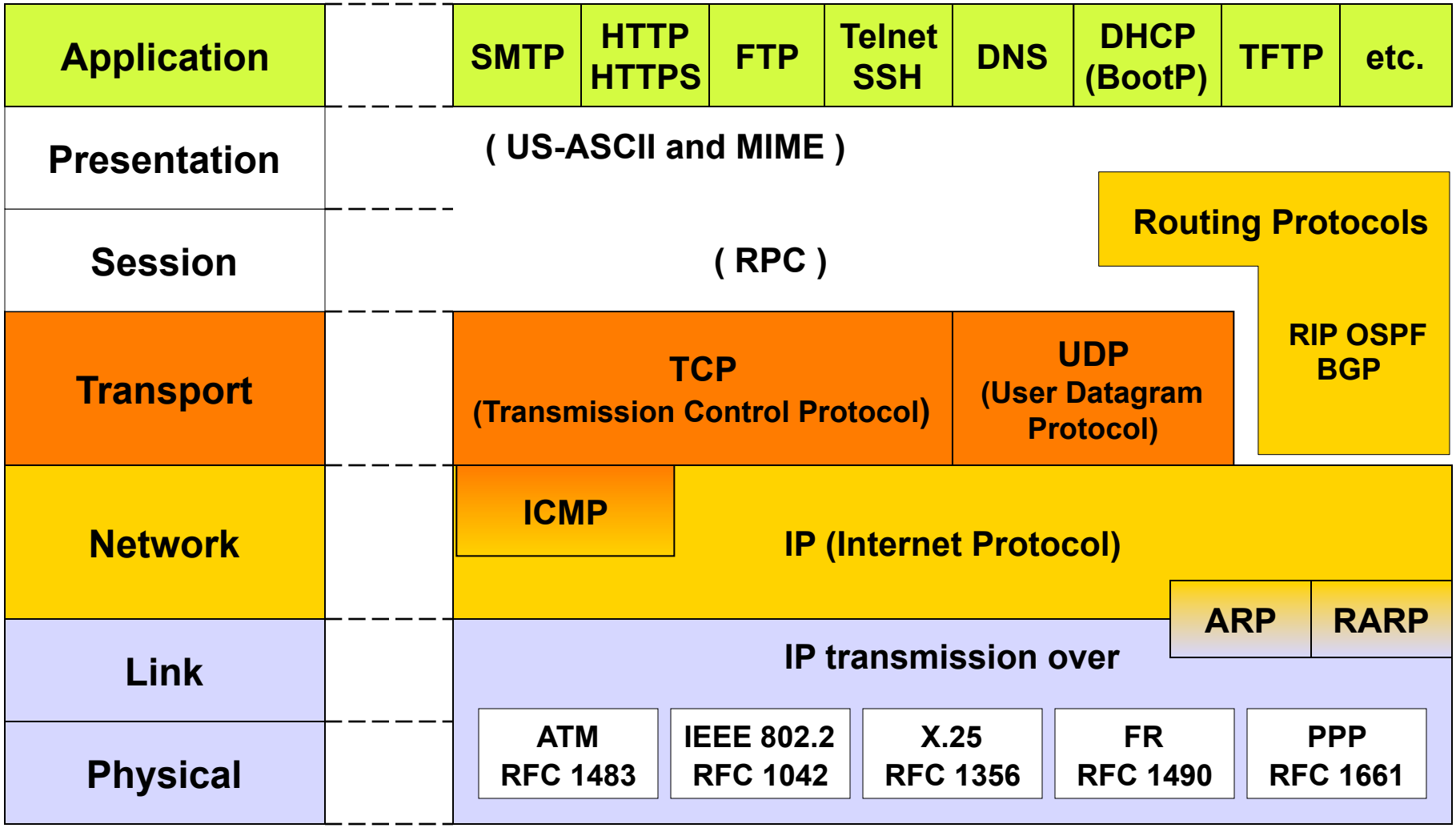
# DoD 4-Layer Model (Internet)



# Internet Encapsulation



# TCP/IP Protocol Suite



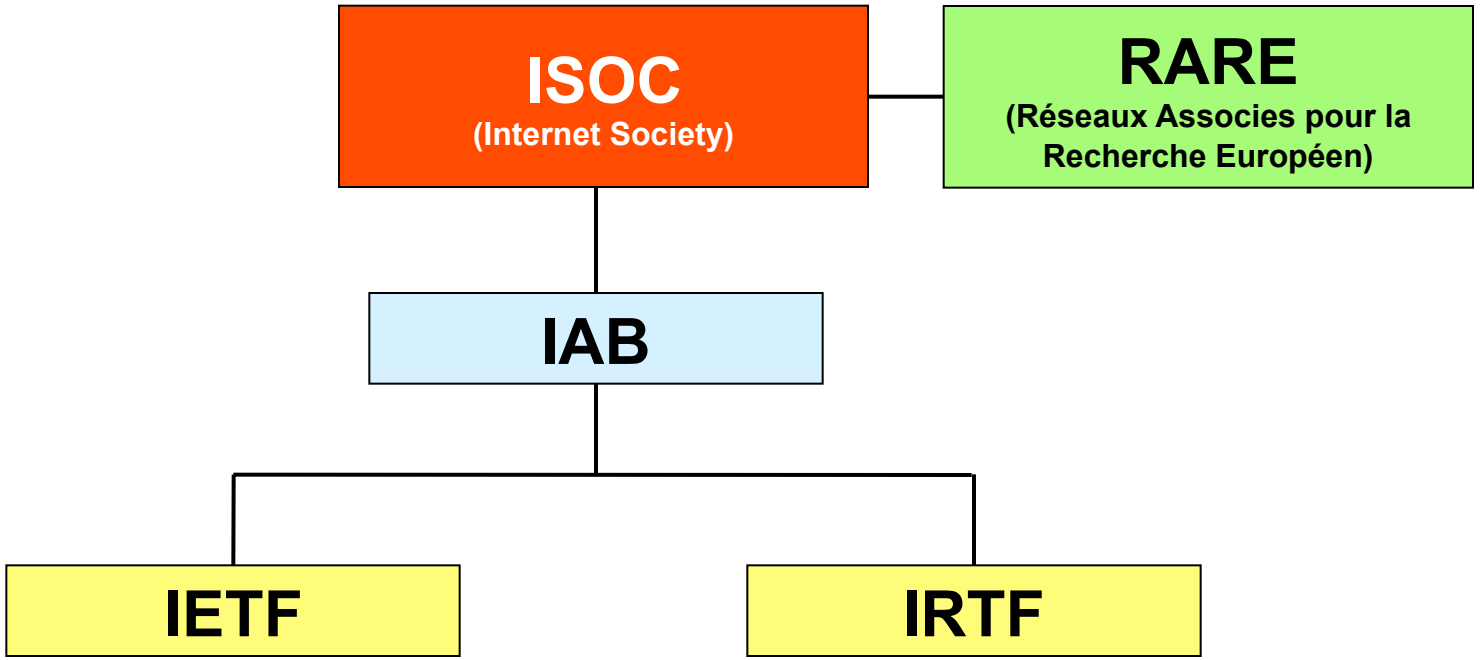
# TCP/IP Story of Success

- **IP over everything**
  - Overlay technique
- **End-to-end principle**
  - Network could be stupid simple
  - End systems do the sophisticated tasks like TCP
- **TCP**
  - Best implementation of a transport protocol nowadays
- **WWW**
  - Killer application in the 1990´s
- **Standardization**
  - Standardization of running code

# Internet Standardization - RFC

- **Requests for Comments (RFC)**
  - "Give me your input to my ideas I have already implemented"
- **Today's process is best described by**
  - RFC-2026 (The Internet Standards Process Revision3)
  - Draft -> IETF decision if new RFC -> RFC number
- **Status April 2012:**
  - RFC 6607
- **Attention:**
  - Not every RFC is an Internet Standard
  - Categories:
    - Informational, Experimental, Historic
    - Proposed Standard
    - Draft Standard
    - Standard
- **Where to find:**
  - http://www.rfc-editor.org/index.html

# Internet Organizations



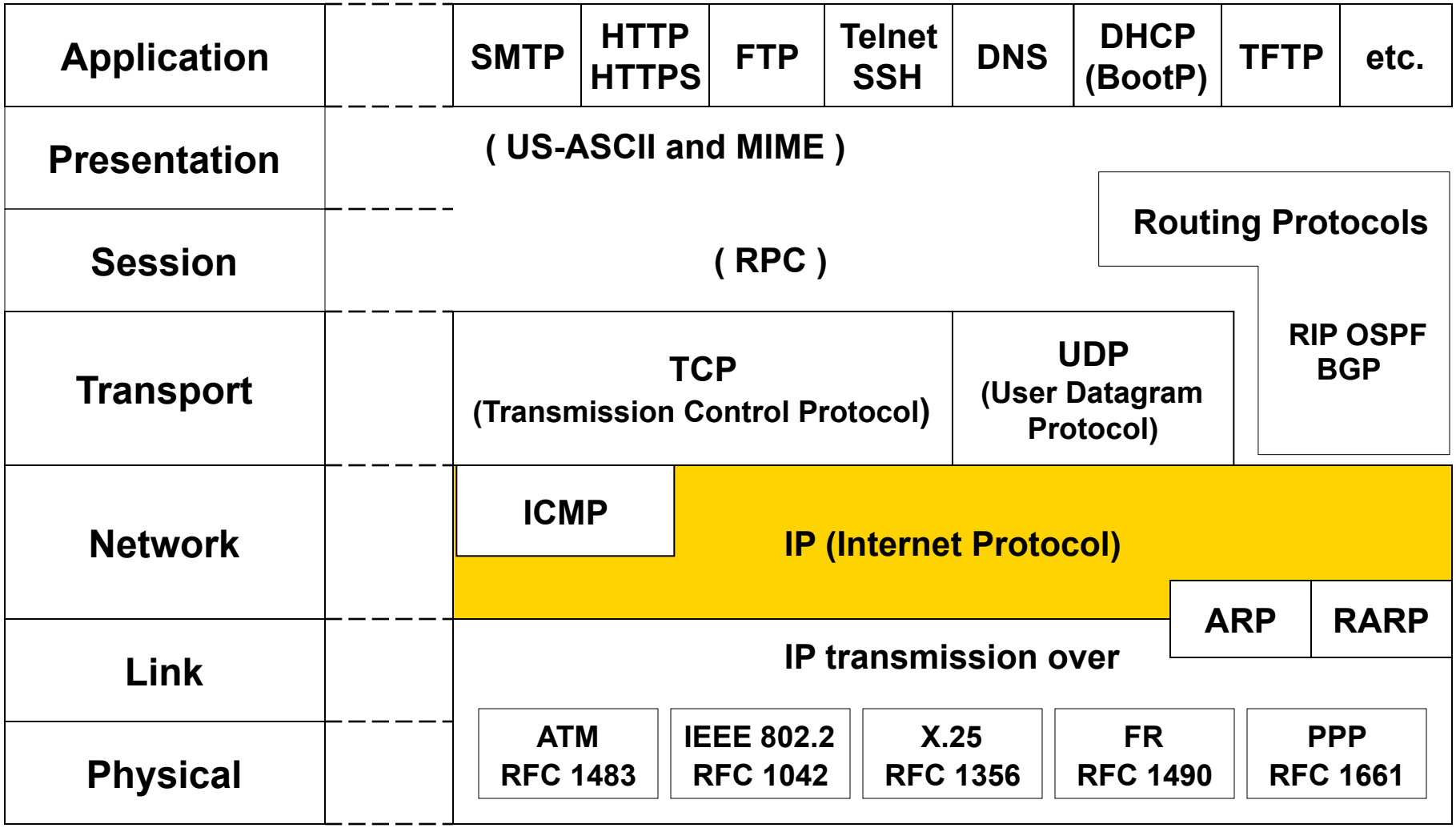
# Internet in Europe

- **RIPE NCC (Réseaux IP Européens Network Coordination Center)**
  - Internet Registry
    - Assigning IP addresses
    - Assigning AS numbers
  - Routing Registry
    - Coordinating policies between Internet Service Providers (ISP)
  - How to contact?
    - RIPE NCC
    - Singel 258
    - 1016 AB Amsterdam
    - The Netherlands
    - Phone: +31 20 535 4444 , Fax: +31 20 535 4445
    - E-Mail: <ncc@ripe.net>, WWW: <http://www.ripe.net>

# Agenda

- **Introduction**
  - Short History of the Internet (not part of the exam!)
  - Basic Principles
- **IP**
  - IP Protocol
  - IP QoS
  - Addressing
  - Classful versus Classless (not part of the exam!)
- **IP Forwarding**
  - Principles
  - ARP
  - ICMP
  - PPP
- **First Hop Redundancy**
  - Proxy ARP, IDRP
  - HSRP
  - VRRP (not part of the exam!)

# TCP/IP Protocol Suite



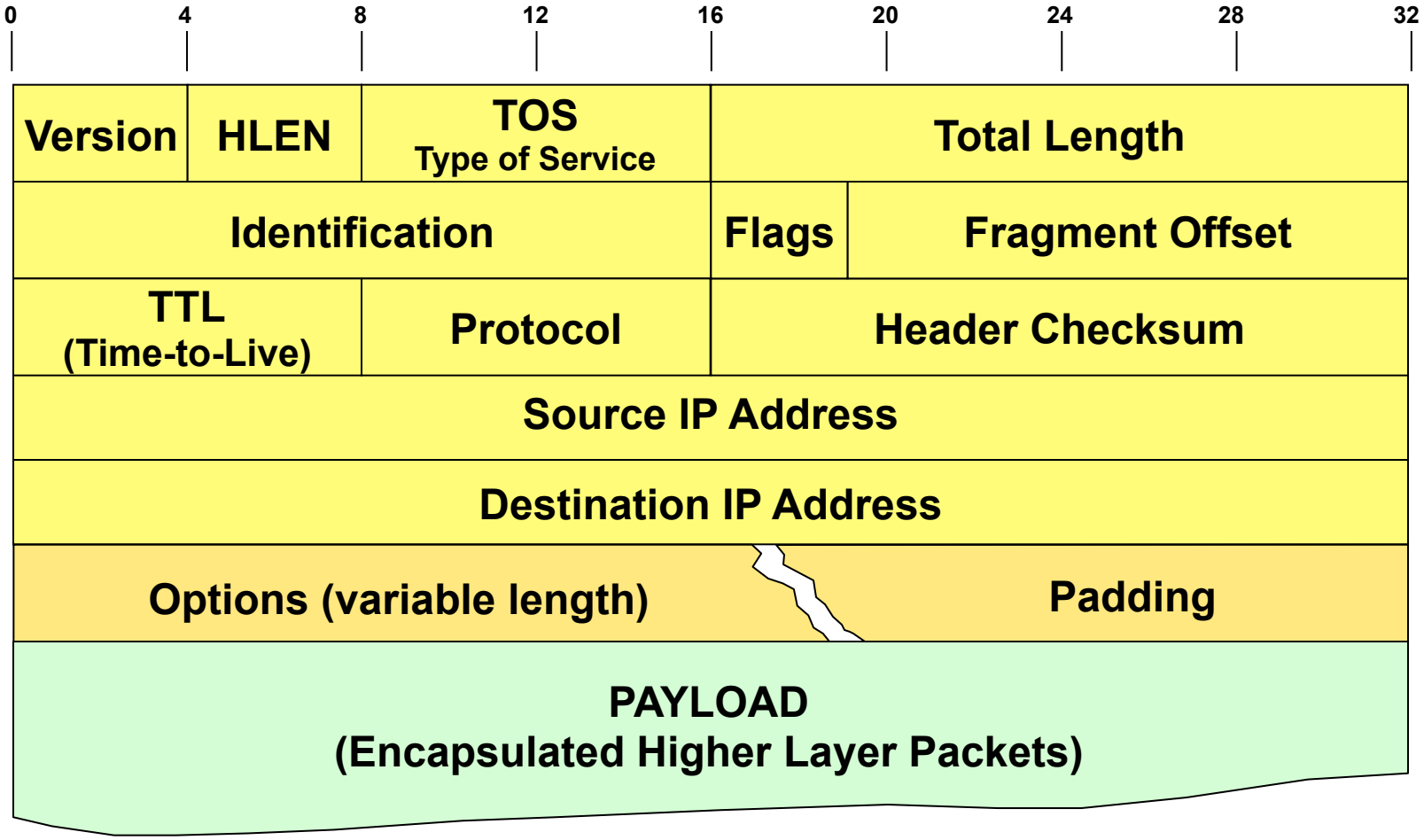
# IP Internet Protocol (RFC 791)

- **OSI layer 3 protocol**
  - With datagram service (unreliable connectionless service, "best effort service")
- **Transports packets (datagrams) from a sender to a receiver**
  - Through one or more networks
- **Doesn't guarantee**
  - Delivery or correct sequence of packets (-> task of higher layers)
- **IP datagrams are encapsulated in layer 2 frames**
  - Encapsulation is a key feature of the TCP/IP suite: It provides versatility and independence from the physical network

# IP Protocol Functions

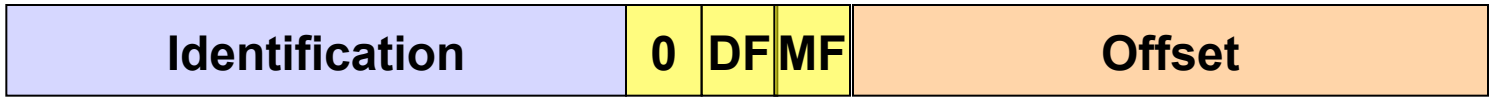
- **Packet forwarding**
  - Based on network addressing (Net-IDs)
- **Error detection**
  - Packet header only
- **Fragmentation and reassembly**
  - Necessary, if a datagram has to pass a network with a smaller maximum frame size
  - MTU (Maximum Transmission Unit)
  - Reassembly is done at the receiver
- **Mechanisms to limit the lifetime of a datagram**
  - To omit an endless circulating of datagrams if routing loops occur in the network

# The IP Header

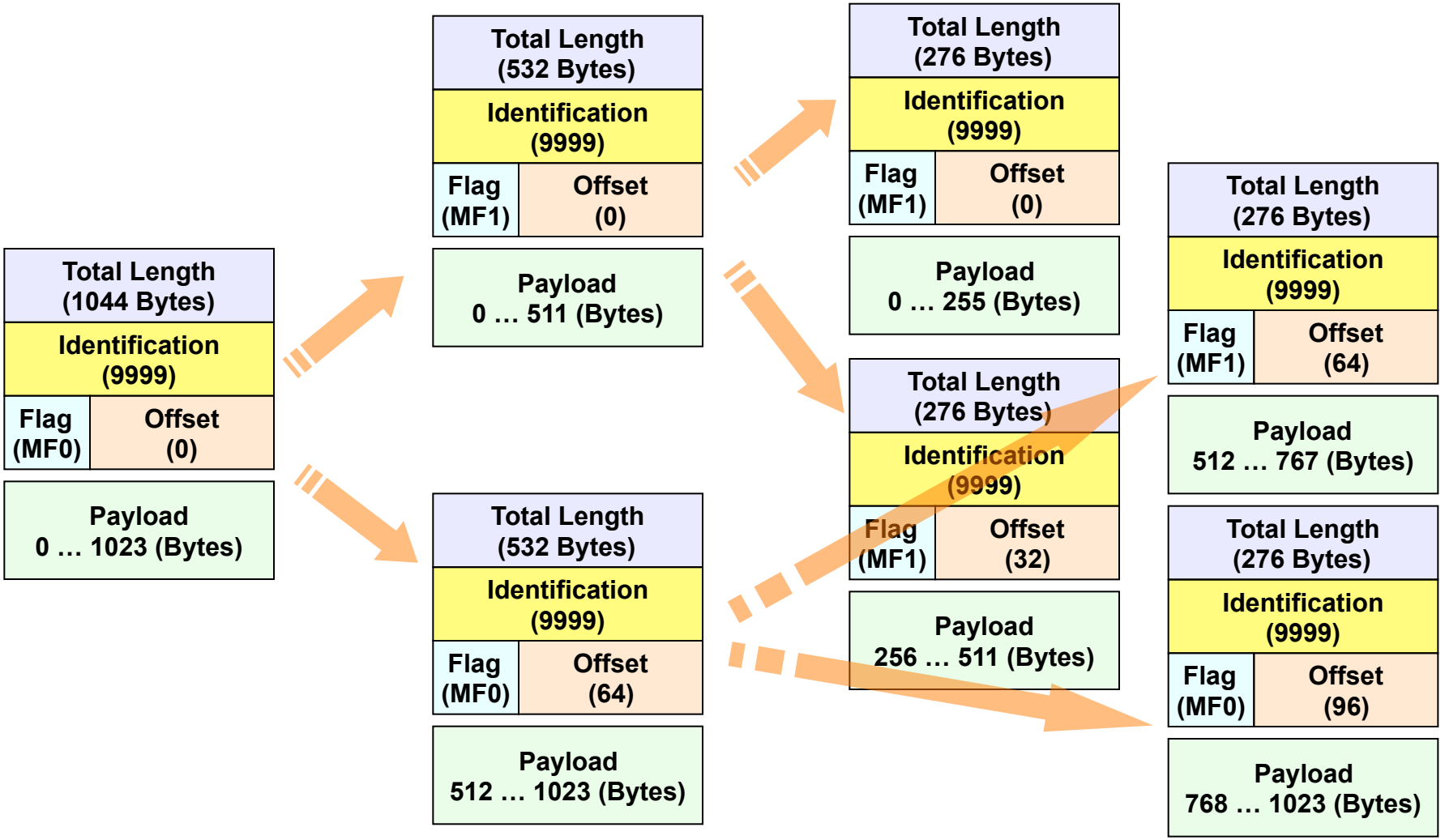


# Fragmentation Fields

- **Identification:**
  - All fragments of a datagram have the same unique identification
  - Necessary for reassembling fragments **at the destination**
  - In praxis a hidden sequence number although not really used because of the connectionless best-effort delivery behavior of IP
- **Fragment Offset:**
  - Indicates the position of a fragment in relation to the beginning of the original datagram
  - Offset is measured in multiples of 8 bytes (64 bits)
- **Flags:**
  - DF (Don't Fragment)
    - Can be used for Path MTU discovery
  - MF (More Fragments)
    - More fragments of the same original datagram will follow



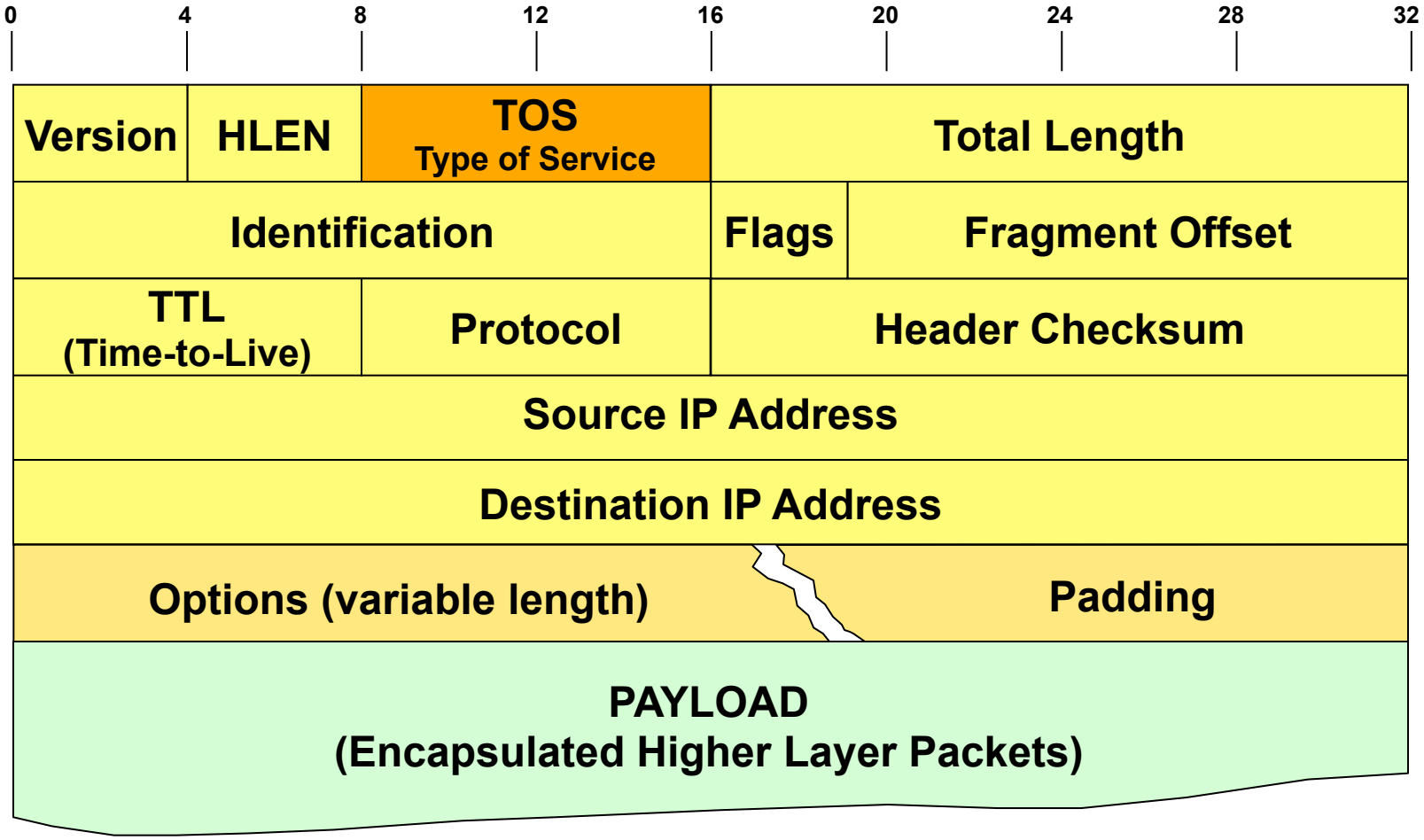
# IP Fragmentation in Action



# Agenda

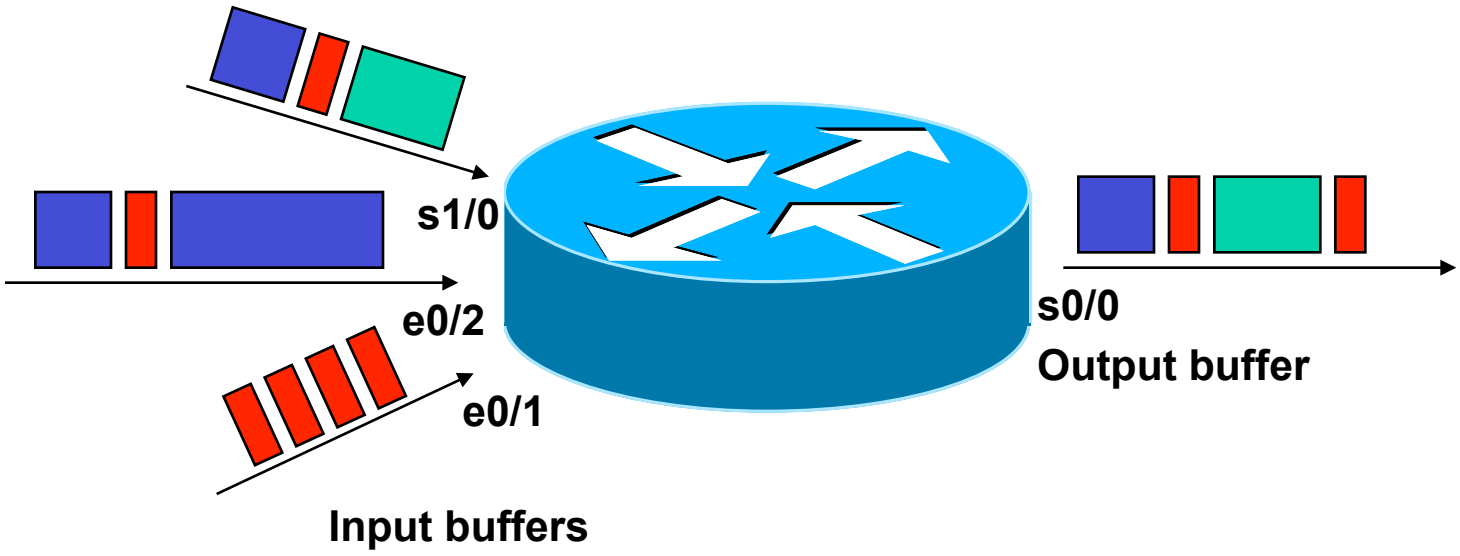
- **Introduction**
  - Short History of the Internet (not part of the exam!)
  - Basic Principles
- **IP**
  - IP Protocol
  - IP QoS
  - Addressing
  - Classful versus Classless (not part of the exam!)
- **IP Forwarding**
  - Principles
  - ARP
  - ICMP
  - PPP
- **First Hop Redundancy**
  - Proxy ARP, IDRP
  - HSRP
  - VRRP (not part of the exam!)

# The Way to IP QoS (0):



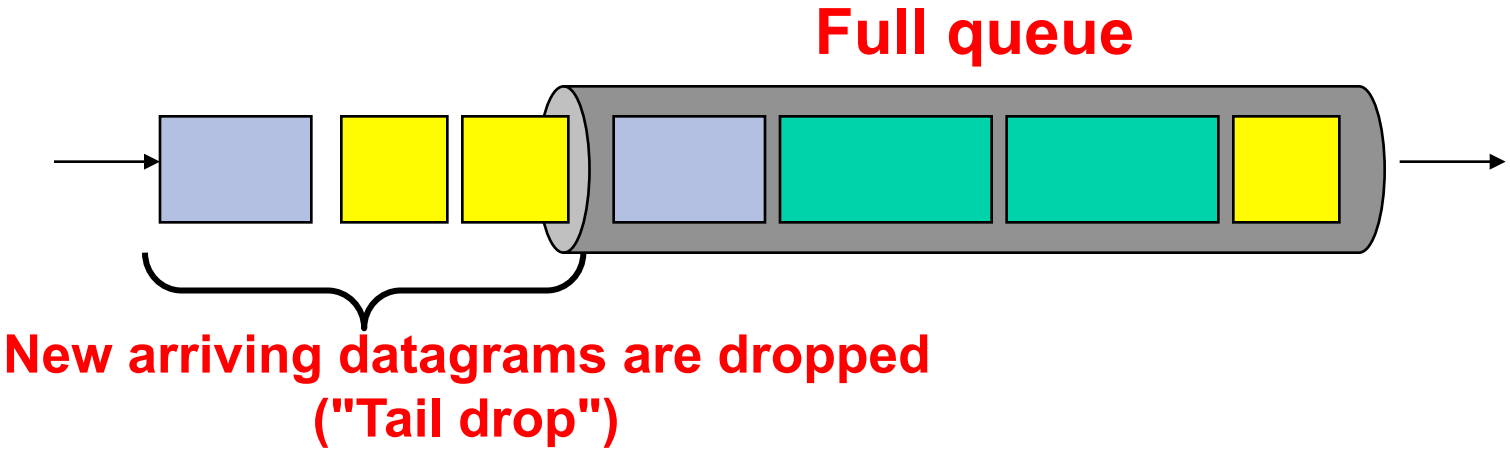
# The Way to IP QoS (1): Need for Queuing

- **Dataram delivery and switching processes work at different (and varying) rates**
- **Buffers are needed to interface between those asynchronous processes**
  - Too large buffers: Introduce more delay
  - Too small buffers: Datagrams might get lost during bursts



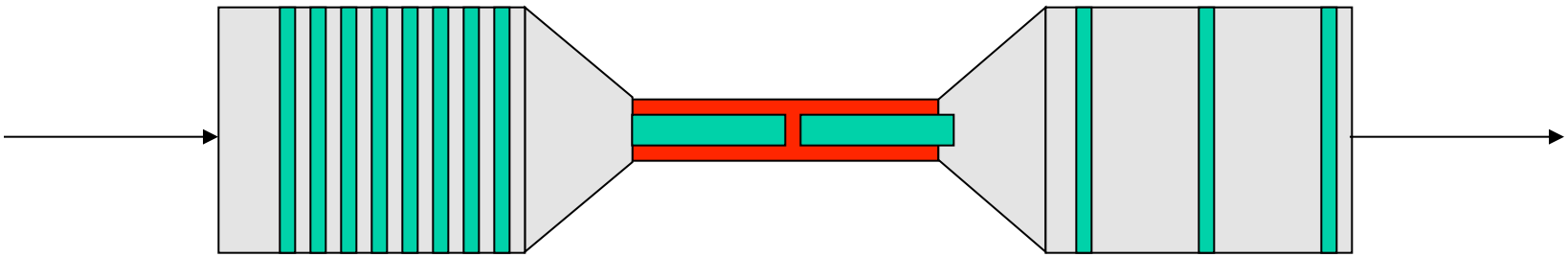
# The Way to IP QoS (2): No QoS with FIFO Queuing

- ***Tail-drop queuing*** **is the standard dropping behavior in FIFO queues**
  - If queue is full all subsequent datagrams are dropped
- **Of course that is not sufficient to implement any kind of QoS**



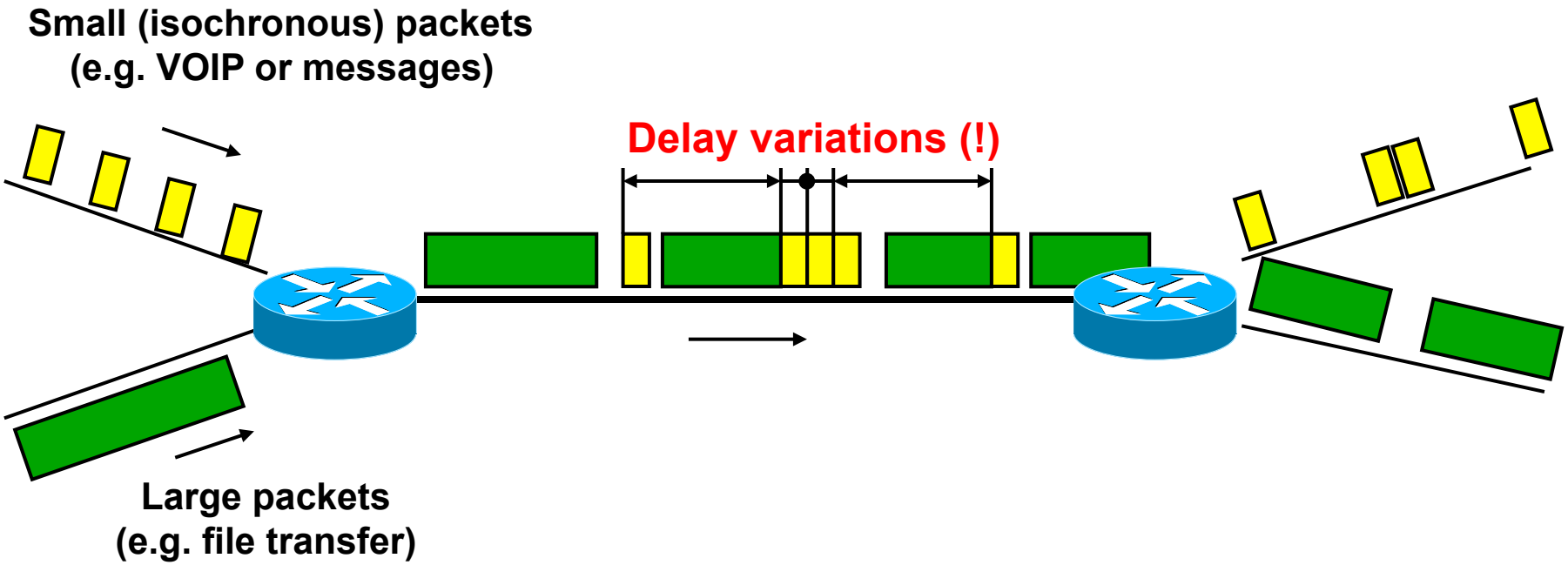
# The Way to IP QoS (3): Bottleneck and Traffic Bursts

- Problem (buffer overflows) appears at bottleneck links



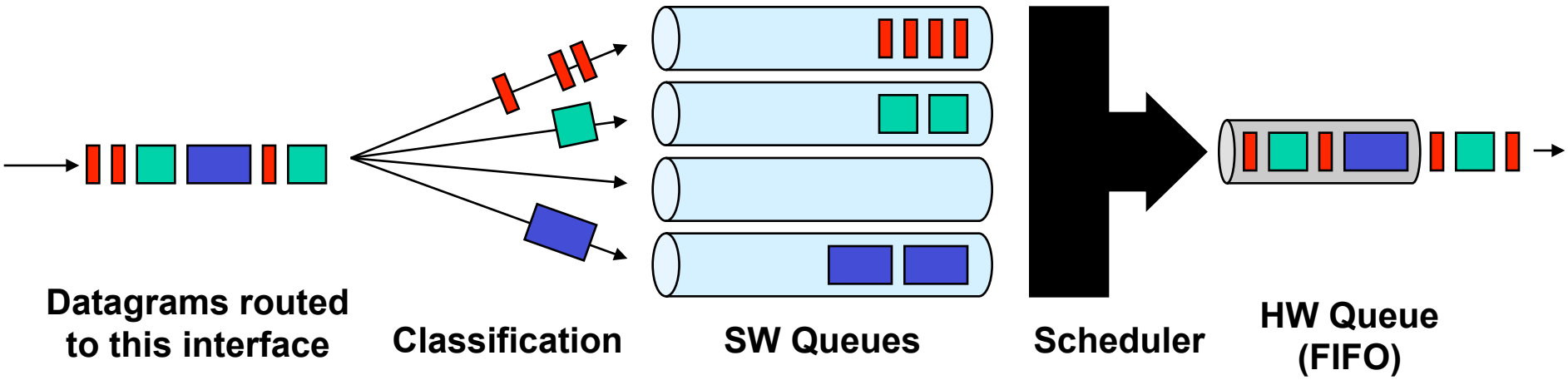
**Pipe model of a network path: Big fat pipes (high data rates) outside, a bottleneck link in the middle. The green packets are sent at the maximum achievable rate so that the inter packet delay is almost zero at the bottleneck link; however there is a significant inter packet gap in the fat pipes.**

# The Way to IP QoS (4): Jitter = Delay Variation



# The Way to IP QoS (5): QoS with SW Queues

- **Queuing actually encompasses two parts: SW and HW queues!**
- **SW queuing is typically more sophisticated**
  - WRR Weighted Round Robin)
  - CBWFQ (Class Based Weighted Fair Queuing)
  - Priority Queuing, LLQ (Low Latency Queuing)
  - These kind of techniques are an important part of any QoS implementation
- **HW queuing is typically only FIFO**
- **SW queue only needed if HW-queue full**
  - Otherwise packet bypasses SW-queue



# The Way to IP QoS (6): QoS Basic Considerations

- **No QoS is necessary in case of over-provisioning**
  - But can you economically justify it?
- **Manages available bandwidth in case of congestion**
  - But cannot create additional bandwidth on the fly
- **Ensures certain upper limits for transmission parameters**
  - Bounded maximum delay, jitter and loss
  - Assured minimum throughput
- **Needs more performance at the network components**
  - Hardware (ASIC), CPU, memory at Ethernet switches, IP routers, firewalls, etc.
- **Needs monitoring**
  - To understand what is going on in your network
  - To recognize trends for deploying additional bandwidth in time

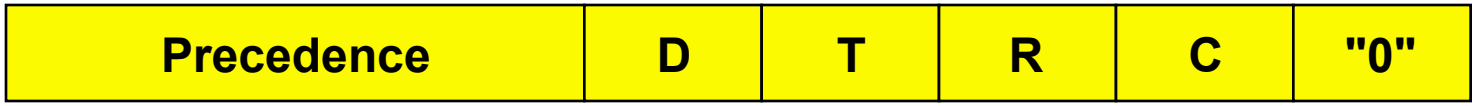
# The Way to IP QoS (6): Original Idea

- **TOS (Type Of Service)**
  - Old meaning (RFC 791 and RFC 1349)
  - Priority (precedence) of a datagram in relation to other datagrams queued up in the router
  - Preferred network characteristics to be expected by that datagram

  - **Precedence bits:**
    - Allow router to queue datagrams in different output queues in case of congestion
    - Allow router to schedule datagrams of different queues according to a QOS (Quality Of Service) policy (e.g. round robin, priority)

  - **D, T, R and C bits**:
    - low **D**elay, high **T**hroughput, high **R**eliability, low monetary **C**ost
    - Can be used to forward a datagram according to a routing table which corresponds to the preferred network characteristics for that destination
      - Needs routing tables per network characteristic

# The Way to IP QoS (7): TOS Field Meaning (RFC 791, 1349)



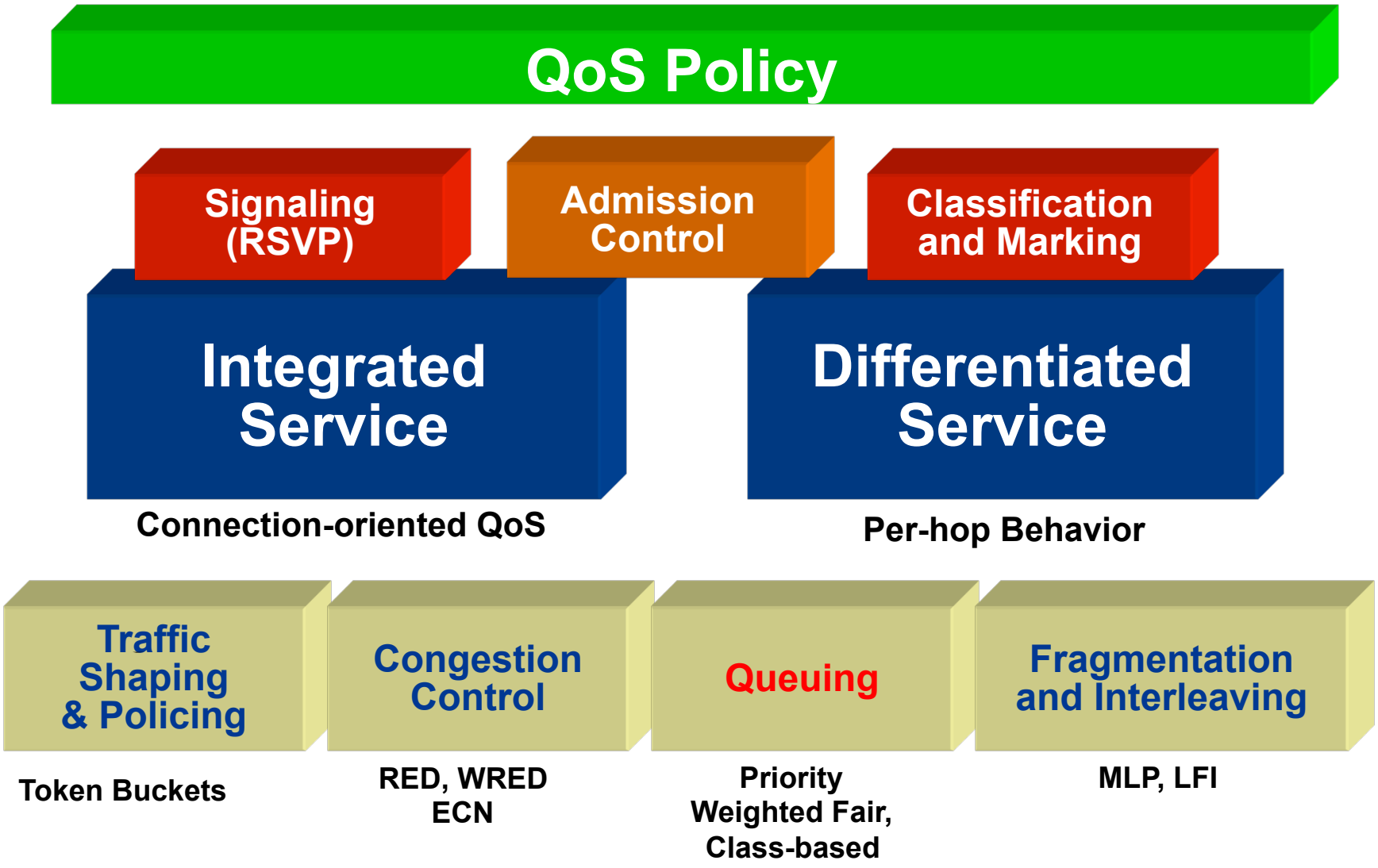

| Precedence (Priority): | DTRC bits: | | |
|---|---|---|---|
| 111 Network Control | 0 0 0 0 | . . . . | normal service |
| 110 Internetwork Control | 1 0 0 0 | D Delay | min. delay |
| 101 Critic/ECP | 0 1 0 0 | T Throughput | max. throughput |
| 100 Flash Override | 0 0 1 0 | R Reliability | max. reliability |
| 011 Flash | 0 0 0 1 | C Cost | min. cost |
| 010 Immediate | | | |
| 001 Priority | No other values are defined but have to be accepted (ignored) by a router or host. | | |
| 000 Routine | | | |

# The Way to IP QoS (8): IntServ versus DiffServ Model

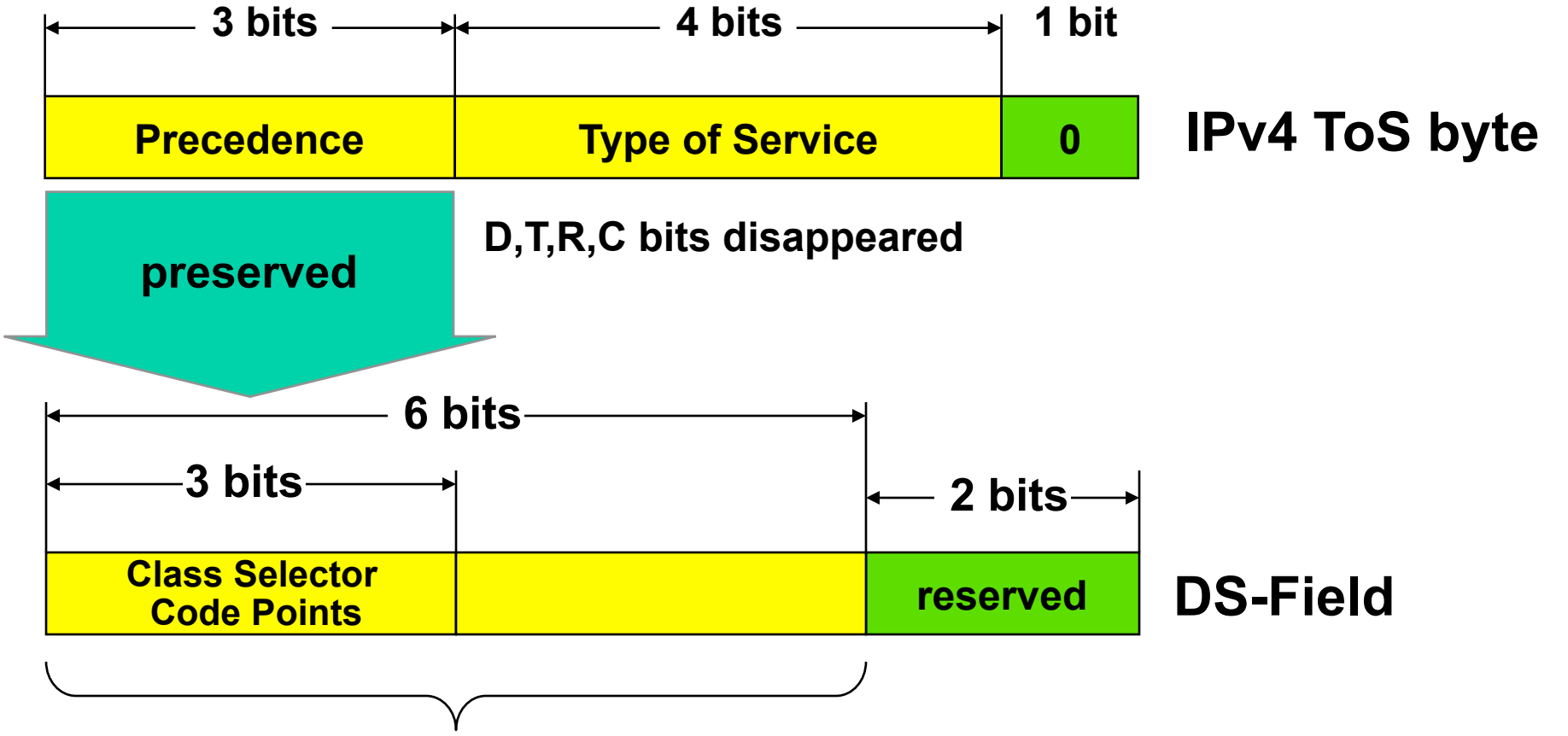
- **Two models for IP QoS:**
  - Integrated Services Model
    - Flow based with RSVP (Resource ReserVation Protocol) and dynamic QoS like ATM QoS
    - Failed because of scalability
  - Differentiated Services Model
    - Based on differentiation of traffic classes and a QoS customer - QoS provider relationship with static traffic contract
    - Precedence idea of old TOS recycled !!!
    - It is the current technique to have something like QoS in the IP world
      - But still not comparable with ATM QoS !!!
    - TOS was redefined by the IETF to become the

      **“Differentiated Service Code Point (DSCP)”**

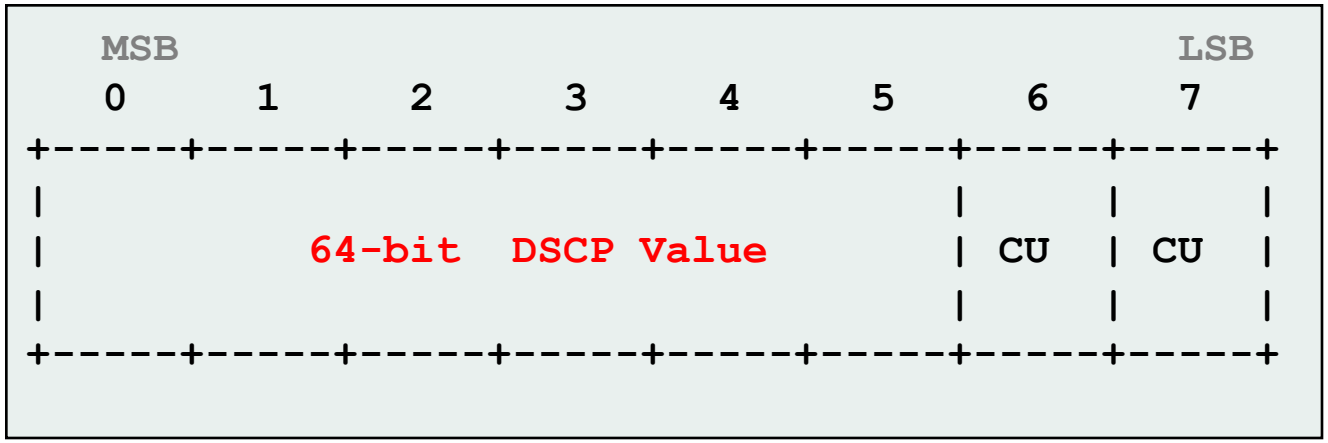
# The Way to IP QoS (9): Fundamental Building Blocks for QoS



# The Way to IP QoS (10): IPv4 TOS Recycling -> DSCP (RFC 2474)

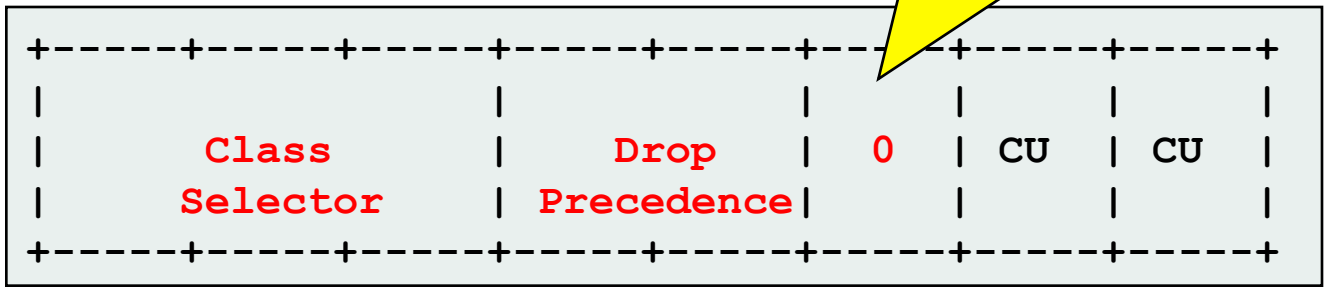


# The Way to IP QoS (11): DSCP Details




**Practically only 5 bits are used:**

**Only zero if bits 3,4 should be interpreted as drop precedence**



# The Way to IP QoS (12): DSCP Values Overview

| Code Point Name | DSCP | | Whole IP TOS byte | | |
|---|---|---|---|---|---|
| | hex | dec | binary | hex | dec |
| EF | 0x2e | 46 | 10111000 | 0xb8 | 184 |
| AF41 | 0x22 | 34 | 10001000 | 0x88 | 136 |
| AF42 | 0x24 | 36 | 10010000 | 0x90 | 144 |
| AF43 | 0x26 | 38 | 10011000 | 0x98 | 152 |
| AF31 | 0x1a | 26 | 01101000 | 0x68 | 104 |
| AF32 | 0x1c | 28 | 01110000 | 0x70 | 112 |
| AF33 | 0x1e | 30 | 01111000 | 0x78 | 120 |
| AF21 | 0x12 | 18 | 01001000 | 0x48 | 72 |
| AF22 | 0x14 | 20 | 01010000 | 0x50 | 80 |
| AF23 | 0x16 | 22 | 01011000 | 0x18 | 24 |
| AF11 | 0x0a | 10 | 00101000 | 0x28 | 40 |
| AF12 | 0x0c | 12 | 00110000 | 0x30 | 48 |
| AF13 | 0x0e | 14 | 00111000 | 0x38 | 56 |
| CS7 | 0x38 | 56 | 11100000 | 0xe0 | 224 |
| CS6 | 0x30 | 48 | 11000000 | 0xc0 | 192 |
| CS5 | 0x28 | 40 | 10100000 | 0xa0 | 160 |
| CS4 | 0x20 | 32 | 10000000 | 0x80 | 128 |
| CS3 | 0x18 | 24 | 01100000 | 0x60 | 96 |
| CS2 | 0x10 | 16 | 01000000 | 0x40 | 64 |
| CS1 | 0x08 | 8 | 00100000 | 0x20 | 32 |
| CS0 = BE | 0x00 | 0 | 00000000 | 0x00 | 0 |

# The Way to IP QoS (13): 14 Recommended Code Points

- **Expedited Forwarding (EF)**
  - DSCP 46 = 101 110 binary
  - For low delay, low loss, and low jitter
  - Defined in RFC 3246
- **Assured Forwarding (AF)**
  - 12 codepoints: 4 classes and 3 drop precedence each
  - Defined in RFC 2597
- **Best Effort (BE)**
  - 000000 binary
- **The legacy IP Precedence values (0-7) are preserved**
  - Can be directly mapped into the three Class Selector bits (0,1,2) *with the three LSBs (3,4,5) set to zero*
  - This results in the seven CSx values
    - CS0 = DSCP 00 = 000000

      ...
    - CS7 = DSCP 56 = 111000

# The Way to IP QoS (14): Assured Forwarding (AF)

- **Guarantees a certain bandwidth to a traffic class**
  - If the traffic exceeds the committed bandwidth the drop probability is raised according to the specified drop precedence
- **There are 12 different AF behavior code points**
  - Consisting of 4 classes (AF1y to AF4y)
  - And 3 drop probabilities (AFx1 to AFx3) for each class (low/med/hi)

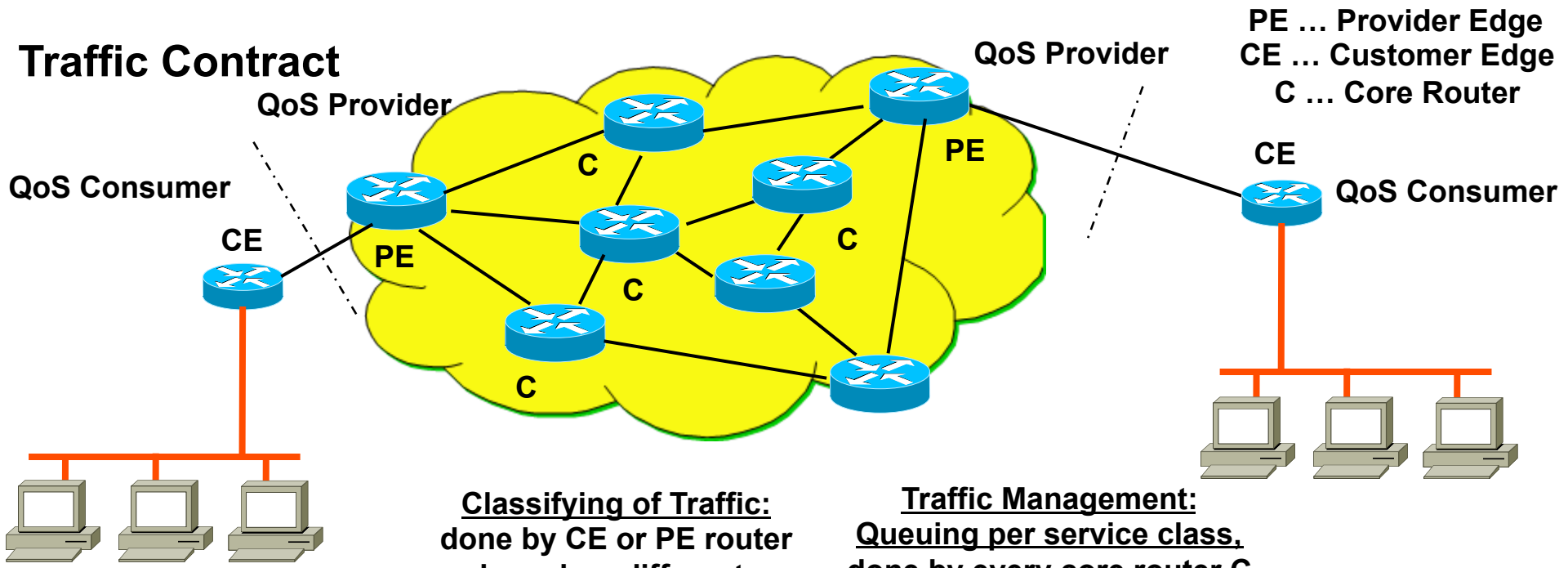
| Drop: | Class 1 | | | Class 2 | | | Class 3 | | | Class 4 | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Low | AF11 | 10 | 001010 | AF21 | 18 | 010010 | AF31 | 26 | 011010 | AF41 | 34 | 100010 |
| Medium | AF12 | 12 | 001100 | AF22 | 20 | 010100 | AF32 | 28 | 011100 | AF42 | 36 | 100100 |
| High | AF13 | 14 | 001110 | AF23 | 22 | 010110 | AF33 | 30 | 011110 | AF43 | 38 | 100110 |

decimal | binary

# The Way to IP QoS (15): DSCP Value Usage

- **DSCP Usage:**
  - Is used to tag (label) the traffic class of a datagram
  - All labeled datagrams of a traffic class will receive a defined PHB (Per Hop behavior)
- **Typical scenario:**
  - QoS service provider <-> QoS customer
  - IP datagrams are classified and can be labeled (marked) at the border of IP QoS domain
  - Border has to perform traffic policing according to the static traffic contract
  - Customer may shape traffic to obey the traffic contract
  - Traffic class will receive their PHP handling within in IP QoS Domain
    - e.g. Limited delay, Guaranteed throughput

# The Way to IP QoS (16): Elements of DiffServ




**Traffic Shaping:**
done by CE router

**Marking of Traffic:**
done by CE or PE router by specifying DSCP (service class)

**Classifying of Traffic:**
done by CE or PE router based on different parameters (e.g. interface, IP, TCP header)

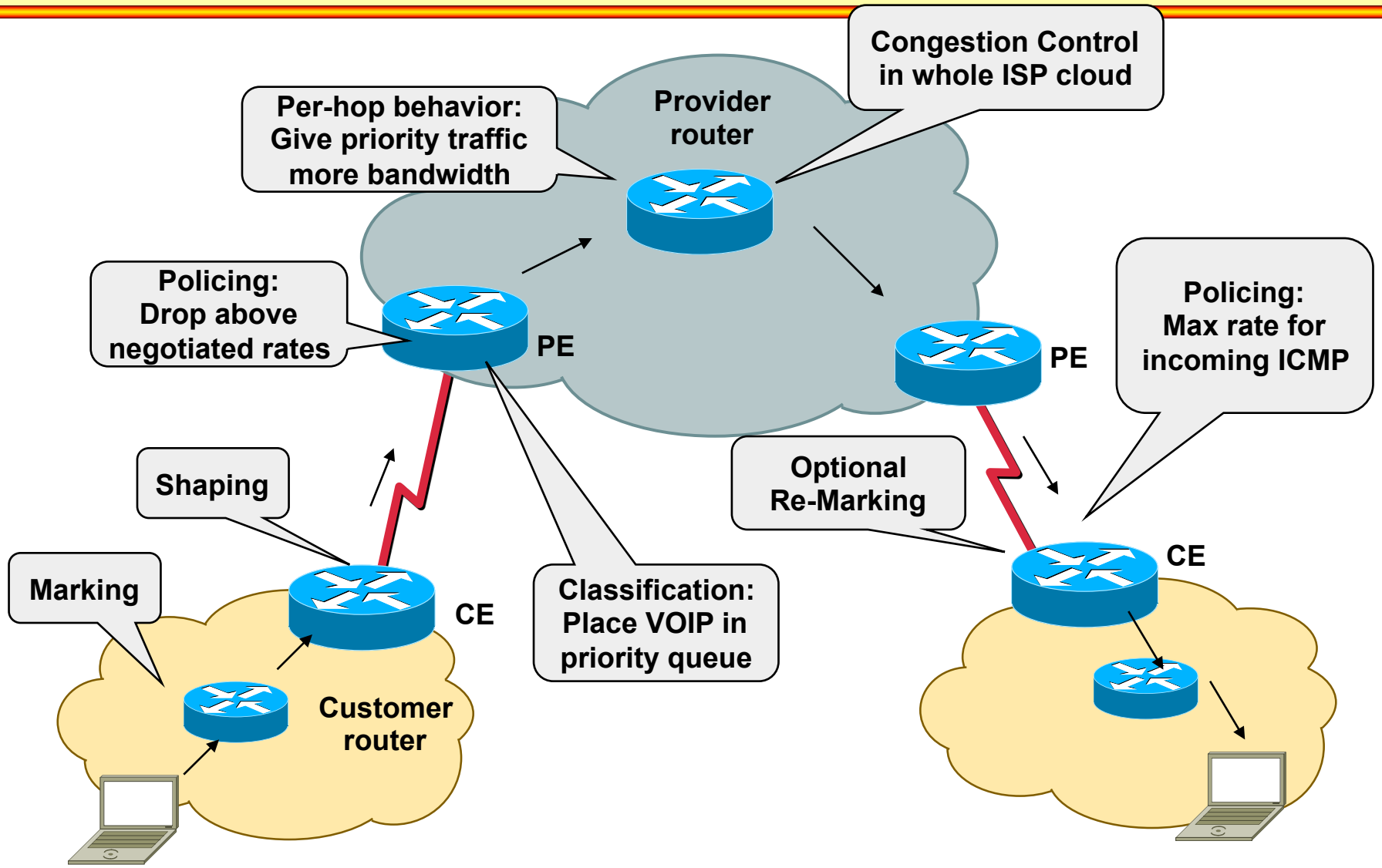
**Traffic Policing:**
done at PE router by CAR (Committed Access Rate)

**Traffic Management:**
**Queuing per service class,**
done by every core router C
**(Per Hop Behavior)**

**Call Admission Control:**
done by provider by provisioning network resources for service classes

**Signaling:**
not necessary because of static approach

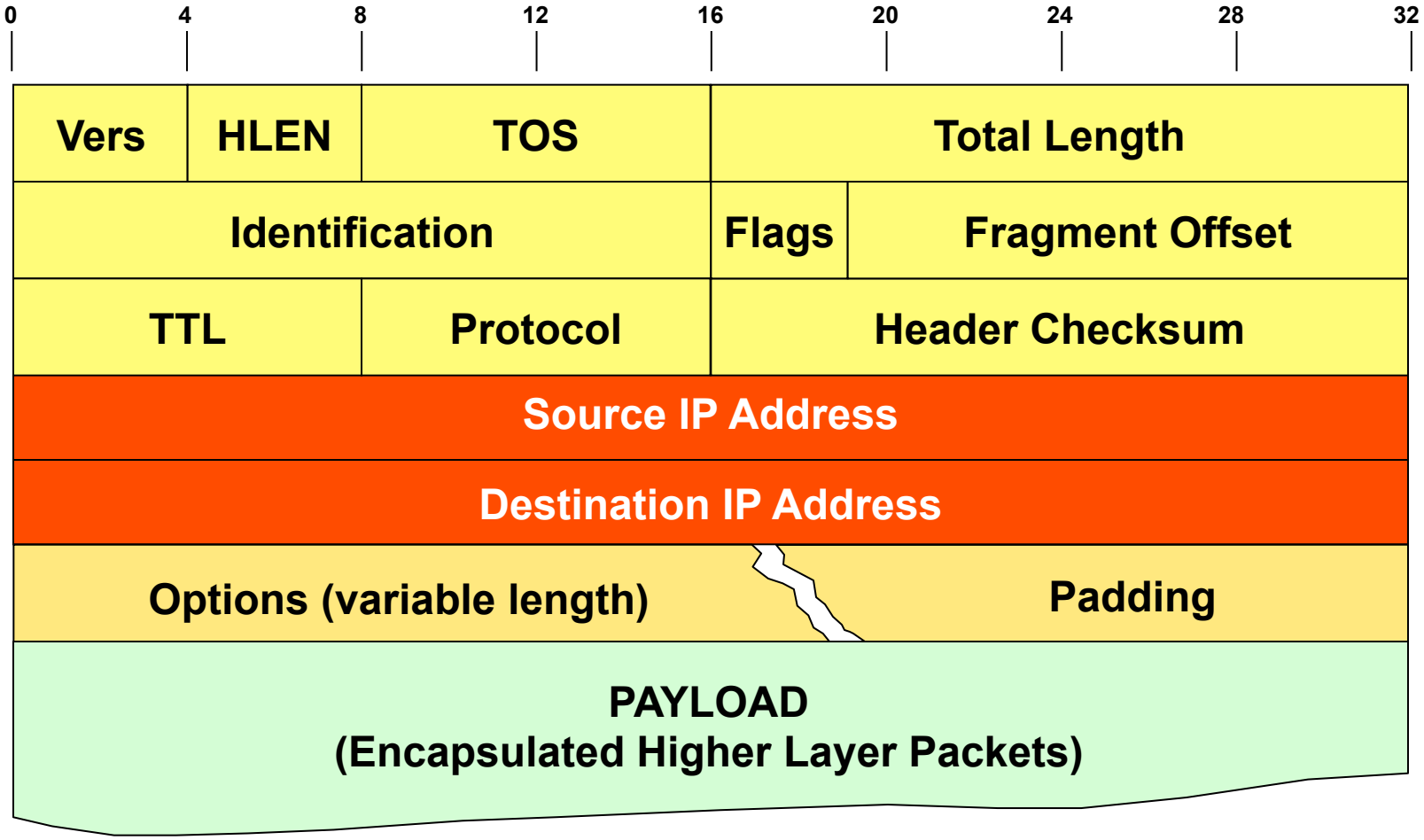
# The Way to IP QoS (17): DiffServ In Action



# Agenda

- **Introduction**
  - Short History of the Internet (not part of the exam!)
  - Basic Principles
- **IP**
  - IP Protocol
  - IP QoS
  - Addressing
  - Classful versus Classless (not part of the exam!)
- **IP Forwarding**
  - Principles
  - ARP
  - ICMP
  - PPP
- **First Hop Redundancy**
  - Proxy ARP, IDRP
  - HSRP
  - VRRP (not part of the exam!)

# IP Header - The IP Addresses



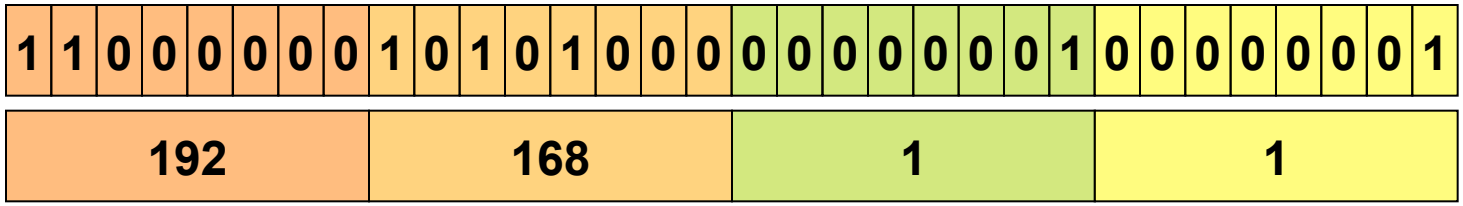
# The IP Address

- **Identifies access to a network (network interface)**
- **Two level hierarchy:**
  - Network number (Net-ID)
  - Host number (Host-ID)
- **Dotted Decimal Notation**

**Binary IP Address: 11000000101010000000000100000001**

**Decimal Value: 3232235777**

**Decimal Representation *per byte*:**



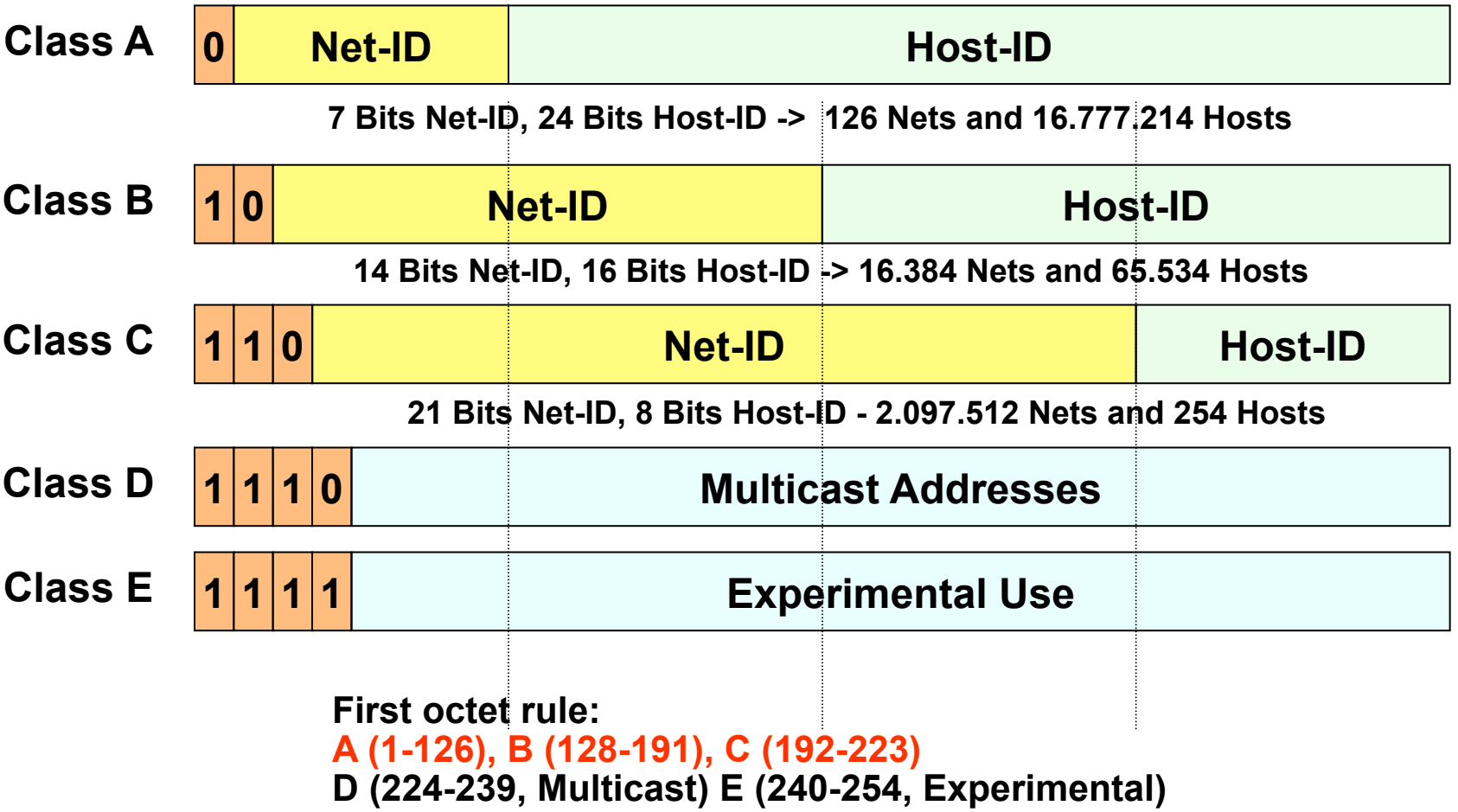

→ **192 . 168 . 1 . 1**

# Binary versus Decimal Notation

| $2^7$ | $2^6$ | $2^5$ | $2^4$ | $2^3$ | $2^2$ | $2^1$ | $2^0$ | |
|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 128 |
| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 64 |
| 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 32 |
| 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 16 |
| 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 8 |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 4 |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 2 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 255 |

# IP Address Classes

**Originally border between Net-ID and Host-ID was identified by ranges within the IP address room -> address classes -> *„First Octet Rule“***



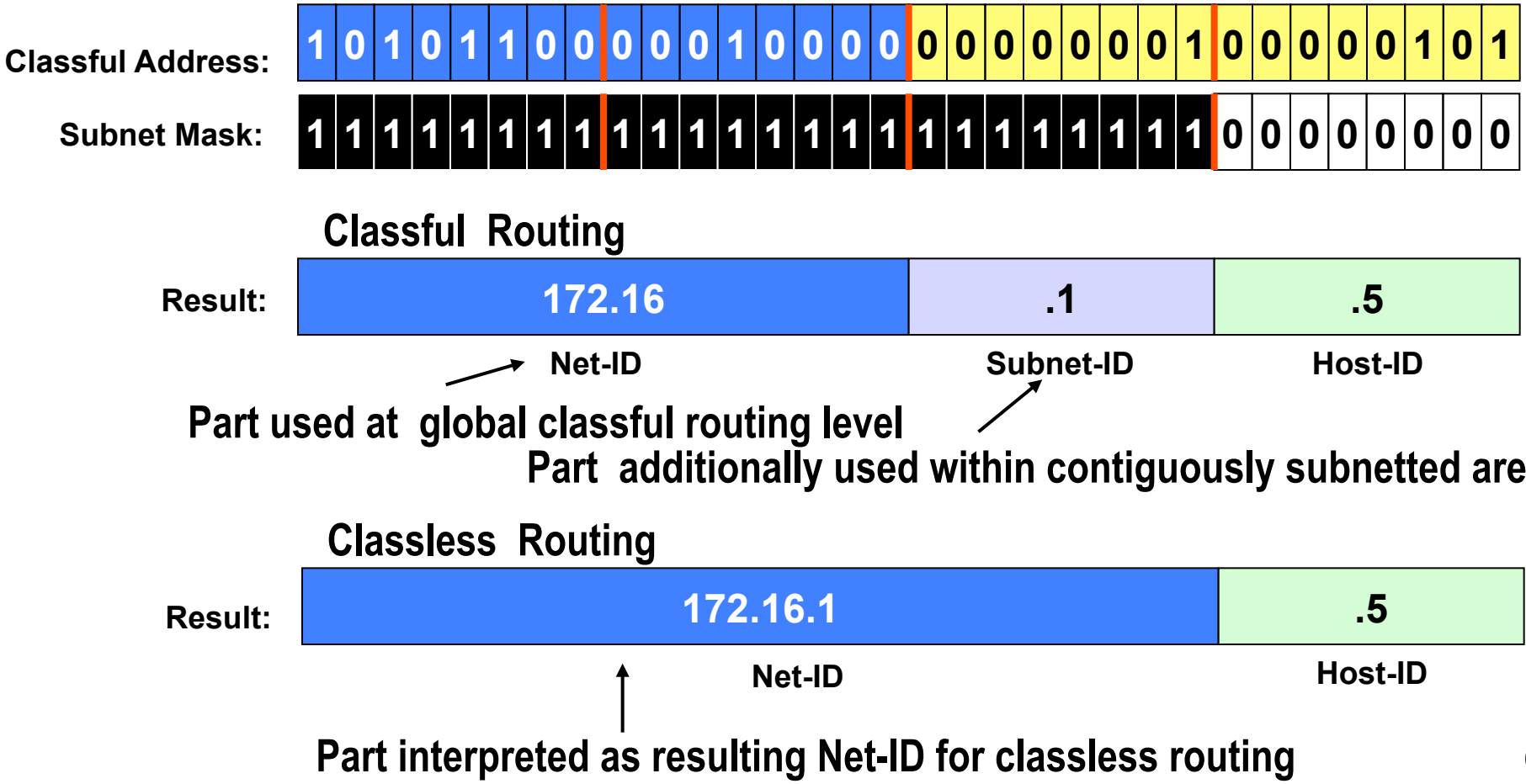
# Nowadays

- **Border between Net-ID and Host-ID of an IP address is identified**
  - by Subnetmask
- **Subnetmask**
  - is either written in IP address style e.g. 255.255.0.0
  - or given by prefix / length notation e.g. 10.3.0.0 / 16
- **Classless Routing**
  - No interpretation of old IP address classes A, B, C
  - Modern IP routing protocols can carry subnetmask
    - hence no classless routing limitations anymore
  - VLSM (Variable Length Subnet Mask)
  - Address room can be managed in the most flexible way

# Subnetting Example

**Class B Address: 172.16.1.5, Subnet Mask: 255.255.255.0**

**Alternative (newer) notation: 172.16.1.5 /24**



# Possible Subnet Mask Values

| $2^7$ | $2^6$ | $2^5$ | $2^4$ | $2^3$ | $2^2$ | $2^1$ | $2^0$ | |
|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 128 |
| 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 192 |
| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 224 |
| 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 240 |
| 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 248 |
| 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 252 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 254 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 255 |

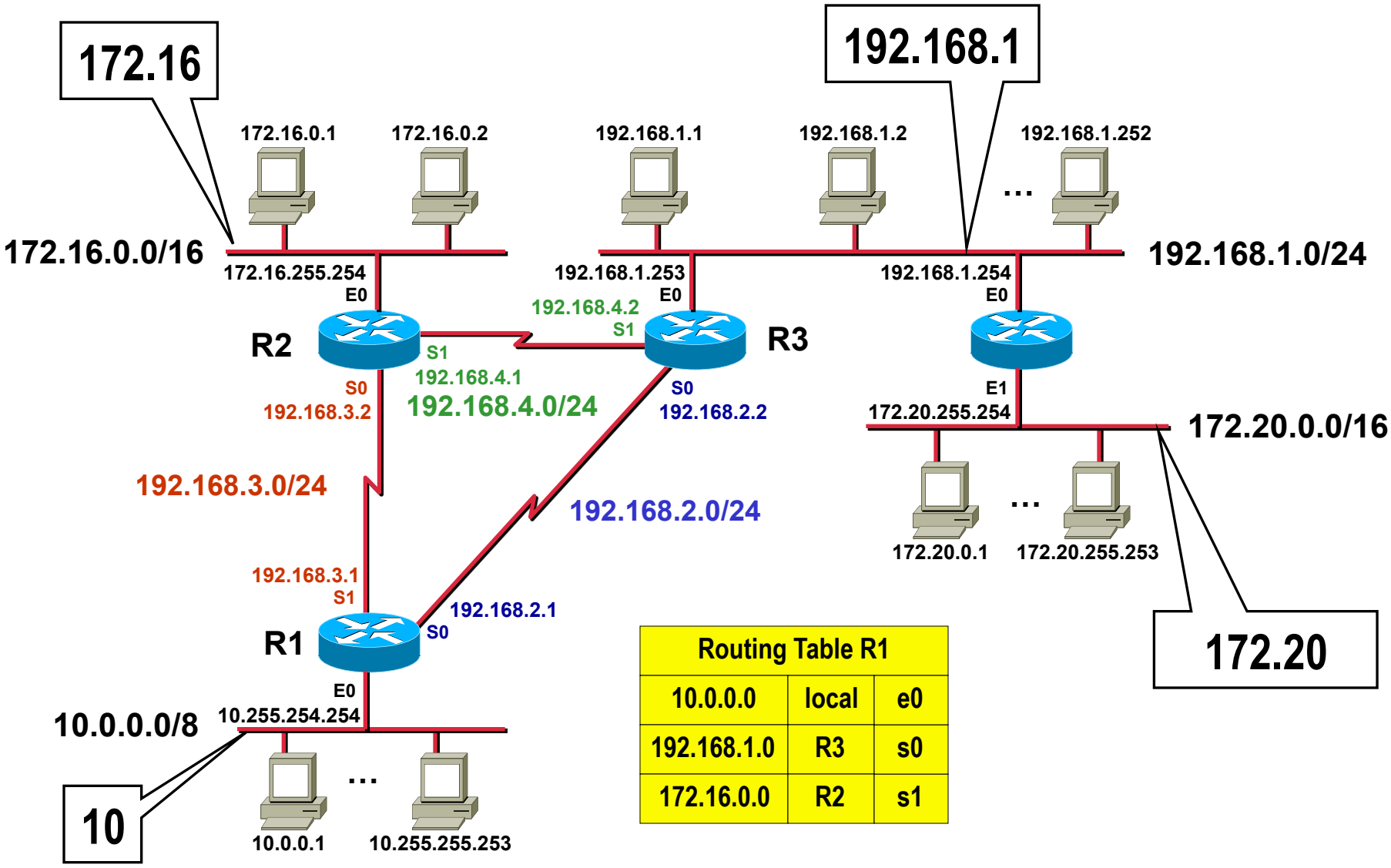
# Special Addresses

- **All ones in the Host-ID represents „IP Directed-Broadcast“ (10.255.255.255)**
- **All ones in the Net-ID and Host-ID represents „IP Limited Broadcast” (255.255.255.255)**
- **All zeros in the Host-ID represents the „Network-Address“ (10.0.0.0)**
- **Network 127.x.x.x is reserved for "Loopback“**
- **All zeros in the Net-ID and Host-ID means**
  - This host on this network (0.0.0.0)
  - Used during initialization phase (DHCP)
    - Host uses IP for communication with DHCP server but has no IP address assigned so far

# Private Addresses / NAT

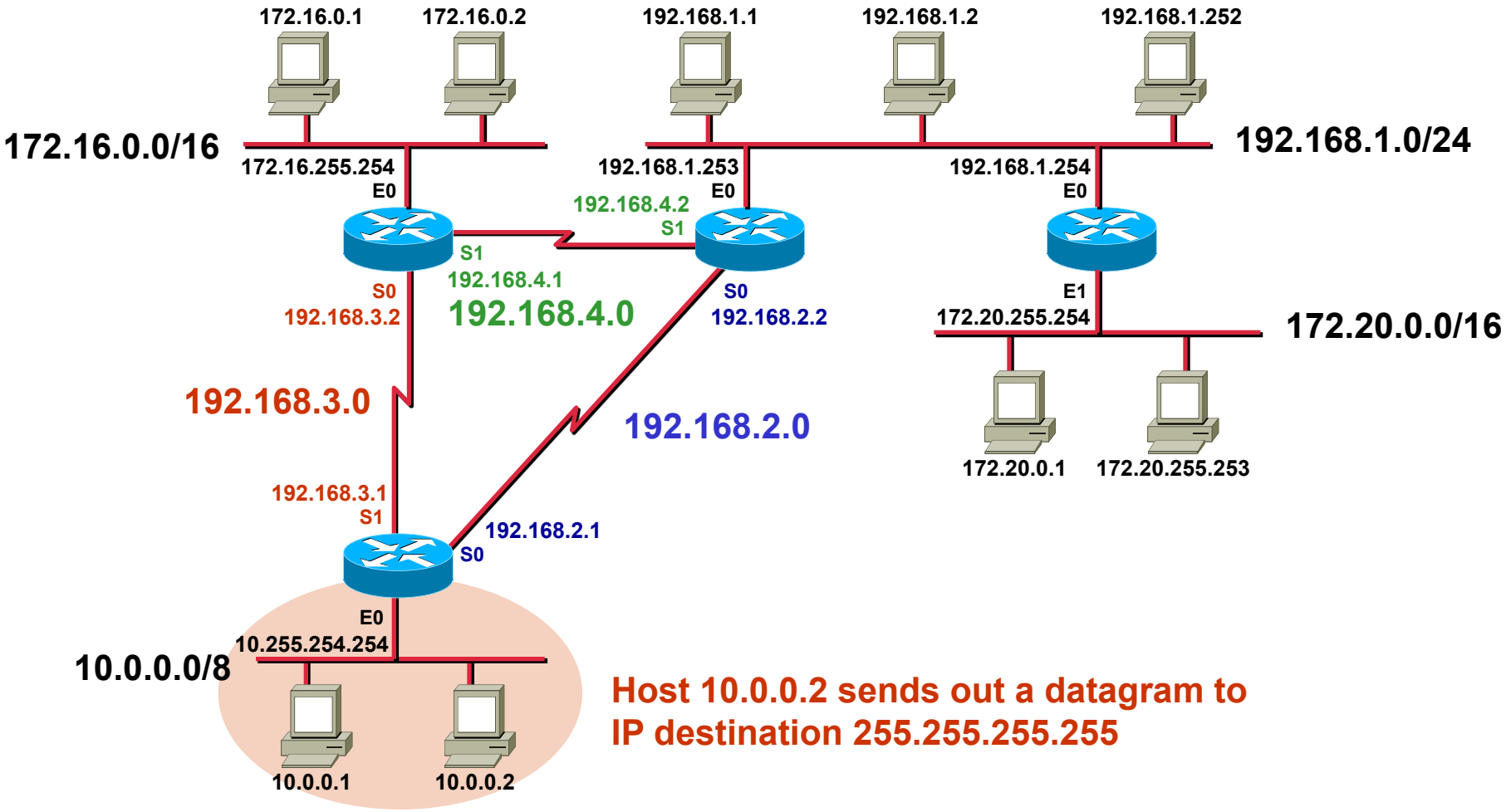
- **Address range for private use**
  - 10.0.0.0 - 10.255.255.255
  - 172.16.0.0 - 172.31.255.255
  - 192.168.0.0 - 192.168.255.255
  - RFC 1918
- **NAT (Network Address Translation)**
  - Is necessary to connect IP hosts with private addresses via NAT Gateway to Internet which needs official IP addresses
  - NAT static 1:1 mapping
  - NAT dynamic n:1 mapping with PAT
    - (UDP/TCP) port address translation
    - 1 official (global routable) IP address may be shared by many internal private stations

# Net-ID Addressing Example



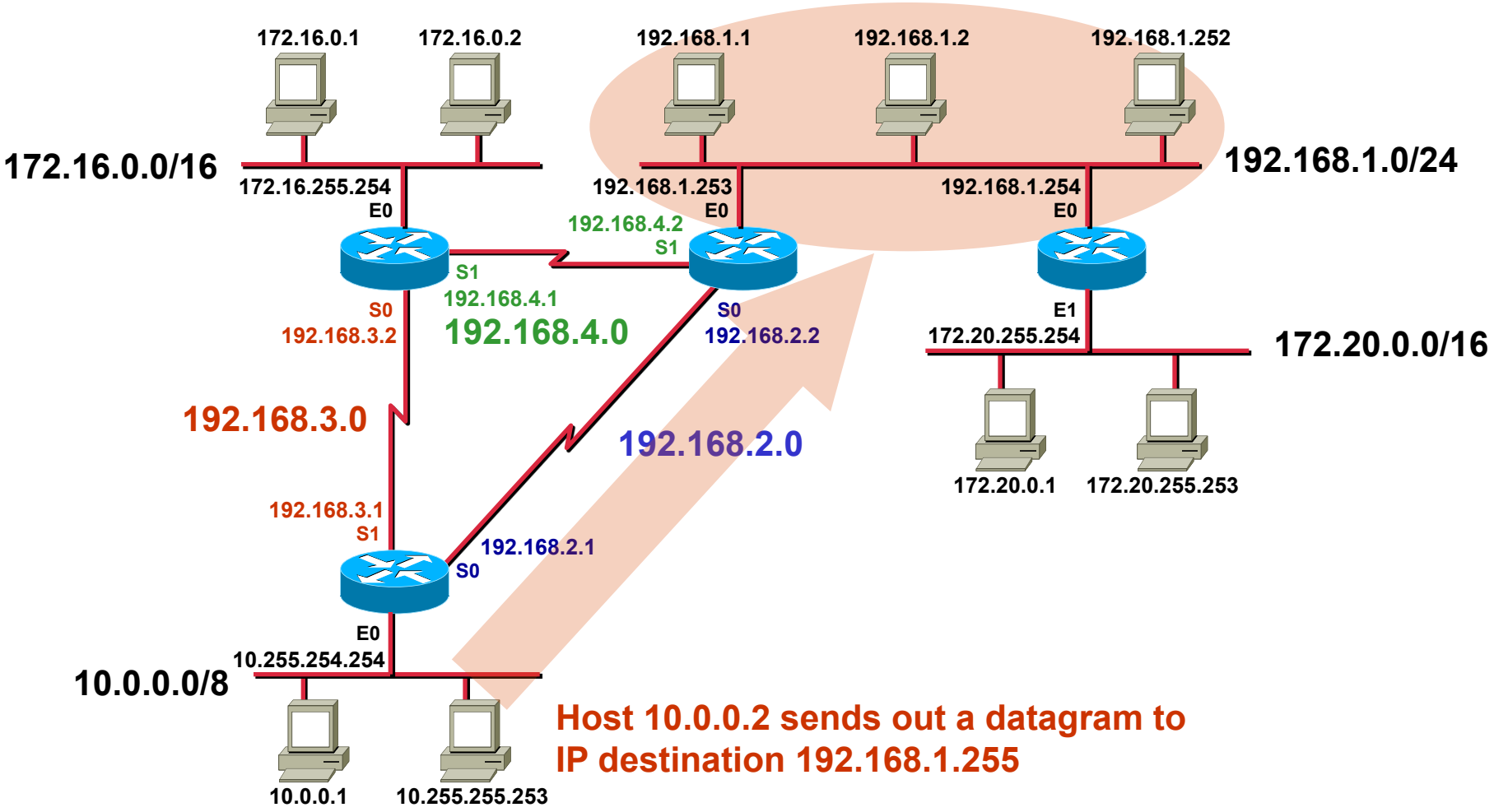

| Routing Table R1 | | |
|---|---|---|
| 10.0.0.0 | local | e0 |
| 192.168.1.0 | R3 | s0 |
| 172.16.0.0 | R2 | s1 |

# IP Limited Broadcast




**Host 10.0.0.2 sends out a datagram to IP destination 255.255.255.255**

# IP Directed Broadcast

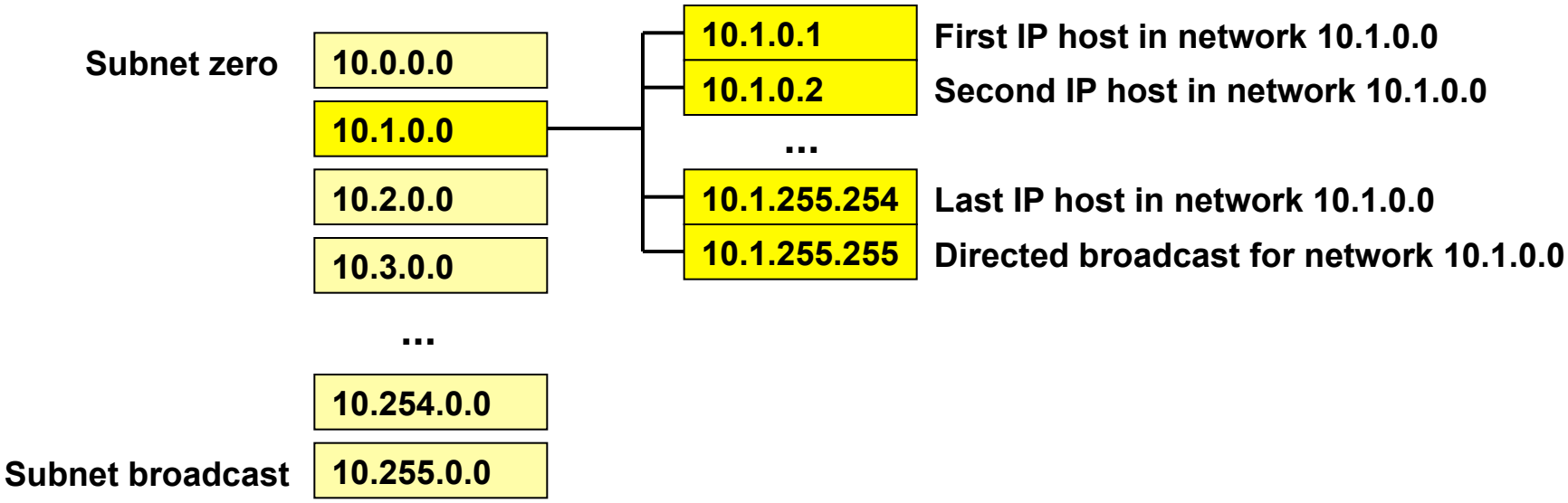


# Subnet Example 1

**"Use the class A network 10.0.0.0 and 8 bit subnetting"**

1) That is: 10.0.0.0 with 255.255.0.0 (pseudo class B)
   or 10.0.0.0/16

2) Resulting subnetworks:



# Subnet Zero / Subnet Broadcast Handling In Case of Classful Routing

FYI

- **Consider network 10.0.0.0**
  - Is it a class A net "10" ?
  - Or do we have a subnet "10.0" ?
- **Consider broadcast 10.255.255.255**
  - Is it a directed broadcast for the whole net 10 ?
  - Or only for the subnet 10.255 ?
- **Subnet zero and subnet broadcast can be ambiguous!**

# Subnet Mask -> Exam 1

- **Class A address**

  Subnet mask 255.255.0.0

  IP- Address 10.3.49.45

  ? Net-ID, ? Host-ID

  **Net-ID = 10.3.0.0**

  Host-ID = 0.0.49.45

  65534 IP hosts

  range: 10.3.0.1 -> 10.3.255.254

  10.3.0.0 -> network itself

  10.3.255.255 -> directed broadcast for this network

# Subnet Mask -> Exam 2

- **Class B address**

  Subnet mask 255.255.255.192

  IP- Address 172.16.3.144

  ? Net-ID, ? Host-ID

| | |
|---|---|
| address binary | **10101110 . 00010000 . 00000011 . 10010000** |
| mask (binary) | **11111111 . 11111111 . 11111111. 11000000** |
| logical AND (bit by bit) | |
| net-id | **10101100 . 00010000 . 00000011 . 10000000** |

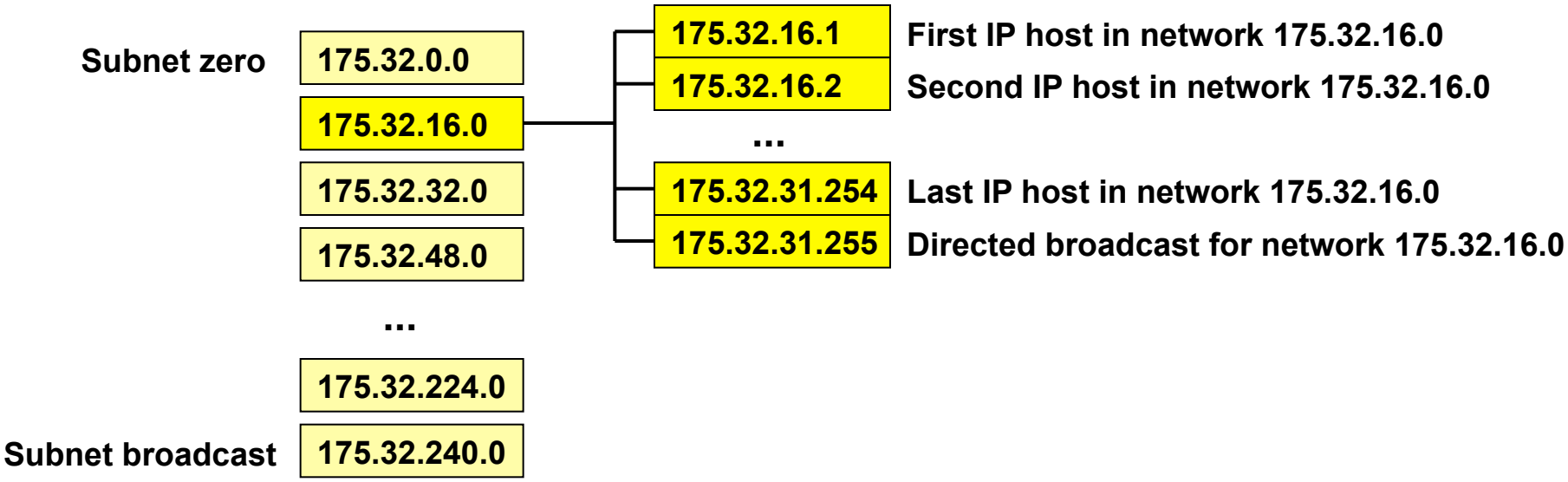
**Net-ID = 172.16.3.128**

**Host-ID = 0.0.0.16**

# Subnet Example 2

**"Use the class B network 175.32.0.0 and 4 bit subnetting"**

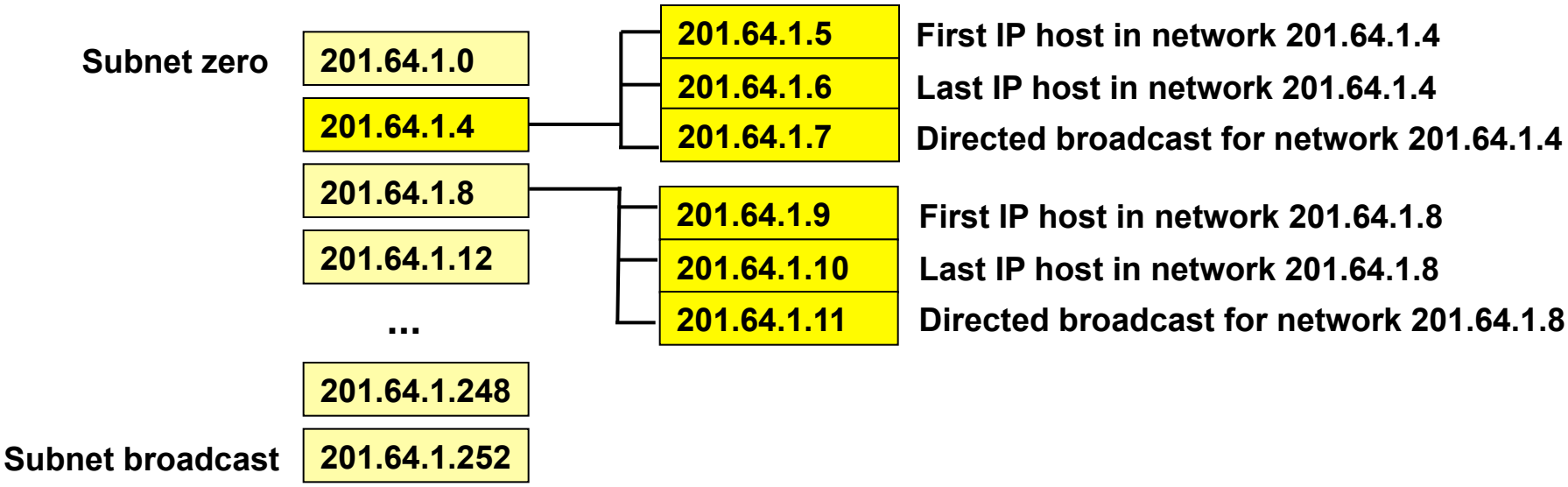
1) That is: 175.32.0.0 with 255.255.240.0 or 175.32.0.0/20
2) Resulting subnetworks:



# Subnet Example 3

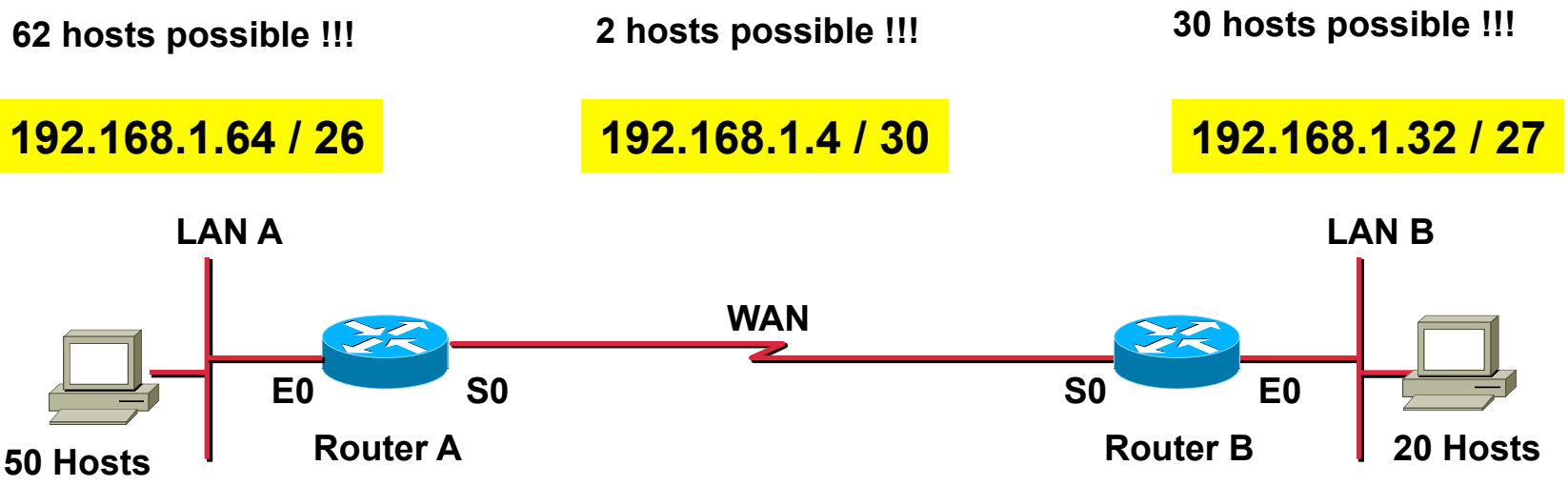
**"Use the class C network 201.64.1.0 and 6 bit subnetting"**

1) That is: 201.64.1.0 with 255.255.255.252 or 201.64.1.0/30
2) Resulting subnetworks:



# Variable Length Subnetting (VLSM)

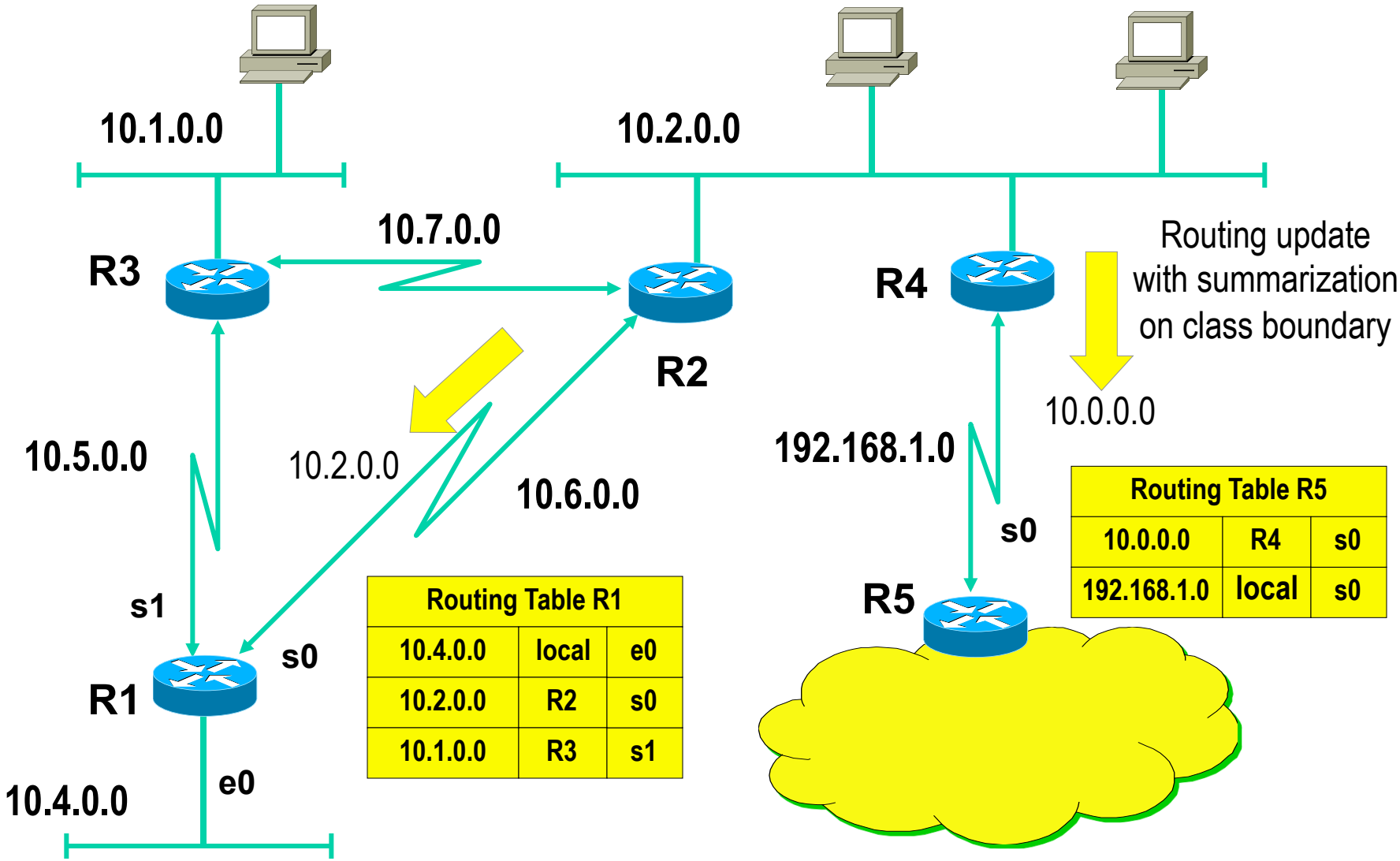
- **Remember:**
  - IP-routing is only possible between different "IP-Networks"
  - Every link must have an IP net-ID
- **Today IP addresses are rare!**
- **The assignment of IP-Addresses must be as efficient as possible!**



# Agenda

- **Introduction**
  - Short History of the Internet (not part of the exam!)
  - Basic Principles
- **IP**
  - IP Protocol
  - IP QoS
  - Addressing
  - Classful versus Classless (not part of the exam!)
- **IP Forwarding**
  - Principles
  - ARP
  - ICMP
  - PPP
- **First Hop Redundancy**
  - Proxy ARP, IDRP
  - HSRP
  - VRRP (not part of the exam!)

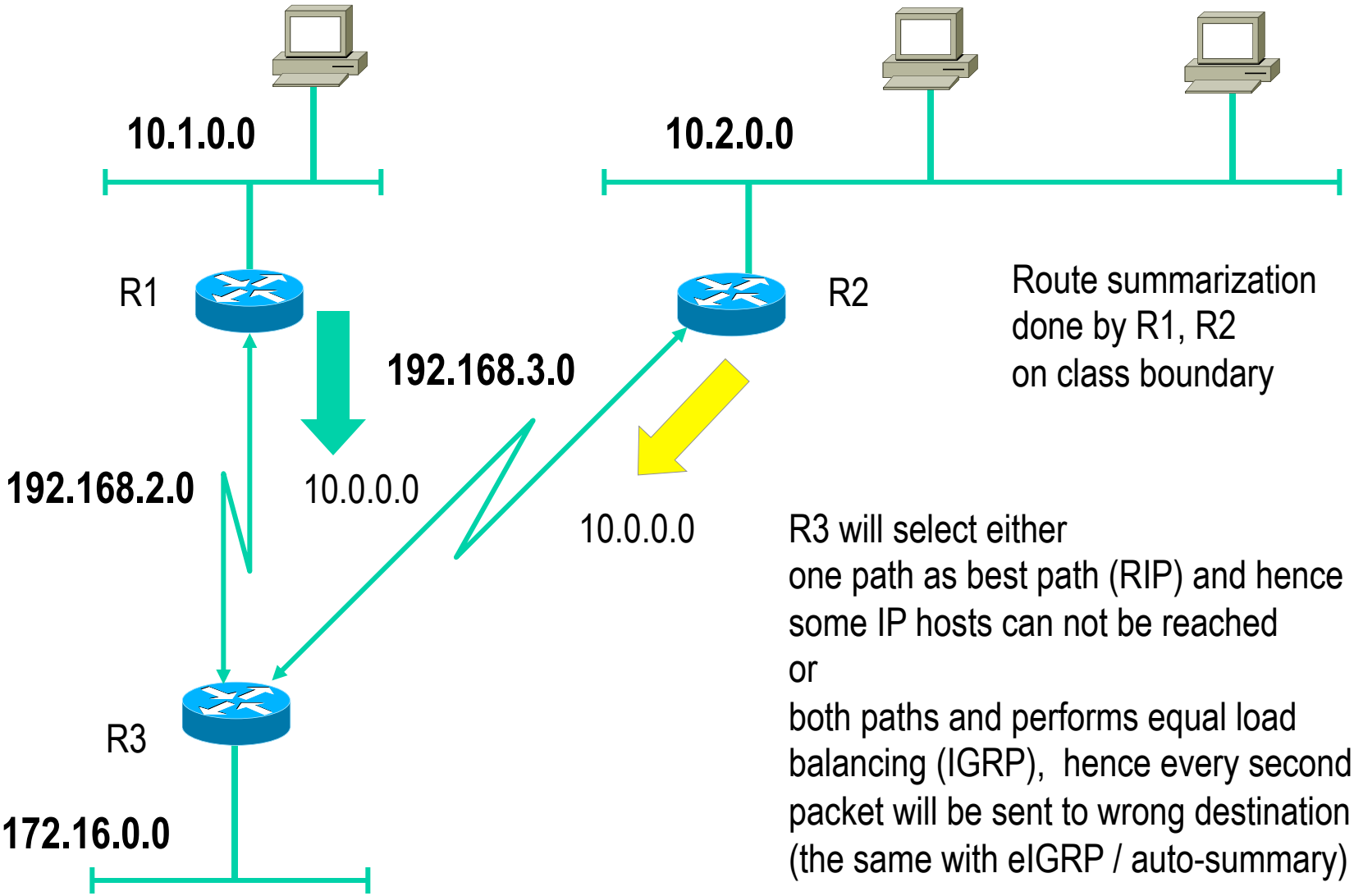
# IP Addressing and Classful Routing




| Routing Table R1 | | |
|---|---|---|
| 10.4.0.0 | local | e0 |
| 10.2.0.0 | R2 | s0 |
| 10.1.0.0 | R3 | s1 |

| Routing Table R5 | | |
|---|---|---|
| 10.0.0.0 | R4 | s0 |
| 192.168.1.0 | local | s0 |

# Non-contiguous Subnetting Classful ???



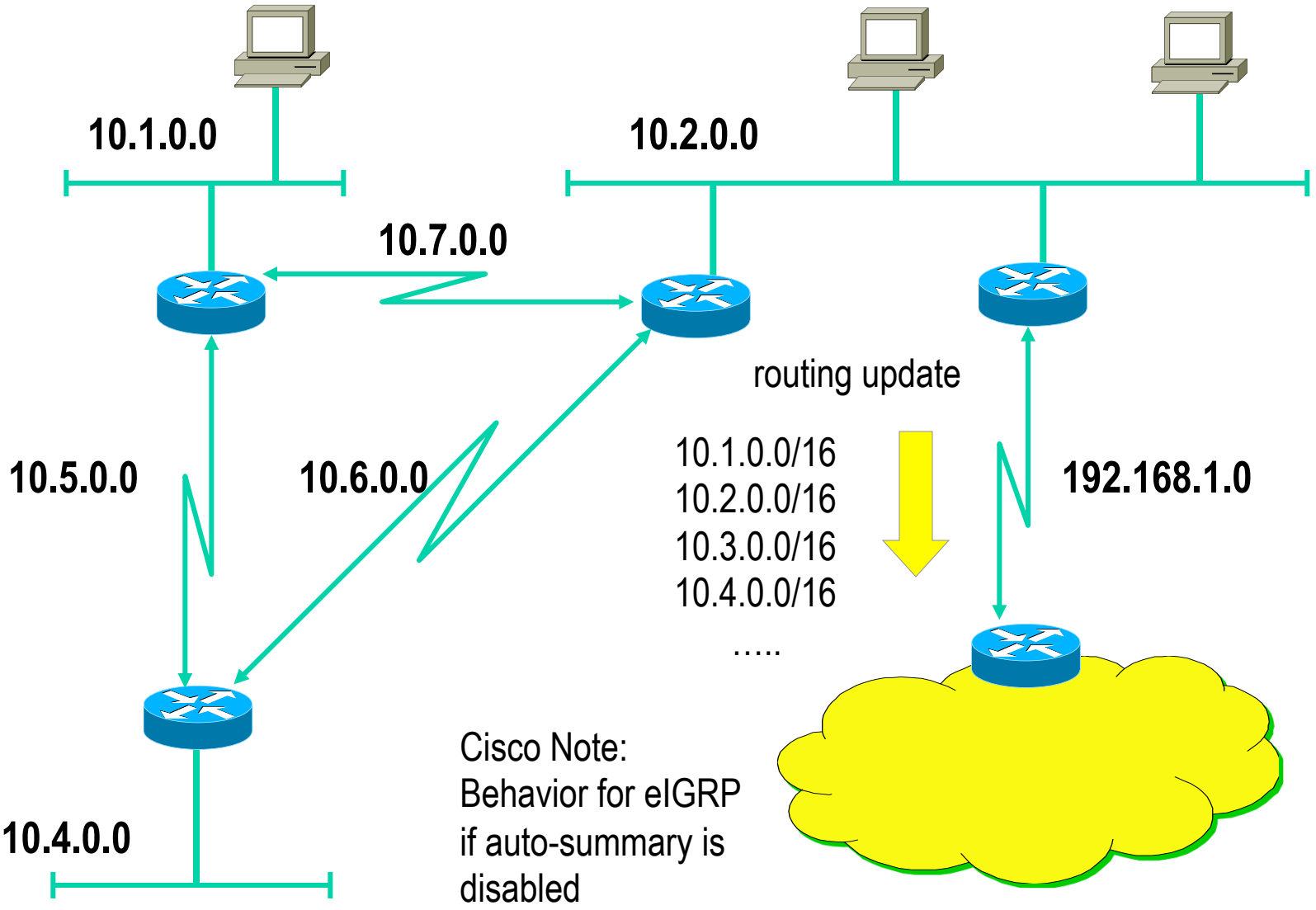

Route summarization done by R1, R2 on class boundary

R3 will select either one path as best path (RIP) and hence some IP hosts can not be reached

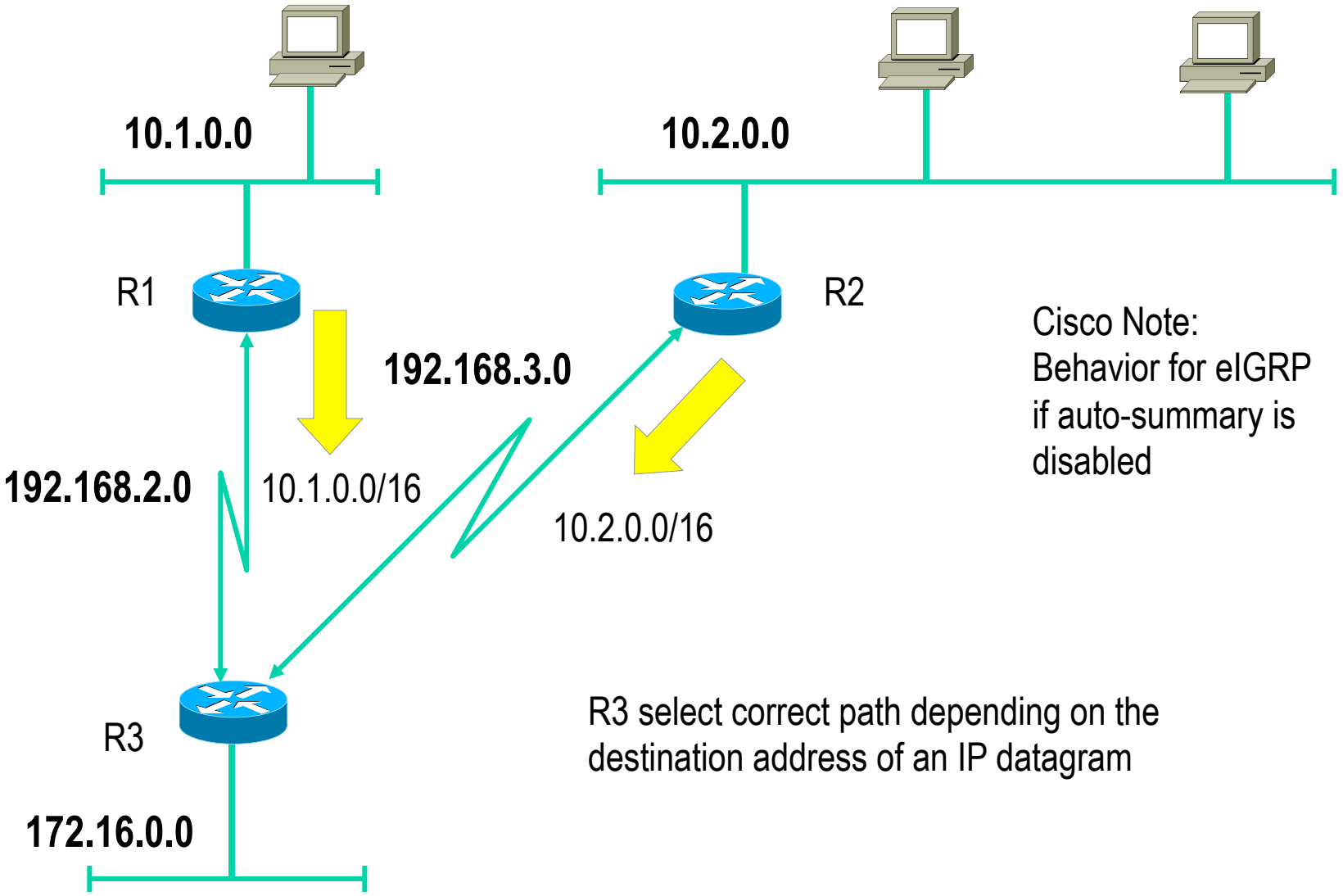
or

both paths and performs equal load balancing (IGRP), hence every second packet will be sent to wrong destination (the same with eIGRP / auto-summary)

# Classless Routing



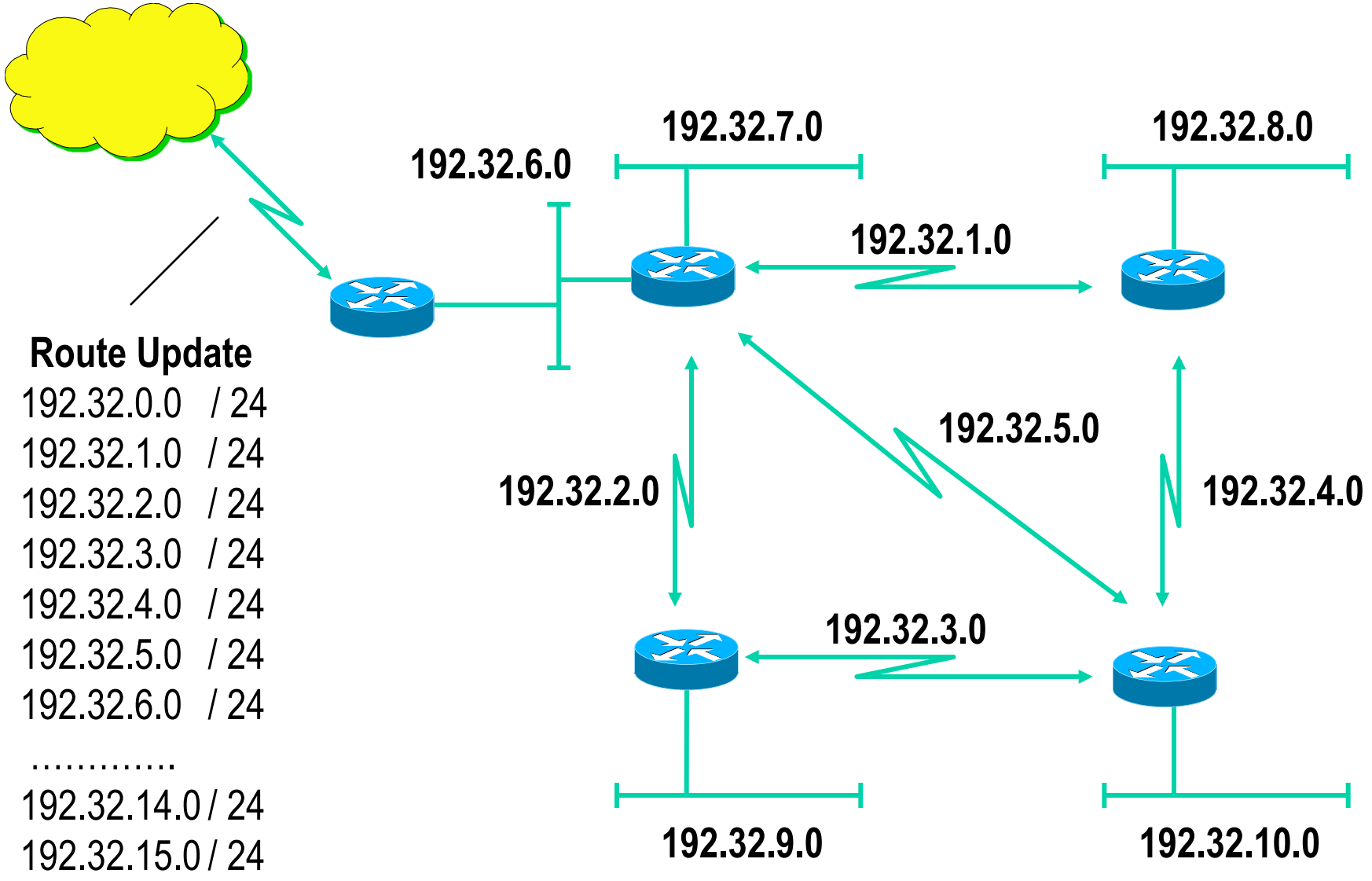
# Non-contiguous Subnetting Classless !!!




Cisco Note:
Behavior for eIGRP if auto-summary is disabled

R3 select correct path depending on the destination address of an IP datagram

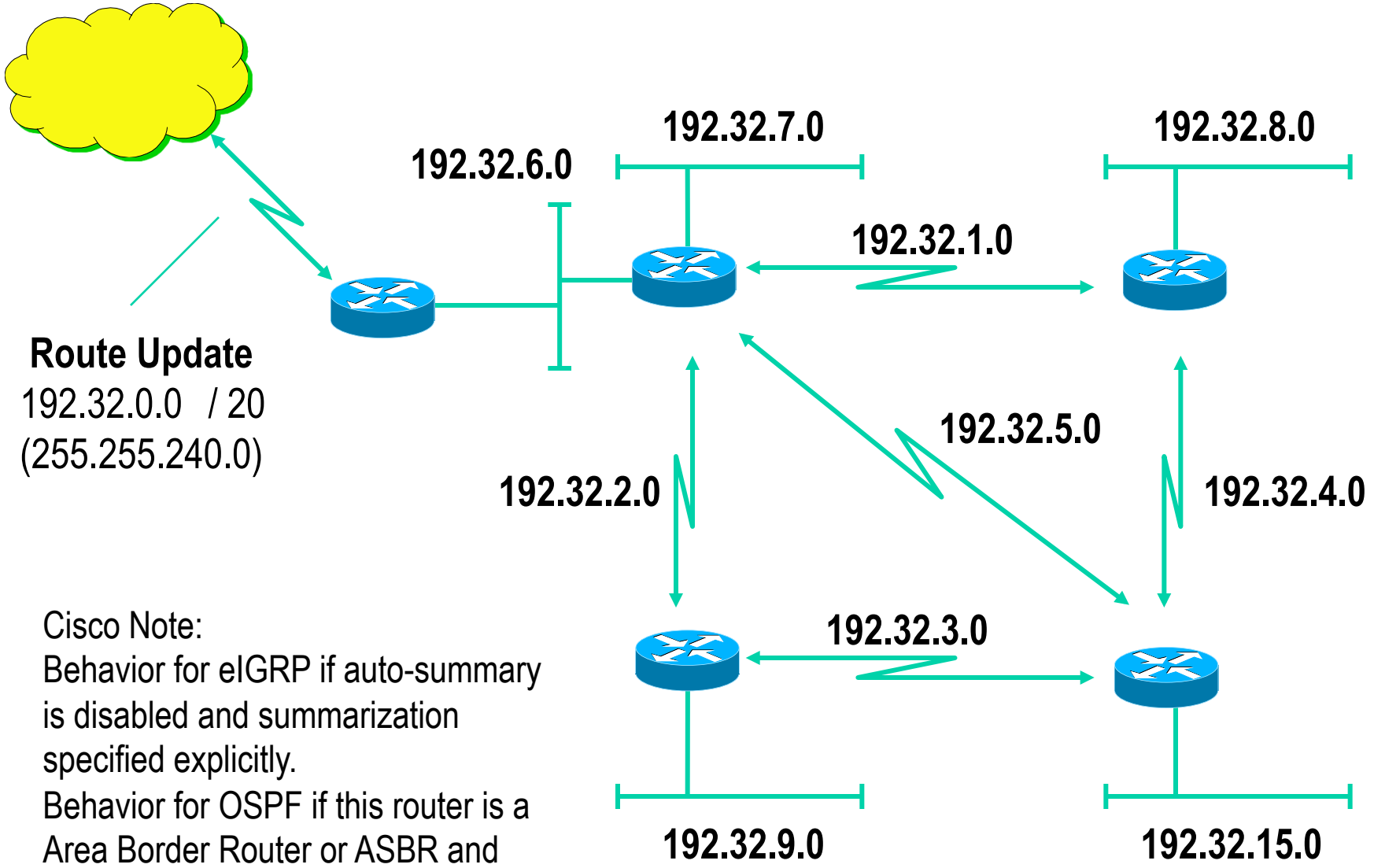
# Routing Updates without Supernetting




**Route Update**

192.32.0.0 / 24
192.32.1.0 / 24
192.32.2.0 / 24
192.32.3.0 / 24
192.32.4.0 / 24
192.32.5.0 / 24
192.32.6.0 / 24
.....
192.32.14.0 / 24
192.32.15.0 / 24

# Route Summarization with Supernetting




Cisco Note:
Behavior for eIGRP if auto-summary is disabled and summarization specified explicitly.
Behavior for OSPF if this router is a Area Border Router or ASBR and summarization specified explicitly

# VLSM Example (1)

- **First step 6 bit subnetting of 172.16.0.0**
  - 172.16.0.0 with 255.255.252.0 (172.16.0.0 / 22)
  - Subnetworks:
    - 172.16.0.0
    - 172.16.4.0
    - 172.16.8.0
    - 172.16.12.0
    - 172.16.16.0

      ……
    - 172.16.248.0
    - 172.16.252.0
  - Subnetworks are capable of addressing 1022 IP systems

# VLSM Example (2)

- **Next step sub-subnetting**
  - Basic subnet 172.16.4.0 255.255.252.0 (172.16.4.0 / 22)
  - Sub-subnetworks with mask 255.255.255.252 (/ 30):
    - 172.16.4.0 / 30
    - 172.16.4.4 / 30
      - 172.16.4.4 net-ID
      - 172.16.4.5 first IP host of subnet 172.16.4.4
      - 172.16.4.6 last IP host of subnet 172.16.4.4
      - 172.16.4.7 directed broadcast of subnet 172.16.4.4
    - 172.16.4.8 / 30
    - 172.16.4.12 / 30
    - …….
    - 172.16.4.252 / 30
  - Sub-subnetworks capable of addressing 2 IP systems

# VLSM Example (3)

- **Next step sub-subnetting**
  - Basic subnet 172.16.8.0 255.255.252.0 (172.16.8.0 / 22)
  - Sub-subnetworks with mask 255.255.255.0 (/ 24):
    - 172.16.8.0 / 24
    - 172.16.9.0 / 24
      - 172.16.9.0 net-ID
      - 172.16.9.1 first IP host of subnet 172.16.9.0

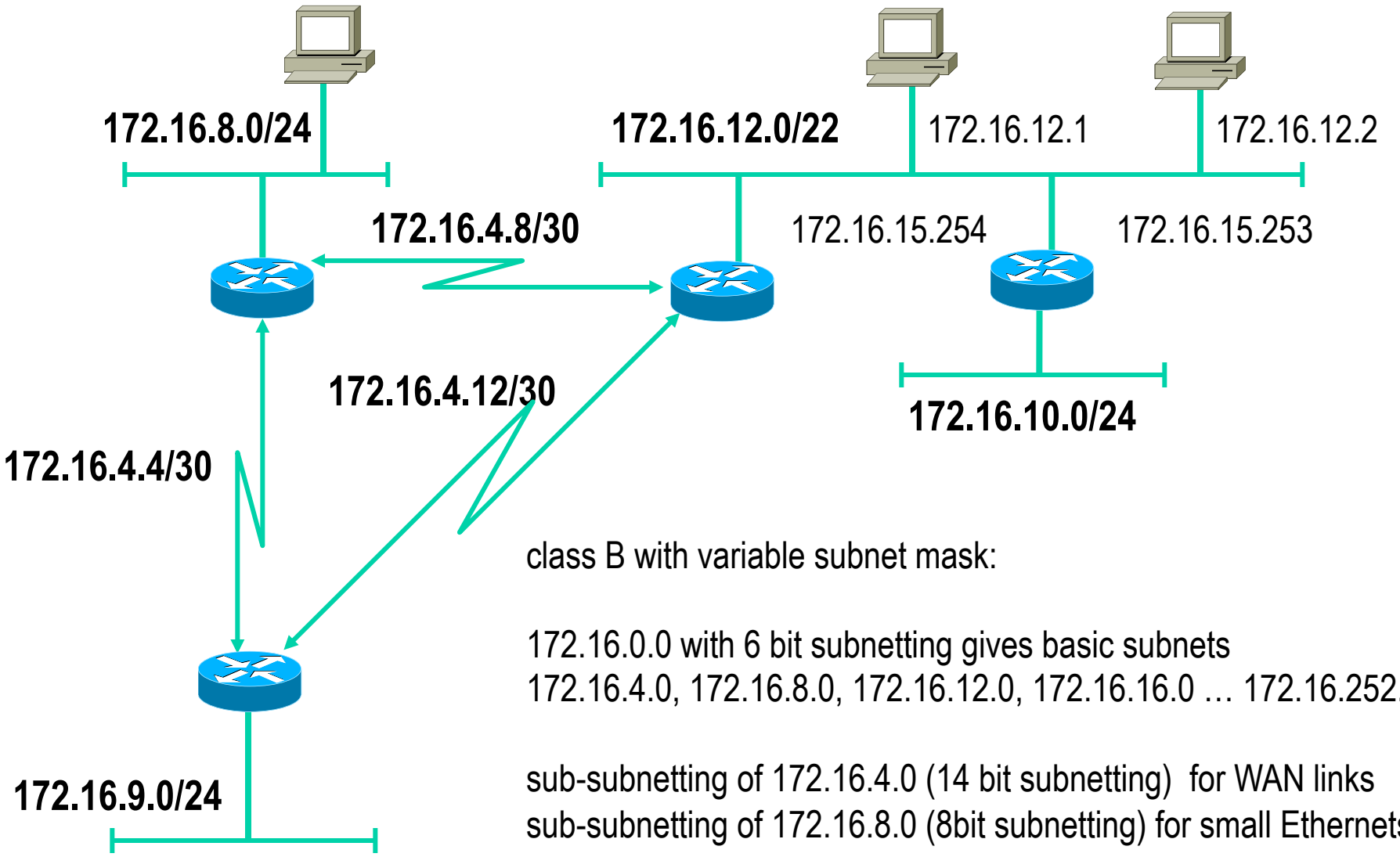
        ----------
      - 172.16.9.254 last IP host of subnet 172.16.9.0
      - 172.16.9.255 directed broadcast of subnet 172.16.9.0
    - 172.16.10.0 / 24
    - 172.16.11.0 / 24
  - Sub-subnetworks capable of addressing 254 IP systems

# VLSM Example (4)

- **No sub-subnetting for basic subnet 172.16.12.0**
  - 172.16.12.0 with 255.255.252.0 (172.16.12.0 / 22)
    - 172.16.12.0 net-ID
    - 172.16.12.1 first IP host of subnet 172.16.12.0

      ---
    - 172.16.15.254 last IP host of subnet 172.16.12.0
    - 172.16.15.255 directed broadcast of subnet 172.16.12.0
  - Subnetwork capable of addressing 1022 IP systems

# Example VLSM




class B with variable subnet mask:

172.16.0.0 with 6 bit subnetting gives basic subnets
172.16.4.0, 172.16.8.0, 172.16.12.0, 172.16.16.0 … 172.16.252.0

sub-subnetting of 172.16.4.0 (14 bit subnetting) for WAN links
sub-subnetting of 172.16.8.0 (8bit subnetting) for small Ethernets

# IP Address Space Depletion

- **The growing demand of IP addresses**
  - Has put a strain on the classful model
  - Class B exhaustion
  - Class C are to small for most organization
  - Many class C addresses given to a certain organization leads to explosion of routing table entries in the Internet core routers
- **Measures to handle these problems**
  - Creative IP address allocation
  - CIDR
  - Private IP addresses and network address translation (NAT)
  - IPv6

# CIDR

- **Classless Interdomain Routing (CIDR)**
  - Address assignment and aggregation (route summarization) strategy
  - Temporary solution to overcome depletion of IP address space and explosion of routing tables in the Internet core routers
- **Basic ideas**
  - Classless routing (prefix, length)
  - Supernetting
  - Coordinated address allocation
    - until 1992 IP addresses had no relation at all to the networks topology

# CIDR

- **CIDR address allocation**
  - Addressing plan for class C addresses by continents
    - 192.0.0.0 - 193.255.255.255 … Multiregional
    - 194.0.0.0 - 195.255.255.255 … Europe
    - 198.0.0.0 - 199.255.255.255 … North America
    - 200.0.0.0 - 201.255.255.255 … Central/South America
  - Provider addressing strategy
    - Internet Service Providers (ISP) are given contiguous blocks of class C addresses which in turn are granted to their customers
    - Consequence: change of provider means renumbering
  - Class C network numbers are allocated in such a way that route summarization (or sometimes called route aggregation) into supernets is possible

# CIDR

- **Definitions of terms often used interchangeably**
  - CIDR block
    - is the <prefix, length> notation
  - Supernets
    - have a prefix length shorter than the networks natural mask
  - Aggregates
    - indicate any summary route
- **In order to implement CIDR**
  - Classless routing protocols between routing domains must be used
    - BGP-4 as interdomain routing protocol
  - Classless routing within a routing domain
    - RIPv2, OSPF, eIGRP

# Private Address Range - RFC 1918

- **Three blocks of address ranges are reserved for addressing of private networks**
  - 10.0.0.0 - 10.255.255.255 (10/8 prefix)
  - 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
  - 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)
  - Note:
    - In pre-CIDR notation the first block is nothing but a single class A network number, while the second block is a set of 16 contiguous class B network numbers, and third block is a set of 256 contiguous class C network numbers.
- **Translation between private addresses and globally unique addresses -> NAT**

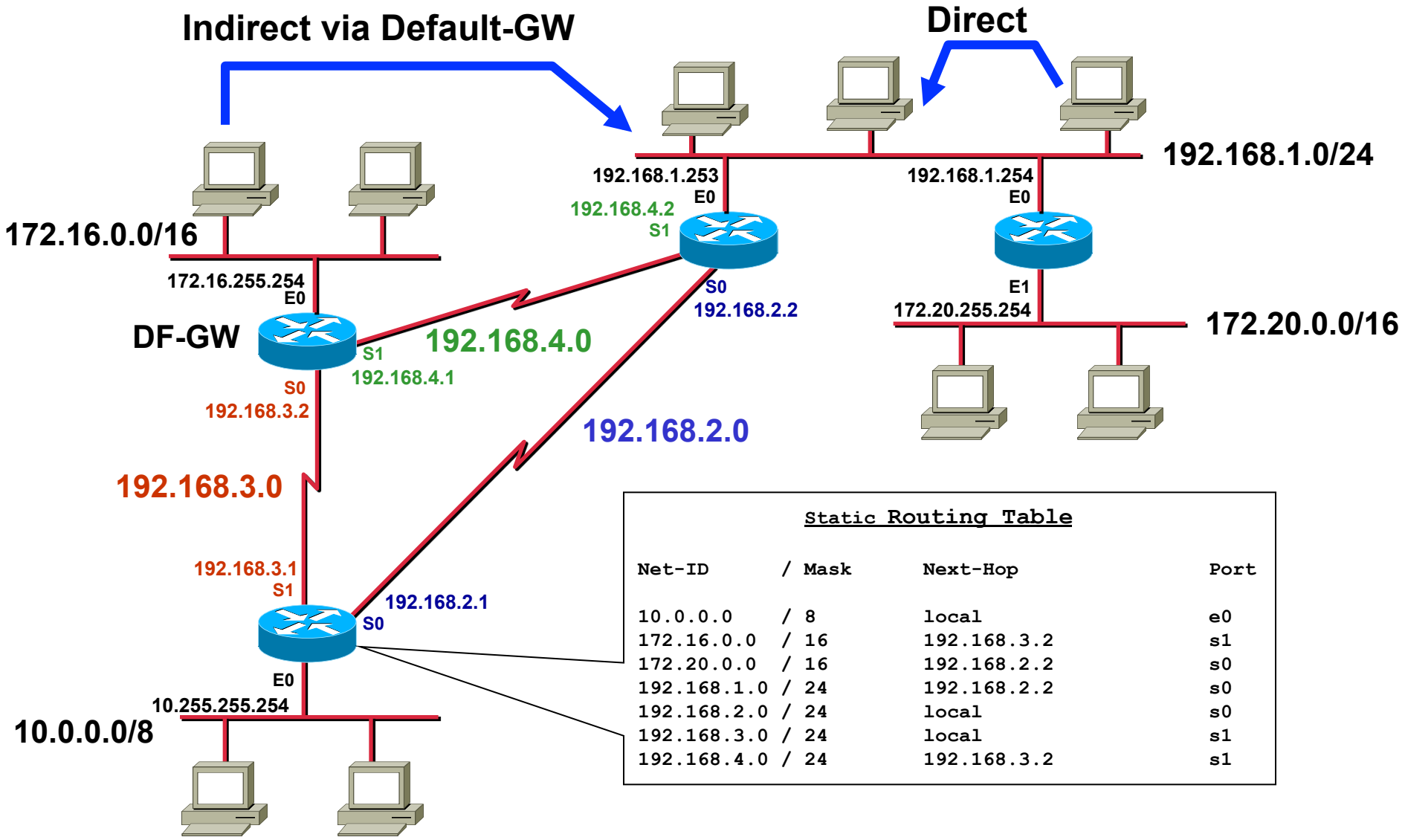
# Agenda

- **Introduction**
  - Short History of the Internet (not part of the exam!)
  - Basic Principles
- **IP**
  - IP Protocol
  - IP QoS
  - Addressing
  - Classful  versus Classless (not part of the exam!)
- **IP Forwarding**
  - Principles
  - ARP
  - ICMP
  - PPP
- **First Hop Redundancy**
  - Proxy ARP, IDRP
  - HSRP
  - VRRP (not part of the exam!)

# IP Forwarding Responsibilities

- **IP hosts and IP routers take part in this process**
  - IP hosts responsible for direct delivery of IP datagram's
  - IP routers responsible for selecting the best path in a meshed network in case of indirect delivery of IP datagram's
    - Decision based on current state of routing table
- **Direct versus indirect delivery**
  - Depends on destination net-ID
    - Net-ID equal source net-ID -> direct delivery
    - Net-ID unequal source net-ID -> indirect delivery
- **IP hosts choose a “default” router aka “Default Gateway”**
  - As next hop in case of indirect delivery of IP datagrams

# Direct versus Indirect Delivery
# Default Gateway / Routing Table




**Static Routing Table**

| Net-ID | / Mask | Next-Hop | Port |
|---|---|---|---|
| 10.0.0.0 | / 8 | local | e0 |
| 172.16.0.0 | / 16 | 192.168.3.2 | s1 |
| 172.20.0.0 | / 16 | 192.168.2.2 | s0 |
| 192.168.1.0 | / 24 | 192.168.2.2 | s0 |
| 192.168.2.0 | / 24 | local | s0 |
| 192.168.3.0 | / 24 | local | s1 |
| 192.168.4.0 | / 24 | 192.168.3.2 | s1 |

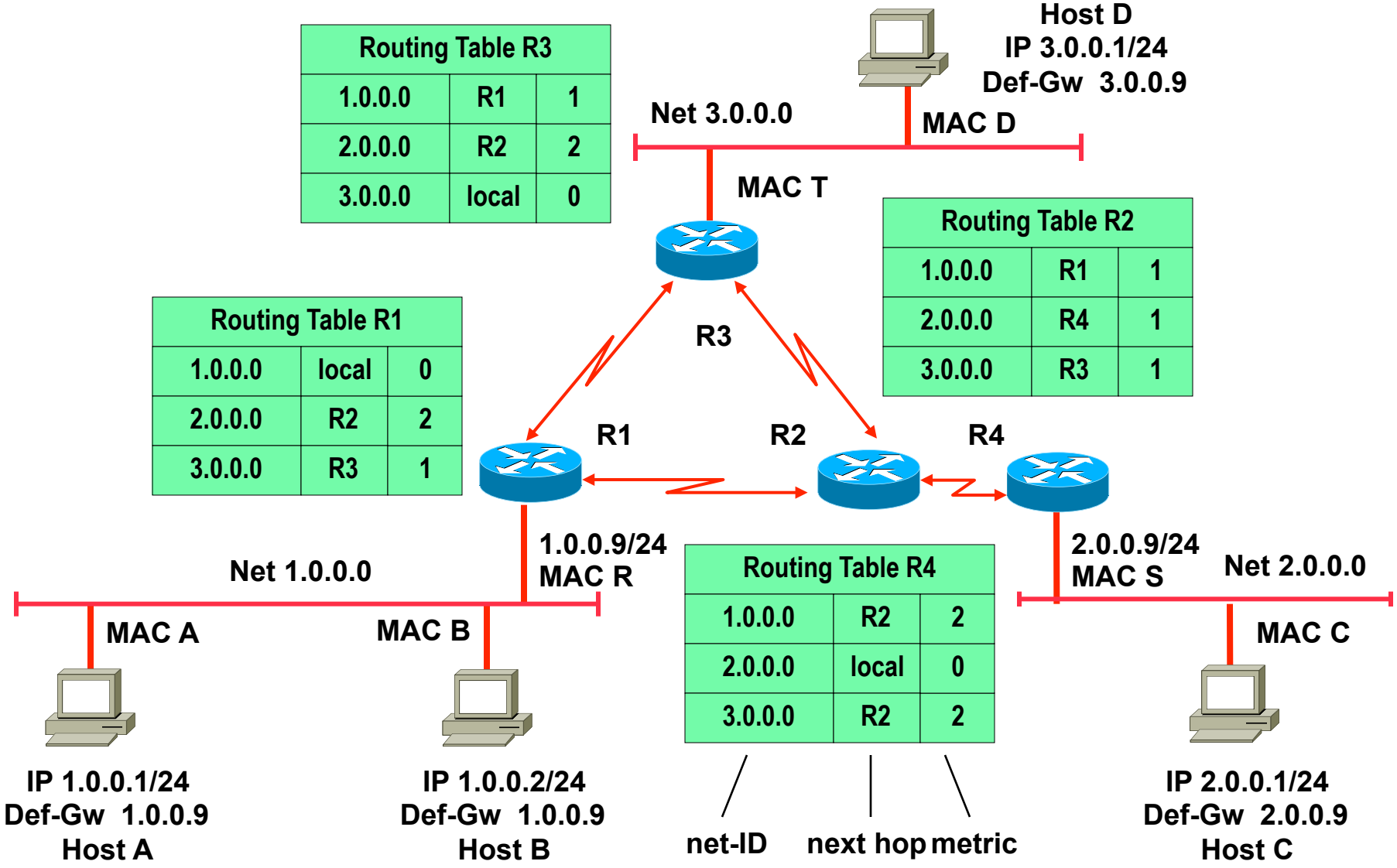
# Principle

- **IP Forwarding is done by routers in case of indirect routing**
  - Based on the destination address of a given IP datagram
  - Following the path to the destination hop by hop
- **Routing tables**
  - Have information about which next hop router a given destination network can be reached
- **L2 header must be changed hop by hop**
  - If LAN then physical L2 address (MAC addresses) must be adapted for direct communication on LAN
- **Mapping between IP and L2 address on LAN**
  - Is done by Address Resolution Protocol (ARP)

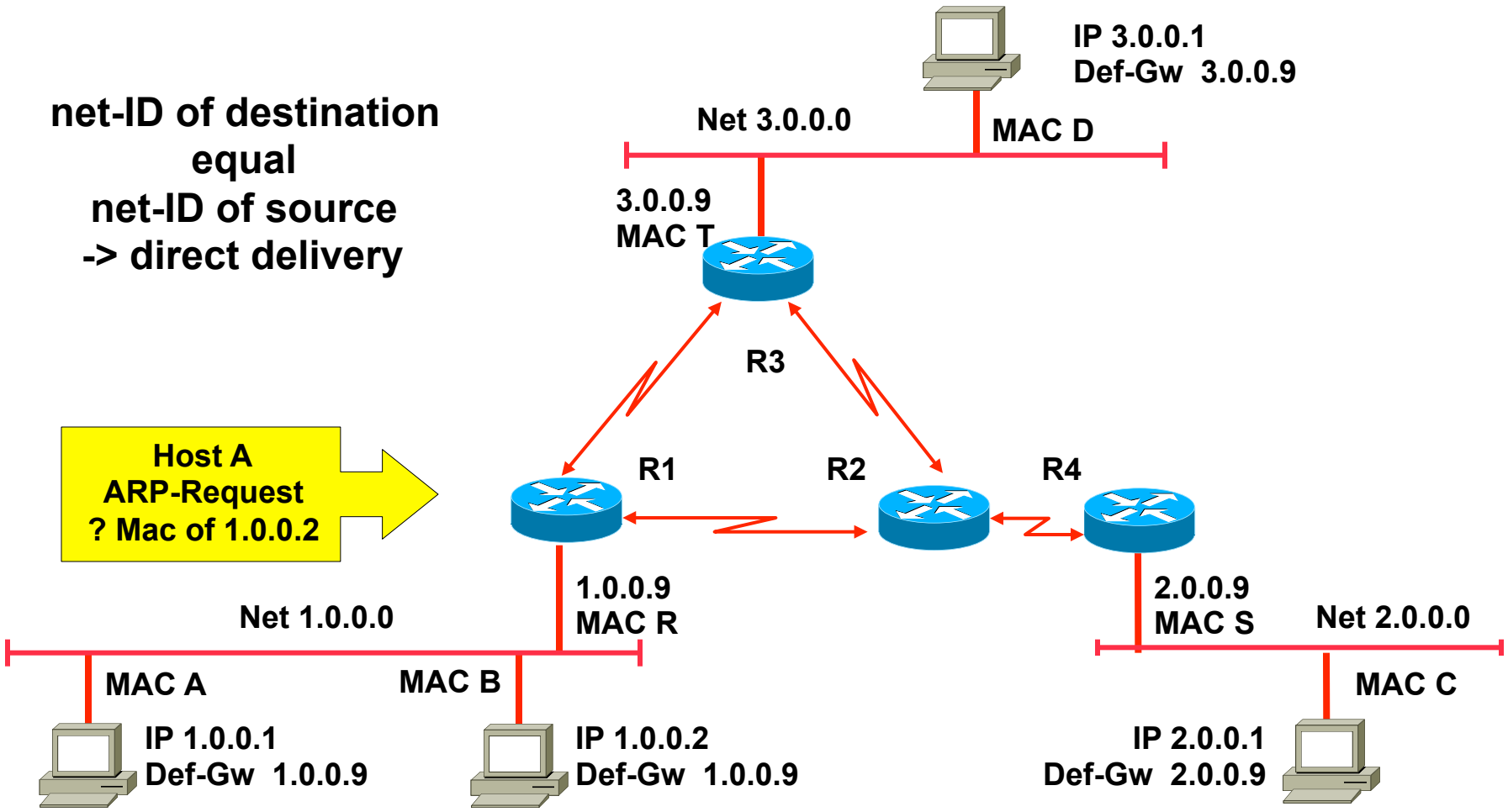
# IP Routing Paradigm

- **Destination Based Routing**
  - Source address is not taken into account for the forward decision
- **Hop by Hop Routing**
  - IP datagrams follow the path, which is pointed by the current state of the routing tables
- **Least Cost Routing**
  - Normally only the best path is considered for forwarding of IP datagrams
  - Alternate paths will not be used in order to reach a given destination

# Example Topology

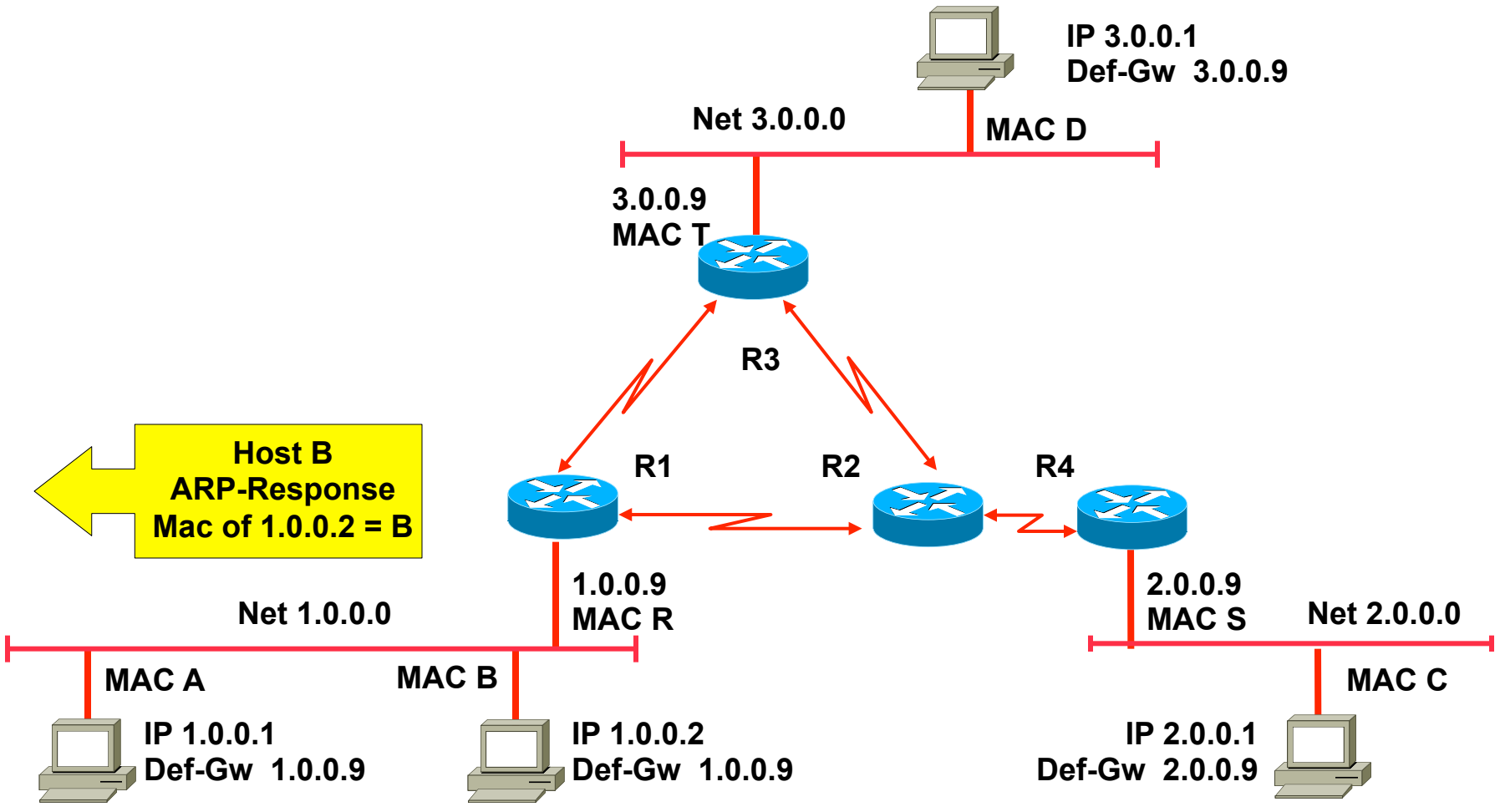


# Direct Delivery 1.0.0.1 - > 1.0.0.2



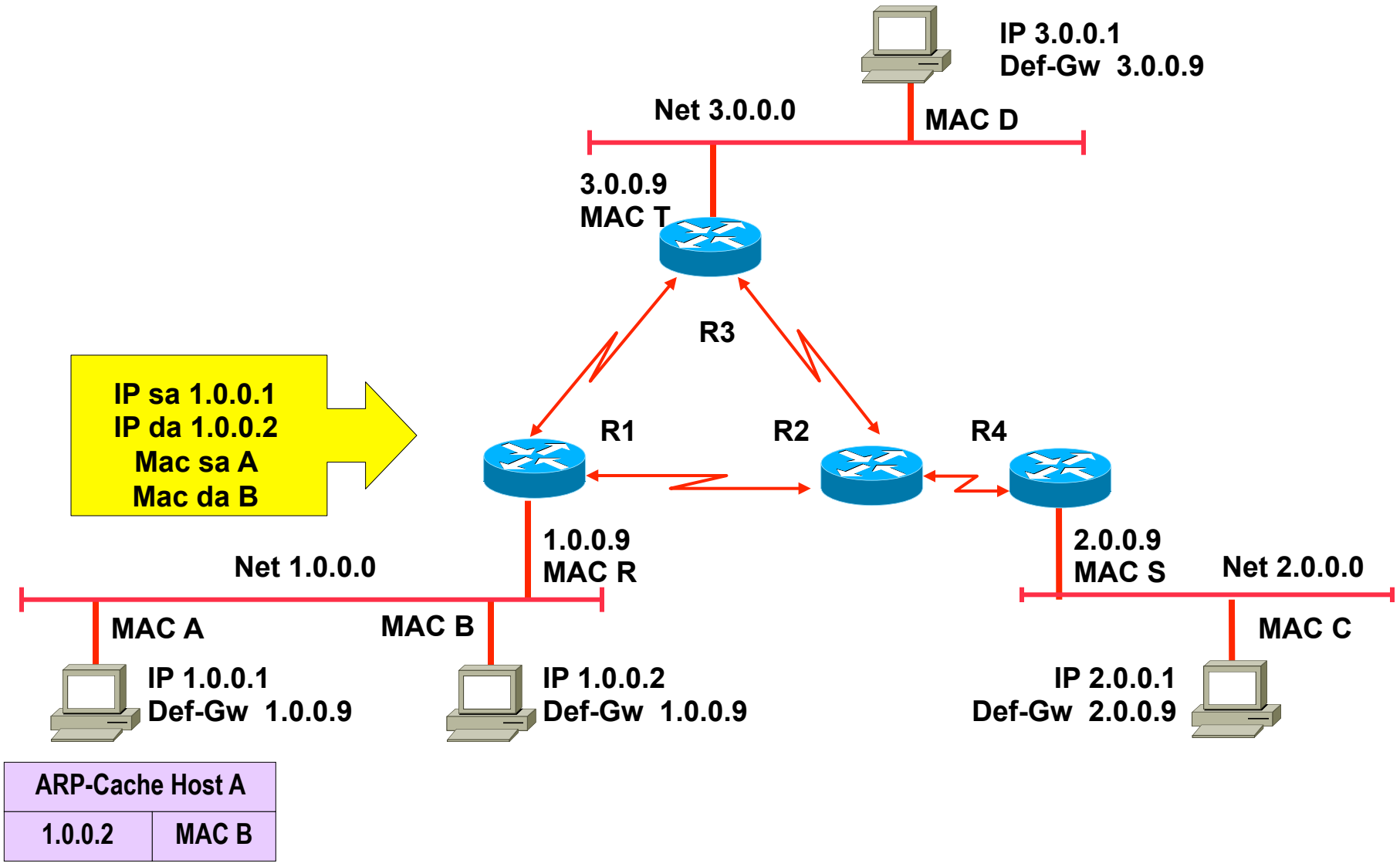

ARP ... Address Resolution Protocol

# Direct Delivery 1.0.0.1 - > 1.0.0.2



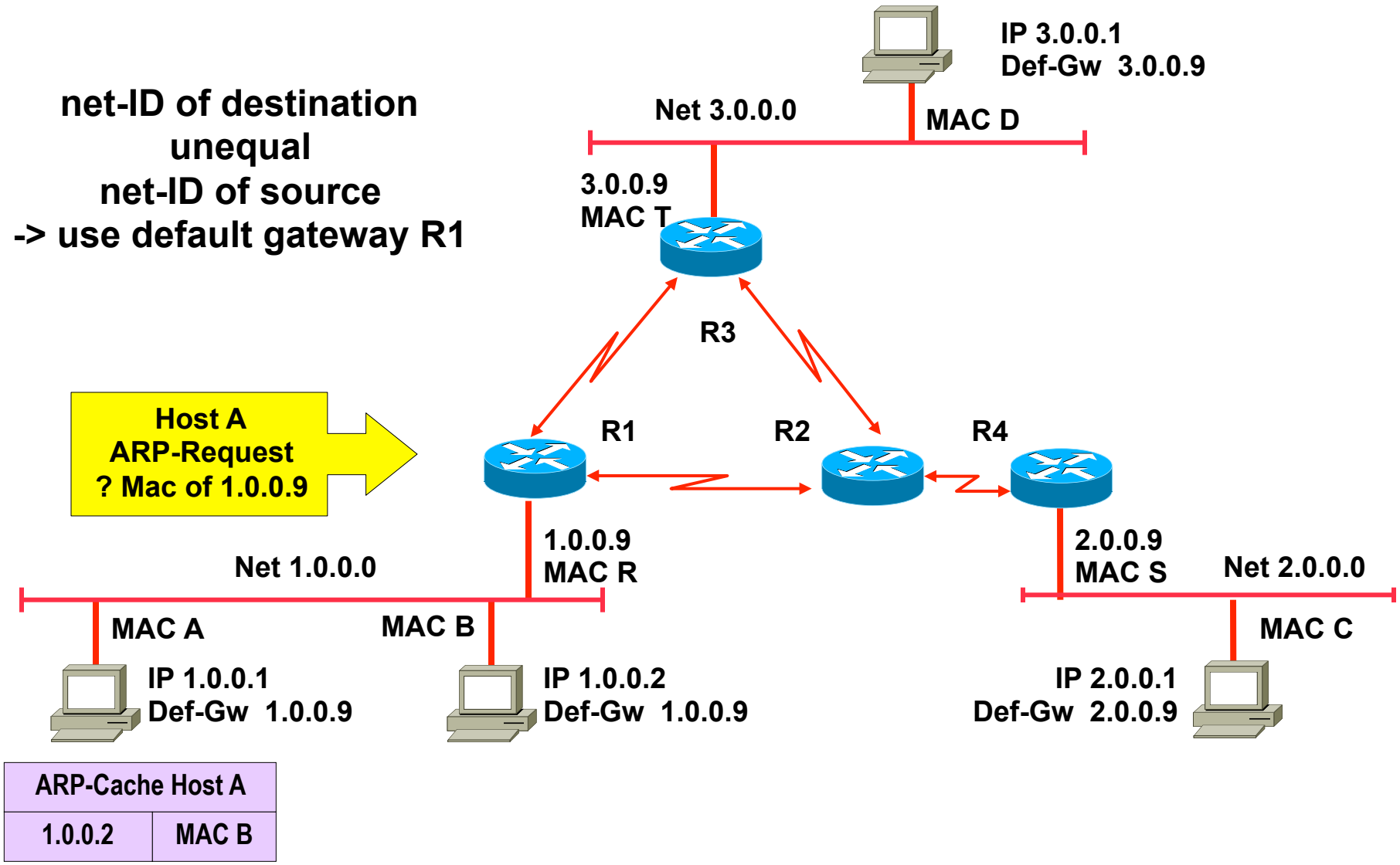

| ARP-Cache Host A | |
|---|---|
| 1.0.0.2 | MAC B |

# Direct Delivery 1.0.0.1 - > 1.0.0.2



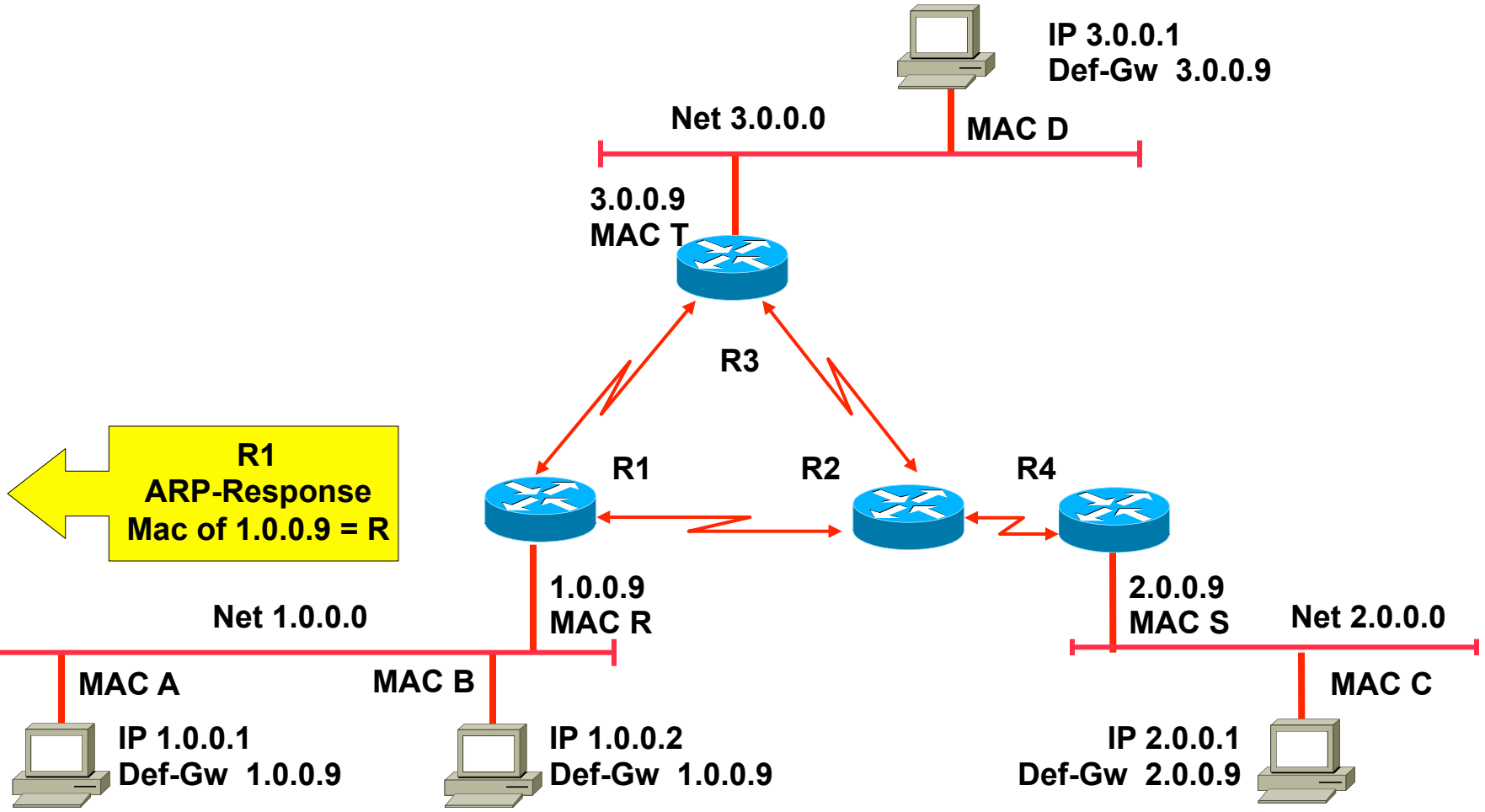

| ARP-Cache Host A | |
|---|---|
| 1.0.0.2 | MAC B |

# Indirect Delivery 1.0.0.1 - > 2.0.0.1



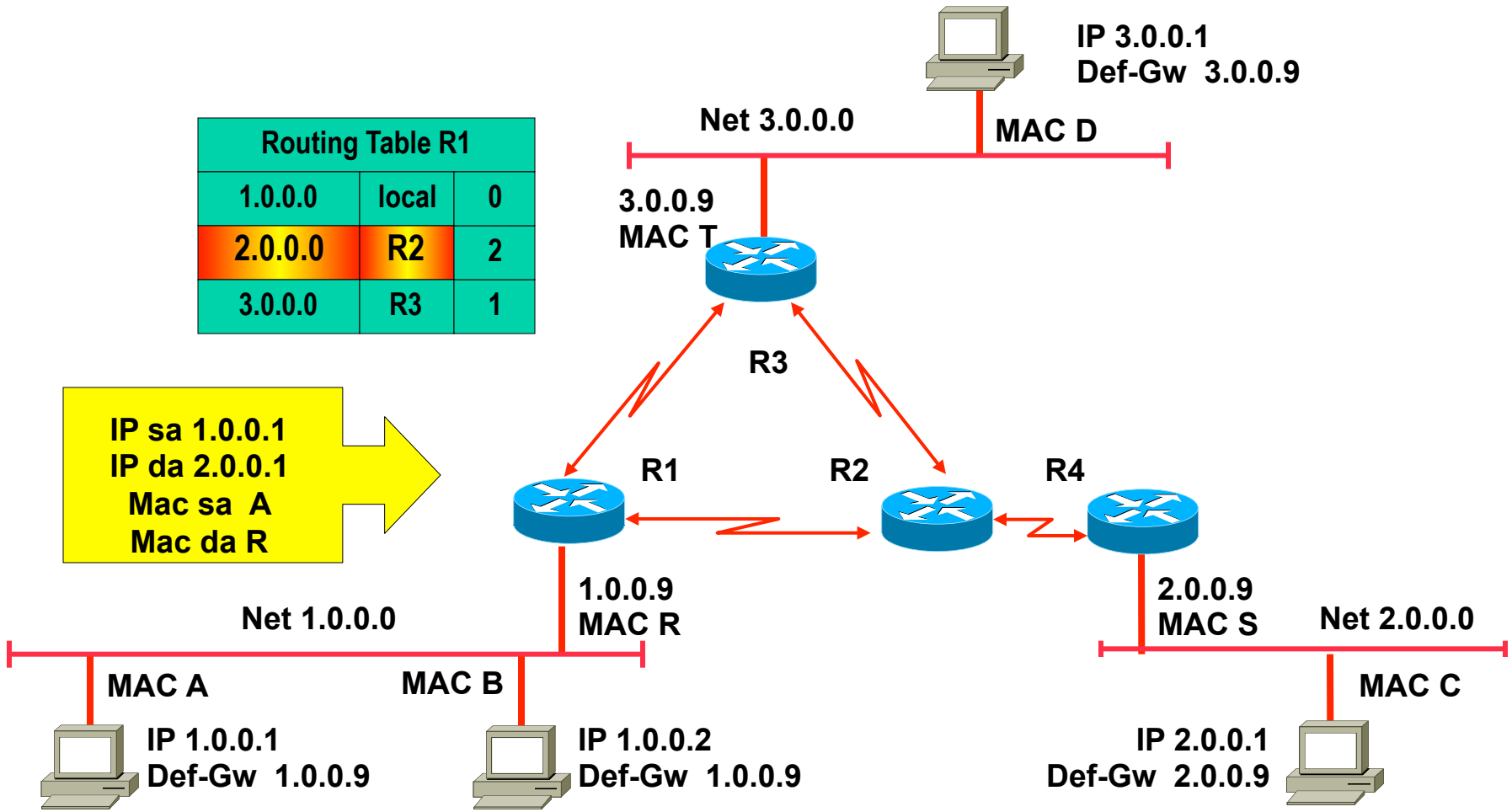

| ARP-Cache Host A | |
|---|---|
| 1.0.0.2 | MAC B |

# Indirect Delivery 1.0.0.1 - > 2.0.0.1




| ARP-Cache Host A | |
|---|---|
| 1.0.0.2 | MAC B |
| 1.0.0.9 | MAC R |

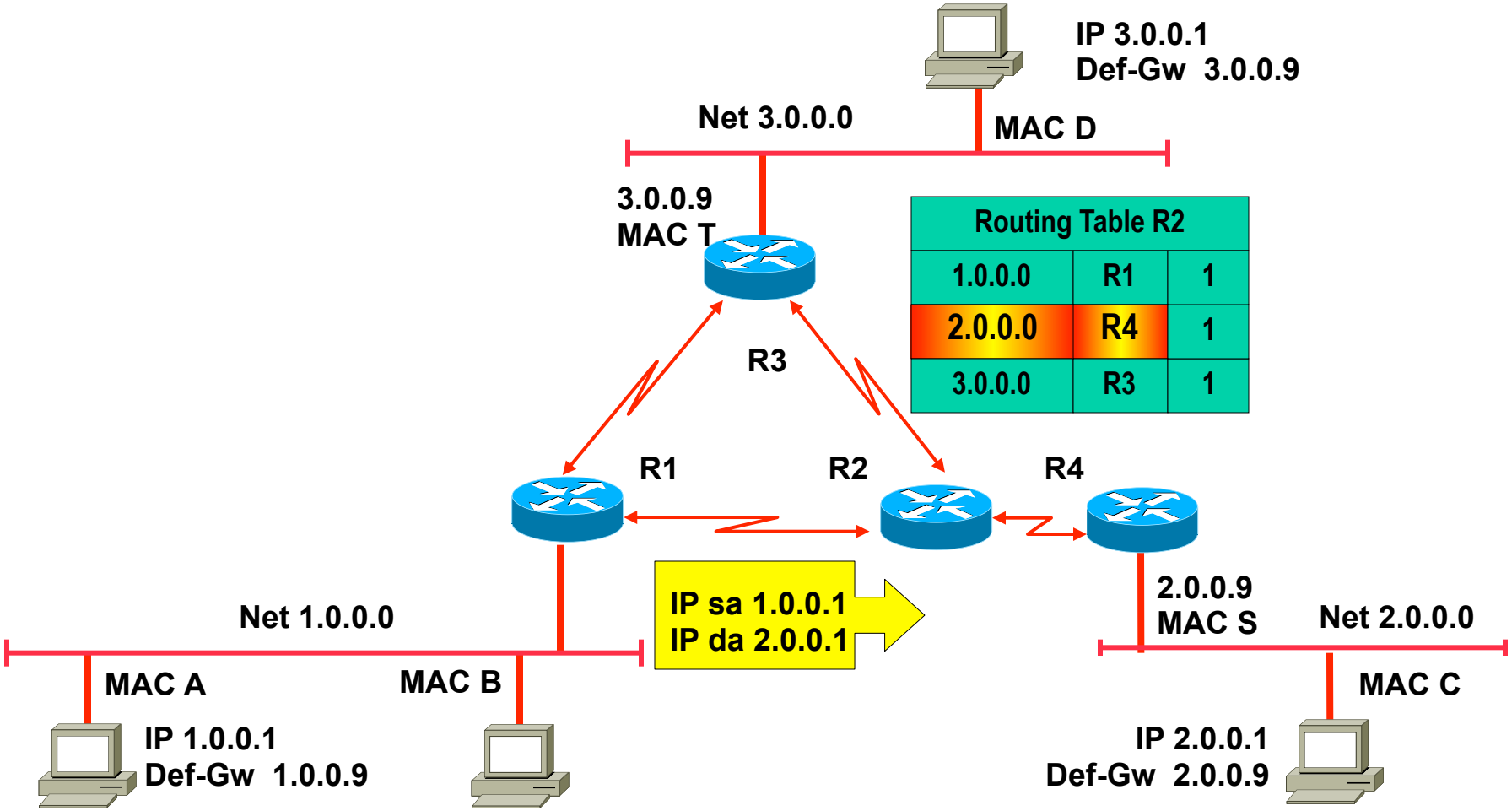
# Indirect Delivery 1.0.0.1 - > 2.0.0.1




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

| ARP-Cache Host A | |
|---|---|
| 1.0.0.2 | MAC B |
| 1.0.0.9 | MAC R |

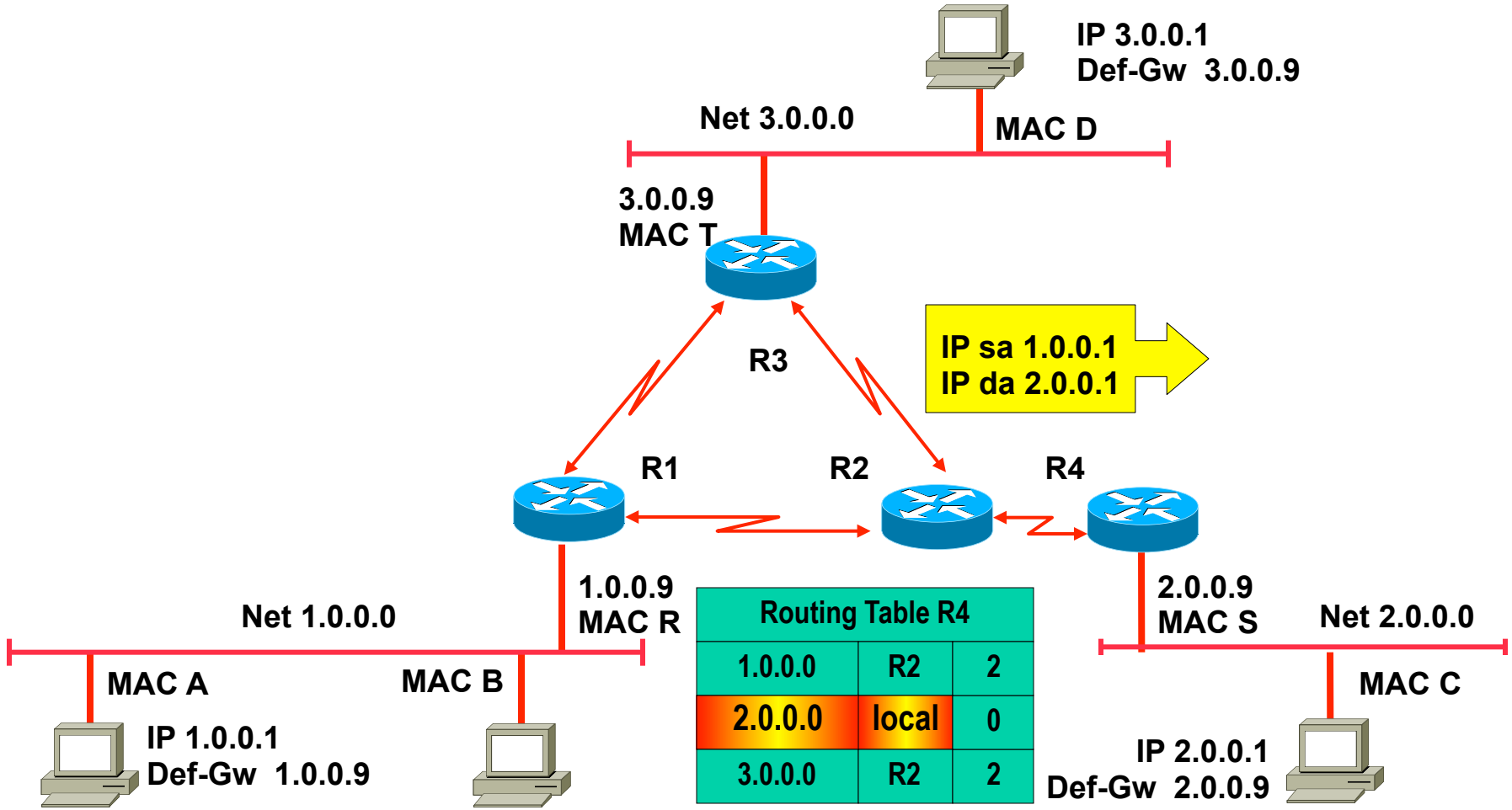
# Indirect Delivery 1.0.0.1 - > 2.0.0.1




| Routing Table R2 | | |
|---|---|---|
| 1.0.0.0 | R1 | 1 |
| 2.0.0.0 | R4 | 1 |
| 3.0.0.0 | R3 | 1 |

| ARP-Cache Host A | |
|---|---|
| 1.0.0.2 | MAC B |
| 1.0.0.9 | MAC R |

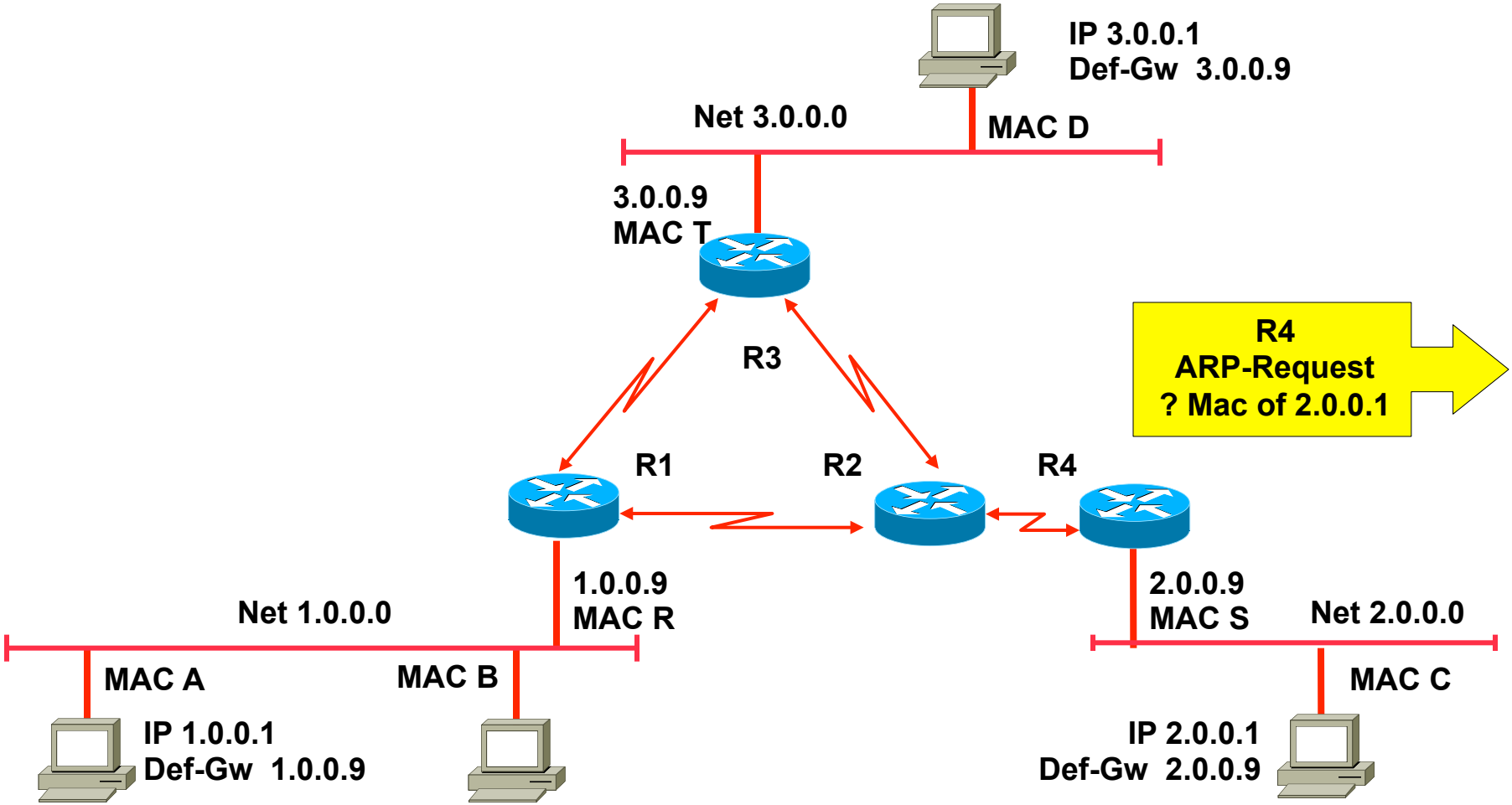
# Indirect Delivery 1.0.0.1 - > 2.0.0.1




| Routing Table R4 | | |
|---|---|---|
| 1.0.0.0 | R2 | 2 |
| 2.0.0.0 | local | 0 |
| 3.0.0.0 | R2 | 2 |

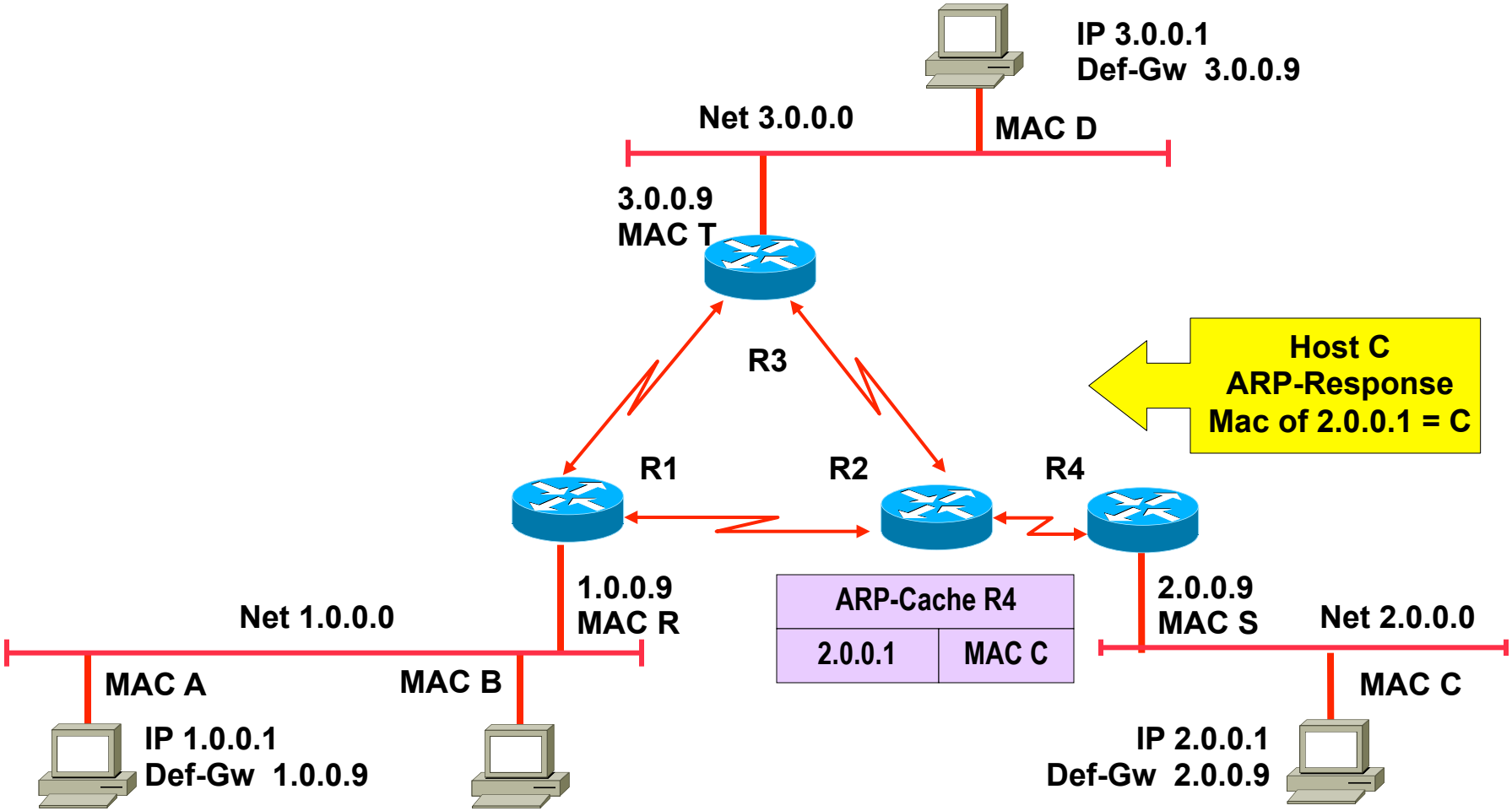
| ARP-Cache Host A | |
|---|---|
| 1.0.0.2 | MAC B |
| 1.0.0.9 | MAC R |

# Indirect Delivery 1.0.0.1 - > 2.0.0.1



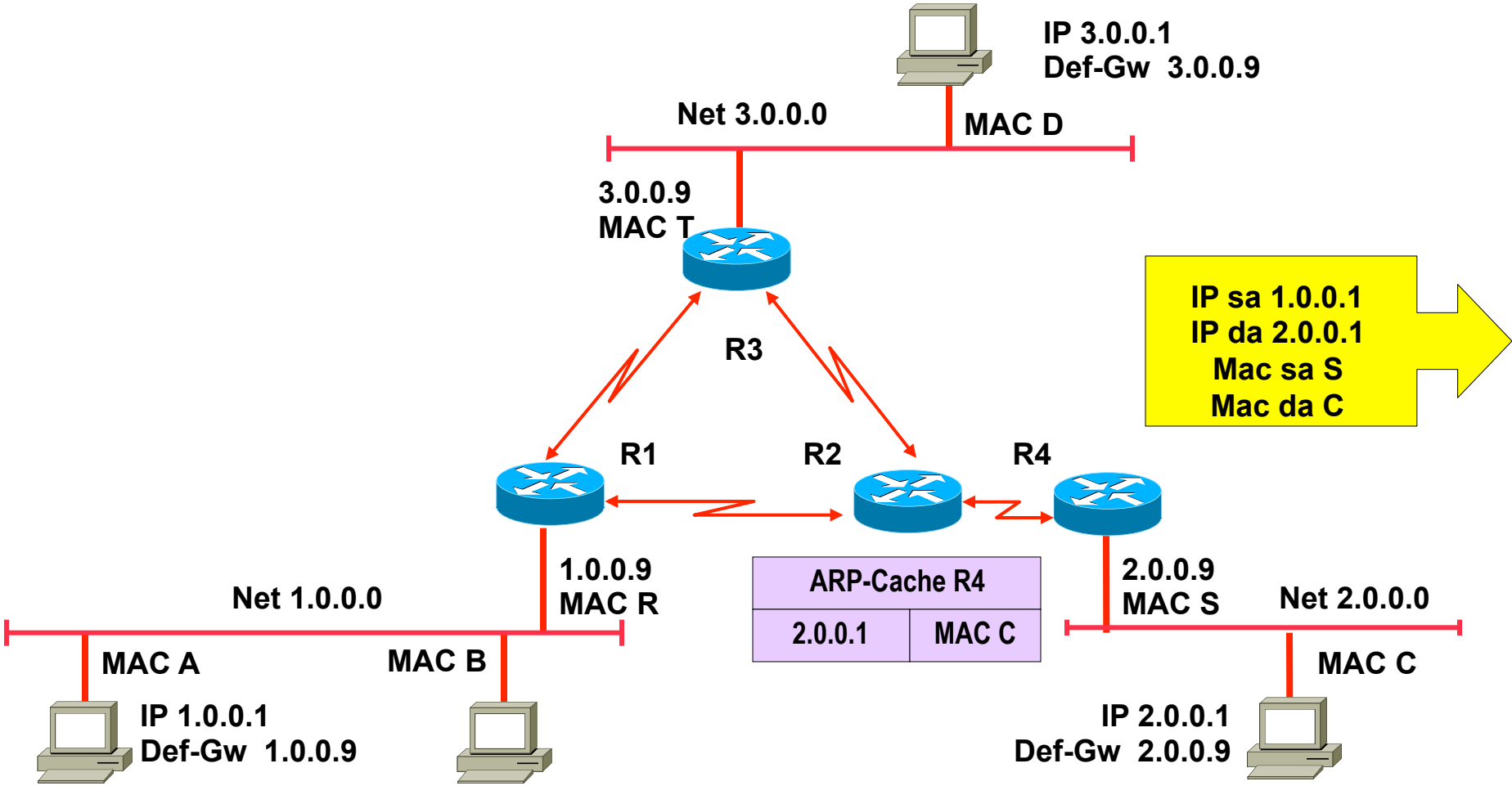

| ARP-Cache Host A | |
|---|---|
| 1.0.0.2 | MAC B |
| 1.0.0.9 | MAC R |

# Indirect Delivery 1.0.0.1 - > 2.0.0.1



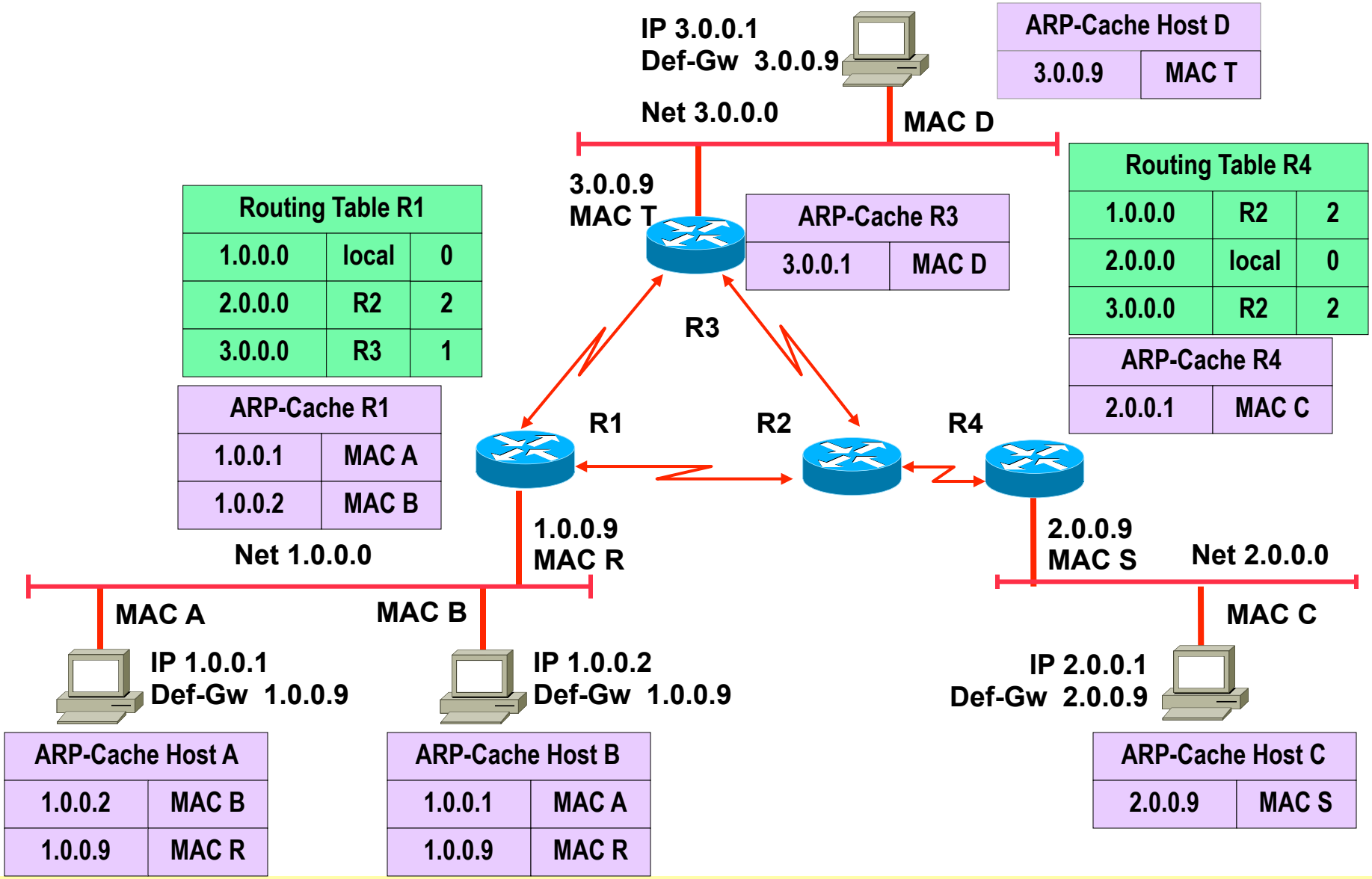

| ARP-Cache Host A | |
|---|---|
| 1.0.0.2 | MAC B |
| 1.0.0.9 | MAC R |

# Indirect Delivery 1.0.0.1 - > 2.0.0.1




| ARP-Cache Host A | |
|---|---|
| 1.0.0.2 | MAC B |
| 1.0.0.9 | MAC R |

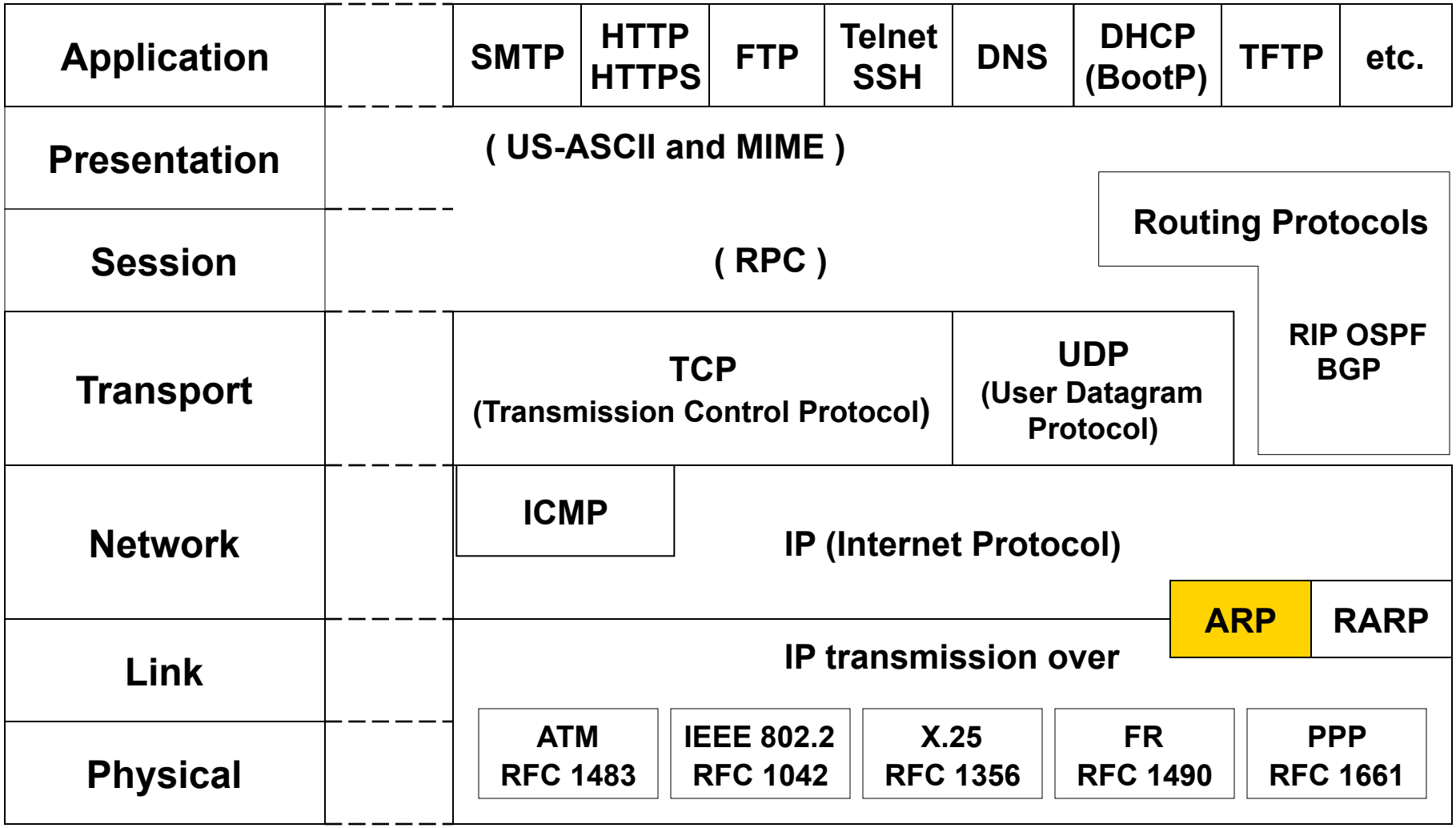
# ARP Cache - Final Picture



# Agenda

- **Introduction**
  - Short History of the Internet (not part of the exam!)
  - Basic Principles
- **IP**
  - IP Protocol
  - IP QoS
  - Addressing
  - Classful versus Classless (not part of the exam!)
- **IP Forwarding**
  - Principles
  - ARP
  - ICMP
  - PPP
- **First Hop Redundancy**
  - Proxy ARP, IDRP
  - HSRP
  - VRRP (not part of the exam!)

# TCP/IP Protocol Suite



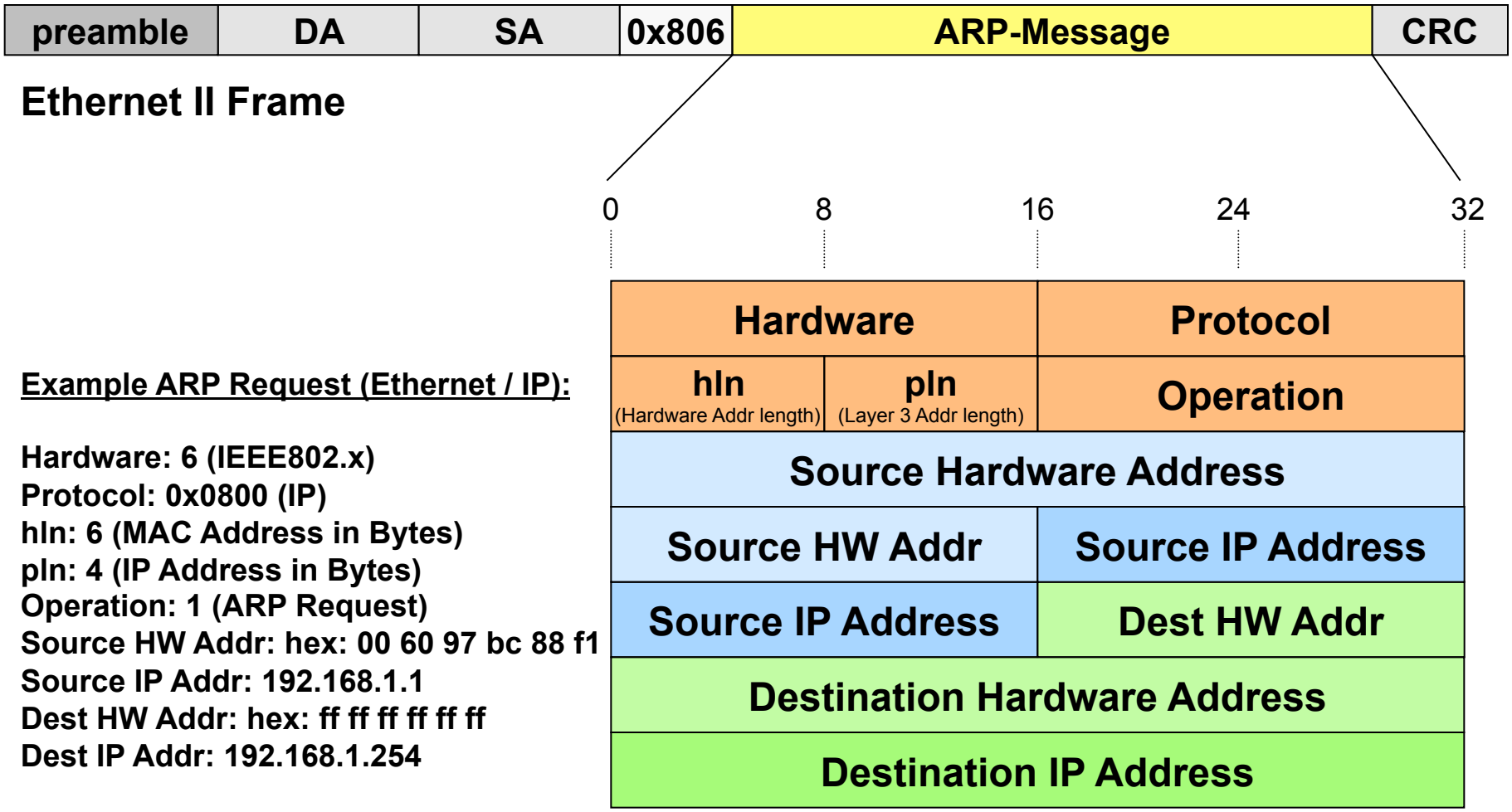
# IP Address versus L2 Address

- **IP address**
  - Identifies the access to a network (interface)
- **If the physical network is of point-to-point link to another IP system**
  - This IP system can be reached without any further addressing on layer 2
- **On a shared media or multipoint-network**
  - Layer 2 addresses are necessary to deliver packets to a specific station using the corresponding L2 technology (LAN, Frame-Relay, ATM ...)
- **Hence a mapping between IP address and L2 address is needed**

# ARP (Address Resolution Protocol)

- **In case of LAN**
  - The mapping is between MAC- and IP-addresses
- **Mapping can be static or dynamic**
- **ARP protocol is used in case of dynamic mapping**
  - RFC 826
  - Defines procedure to request a mapping for a given IP address and stores the result in the so called ARP cache memory
  - ARP cache will be checked first before new requests are sent
  - ARP cache can be refreshed or times out

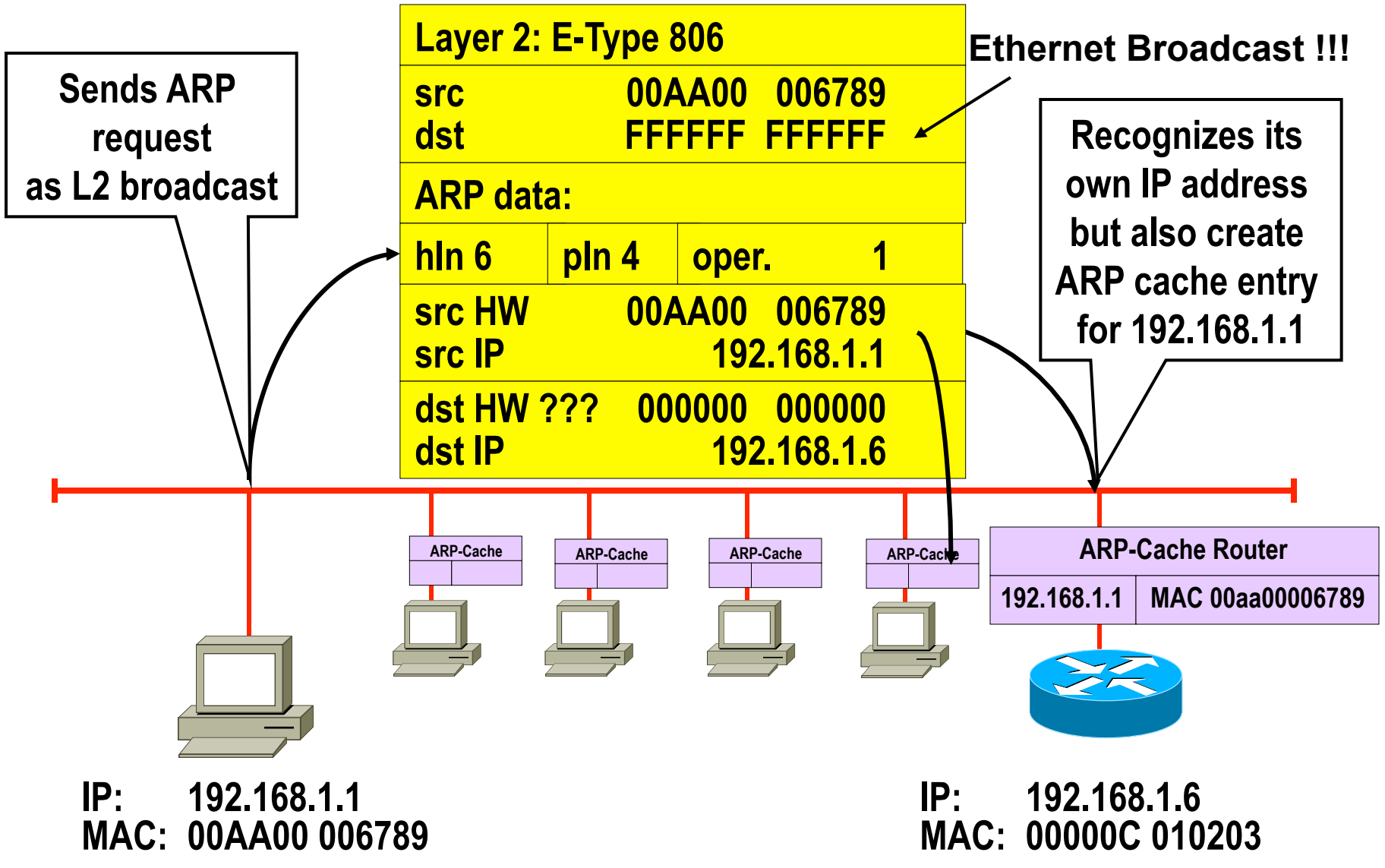
# ARP Format



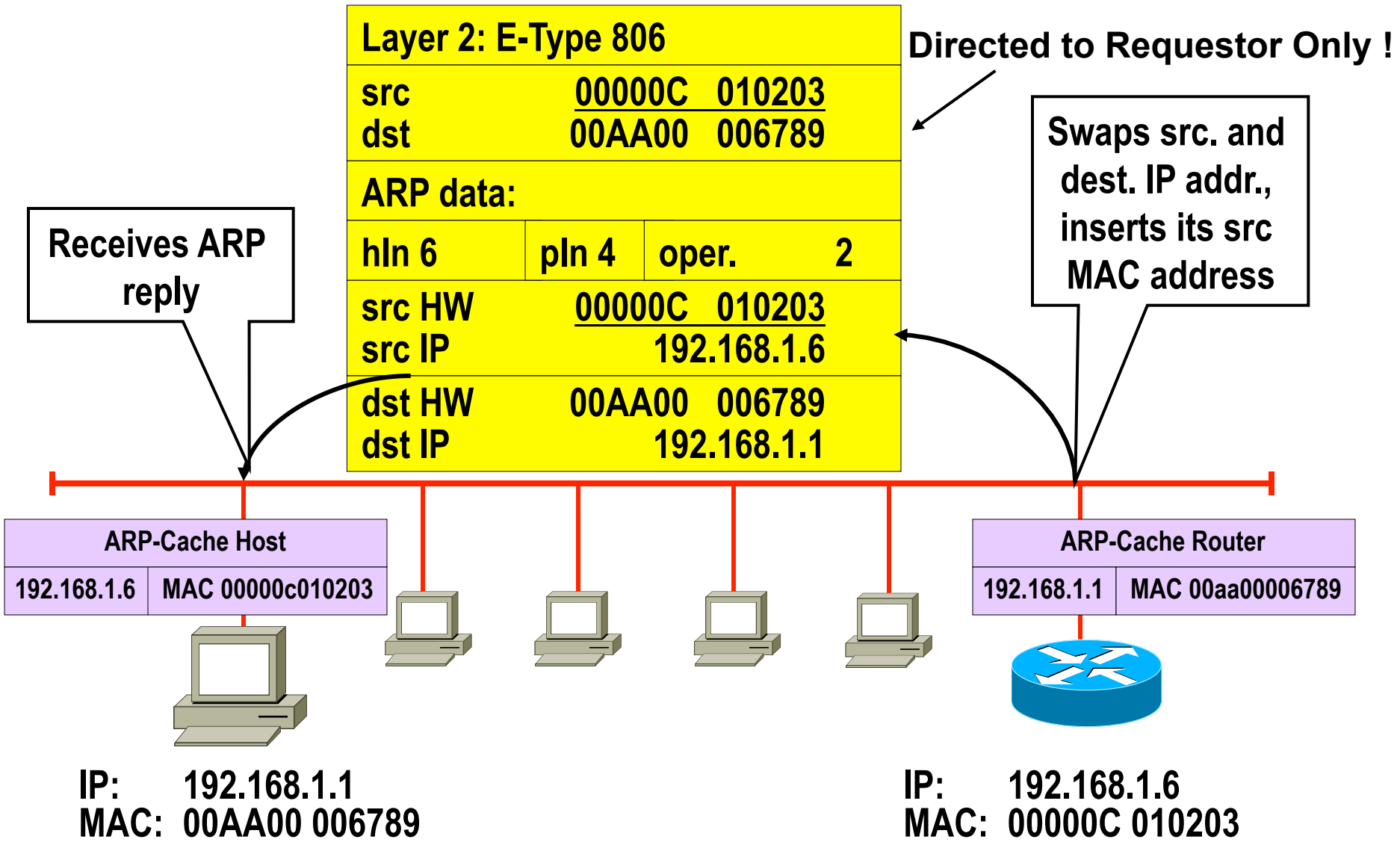

**Example ARP Request (Ethernet / IP):**

**Hardware: 6 (IEEE802.x)**
**Protocol: 0x0800 (IP)**
**hln: 6 (MAC Address in Bytes)**
**pln: 4 (IP Address in Bytes)**
**Operation: 1 (ARP Request)**
**Source HW Addr: hex: 00 60 97 bc 88 f1**
**Source IP Addr: 192.168.1.1**
**Dest HW Addr: hex: ff ff ff ff ff ff**
**Dest IP Addr: 192.168.1.254**

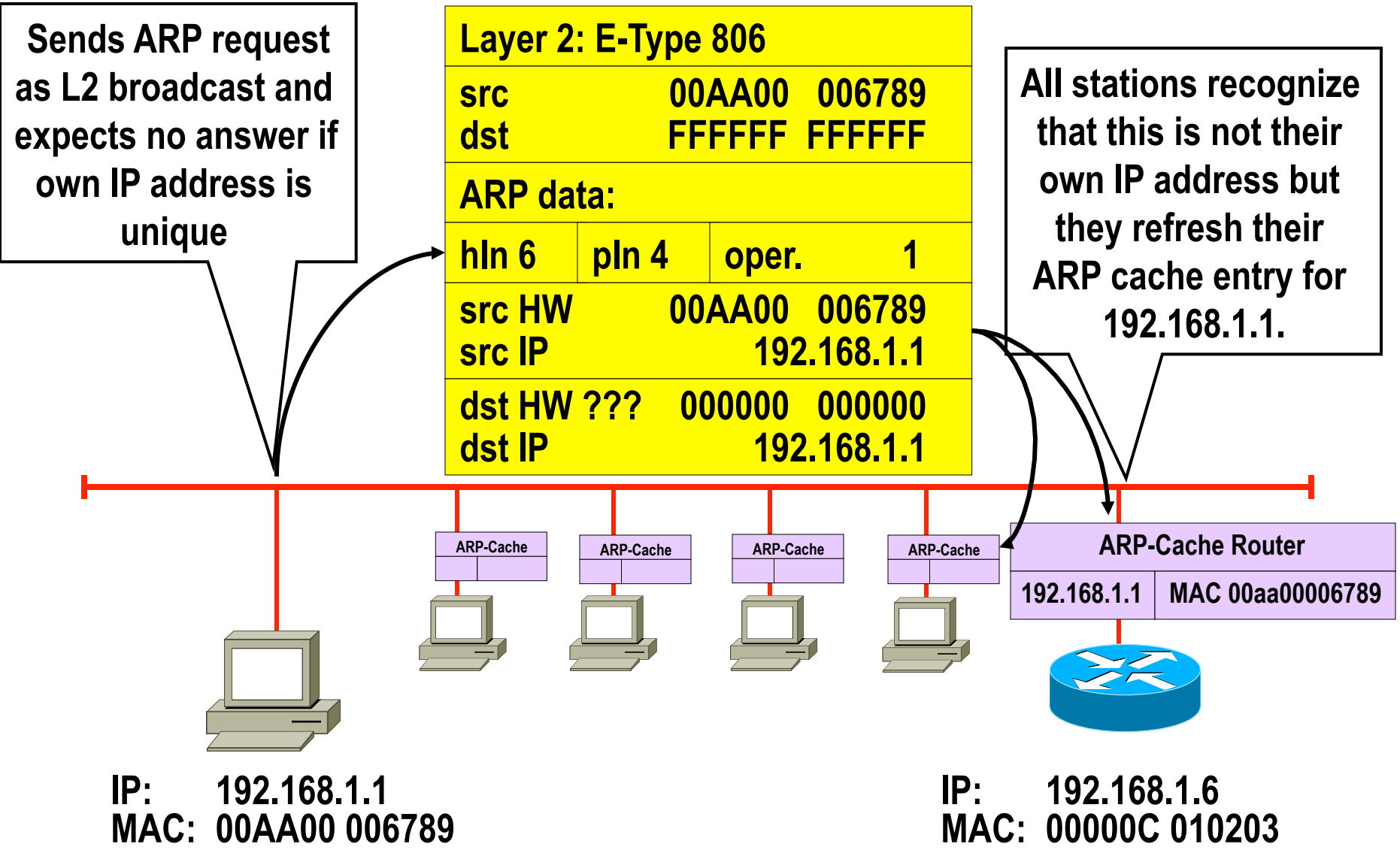
# ARP Request


Layer 2: E-Type 806
src 00AA00 006789
dst FFFFFF FFFFFF
ARP data:
hln 6
pln 4
oper. 1
src HW 00AA00 006789
src IP 192.168.1.1
dst HW ??? 000000 000000
dst IP 192.168.1.6
Ethernet Broadcast !!!
Sends ARP request as L2 broadcast
Recognizes its own IP address but also create ARP cache entry for 192.168.1.1
ARP-Cache
ARP-Cache
ARP-Cache
ARP-Cache
ARP-Cache Router
192.168.1.1
MAC 00aa00006789
IP: 192.168.1.1
MAC: 00AA00 006789
IP: 192.168.1.6
MAC: 00000C 010203

# ARP Reply


Layer 2: E-Type 806
src 00000C 010203
dst 00AA00 006789
ARP data:
hln 6
pln 4
oper. 2
src HW 00000C 010203
src IP 192.168.1.6
dst HW 00AA00 006789
dst IP 192.168.1.1
Directed to Requestor Only !
Swaps src. and dest. IP addr., inserts its src MAC address
Receives ARP reply
ARP-Cache Host
192.168.1.6
MAC 00000c010203
ARP-Cache Router
192.168.1.1
MAC 00aa00006789
IP: 192.168.1.1
MAC: 00AA00 006789
IP: 192.168.1.6
MAC: 00000C 010203

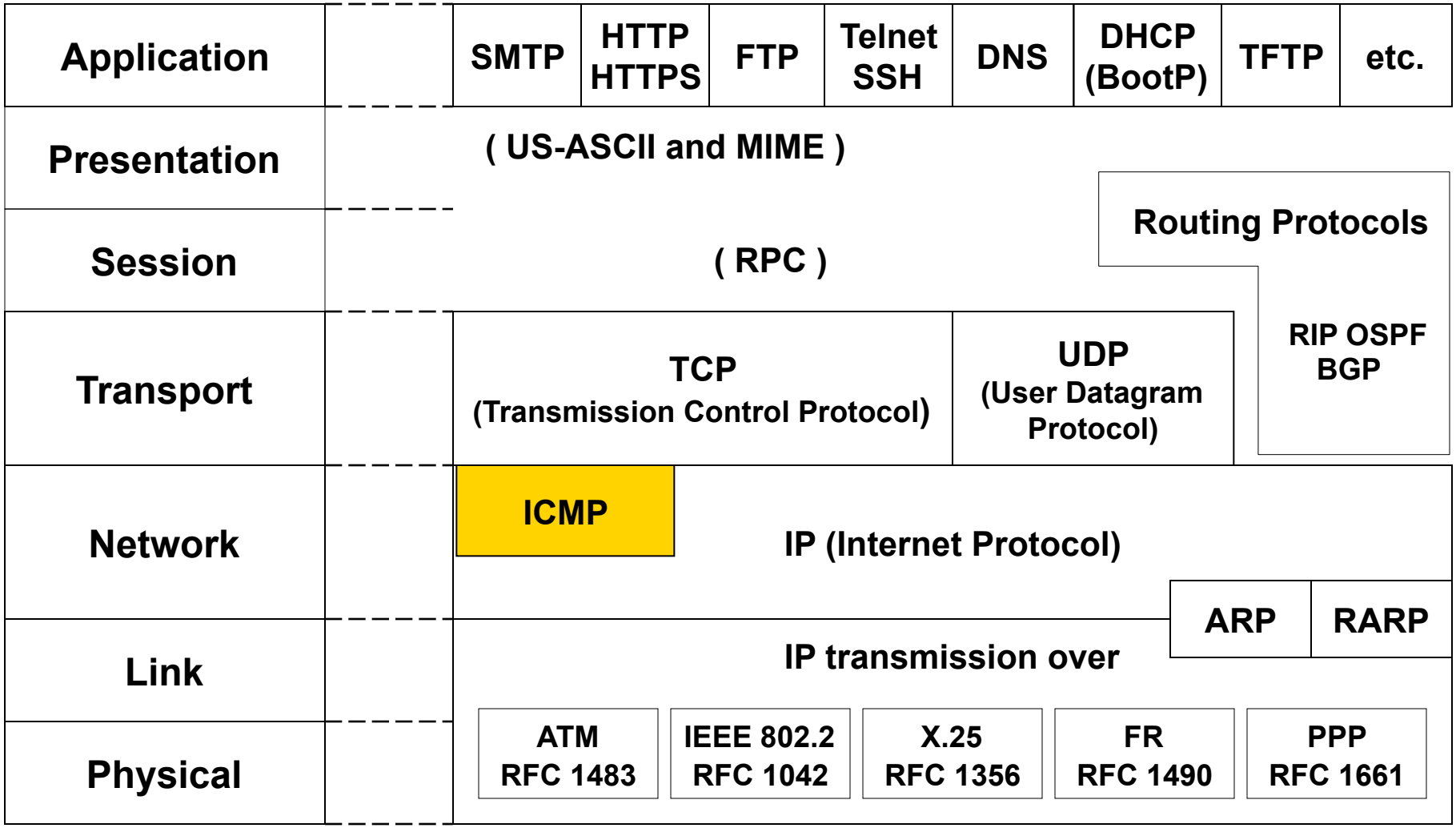
# Gratuitous ARP for Duplicate Address Check and ARP Cache Refresh



# Agenda

- **Introduction**
  - Short History of the Internet (not part of the exam!)
  - Basic Principles
- **IP**
  - IP Protocol
  - IP QoS
  - Addressing
  - Classful versus Classless (not part of the exam!)
- **IP Forwarding**
  - Principles
  - ARP
  - ICMP
  - PPP
- **First Hop Redundancy**
  - Proxy ARP, IDRP
  - HSRP
  - VRRP (not part of the exam!)

# TCP/IP Protocol Suite



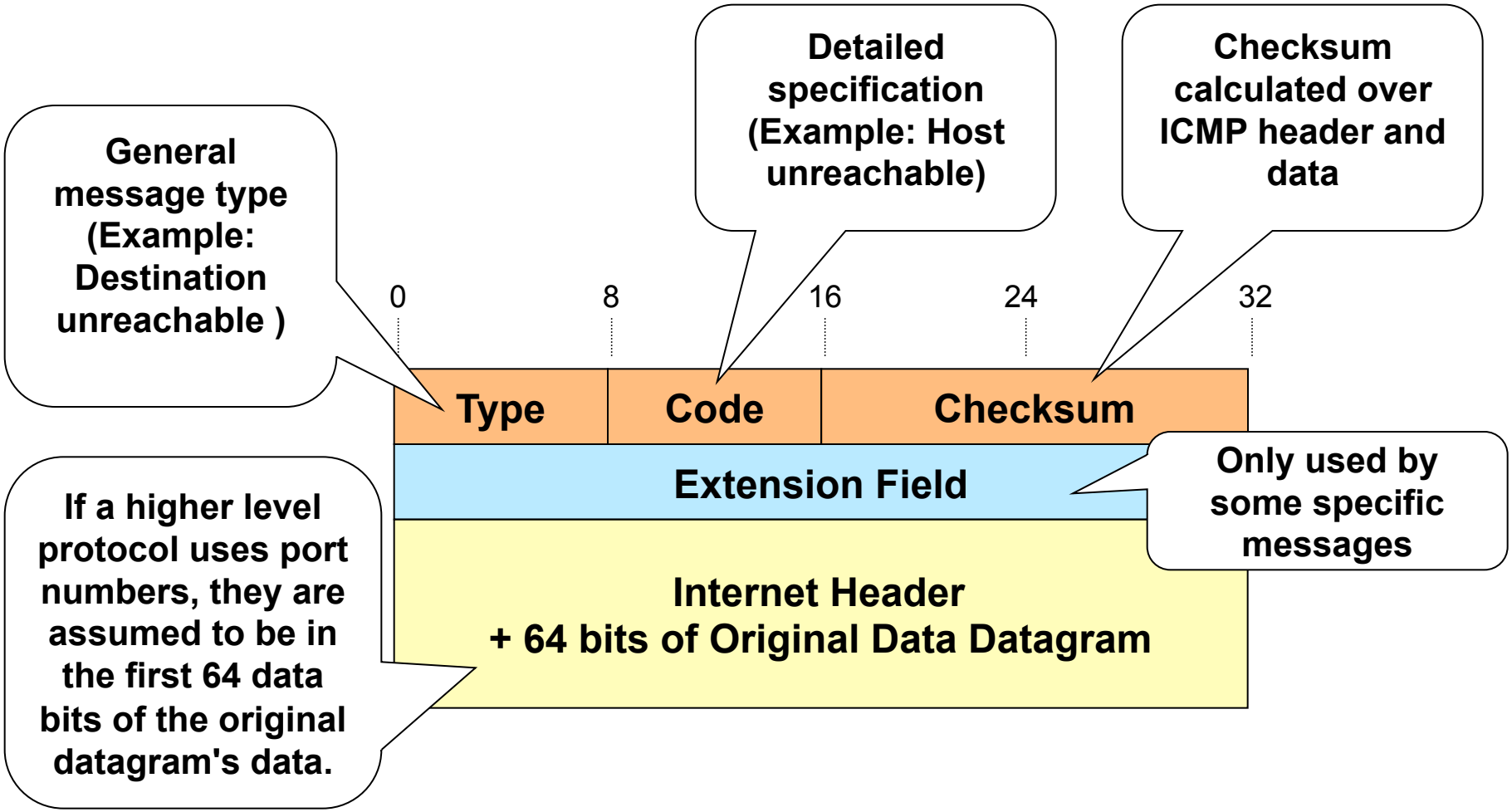
# ICMP (RFC 792)

- **Datagram service of IP**
  - Best effort -> IP datagrams can be lost
  - If network cannot deliver packets the sender must be informed somehow !
    - Reasons: no route, TTL expired, ...
- **ICMP (Internet Control Message Protocol)**
  - Enhances network reliability and performance by carrying error and diagnostic messages
- **ICMP must be supported by every IP station**
  - Implementation differences!
- **Analysis of ICMP messages**
  - Network management systems or can give valuable hints for the network administrator

# ICMP

- **Principle of ICMP operation**
  - IP station (router or destination), which detects any transmission problems, generates an ICMP message
  - ICMP message is addressed to the originating station (sender of the original IP packet)
- **ICMP messages are sent as IP packets**
  - Protocol field = 1, ICMP header and code in the IP data area
- **If an IP datagram 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)

# ICMP Message Format



# ICMP Message Types

| | |
|---|---|
| 0 | Echo Reply ("Ping Response") |
| 3 | Destination Unreachable |
| | Reason specified in Code field of ICMP message |
| 4 | Source Quench (decrease data rate of sender) |
| | Theoretical Flow Control Possibility of IP |
| 5 | Redirect (use different router) |
| | More information in Code field of ICMP message |
| 8 | Echo Request ("Ping Request") |
| 11 | Time Exceeded |
| | code = 0 time to live exceeded in transit |
| | code = 1 reassembly timer expired |
| 12 | Parameter Problem (IP header) |
| 13/14 | Time Stamp Request / Time Stamp Reply |
| 15/16 | Information Request / Reply |
| | e.g. finding the Net-ID of the network |
| 17/18 | Address Mask Request / Reply |

# Code Field for Type 3 (Destination Unreachable)

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

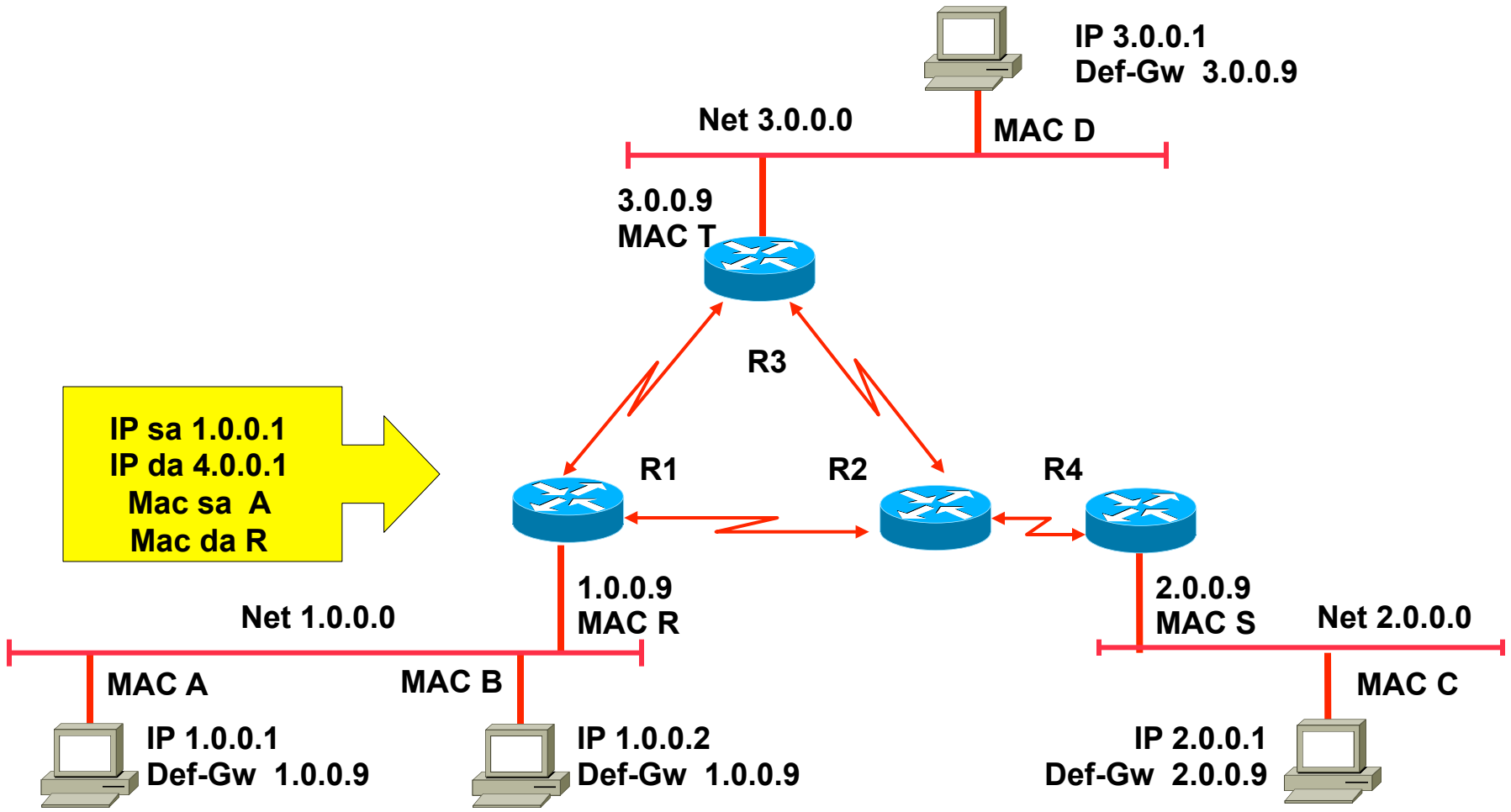
5 ... **Source route failed**: Path in IP Options couldn't be followed; generated by intermediate or far-end router

# Code Field for Type 3 (Destination Unreachable)

The following additional codes are defined in RFC1122 (Host Requirements) page 38:

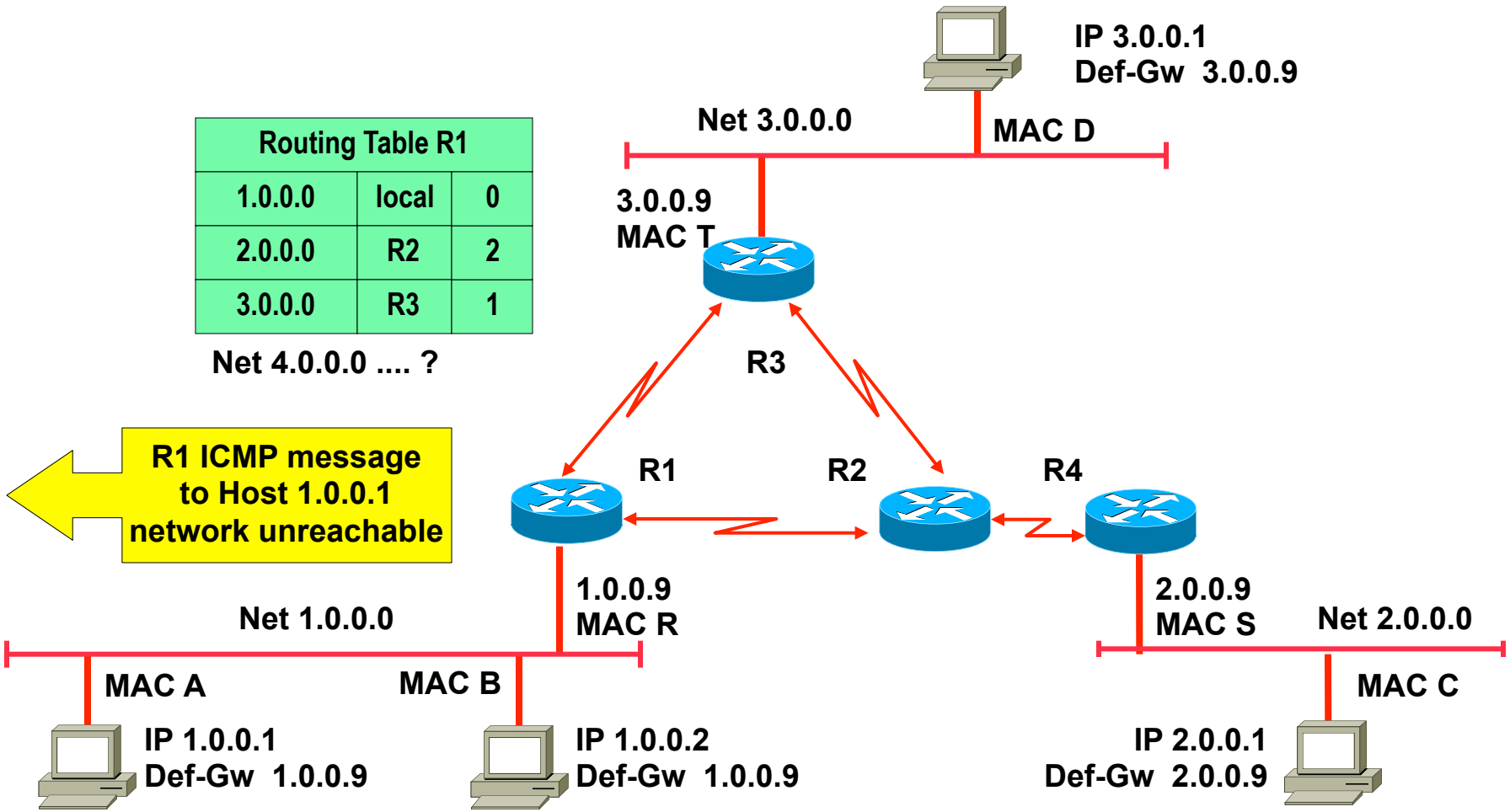
6 … Destination network unknown
7 … Destination host unknown
8 … Source host isolated
9 … Communication with destination network administratively prohibited
10 … Communication with destination host administratively prohibited
11 … Network unreachable for type of service
12 … Host unreachable for type of service

# Delivery 1.0.0.1 - > 4.0.0.1

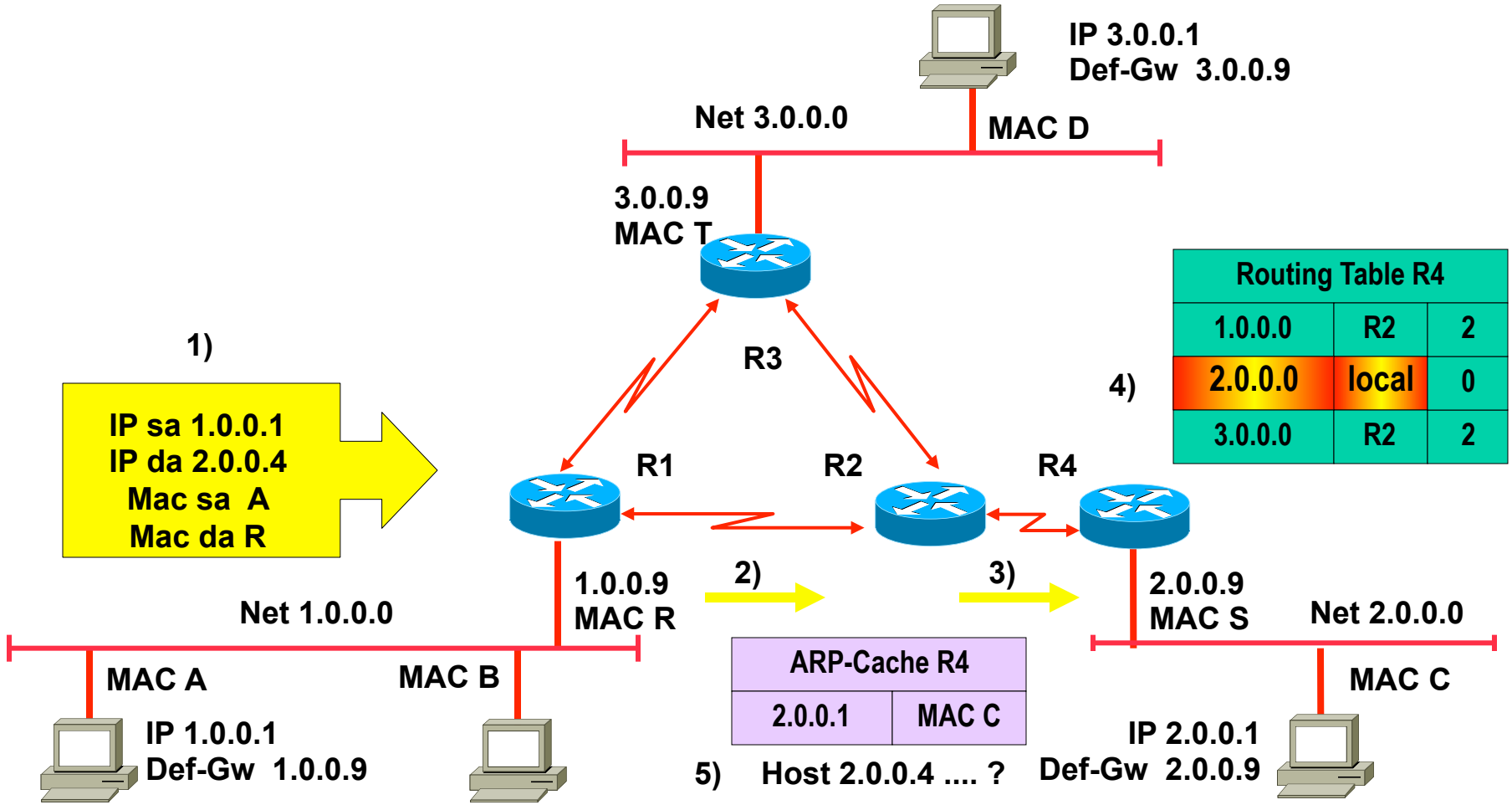



| ARP-Cache Host A | |
|---|---|
| 1.0.0.2 | MAC B |
| 1.0.0.9 | MAC R |

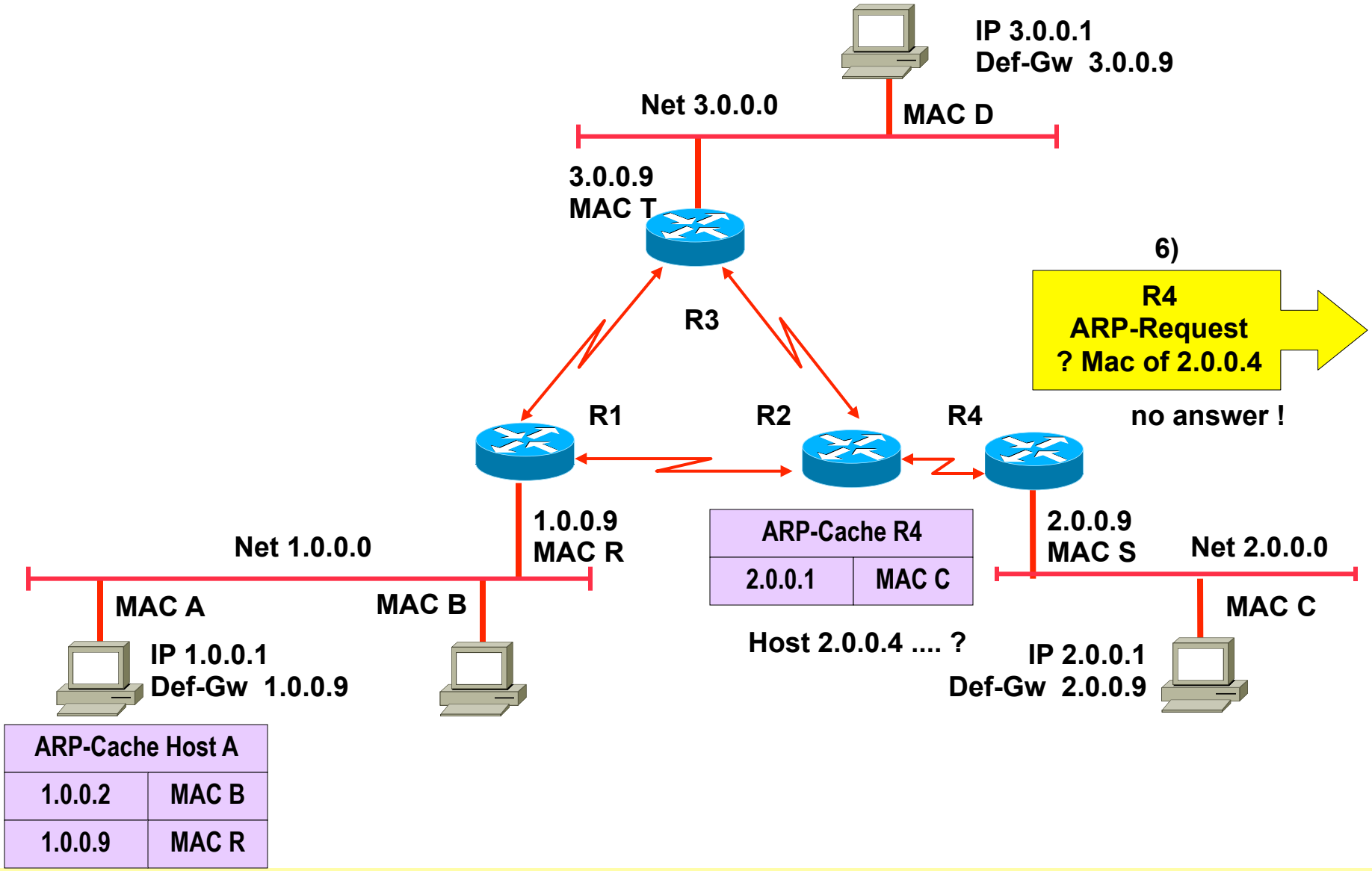
# ICMP Destination Unreachable (code: network unreachable)



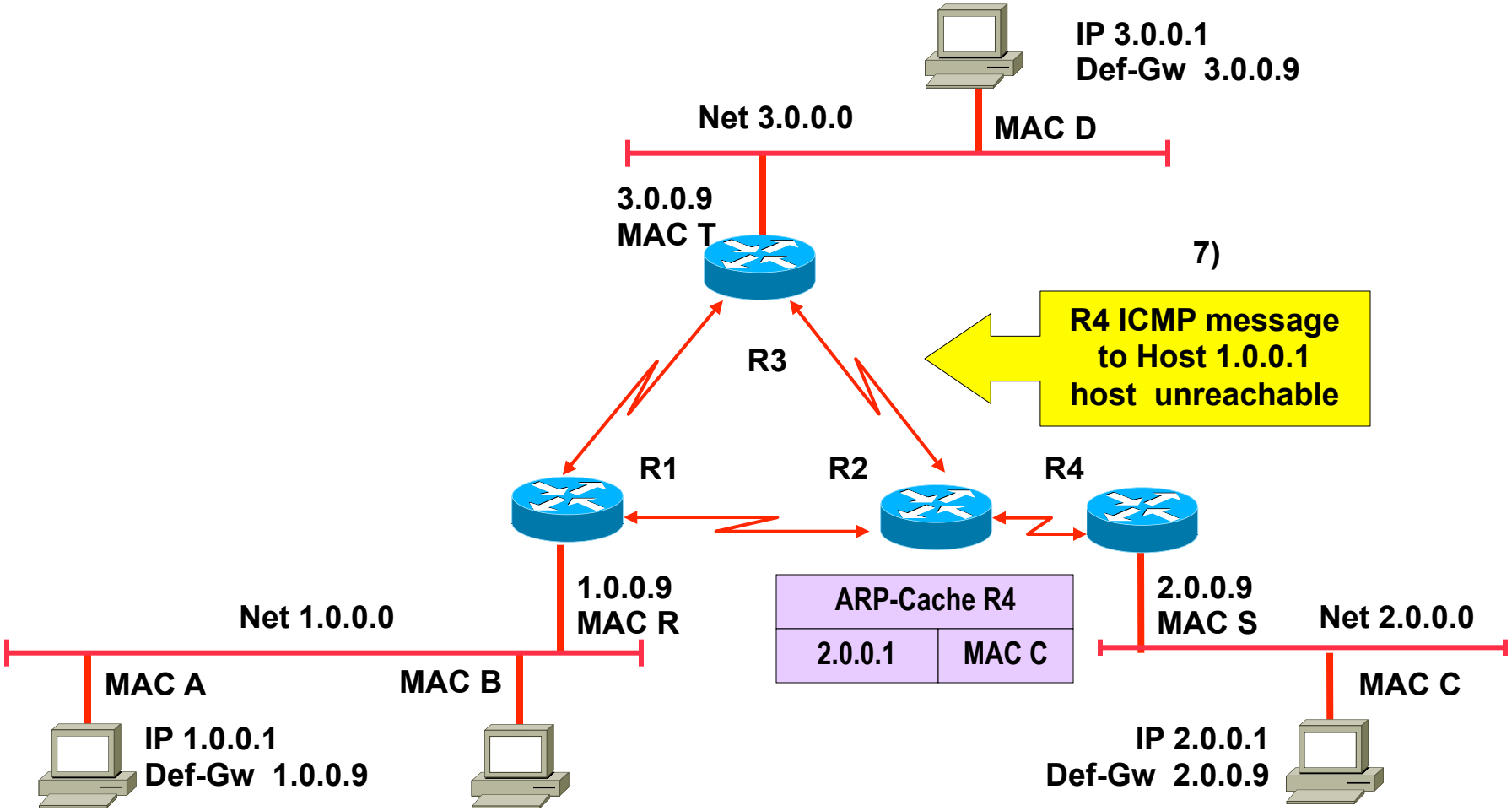
# Delivery 1.0.0.1 - > 2.0.0.4



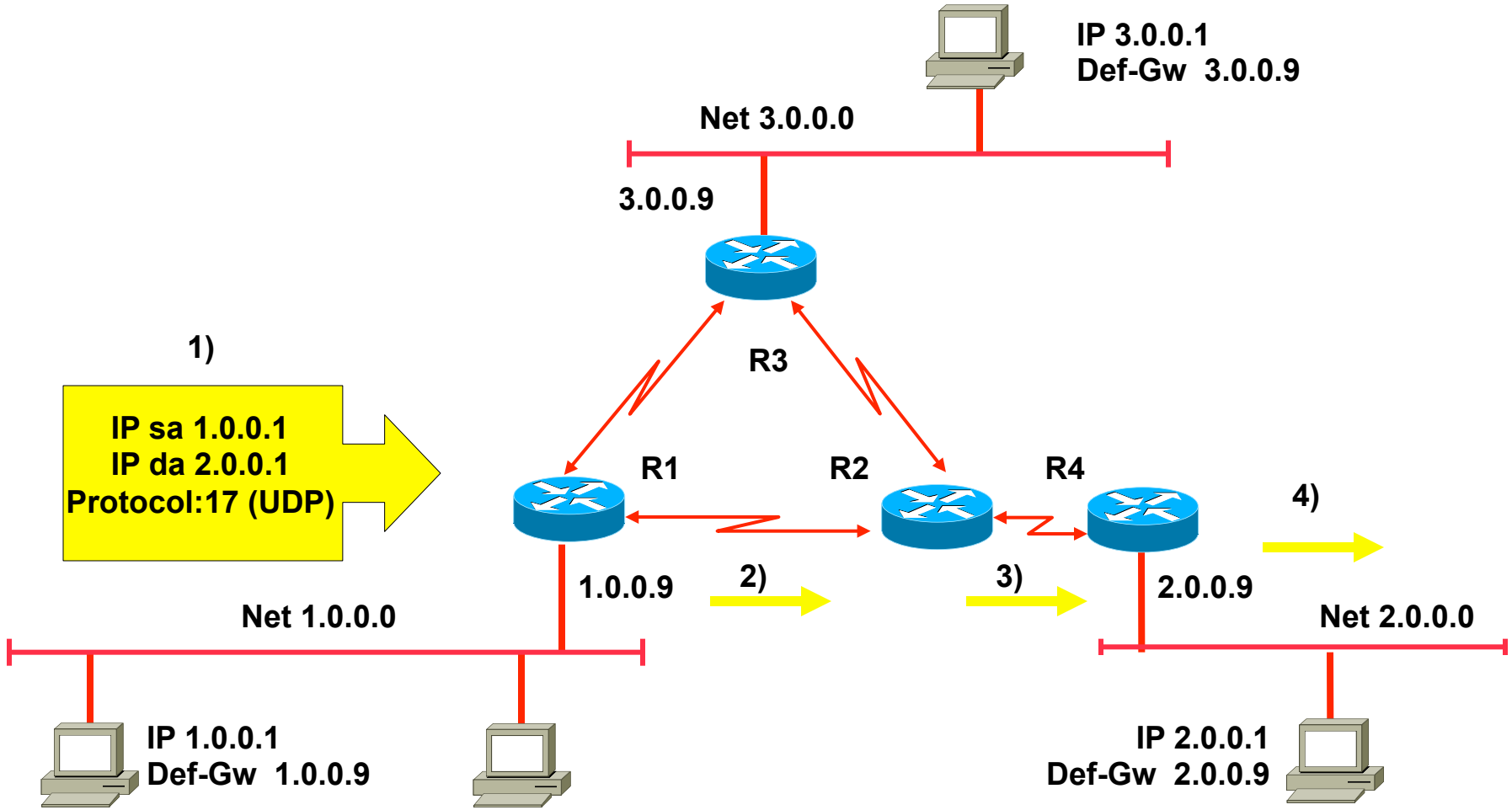
# Delivery 1.0.0.1 - > 2.0.0.4



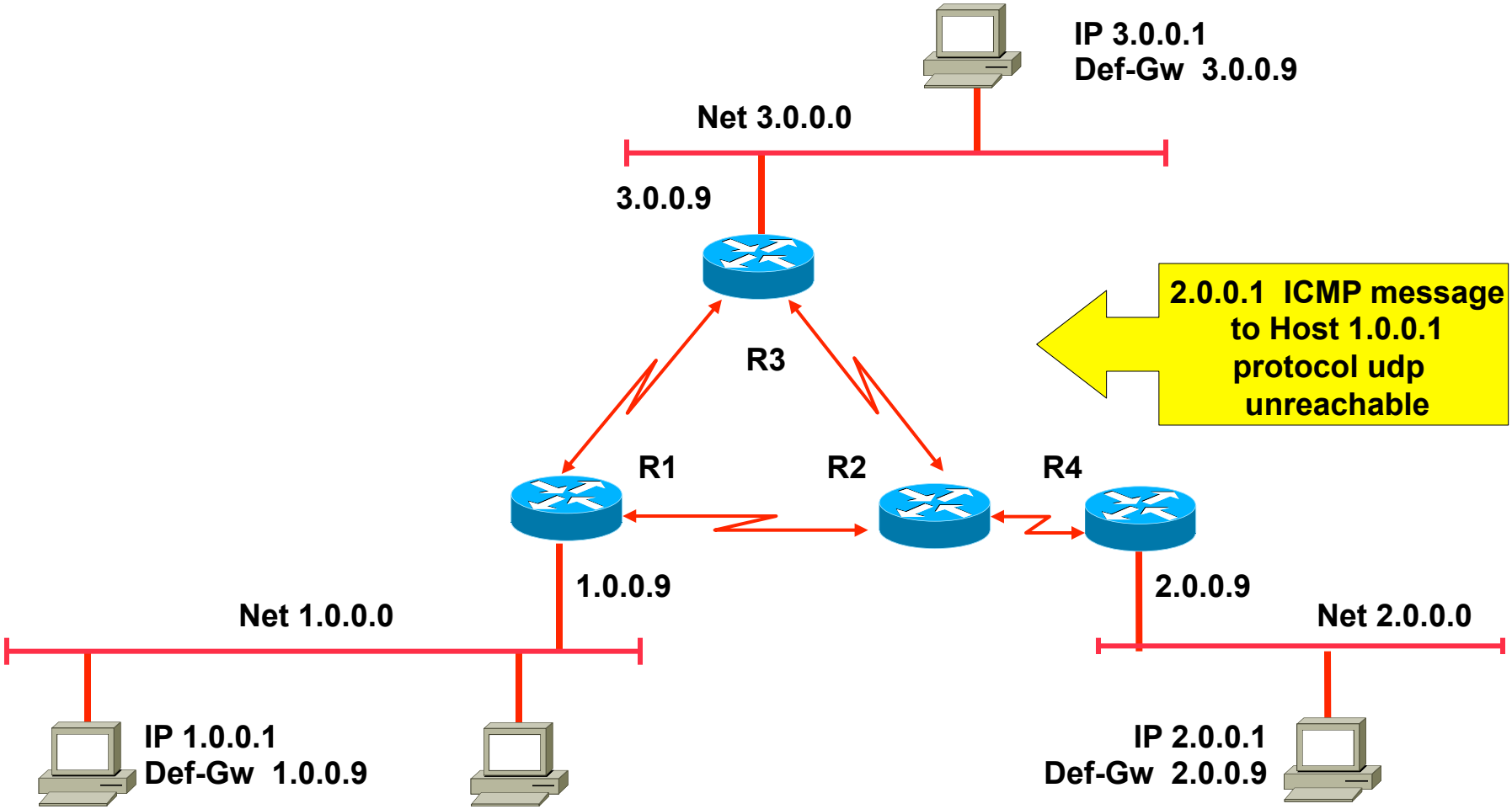
# ICMP Destination Unreachable (code: host unreachable)



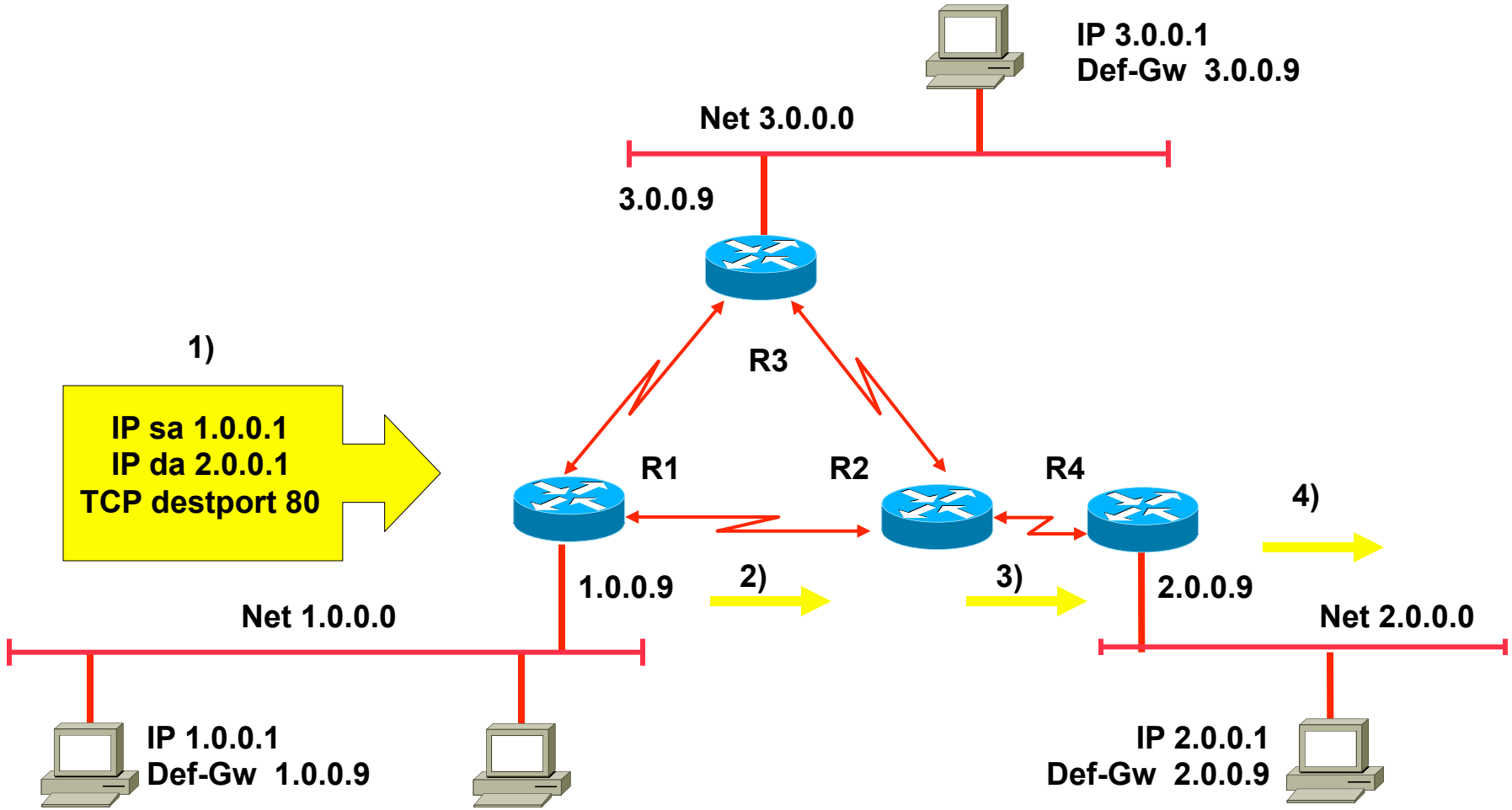
# Delivery 1.0.0.1 - > 2.0.0.1 (protocol udp)



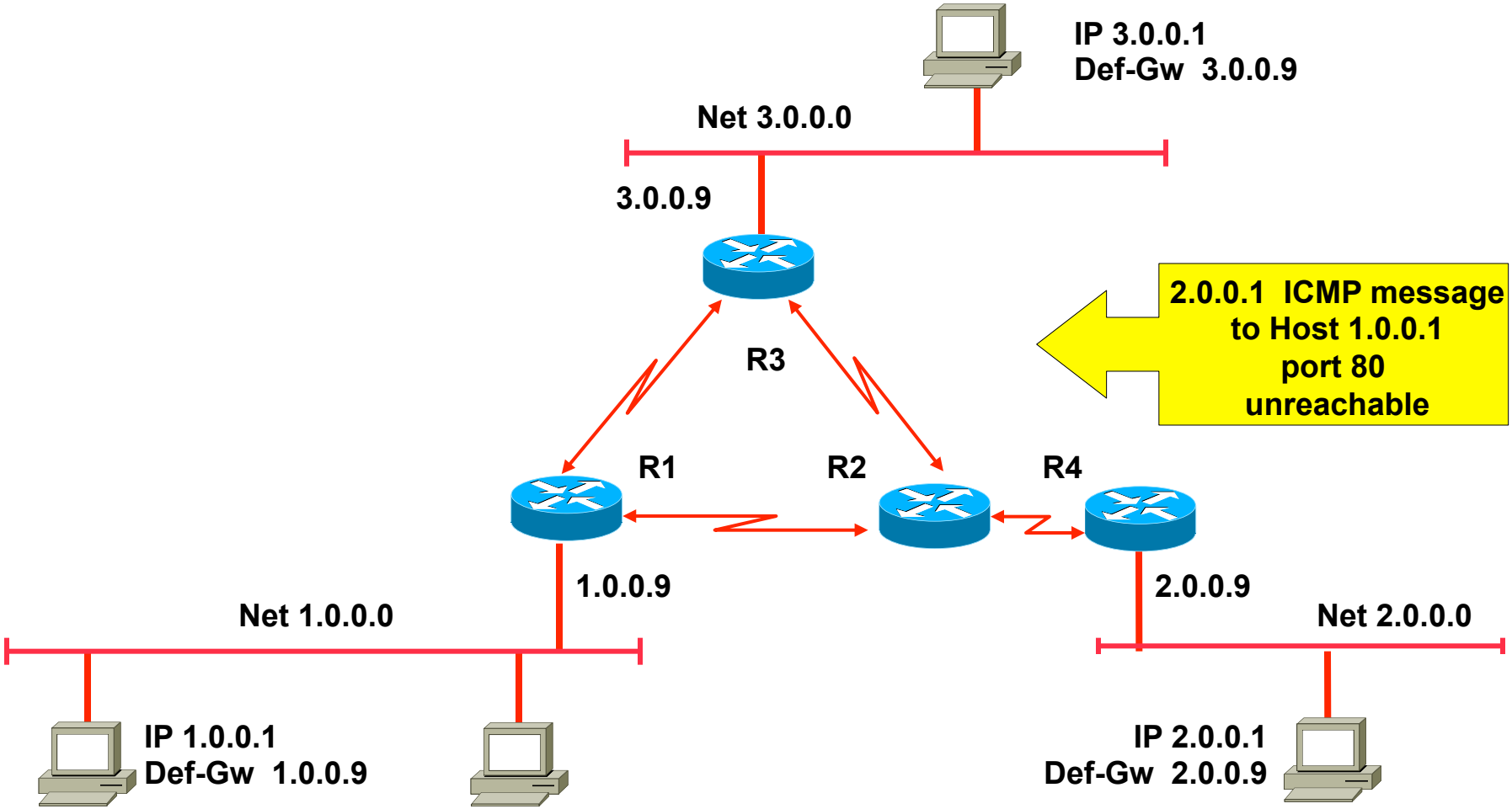
# ICMP protocol unreachable



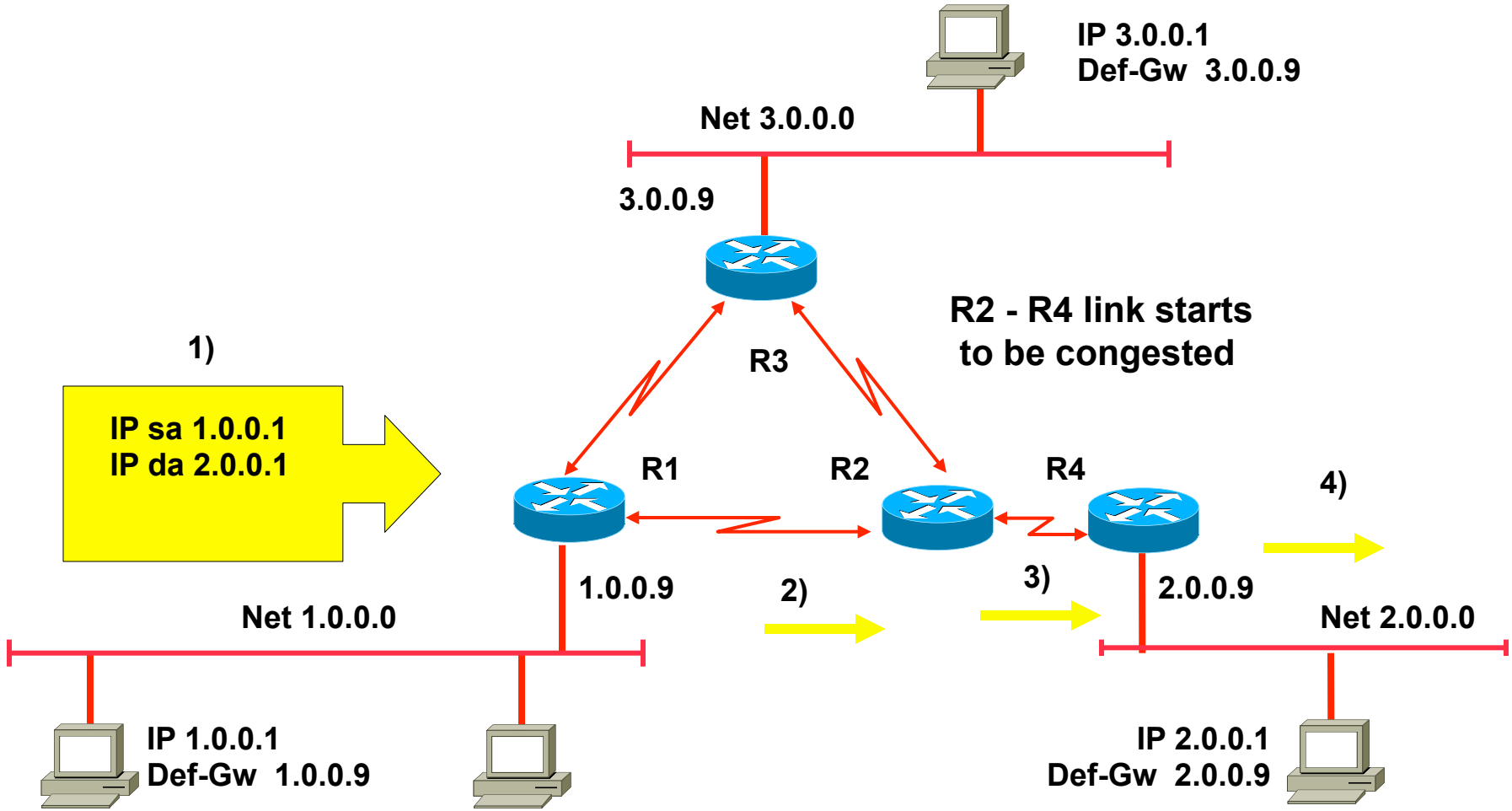
# Delivery 1.0.0.1 - > 2.0.0.1 (http_server_proc)



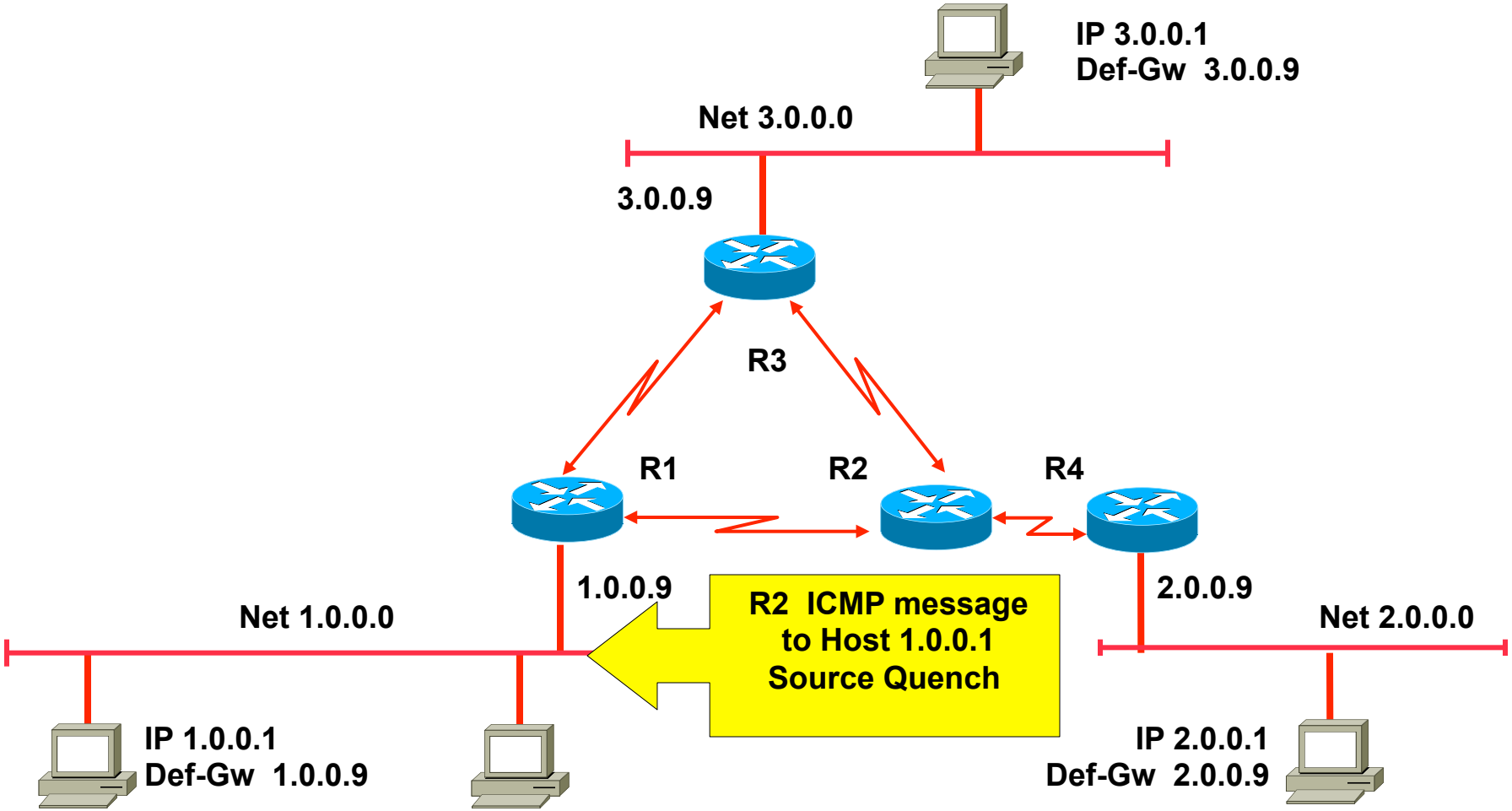
# ICMP port unreachable (no http_server_proc)



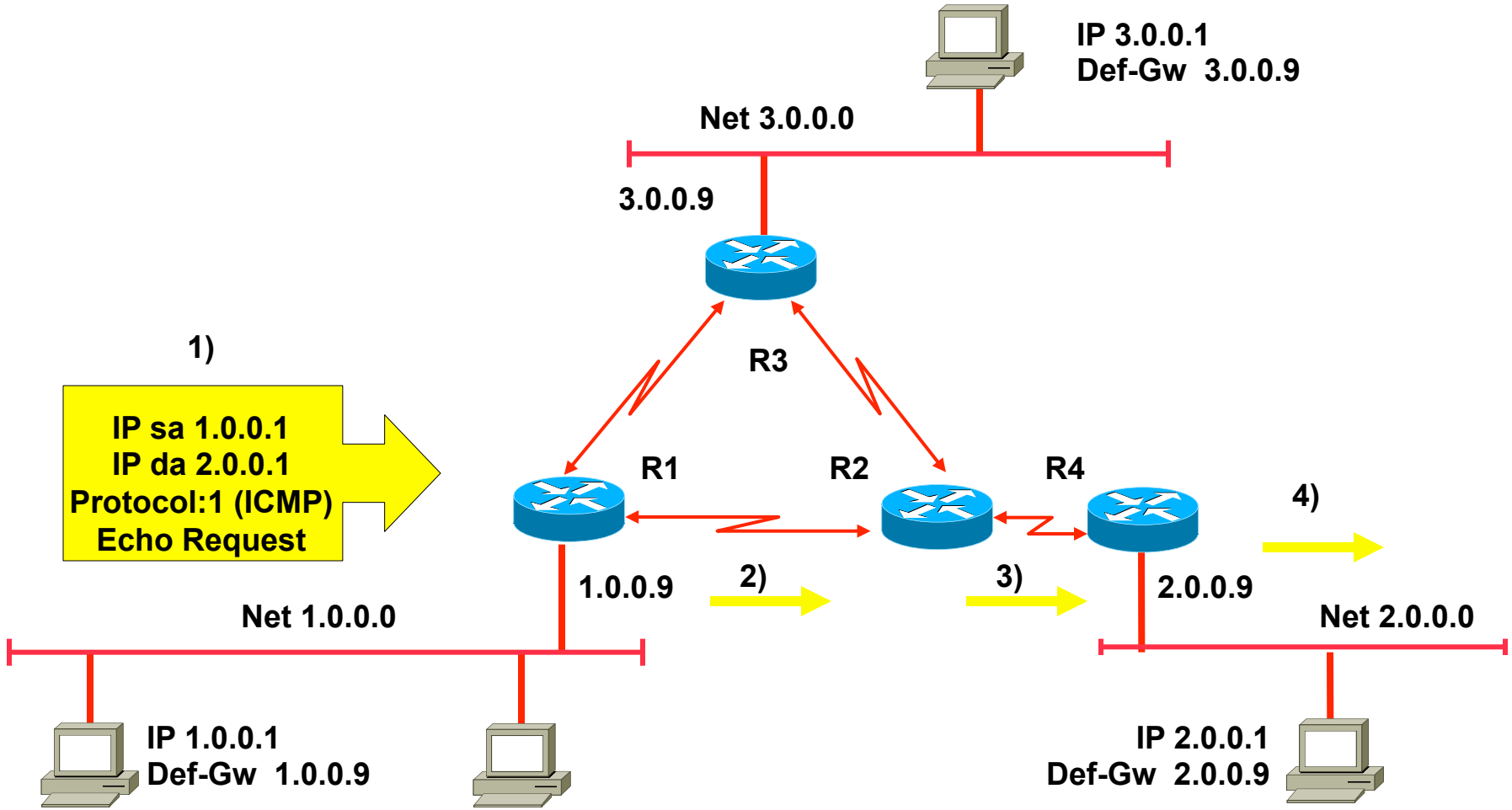
# R2 -> R4 Link Congested



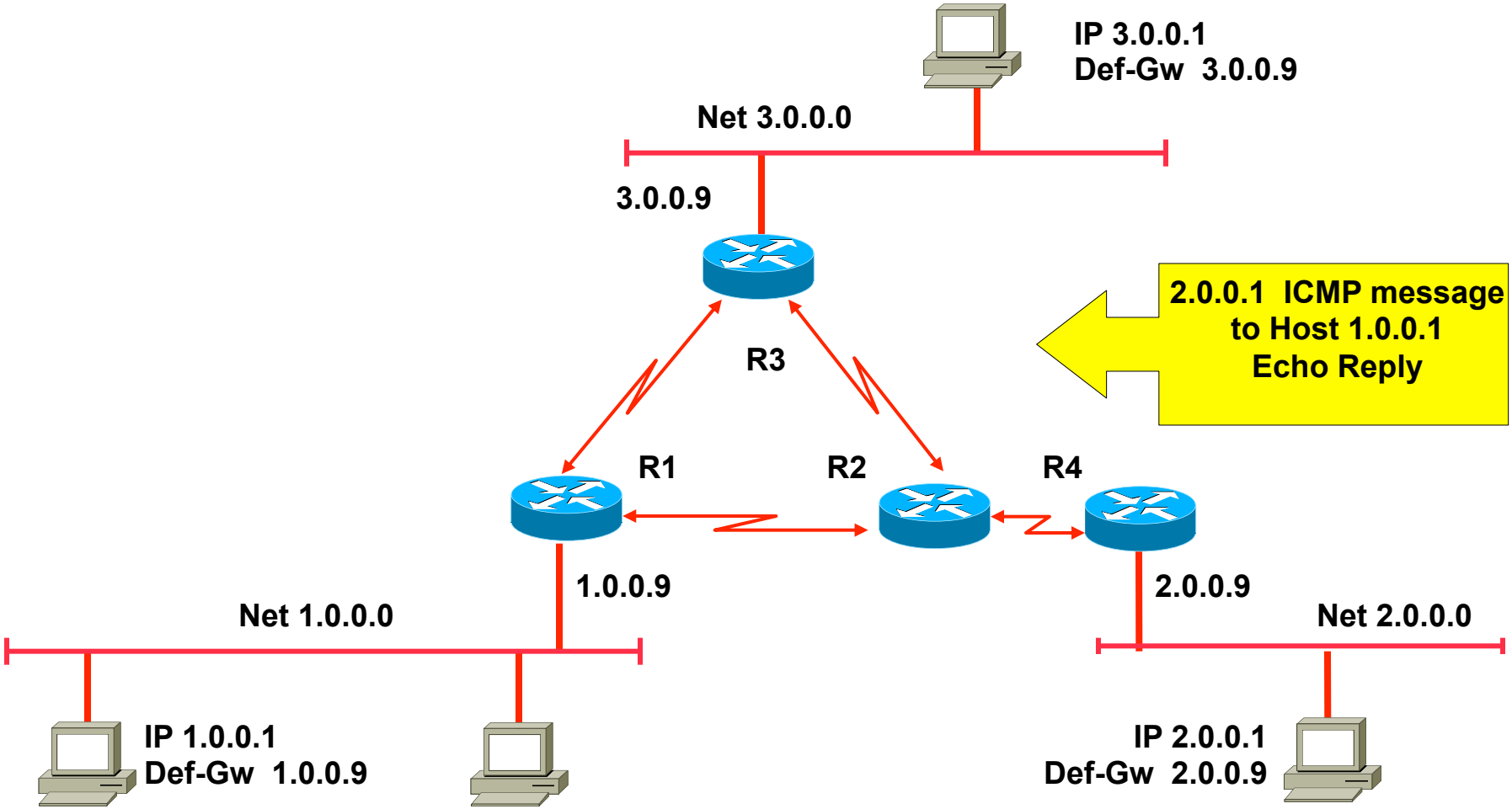
# ICMP Source Quench (Flow Control STOP?)



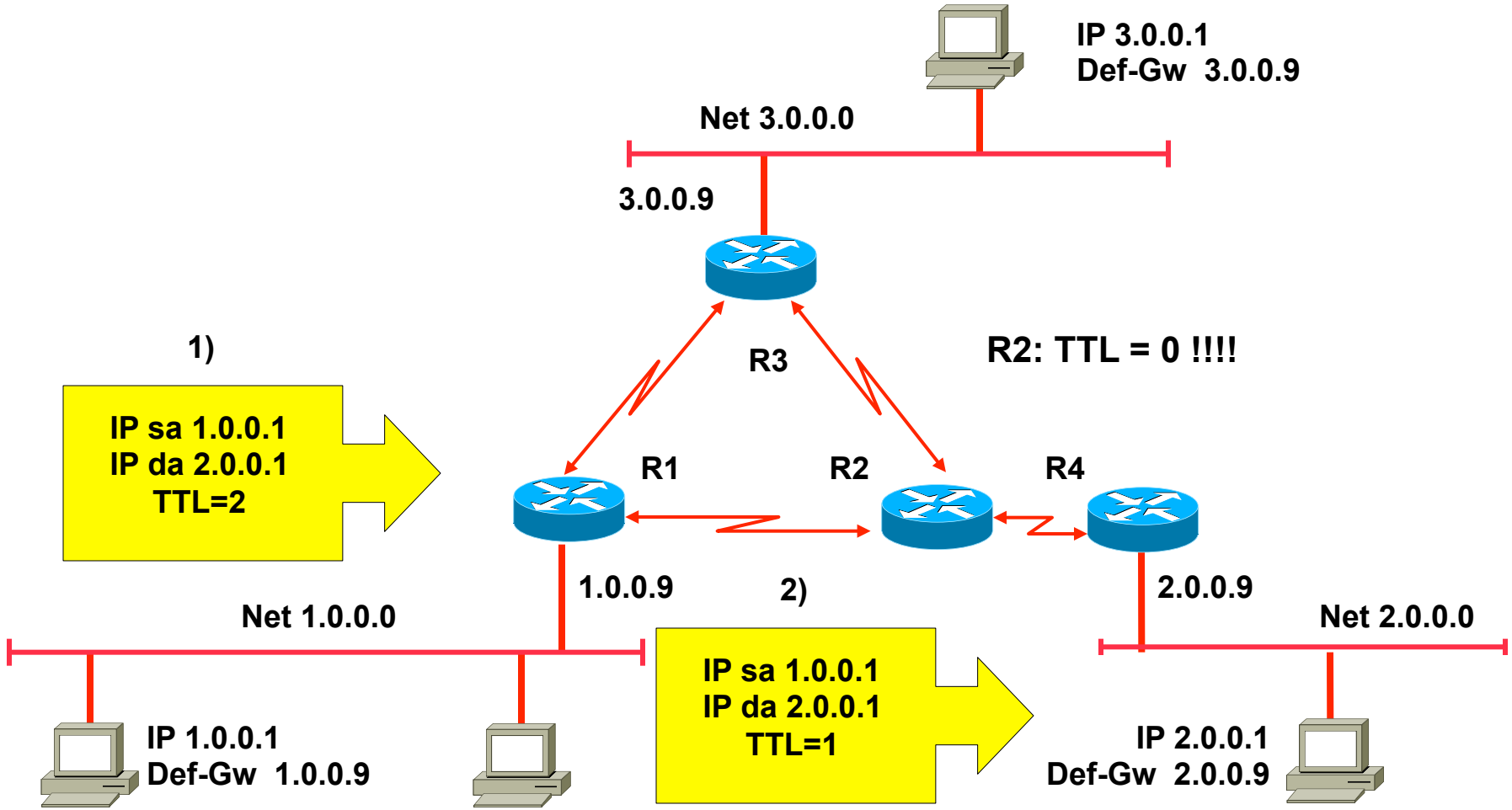
# Ping 1.0.0.1 - > 2.0.0.1



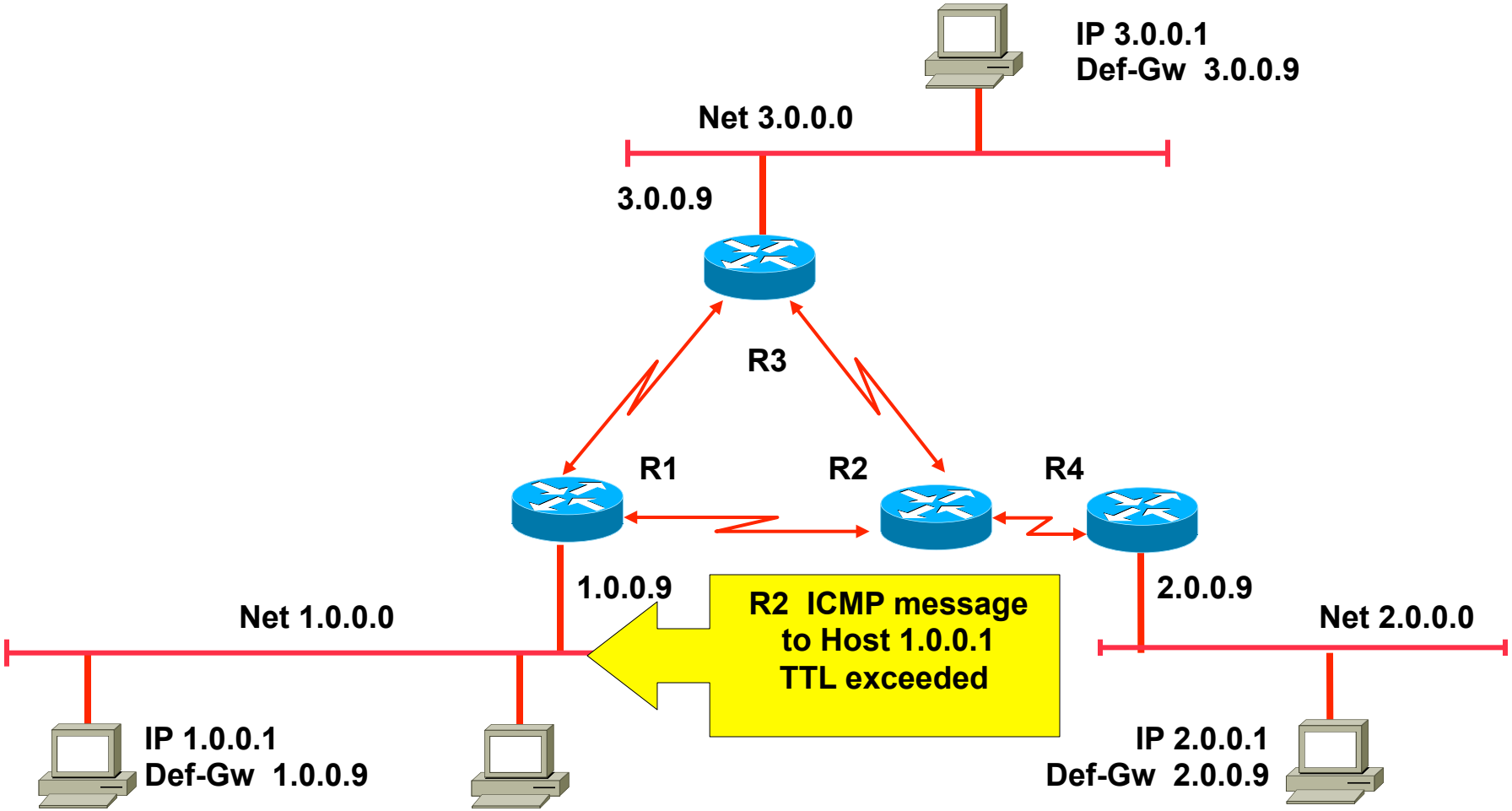
# Ping Echo 2.0.0.1 - > 1.0.0.1



# Delivery 1.0.0.1 - > 2.0.0.1 (TTL=2)



# ICMP TTL exceeded

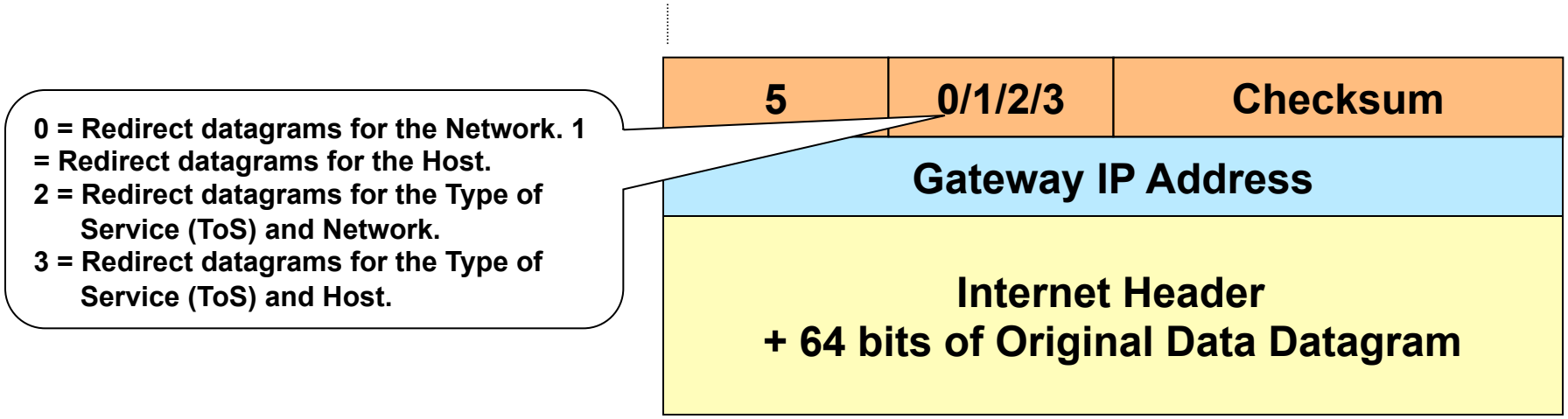


# Traceroute

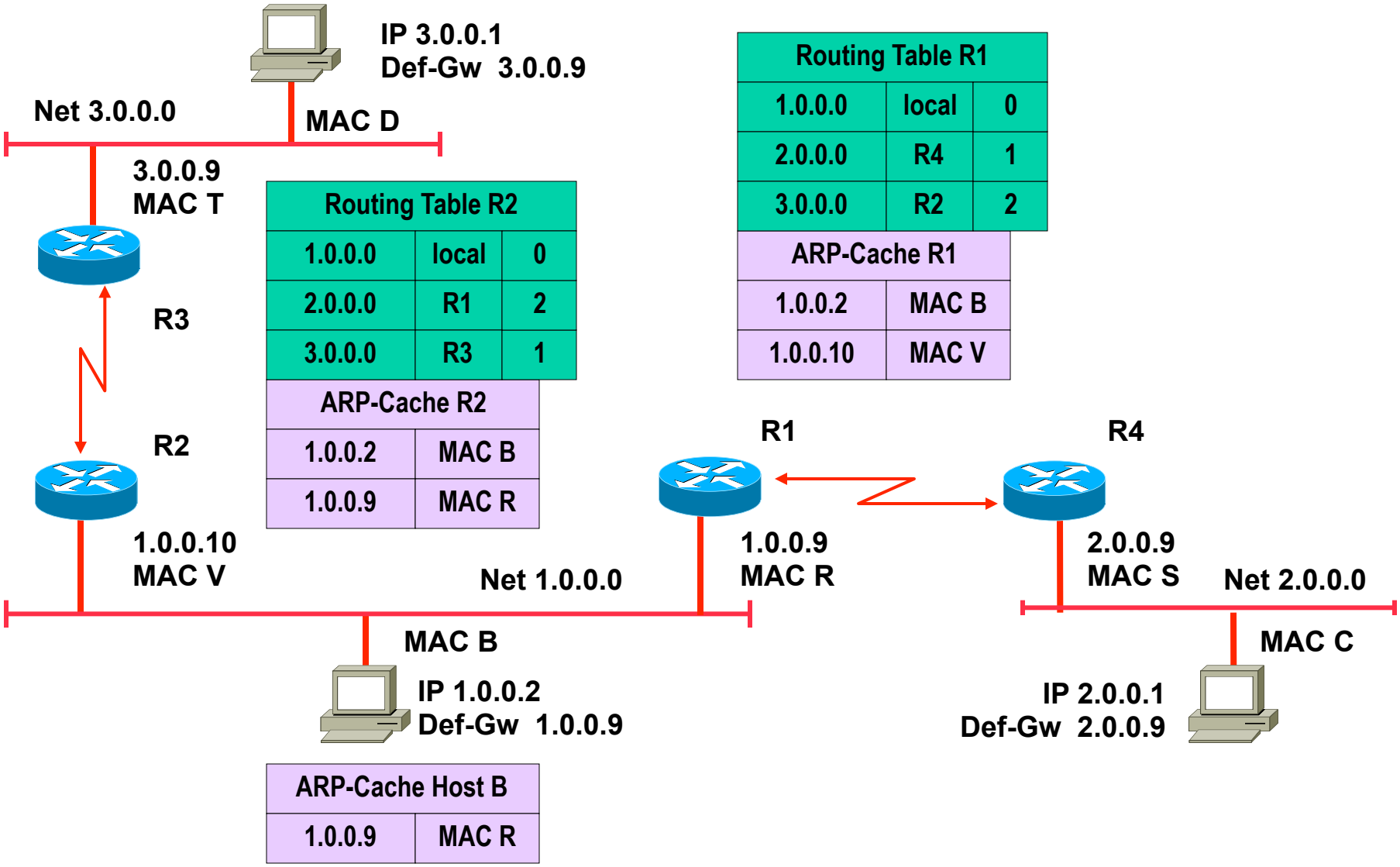
- **Using ICMP TTL exceed messages**
  - The current route, a datagram will take through the network, can be find
- **Just generate IP messages**
  - With increasing values for TTL
- **You will find the route**
  - Hop by hop
- **Two types of messages generated by of trace route CLI commands:**
  - ICMP-Echo
  - UDP

# Code Field for Type 5 (Redirect)

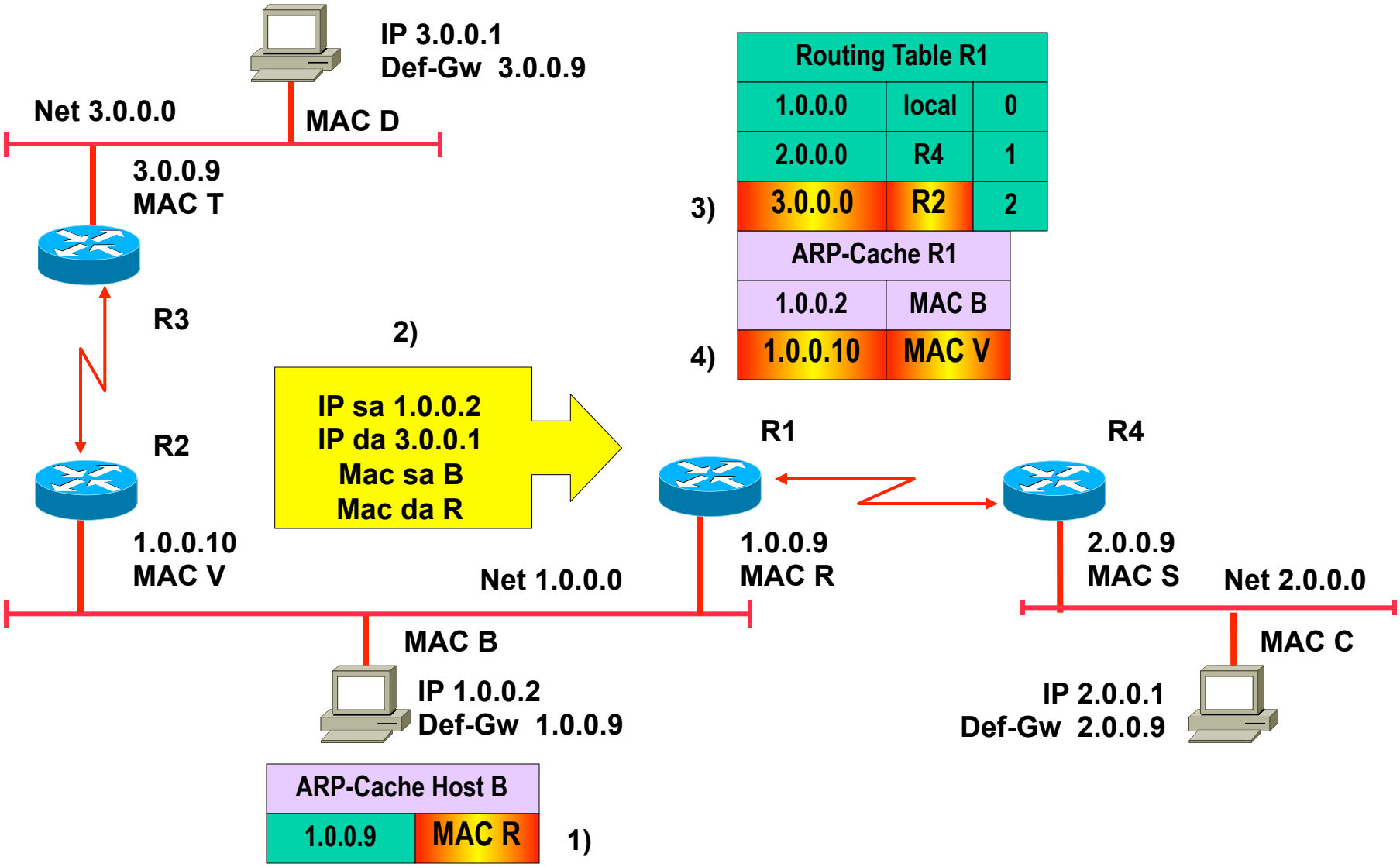
- **If a router knows of a better (faster, shorter) path to a target then it will notify the sender through ICMP redirect**
  - In any case the router will still forward the packets on the inefficient path
  - Datagrams will be sent twice through a LAN, if the sender ignores the redirect message



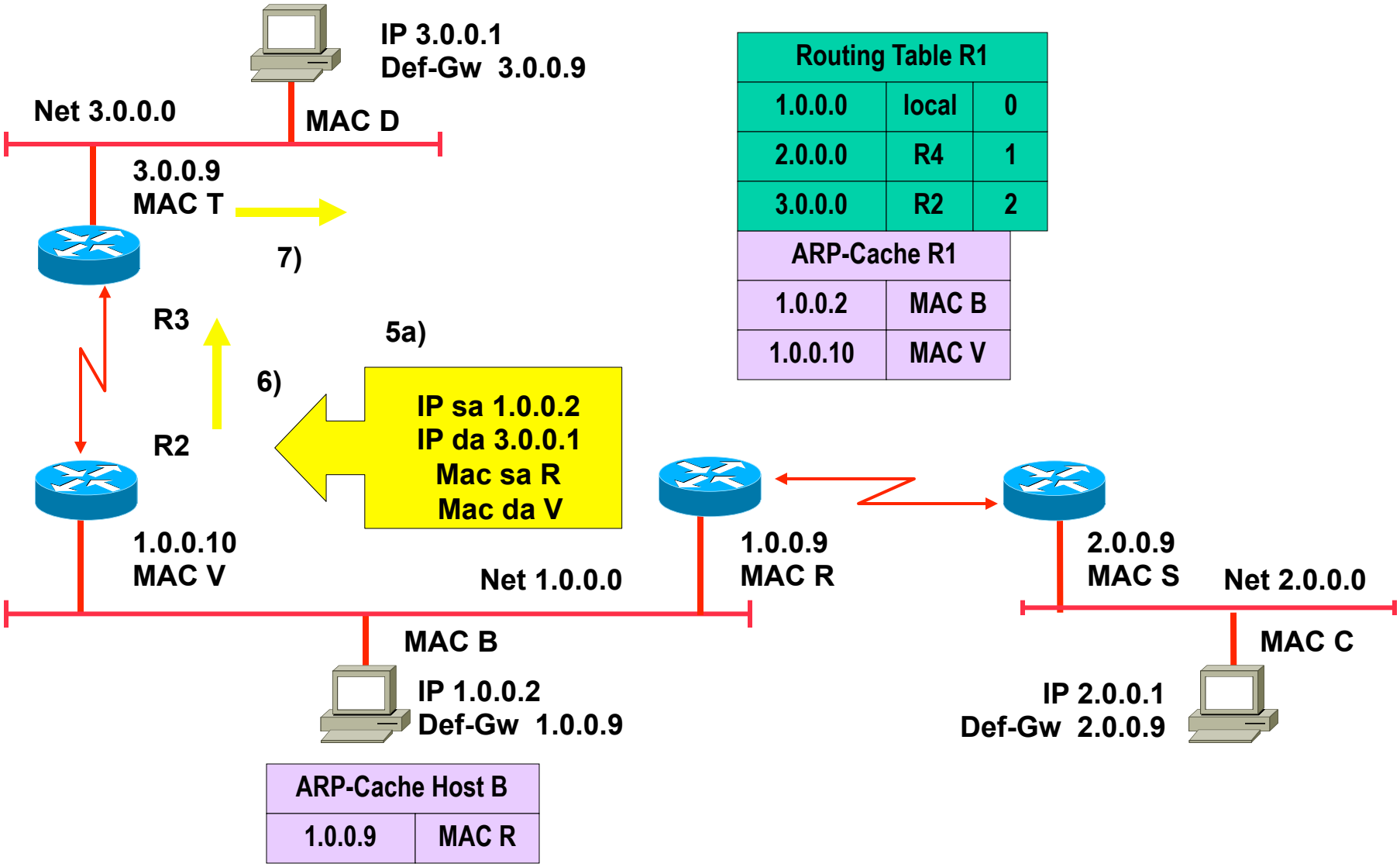
# Delivery 1.0.0.2 -> 3.0.0.1



# Delivery 1.0.0.2 -> 3.0.0.1



# Delivery 1.0.0.2 -> 3.0.0.1

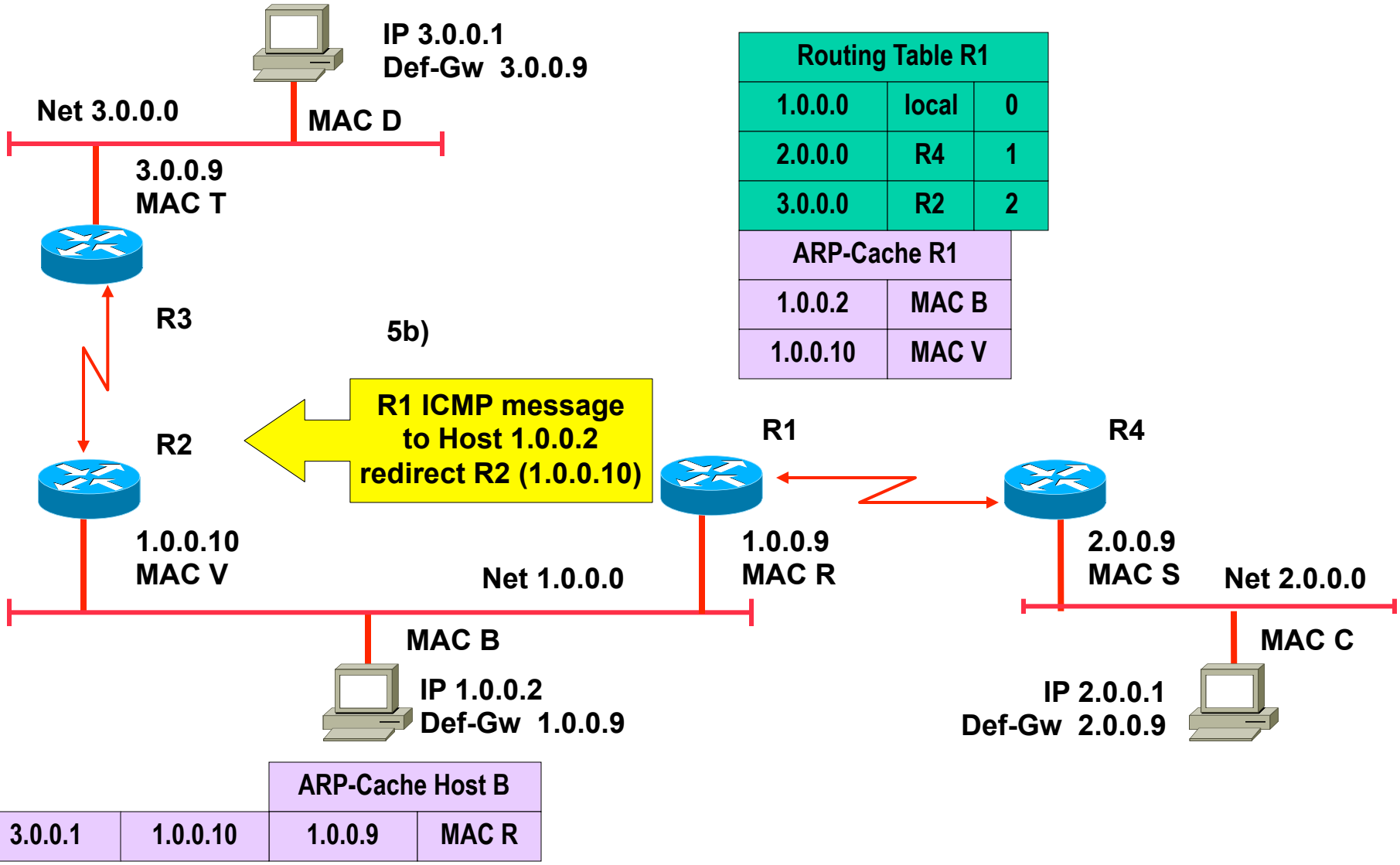



| Routing Table R1 | | |
|---|---|---|
| 1.0.0.0 | local | 0 |
| 2.0.0.0 | R4 | 1 |
| 3.0.0.0 | R2 | 2 |

| ARP-Cache R1 | |
|---|---|
| 1.0.0.2 | MAC B |
| 1.0.0.10 | MAC V |

| ARP-Cache Host B | |
|---|---|
| 1.0.0.9 | MAC R |

# ICMP redirect

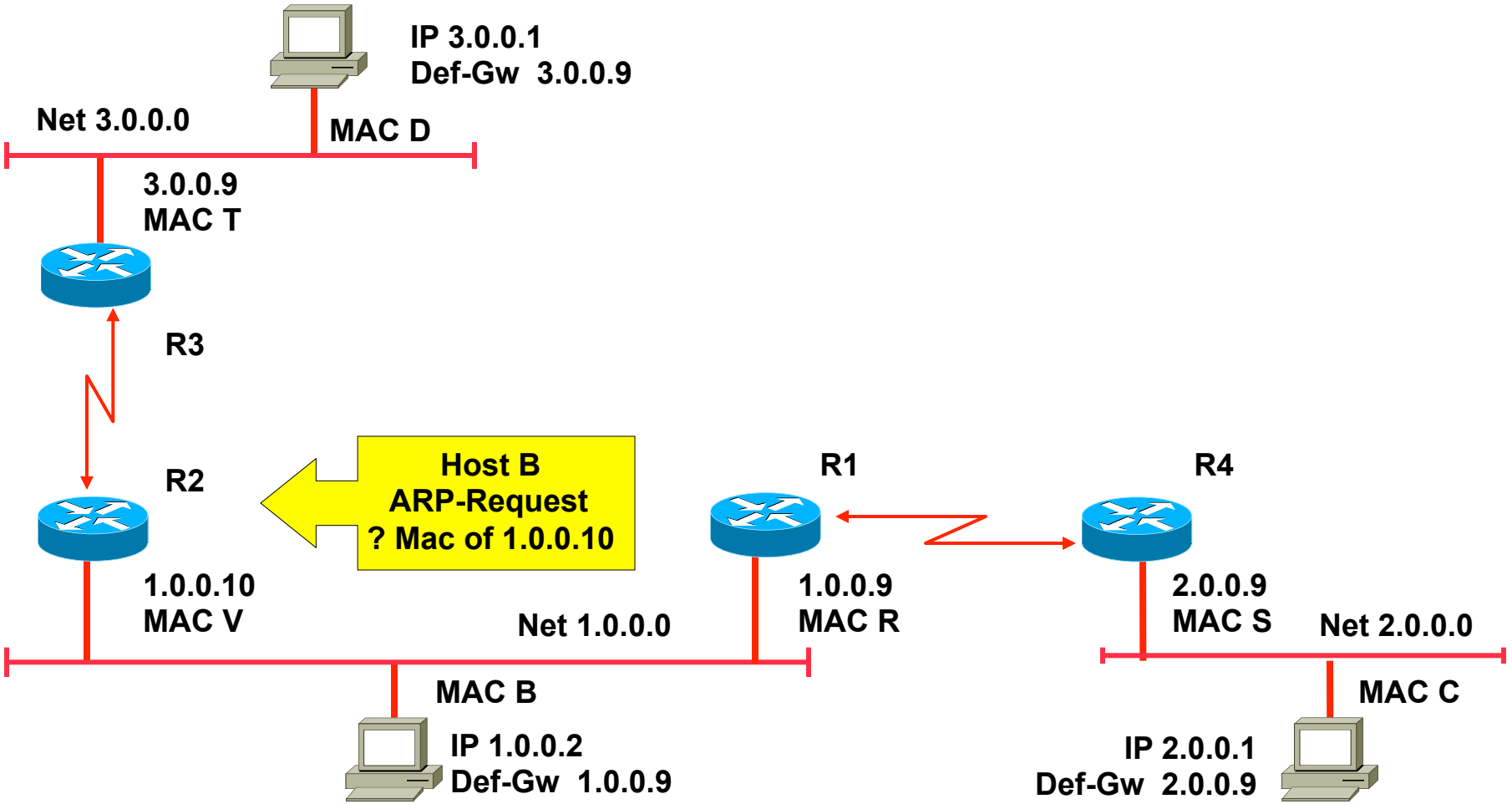



| Routing Table R1 | | |
|---|---|---|
| 1.0.0.0 | local | 0 |
| 2.0.0.0 | R4 | 1 |
| 3.0.0.0 | R2 | 2 |

| ARP-Cache R1 | |
|---|---|
| 1.0.0.2 | MAC B |
| 1.0.0.10 | MAC V |

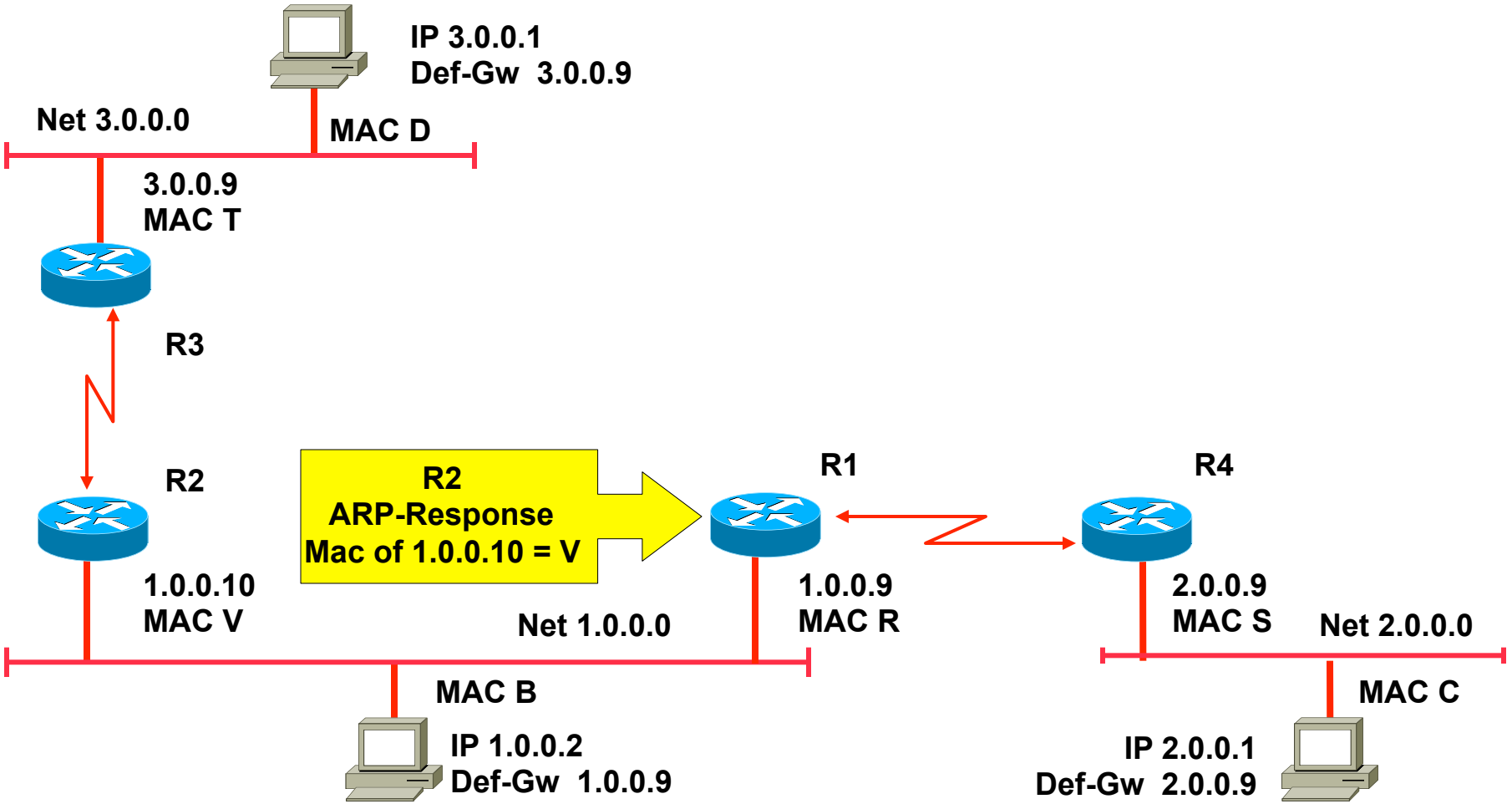
| ARP-Cache Host B | | | |
|---|---|---|---|
| 3.0.0.1 | 1.0.0.10 | 1.0.0.9 | MAC R |

# Delivery 1.0.0.2 -> 3.0.0.1



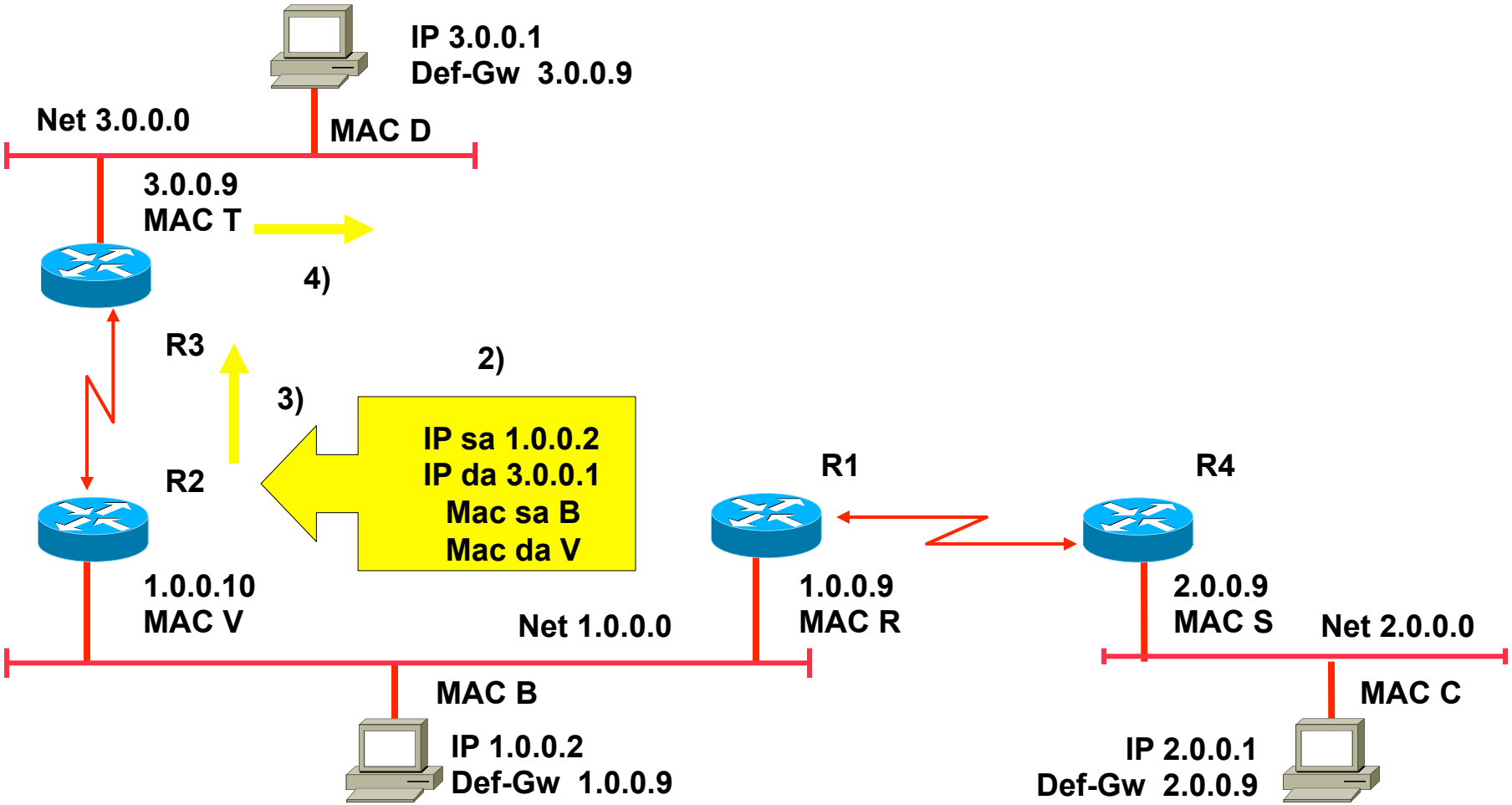

| ARP-Cache Host B | | | |
|---|---|---|---|
| 3.0.0.1 | 1.0.0.10 | 1.0.0.9 | MAC R |

# 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



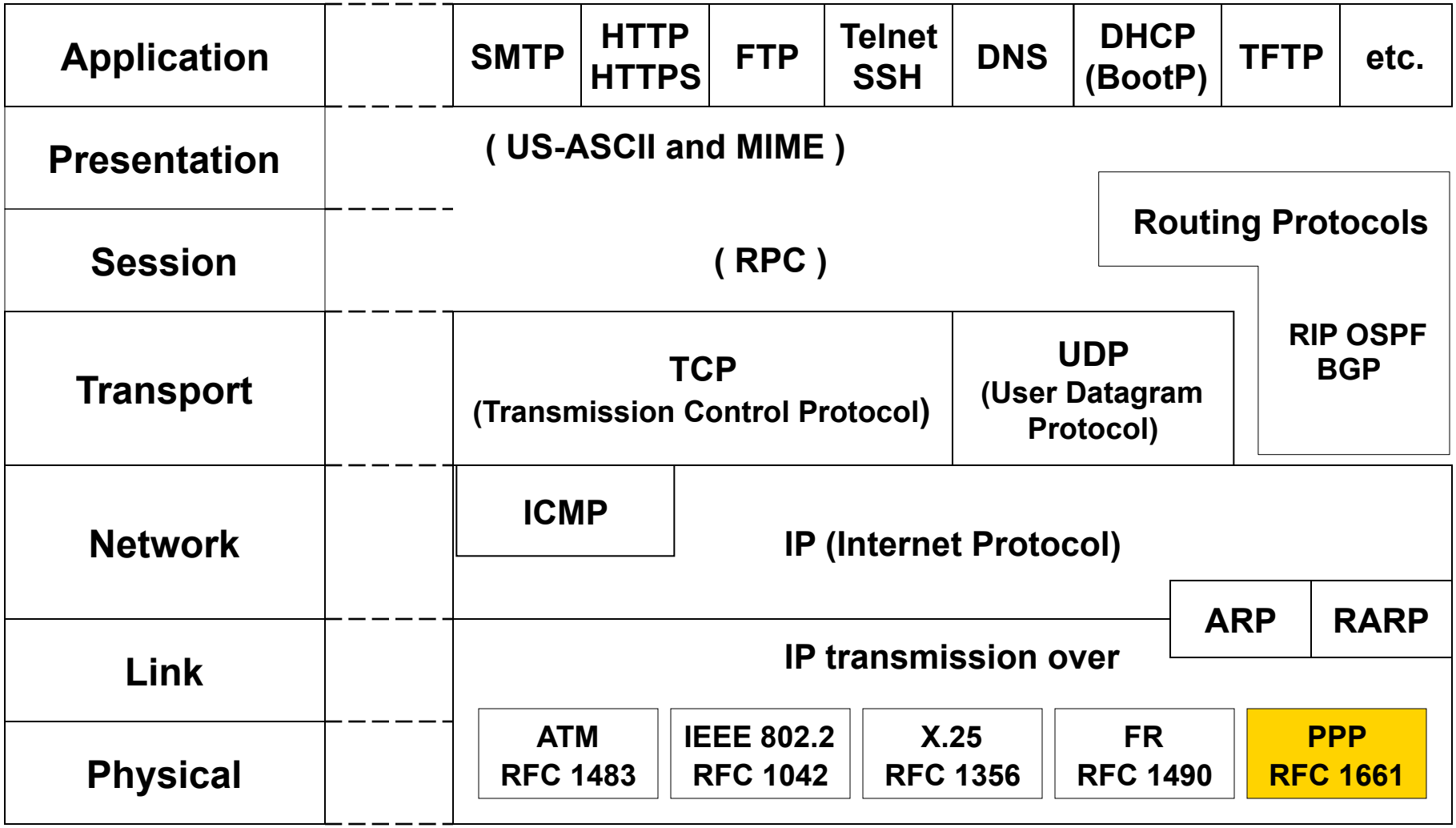

| ARP-Cache Host B | | | |
|---|---|---|---|
| 3.0.0.1 | 1.0.0.10 | 1.0.0.9 | MAC R |
| | | 1.0.0.10 | MAC V |

1)

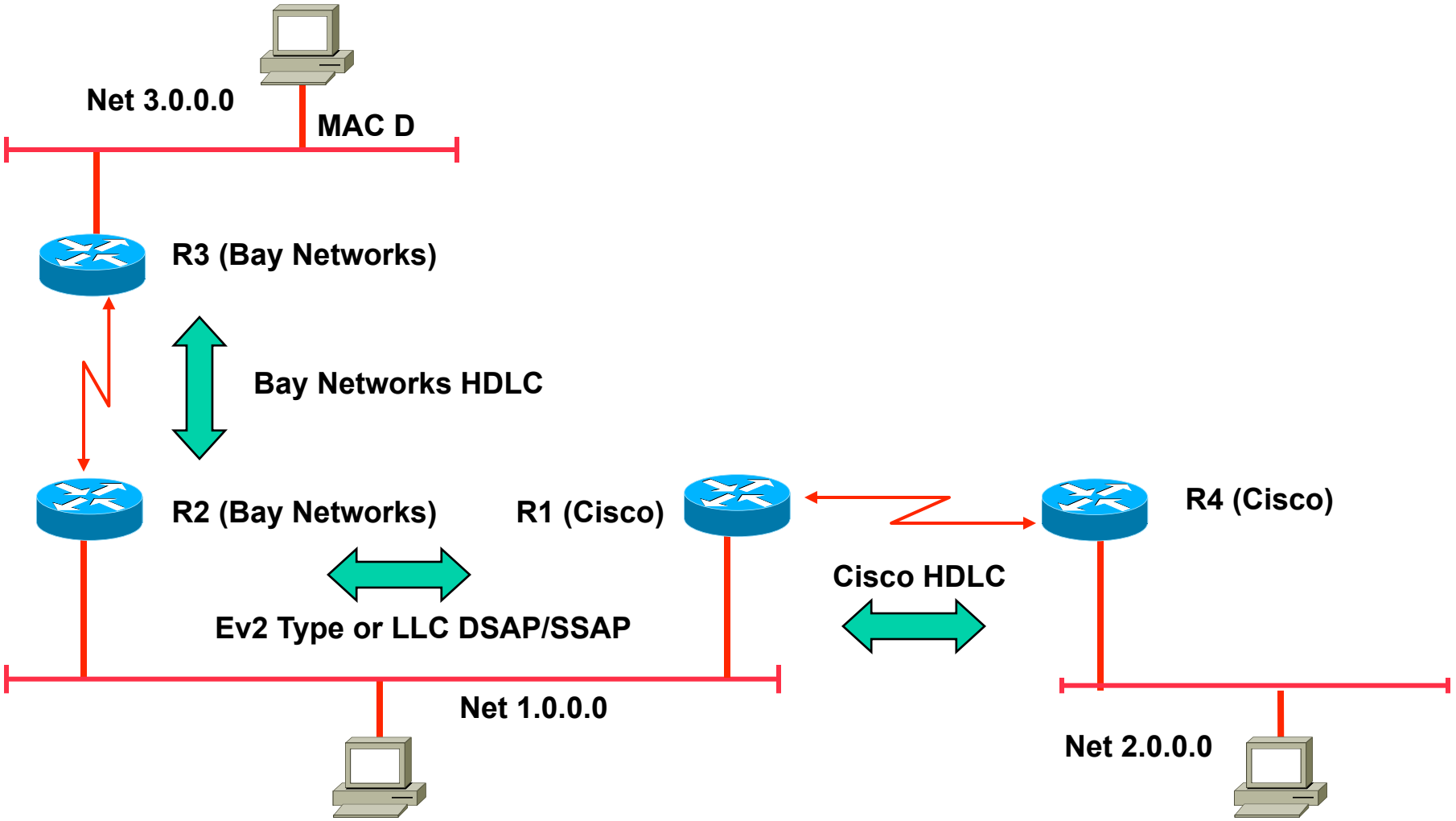
# Agenda

- **Introduction**
  - Short History of the Internet (not part of the exam!)
  - Basic Principles
- **IP**
  - IP Protocol
  - IP QoS
  - Addressing
  - Classful  versus Classless (not part of the exam!)
- **IP Forwarding**
  - Principles
  - ARP
  - ICMP
  - PPP
- **First Hop Redundancy**
  - Proxy ARP, IDRP
  - HSRP
  - VRRP (not part of the exam!)

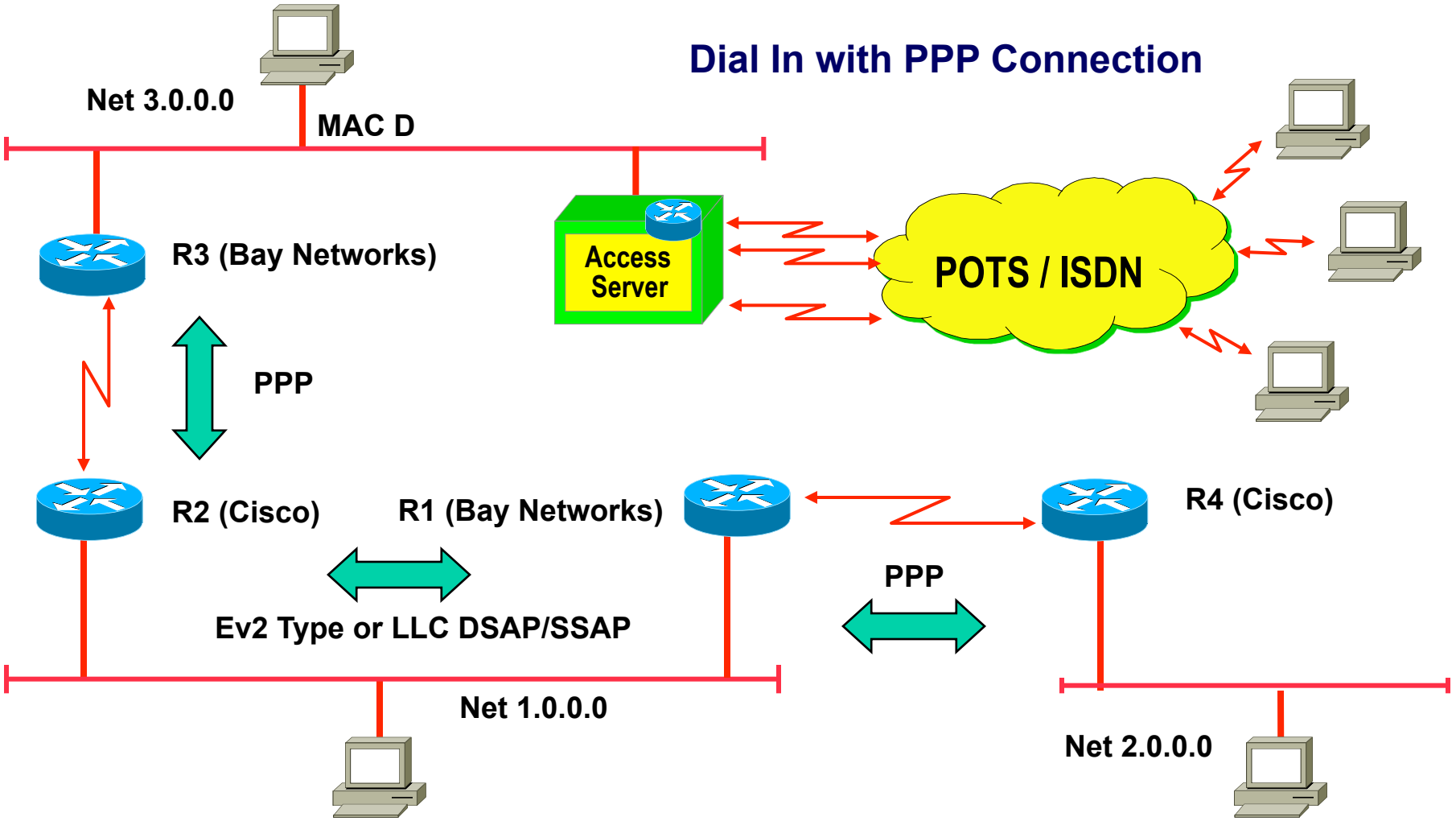
# TCP/IP Protocol Suite



# Interoperability without PPP



# Interoperability with PPP



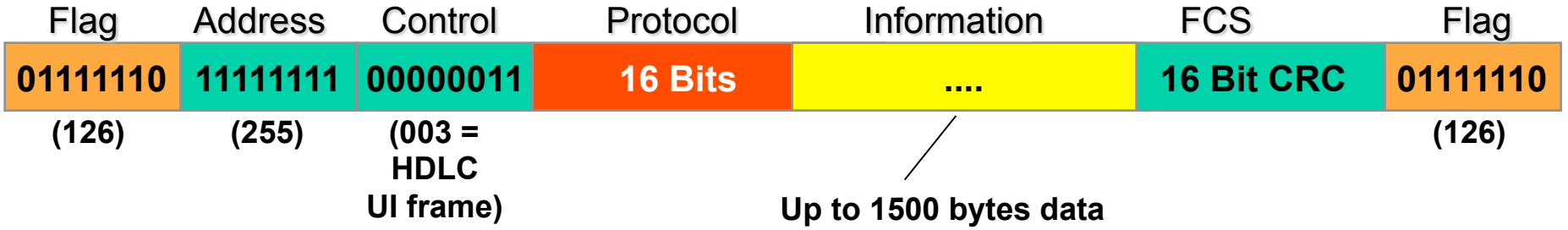
# PPP Overview

- **Data link protocol (L2)**
- **Used to encapsulate network layer datagrams or bridged packets (multiprotocol traffic)**
  - Over serial communication links in a well defined manner
- **Connectionless service**
  - Although we speak about a PPP connection, details are provided later
- **Symmetric point-to-point protocol**
- **Industry standard for dial-in service**
  - Used for interoperability, even over leased lines
- **Supports the simultaneous use of network protocols**

# PPP Components

- **HDLC framing and encapsulation (RFC 1662)**
  - Bitstuffing for synchronous serial lines
  - Modified bytestuffing for asynchronous serial
  - Only connectionless service used (UI frame)
- **Link Control Protocol (LCP, RFC 1661)**
  - Establishes and closes the PPP connection / PPP link
  - Tests the link for quality of service features
  - Negotiation of parameters
  - Configures the PPP connection / PPP link
- **Family of Network Control Protocols (NCPs, div. RFCs)**
  - Configures and maintains network layer protocols
  - NCPs exist for IP, OSI, DECnet, AppleTalk, Novell
  - NCPs are started after PPP link establishment through LCP

# PPP Frame Format




- **Some protocol fields (hex values)**
  - 0021 Internet Protocol
  - 0029 AppleTalk
  - 8021 IP Control Protocol
  - 8029 AppleTalk Control Prot.
  - C021 Link Control Protocol
  - C223 Authentication CHAP
  - 0027 DECnet Phase 4
  - 002B Novell IPX
  - 8027 DECnet Control Protocol
  - 802B IPX Control Protocol
  - C023 Authentication Protocol

# Protocol Field

| | |
|---|---|
| 0xxx – 3xxx | L3 protocol type |
| 4xxx – 7xxx | L3 protocol type without associated NCPs |
| 8xxx – bxxx | Associated NCPs for protocols in range 0xxx – 3xxx |
| cxxx – fxxx | LCP, PAP, CHAP, ... |

| | |
|---|---|
| 0021 | IP |
| 002b | Novell IPX |
| 002d | Van Jacobson Compressed TCP/IP |
| 002f | Van Jacobson Uncompressed TCP/IP |

| | |
|---|---|
| 8021 | IP-NCP (IPCP) |
| 802b | IPX-NCP (IPXCP) |

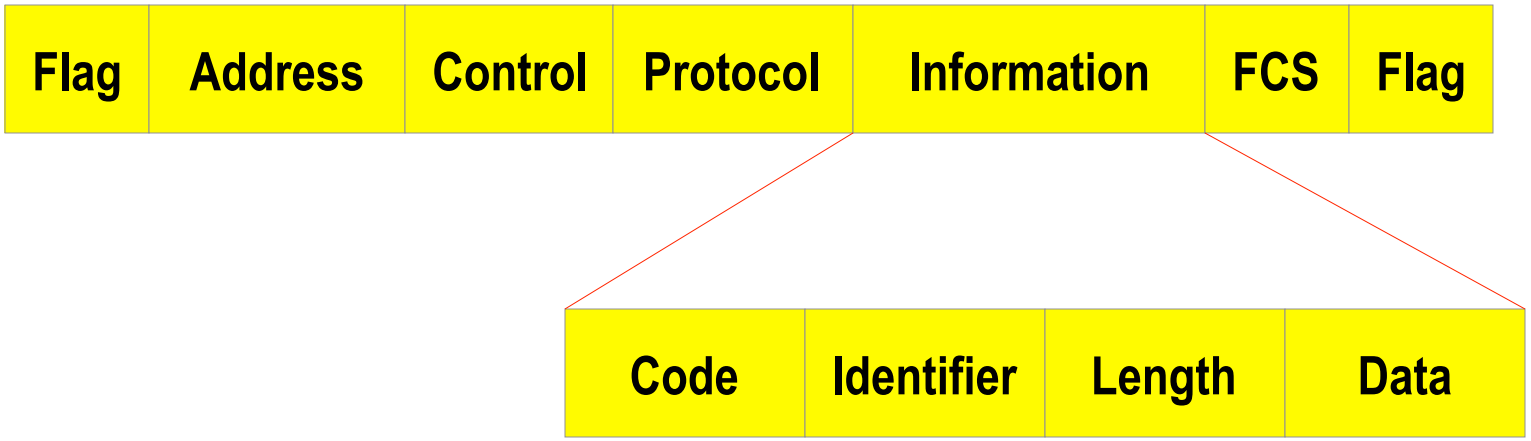
**Important Examples**

| | |
|---|---|
| c021 | Link Control Protocol (LCP) |
| c023 | Password Auth. Protocol (PAP) |
| c025 | Link Quality Report |
| c223 | Challenge Handshake Auth. Protocol (CHAP) |

# LCP Tasks

- **Establishment of PPP connection**
  - Setup, configure, test and terminate PPP connection
  - Supports various environments
  - Allows certain configuration options to be negotiated
- **Negotiation of options**
  - Encapsulation format options
  - Maximal packet sizes
  - Identification and authentication of peers (!)
  - Determination of proper link functionality

# LCP Frame Format




- **Carried in PPP information field**
  - Protocol field has to be 0xC021
  - Code field indicates type of LCP packet
  - Identifier field is used to match requests and replies
  - Data field values are determined by the code field (e.g. contains options to be negotiated)

# Types of LCP Packets

- **There are three classes of LCP packets:**
  - Class 1: Link Configuration packets used to establish and configure a PPP link
    - Configure-Request (code 1, details in option field), Configure-Ack (code 2), Configure-Nak (code 3, not supported option) and Configure-Reject (code 4, not supported option)
  - Class 2: Link Termination packets used to terminate a link
    - Terminate-Request (code 5) and Terminate-Ack (code 6)
  - Class 3: Link Maintenance packets used to manage and debug a PPP link
    - Code-Reject (code 7, unknown LCP code field), Protocol-Reject (code 8, unknown PPP protocol field), Echo-Request (code 9), Echo-Reply (code 10) and Discard-Request (code 11)

# PPP Connection

- **PPP connection is established in four phases**
  - Phase 1: Link establishment and configuration negotiation
    - Done by LCP (note: deals only with link operations, does not negotiate the implementation of network layer protocols)
  - Phase 2: Optional procedures that were agreed during negotiation of phase 1 (e.g. CHAP authentication or compression)
  - Phase 3: Network layer protocol configuration negotiation done by corresponding NCP´s
    - E.g. IPCP, IPXCP, …
    - Actual PPP usage for configured protocols after phase 3
  - Phase 4: Link termination

# PPP Phases

- **Task of phase 1**
  - LCP is used to automatically
    - Agree upon the encapsulation format options
    - Handle varying limits on sizes of packets
    - Detect a looped-back link and other common configuration errors (magic number for loopback detection)
  - Options which may be negotiated
    - Maximum receive unit
    - Usage of an authentication protocol
    - Quality protocol
    - Protocol-Field-Compression
    - Address-and-Control-Field-Compression
    - These options are described in RFC 1661 (except authentication protocols)

# PPP Phases (cont.)

- **Task of phase 1 (cont.)**
  - Options which may be negotiated but implementations are specified in other RFCs
    - PPP link quality protocol (RFC 1989)
    - PPP compression control protocol (RFC 1962)
    - PPP compression STAC (RFC 1974)
    - PPP compression PREDICTOR (RFC 1978)
    - PPP multilink (RFC 1990)
    - PPP callback (draft-ietf-pppext-callback-ds-01.txt)
    - PPP authentication CHAP (RFC 1994)
    - PPP authentication PAP (RFC 1334)
    - PPP Extensible Authentication Protocol (EAP), RFC 2284

# PPP Phases (cont.)

- **Task of phase 2**
  - Providing of optional facilities
    - Authentication, compression initialization, multilink, etc.
- **Task of phase 3**
  - Network layer protocol configuration negotiation
    - After link establishment, stations negotiate/configure the protocols that will be used at the network layer; performed by the appropriate network control protocol
    - Particular protocol used depends on which family of NCPs is implemented
- **Task of phase 4**
  - Link termination
    - Responsibility of LCP, usually triggered by an upper layer protocol of a specific event

# PPP Link Operation Example

Phase 1

Configure Request

Configure ACK

Configure Request

Configure ACK

LCP Operations (several LCP options are exchanged and accepted options acknowledged)

Phase 3

Configure Request IP

Configure ACK

Configure Request IP

Configure ACK

NCP Operations for IPCP

Exchange Traffic

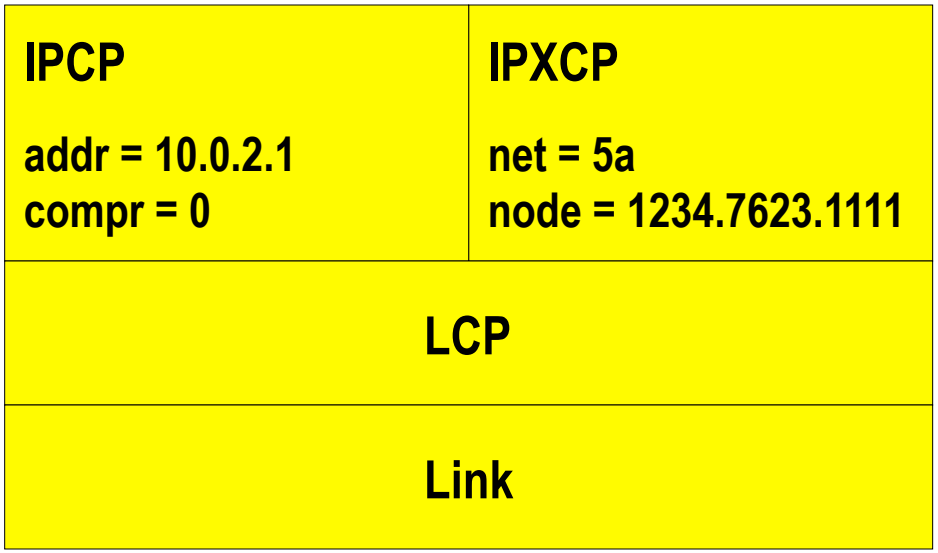
Phase 4

Terminate Request

Terminate ACK

# Network Control Protocol

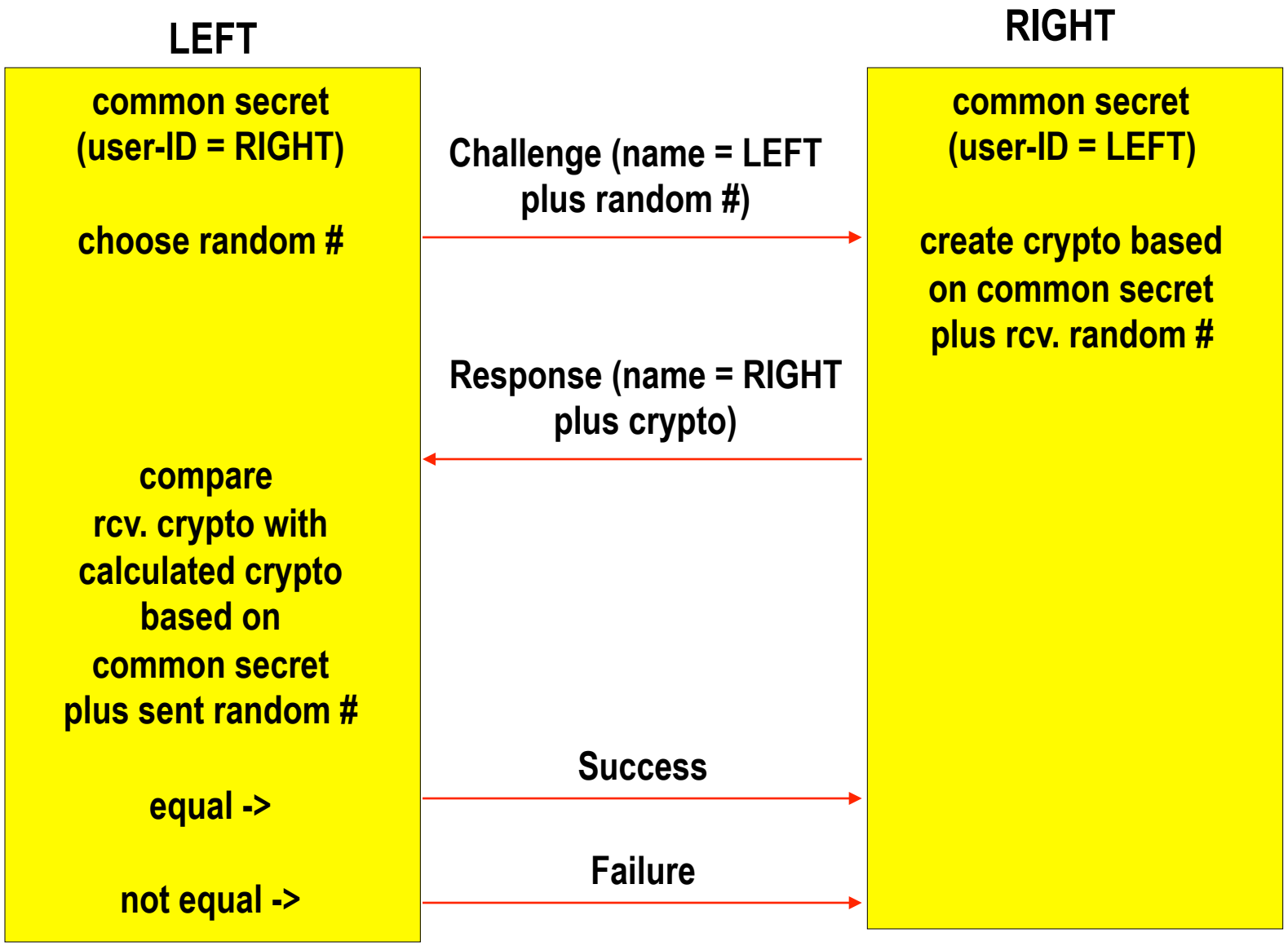
- One per upper layer protocol (IP, IPX…)
- Each NCP negotiates parameters appropriate for that protocol
- **NCP for IP (IPCP)**
  - **Provides similar functionality as DHCP for LAN**
    - IP address, Default Gateway, DNS Server, TTL, TCP header compression can be negotiated or assigned



# CHAP Authentication RFC 1994

- **Challenge Authentication Protocol**
  - Follows establishment of LCP
  - Identifies user
  - Three way handshake procedure
  - One way authentication only
  - Station which starts the three way handshake proofs authentication of other station
  - Cryptographic hash function (e.g. keyed MD5) is applied to random numbers used (hopefully) only once
    - Network snooping does not reveal any passwords
    - Offline dictionary attacks are possible
  - Overcomes weaknesses of PAP (Password Authentication Protocol) which used transmission of cleartext passwords (!!!)
- **Three way handshake have to be performed in both directions**
  - If two way authentication is necessary

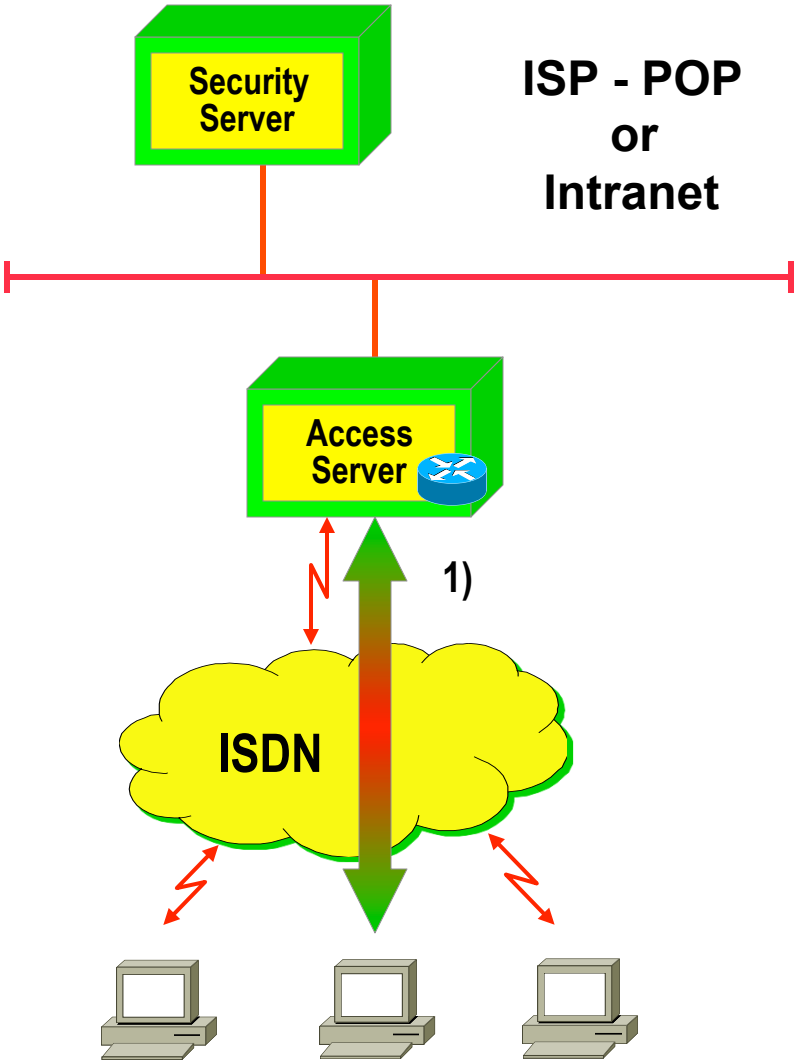
# CHAP Authentication Procedure



# PPP as Dial-In Technology

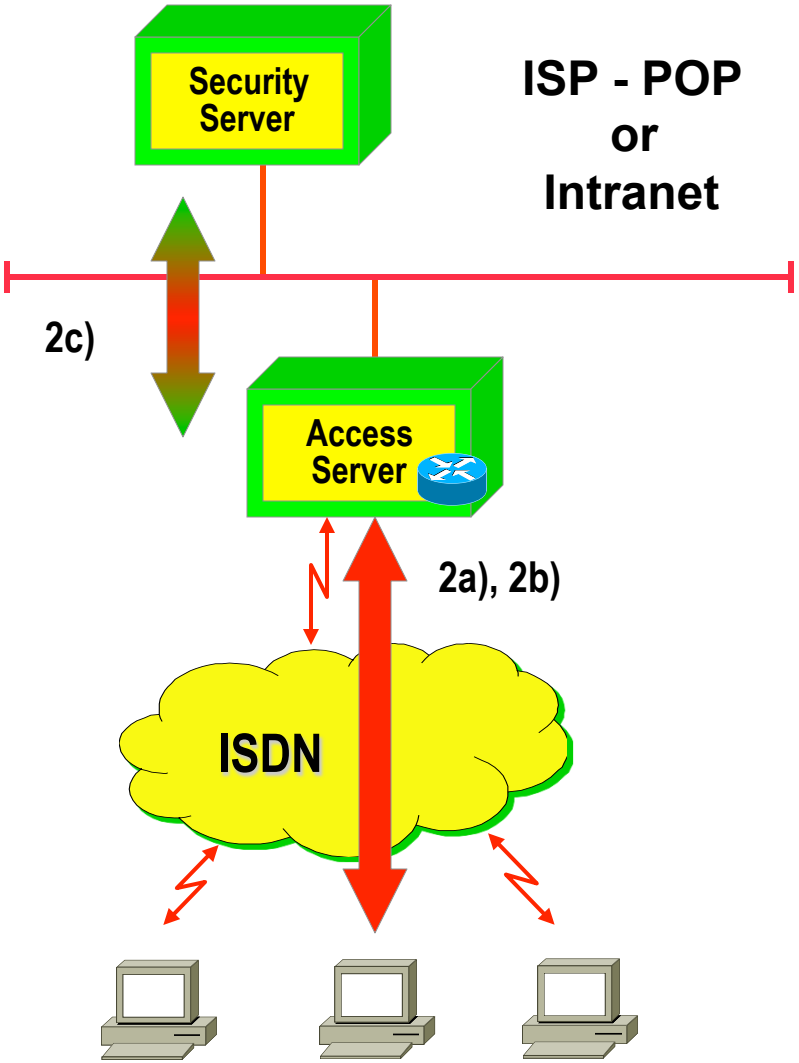
- **Dial-In:**
  - Into a corporate network (Intranet) of a company
    - Here the term RAS (remote access server) is commonly used to describe the point for accessing the dial-in service
  - Into the Internet by having an dial-in account with an Internet Service Provider (ISP)
    - Here the term POP (point-of-presence) is used to describe the point for accessing the service

# RAS Operation 1



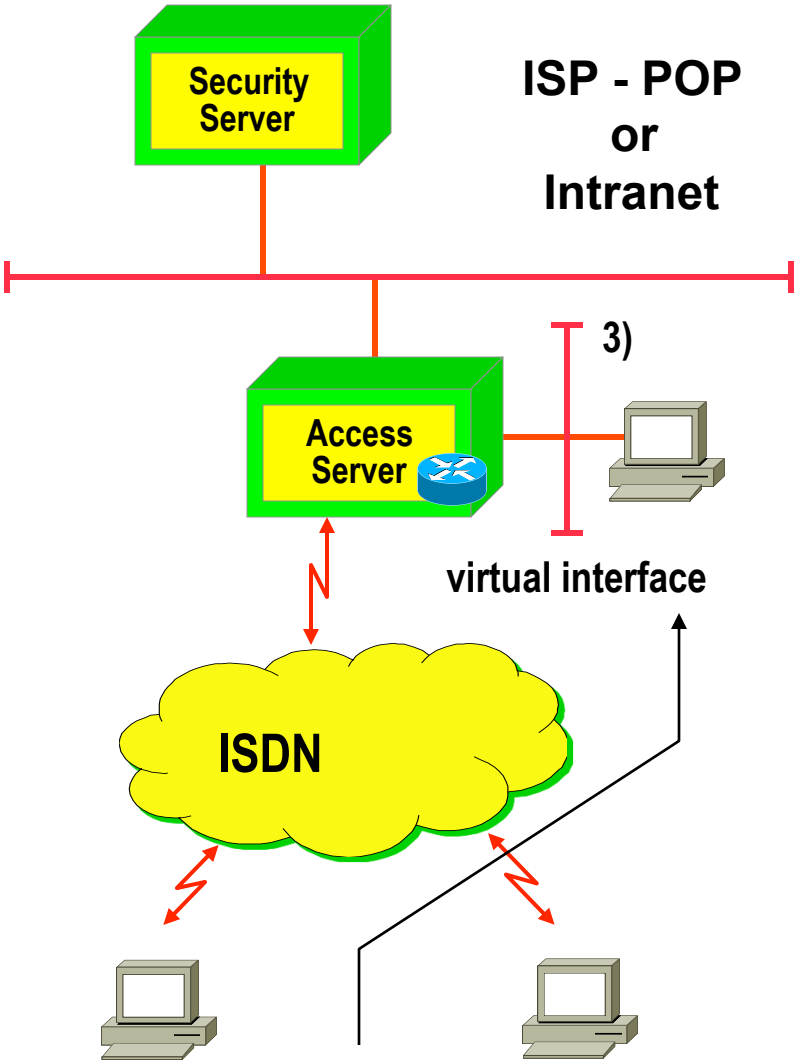

- remote PC places ISDN call to access server, ISDN link is established (1)

# RAS Operation 2



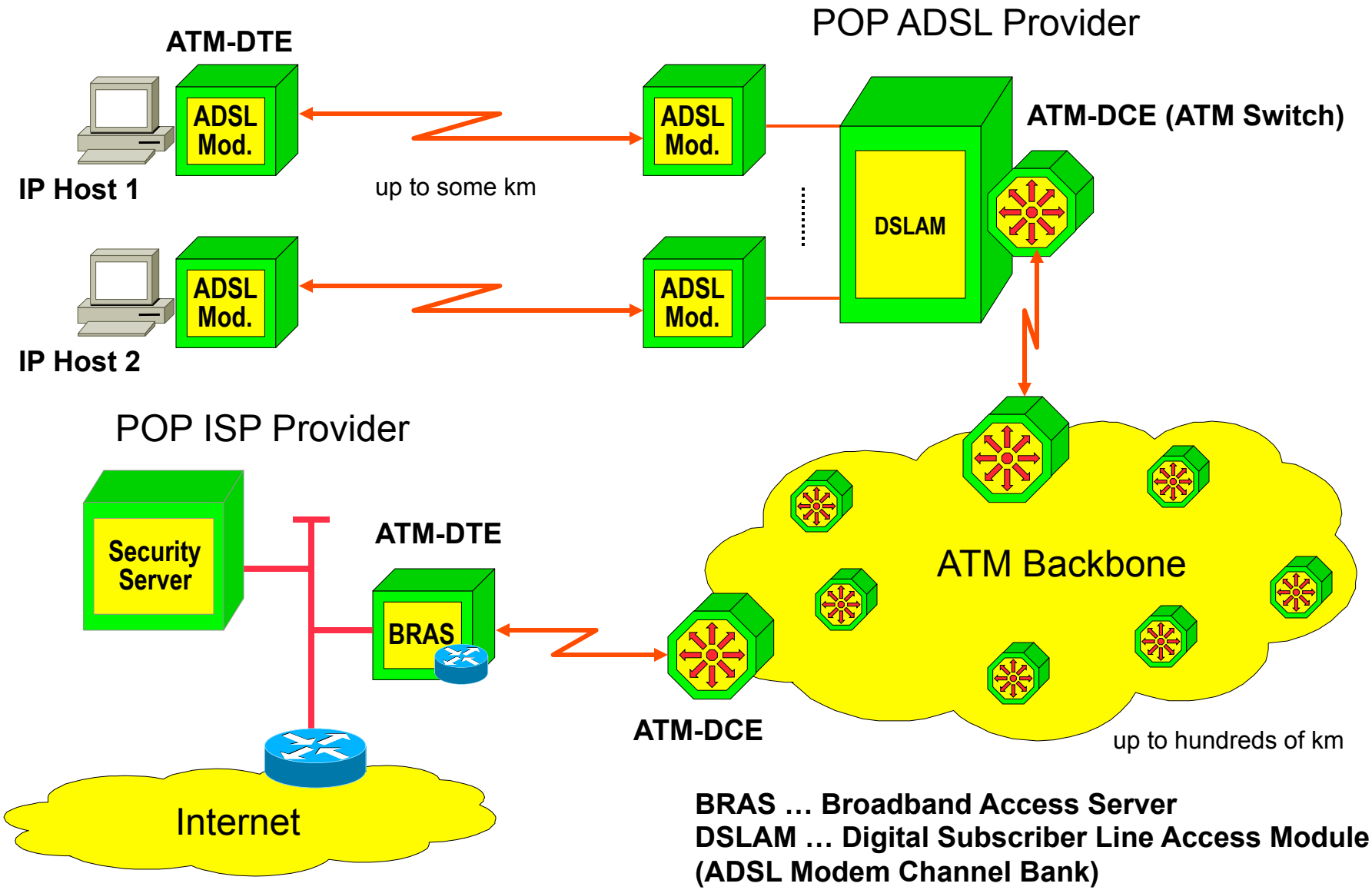

- **PPP link (multiprotocol over serial line) is established**
  - LCP Link Control Protocol (2a)
    - Establishes PPP link plus negotiates parameters like authentication CHAP
  - Authentication
    - CHAP Challenge Authentication Protocol to transport passwords (2b)
    - Verification maybe done by central security server (2c) -> Radius, TACACS, TACACS+

# RAS Operation 3



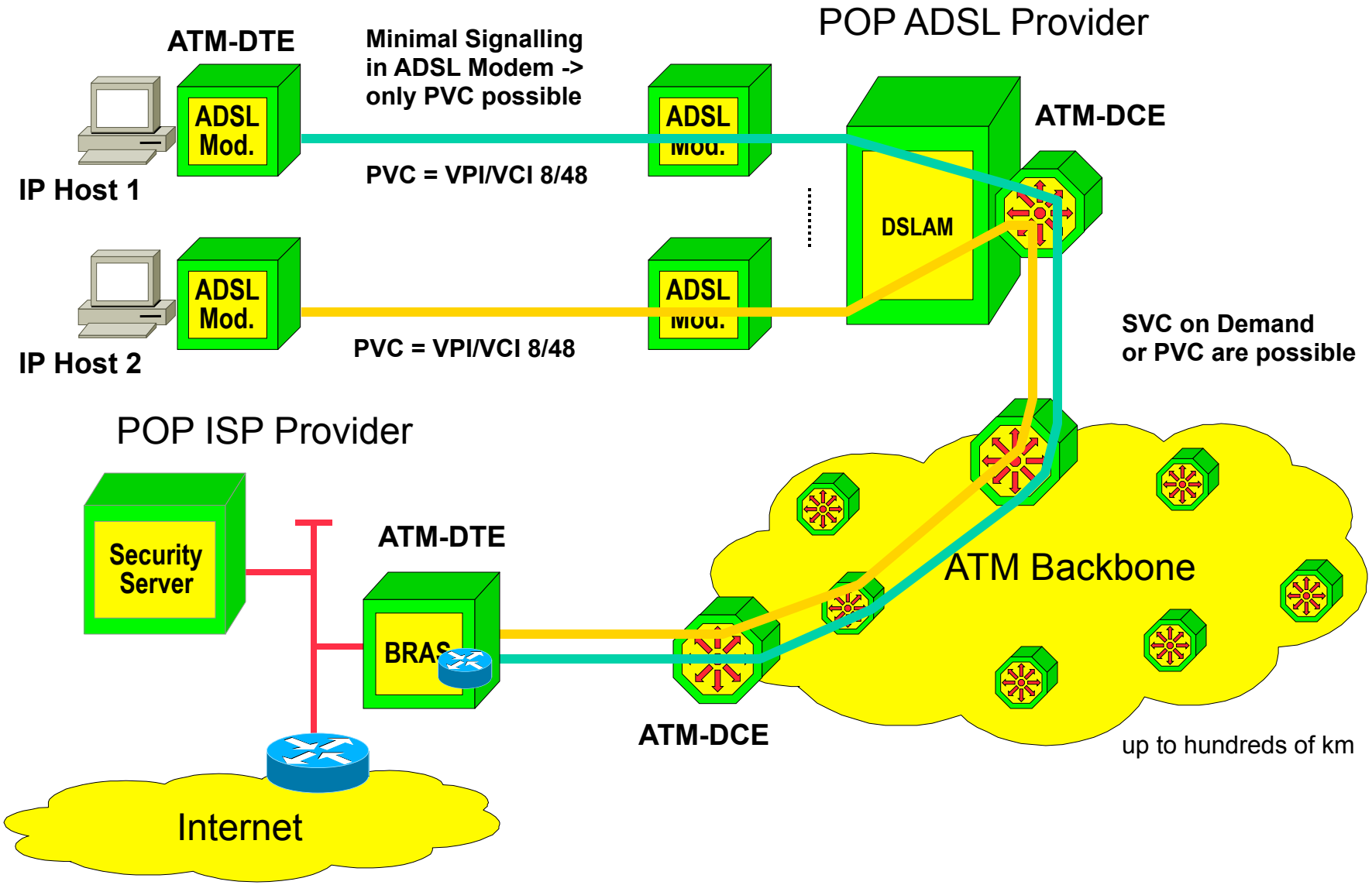

- **PPP NCP (Network Control Protocol) IPCP**
  - Assigns IP address, Def. GW, DNS to remote PC
- **Remote PC appears as**
  - Device reachable via virtual interface (3), IP host Route
- **Optionally**
  - Filter could be established on that virtual interface
    - Authorization
  - Accounting may be performed
    - Actually done by security server (AAA server)
    - TACACS, Radius

# ADSL: Physical Topology

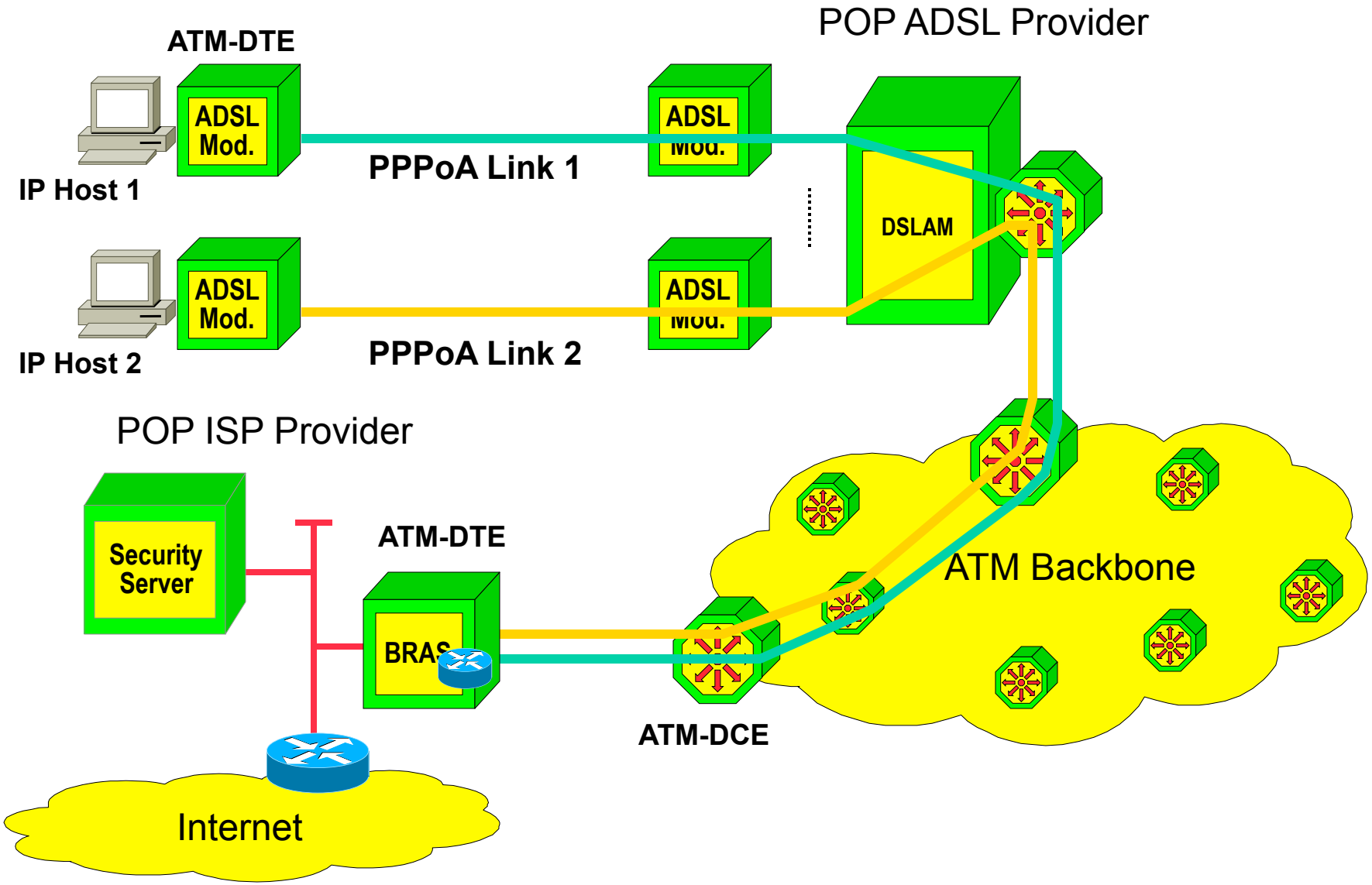



**BRAS … Broadband Access Server**
**DSLAM … Digital Subscriber Line Access Module (ADSL Modem Channel Bank)**

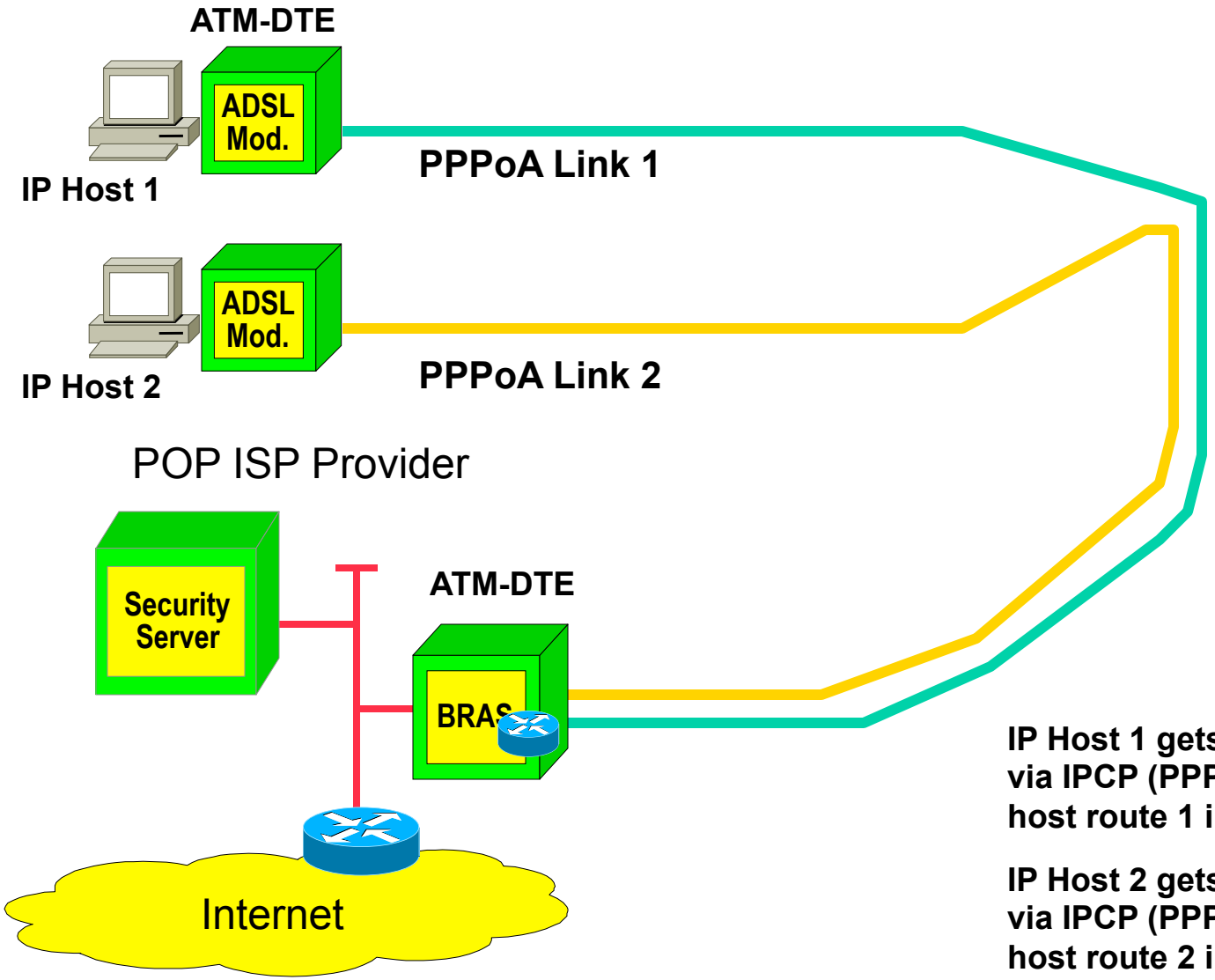
# ADSL: ATM Virtual Circuits



# ADSL: PPP over ATM (PPPoA)



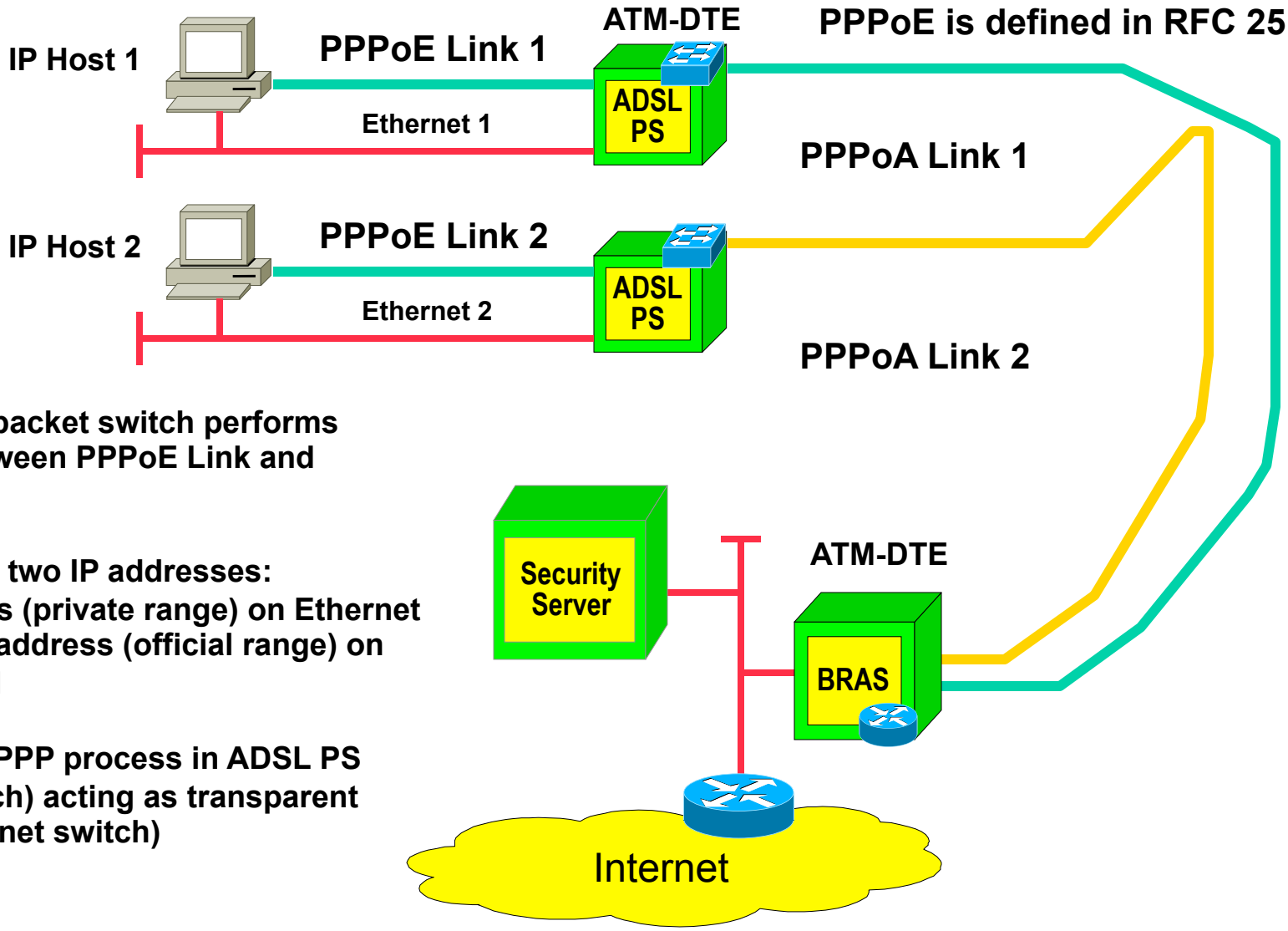
# ADSL: PPP over ATM (PPPoA), IPCP




**IP Host 1 gets global IP address via IPCP (PPP-NCP), appears as host route 1 in BRAS**

**IP Host 2 gets global IP address via IPCP (PPP-NCP), appears as host route 2 in BRAS**

# ADSL: PPP over Ethernet (PPPoE)

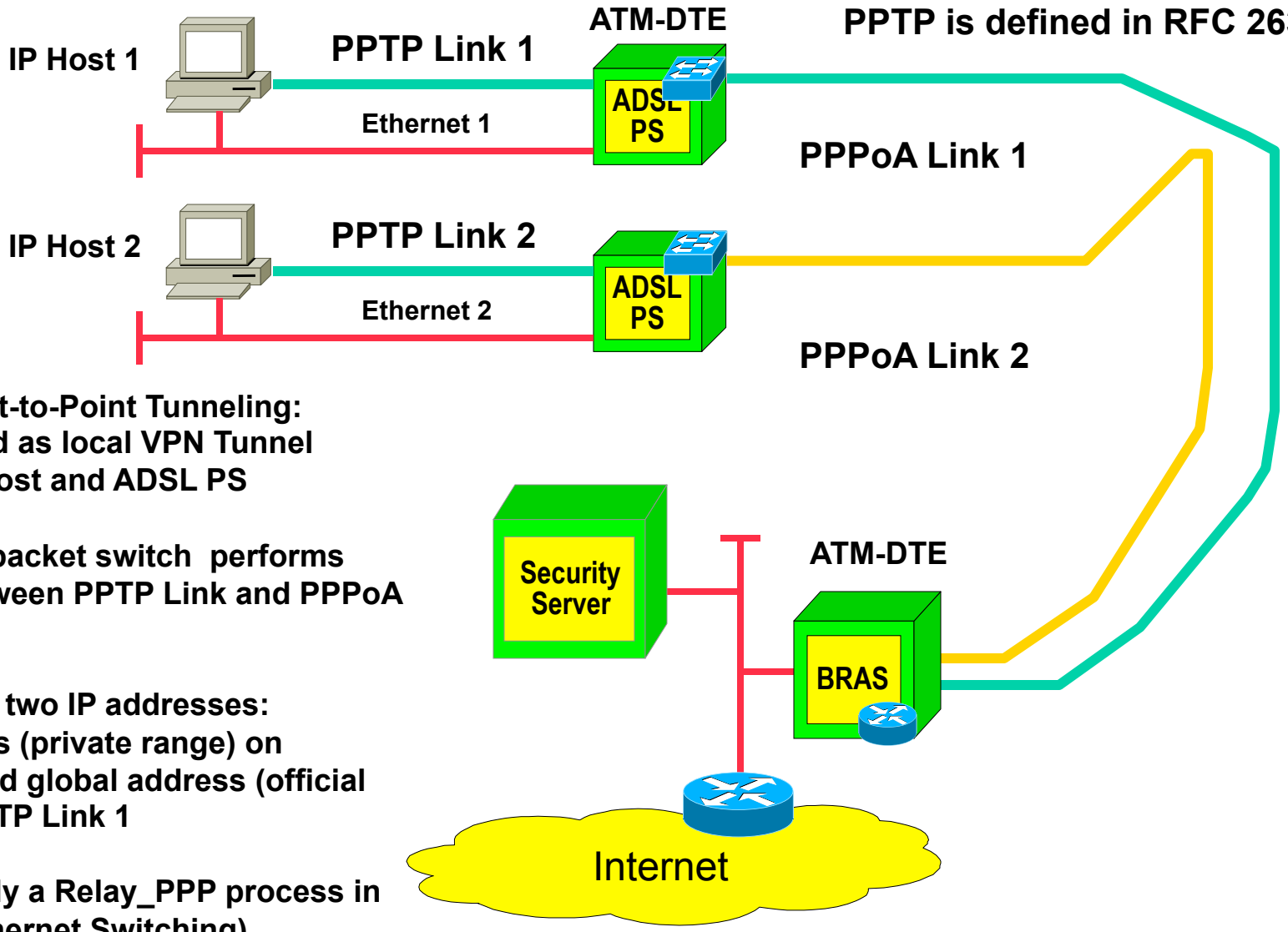



**ADSL PS as packet switch performs mapping between PPPoE Link and PPPoA Link**

**IP Host 1 has two IP addresses: Local address (private range) on Ethernet 1 and global address (official range) on PPPoE Link 1**

**Note: Relay_PPP process in ADSL PS (Packet Switch) acting as transparent bridge (Ethernet switch)**

# ADSL: PPTP over Ethernet (Microsoft VPN)



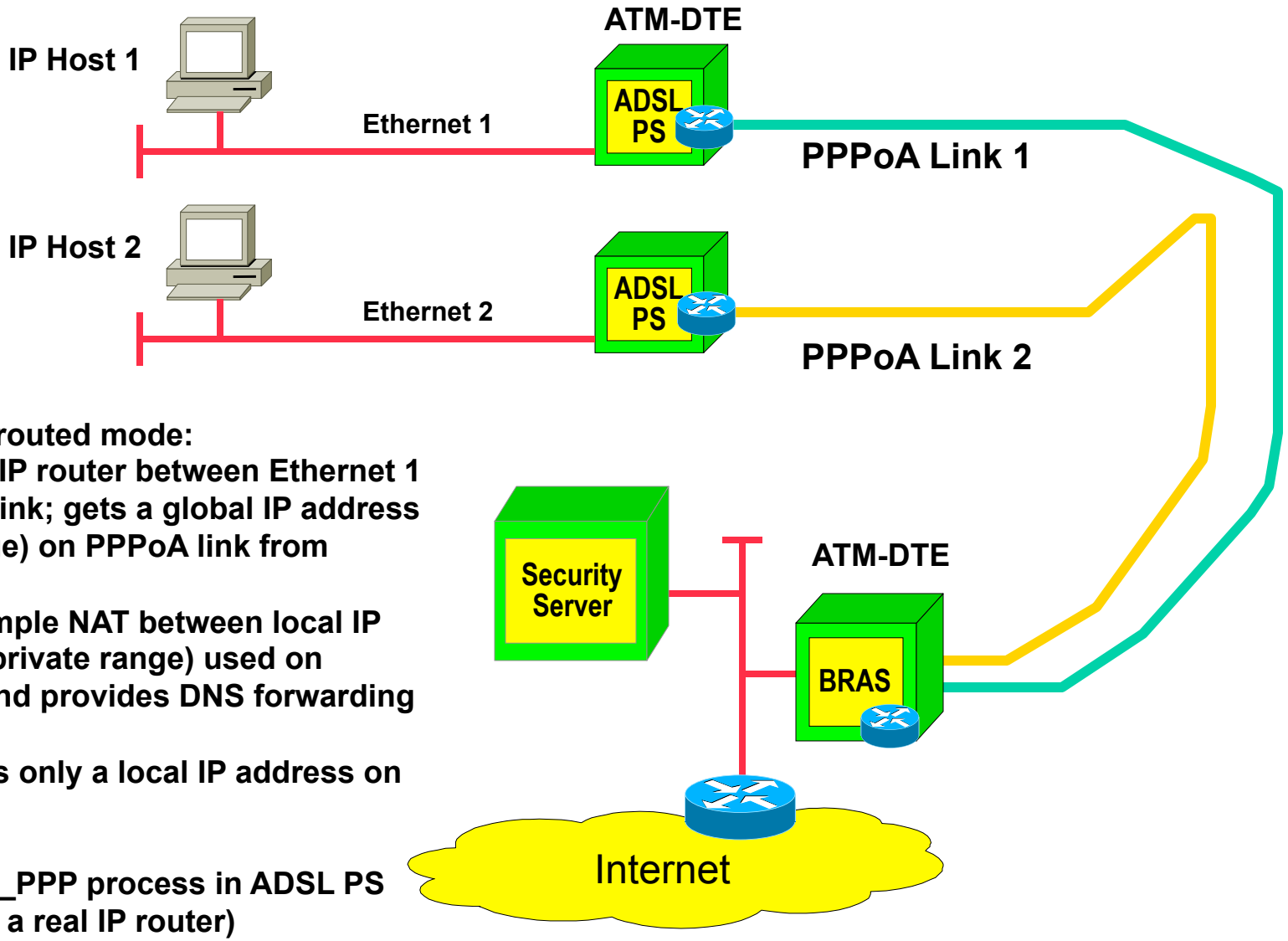

**PPTP … Point-to-Point Tunneling: Protocol used as local VPN Tunnel between IP Host and ADSL PS**

**ADSL PS as packet switch performs mapping between PPTP Link and PPPoA Link**

**IP Host 1 has two IP addresses: Local address (private range) on Ethernet 1 and global address (official range) on PPTP Link 1**

**Note: Still only a Relay_PPP process in ADSL PS (Ethernet Switching)**

# ADSL: Routed PPPoA




**ADSL PS in routed mode:**
**Acts as real IP router between Ethernet 1 and PPPoA link; gets a global IP address (official range) on PPPoA link from provider.**
**Performs simple NAT between local IP addresses (private range) used on Ethernet 1 and provides DNS forwarding**

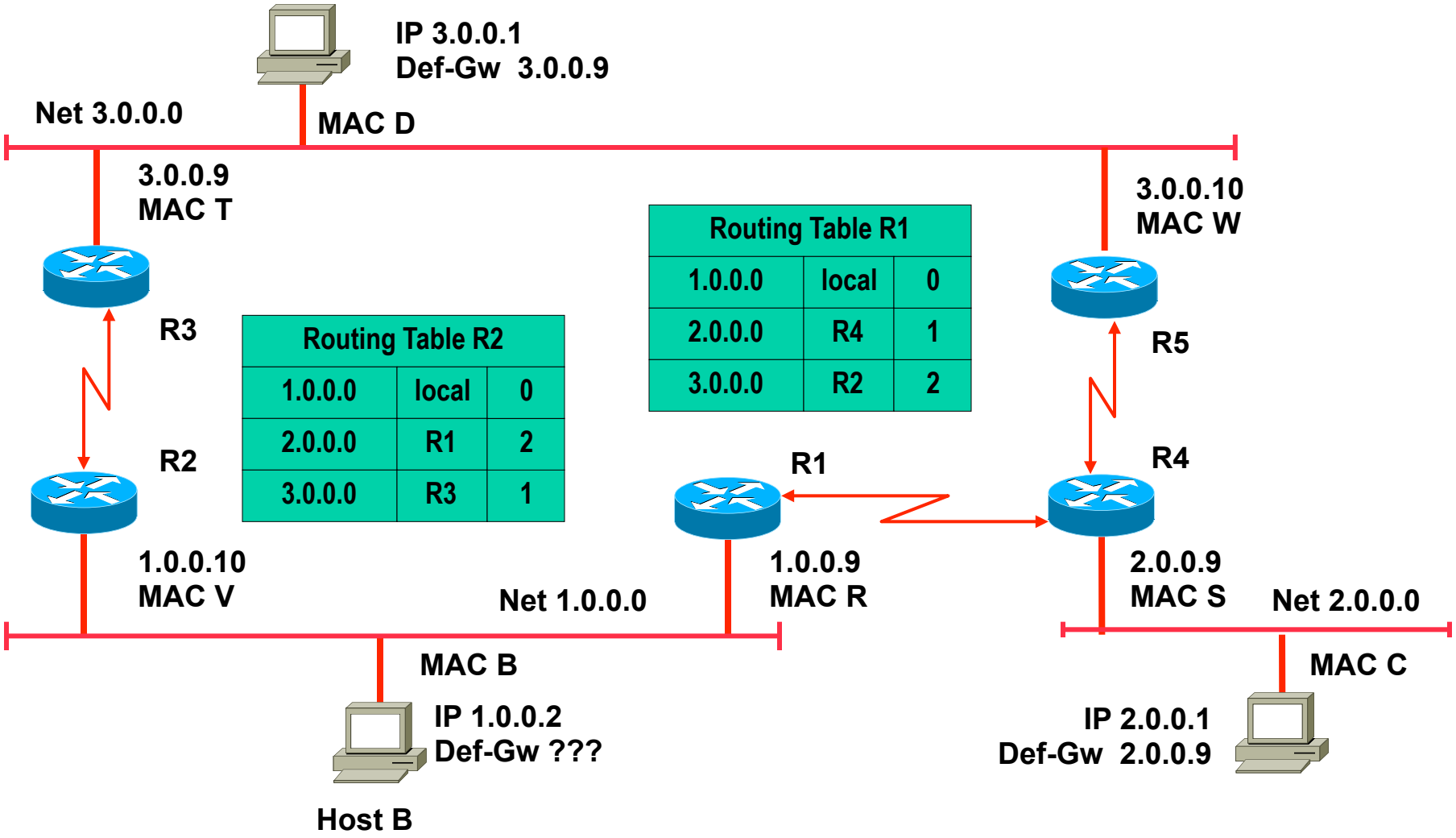
**IP Host 1 has only a local IP address on Ethernet 1**

**Note: Dialup_PPP process in ADSL PS (PS is a now a real IP router)**

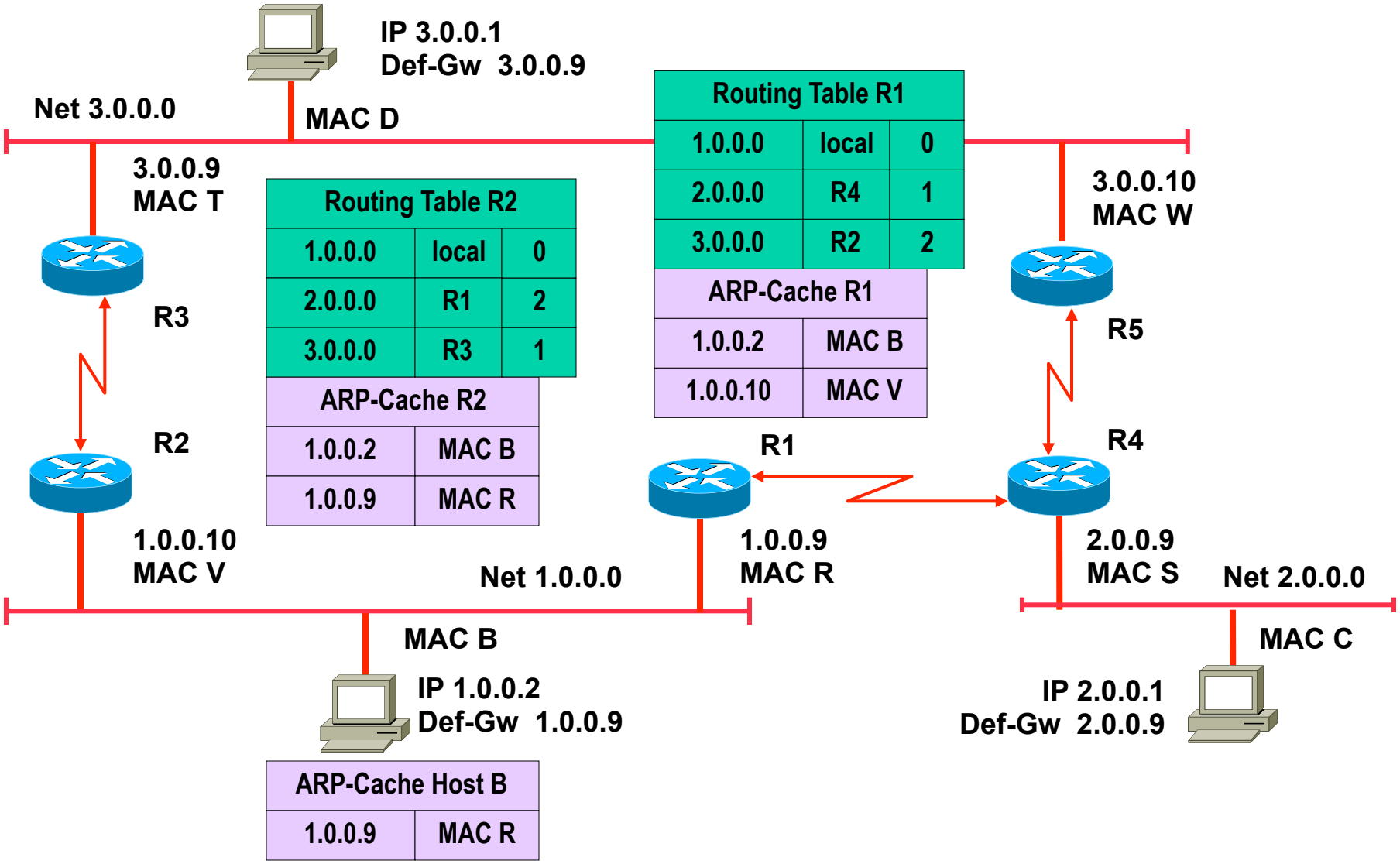
# Agenda

- **Introduction**
  - Short History of the Internet (not part of the exam!)
  - Basic Principles
- **IP**
  - IP Protocol
  - IP QoS
  - Addressing
  - Classful  versus Classless (not part of the exam!)
- **IP Forwarding**
  - Principles
  - ARP
  - ICMP
  - PPP
- **First Hop Redundancy**
  - Proxy ARP, IDRP
  - HSRP
  - VRRP (not part of the exam!)

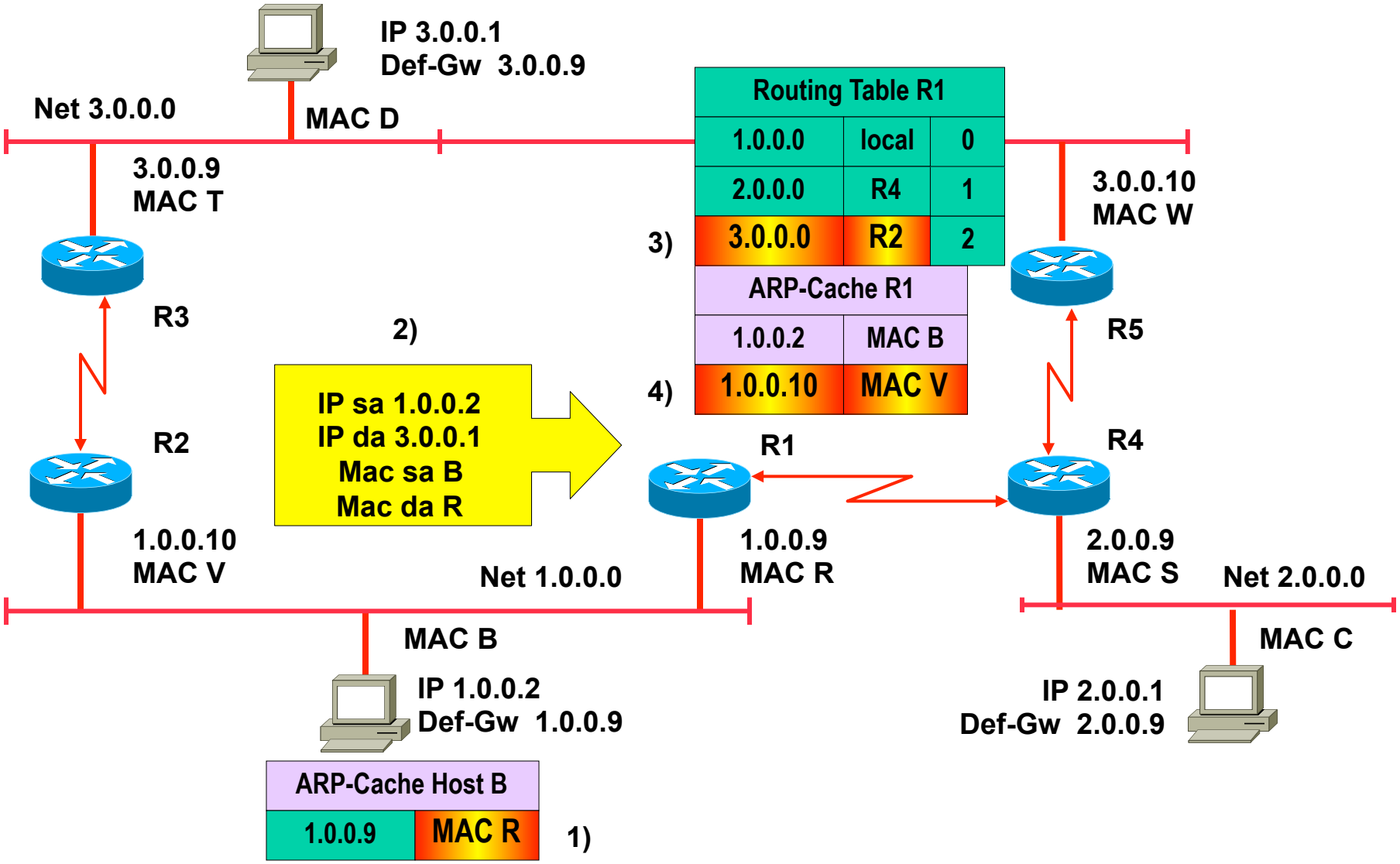
# First L3 Hop?


IP 3.0.0.1
Def-Gw 3.0.0.9
Net 3.0.0.0
MAC D
3.0.0.9
MAC T
3.0.0.10
MAC W
R3
R5
Routing Table R2
1.0.0.0 local 0
2.0.0.0 R1 2
3.0.0.0 R3 1
Routing Table R1
1.0.0.0 local 0
2.0.0.0 R4 1
3.0.0.0 R2 2
R2
R1
R4
1.0.0.10
MAC V
1.0.0.9
MAC R
2.0.0.9
MAC S
Net 1.0.0.0
Net 2.0.0.0
MAC B
MAC C
IP 1.0.0.2
Def-Gw ???
IP 2.0.0.1
Def-Gw 2.0.0.9
Host B

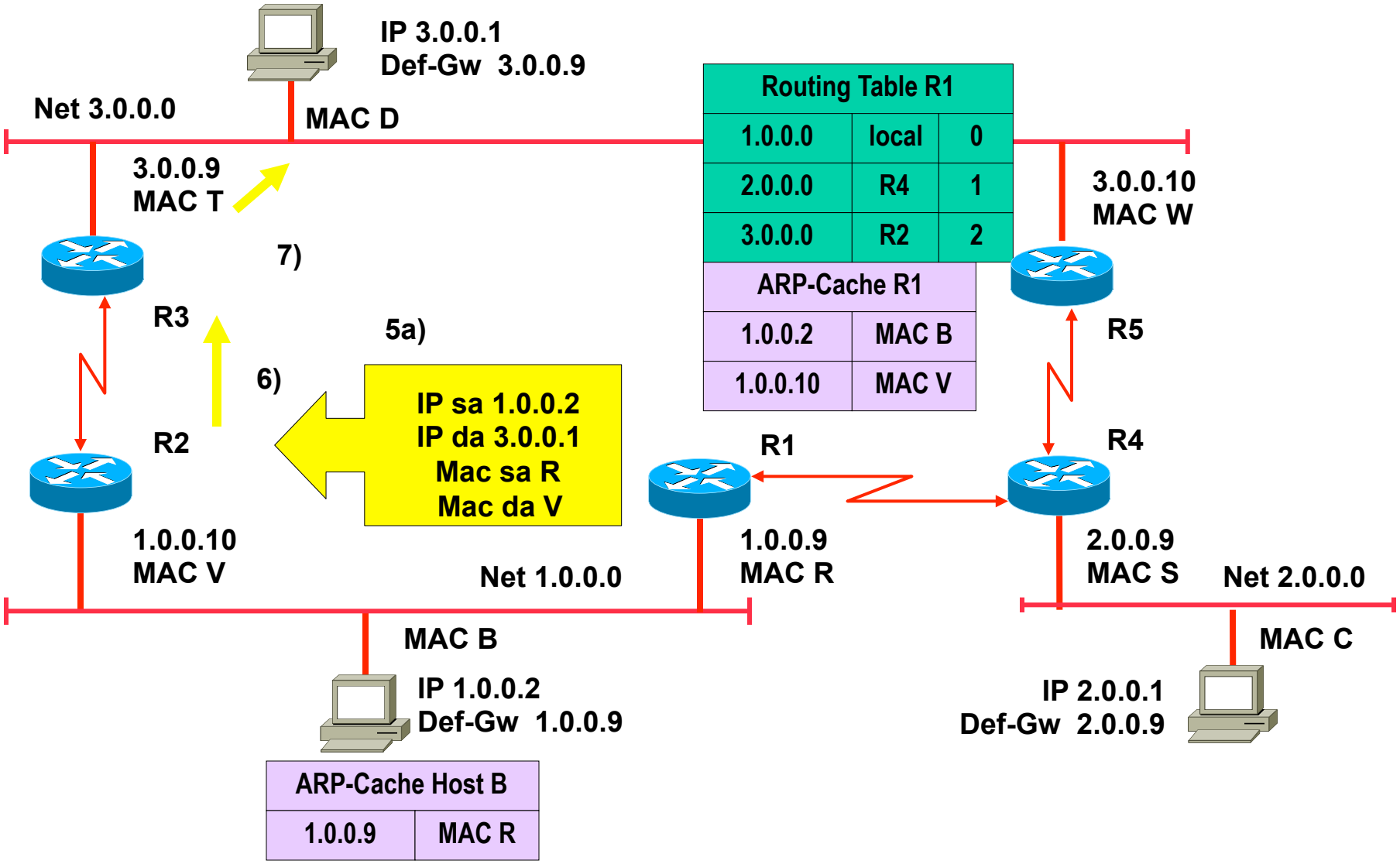
# Delivery 1.0.0.2 -> 3.0.0.1



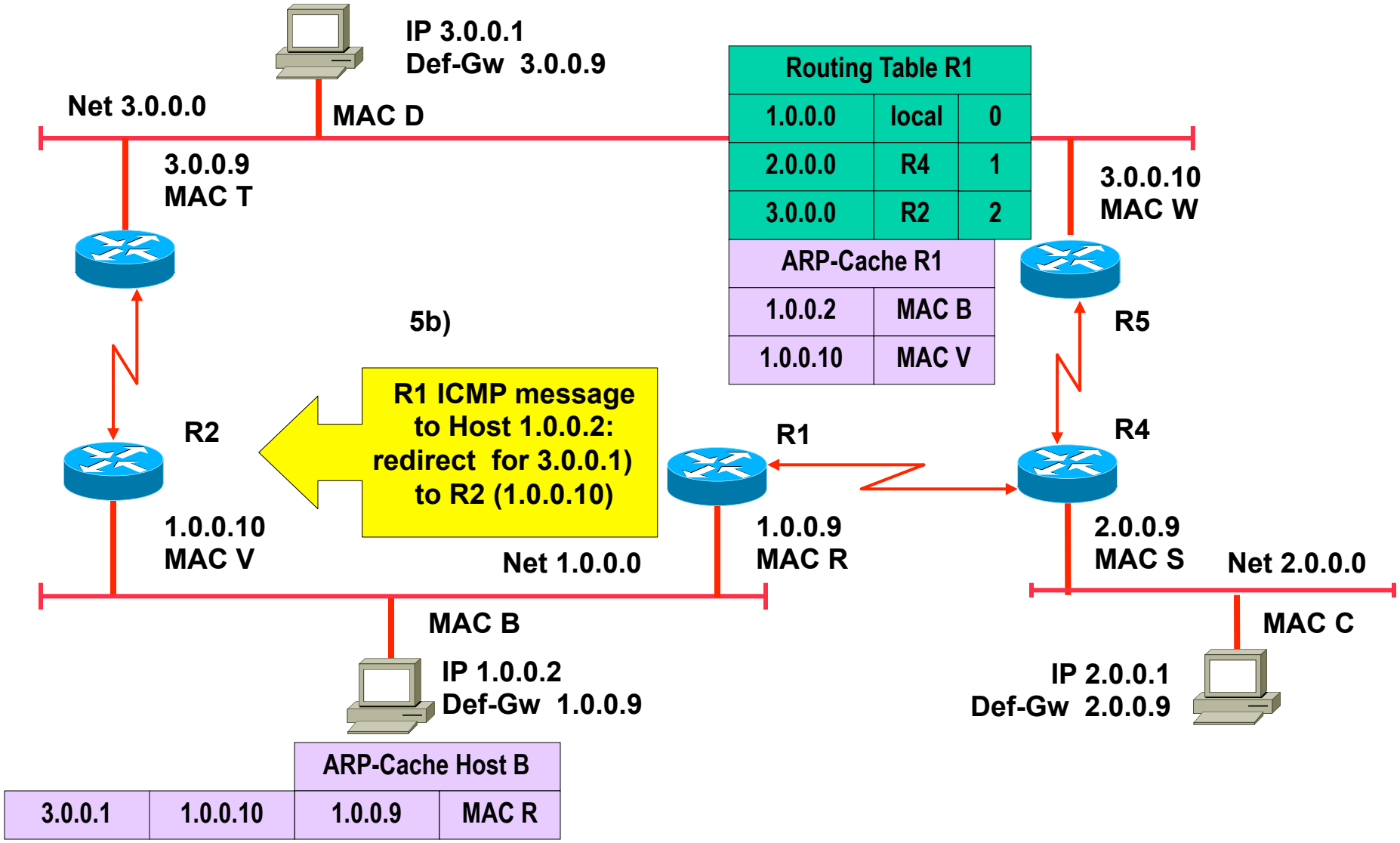
# Delivery 1.0.0.2 -> 3.0.0.1



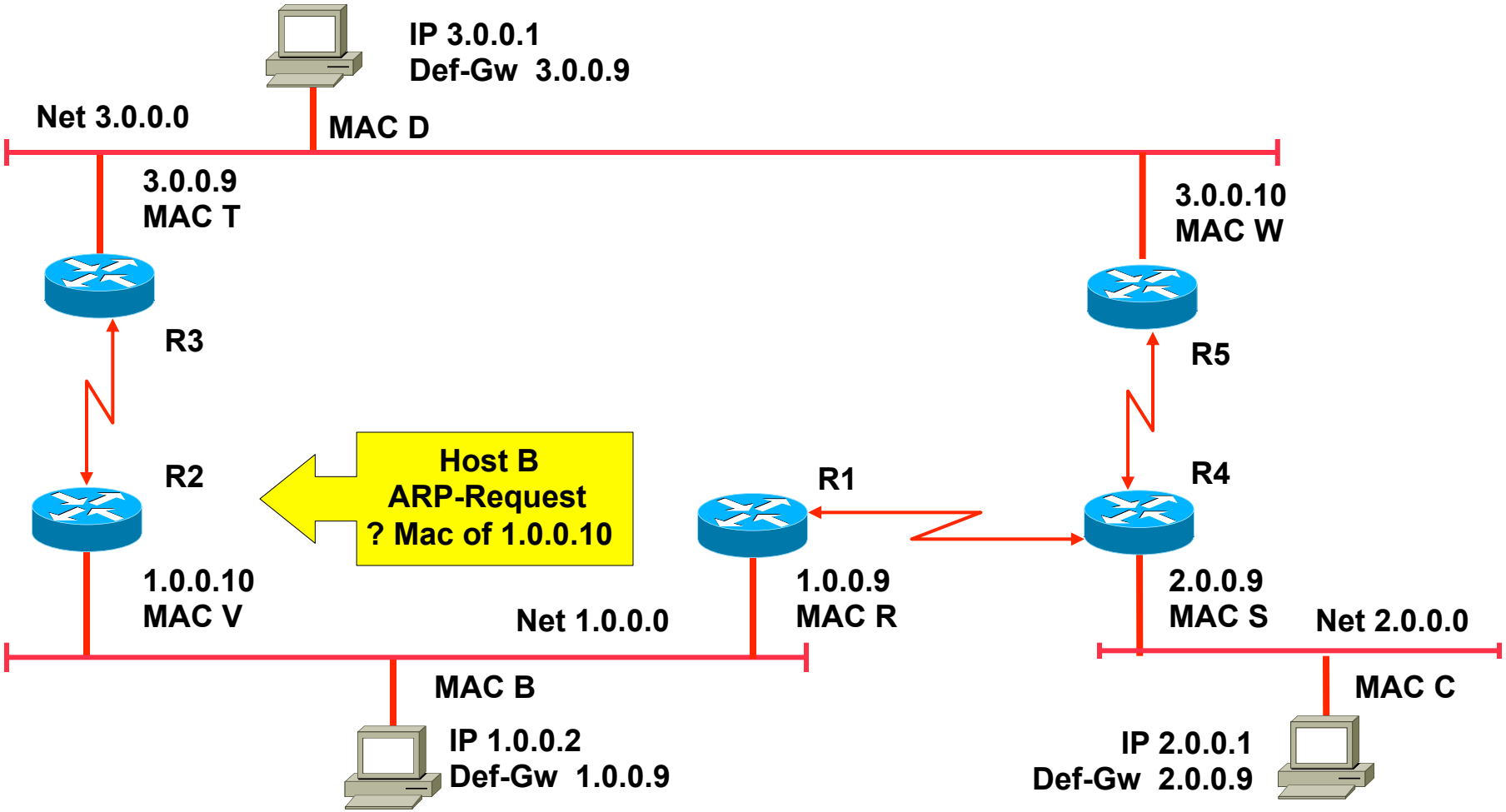
# Delivery 1.0.0.2 -> 3.0.0.1



# ICMP redirect

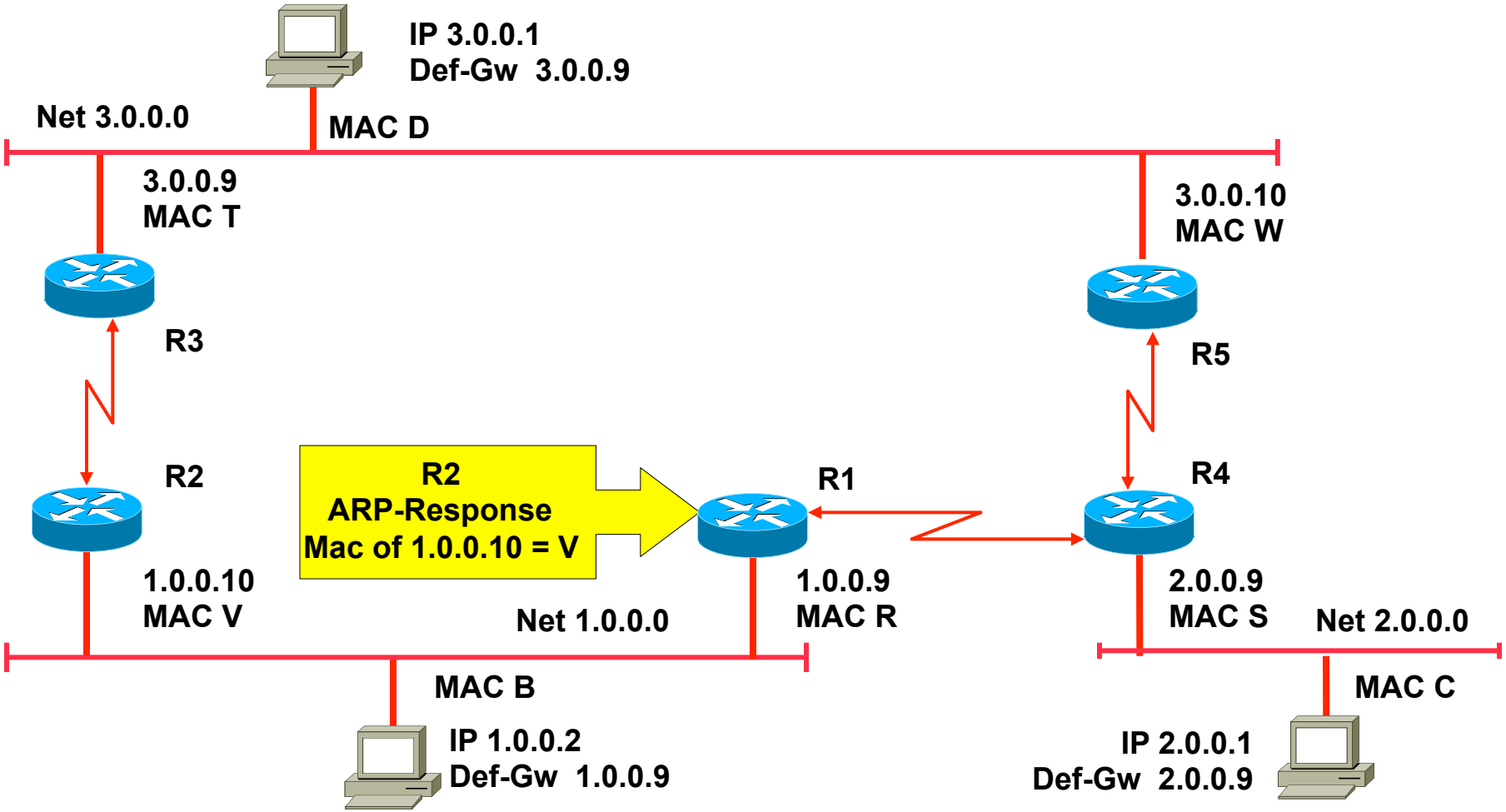


# Delivery 1.0.0.2 -> 3.0.0.1



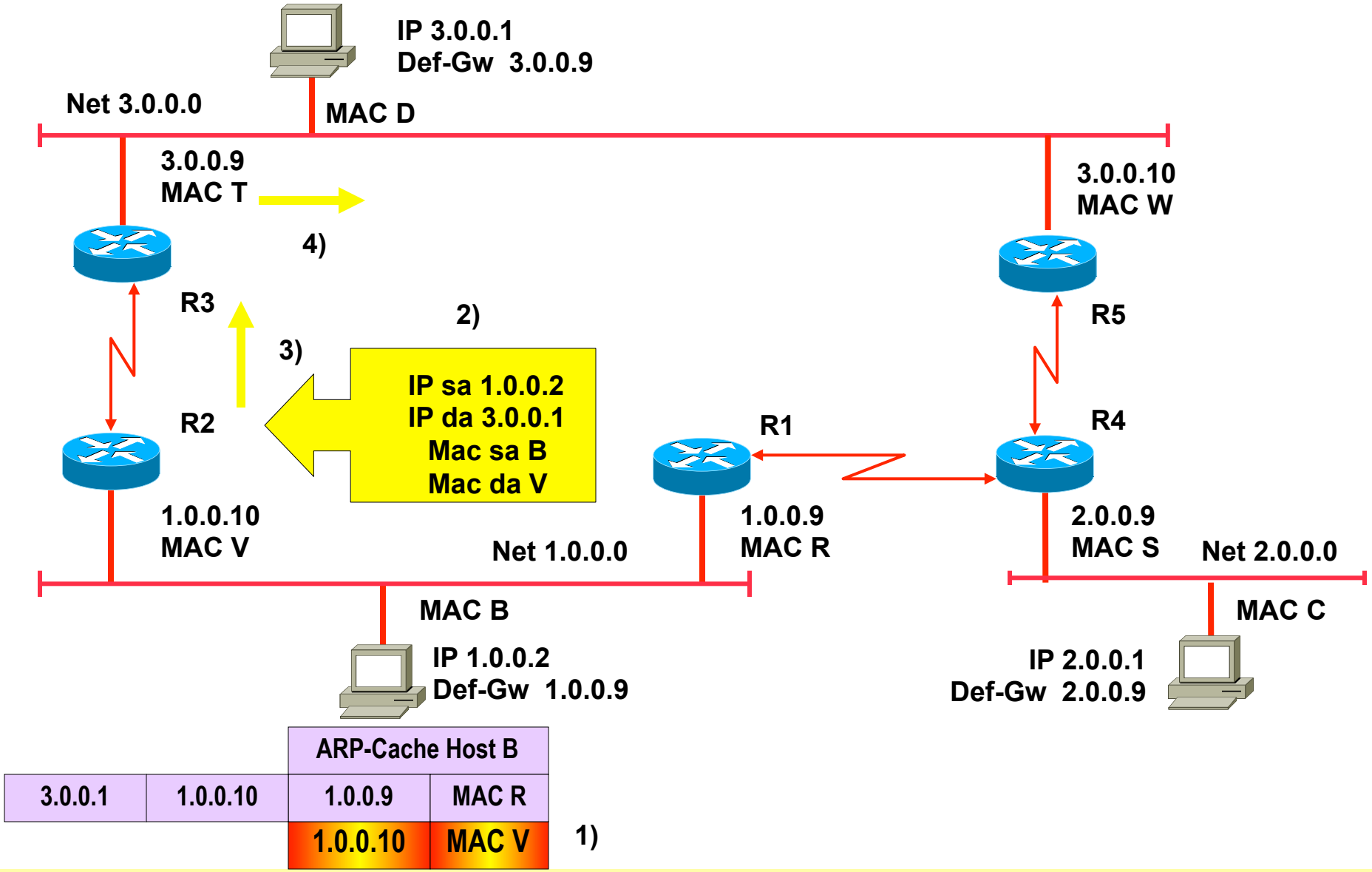

| ARP-Cache Host B | | | |
|---|---|---|---|
| 3.0.0.1 | 1.0.0.10 | 1.0.0.9 | MAC R |

# Delivery 1.0.0.2 -> 3.0.0.1

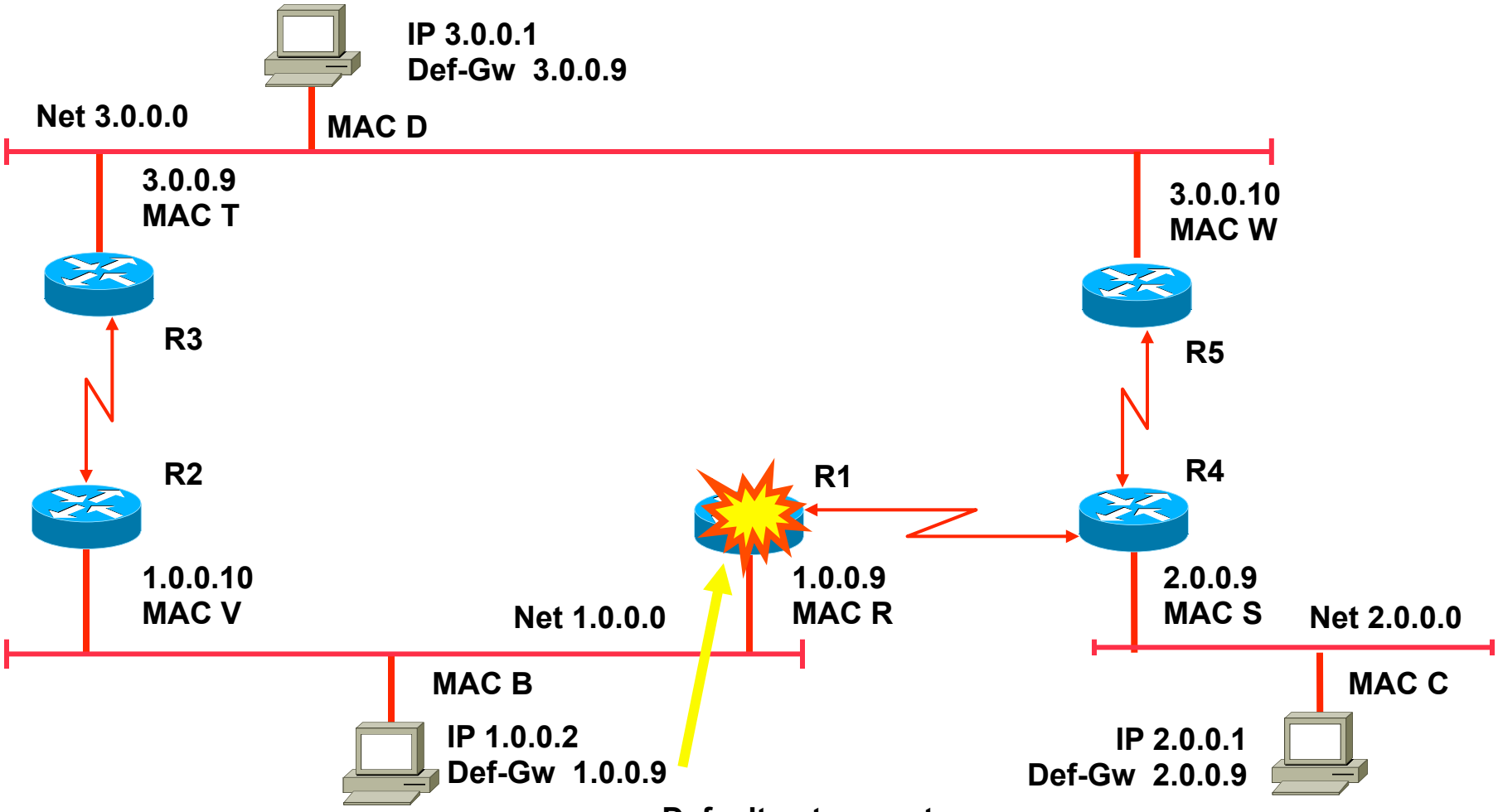



| ARP-Cache Host B | | | |
|---|---|---|---|
| 3.0.0.1 | 1.0.0.10 | 1.0.0.9 | MAC R |
| | | 1.0.0.10 | MAC V |

# Next Packet 1.0.0.2 -> 3.0.0.1



# Unavailability of R1:
# System B losses connectivity to Net 3.0.0.0 or 2.0.0.0




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

Default gateway at system B still points to router 1.0.0.9 !!!

# First Hop Redundancy (Layer 3) 1

- **The problem:**
  - How can local routers be recognized by IP hosts?
  - Note: Normally IP host has limited view of topology
    - IP host knows to which IP subnet connected
    - IP host knows one "Default Gateway" to reach other IP networks
  - Static configuration of "Default Gateway" means:
    - Loss of the default router results in a catastrophic event, isolating all end-hosts that are unable to detect any alternate path that might be available
- **Two design philosophies:**
  - Solve the problem at the IP host level
    - OS of the IP host has to support an appropriate functionality
  - Solve the problem at the IP router level
    - OS of the IP host has to support the basic functionality only
      - That is static configuration of one "Default Gateway"
    - Appropriate functionality needed at the router

# First Hop Redundancy (Layer 3) 2

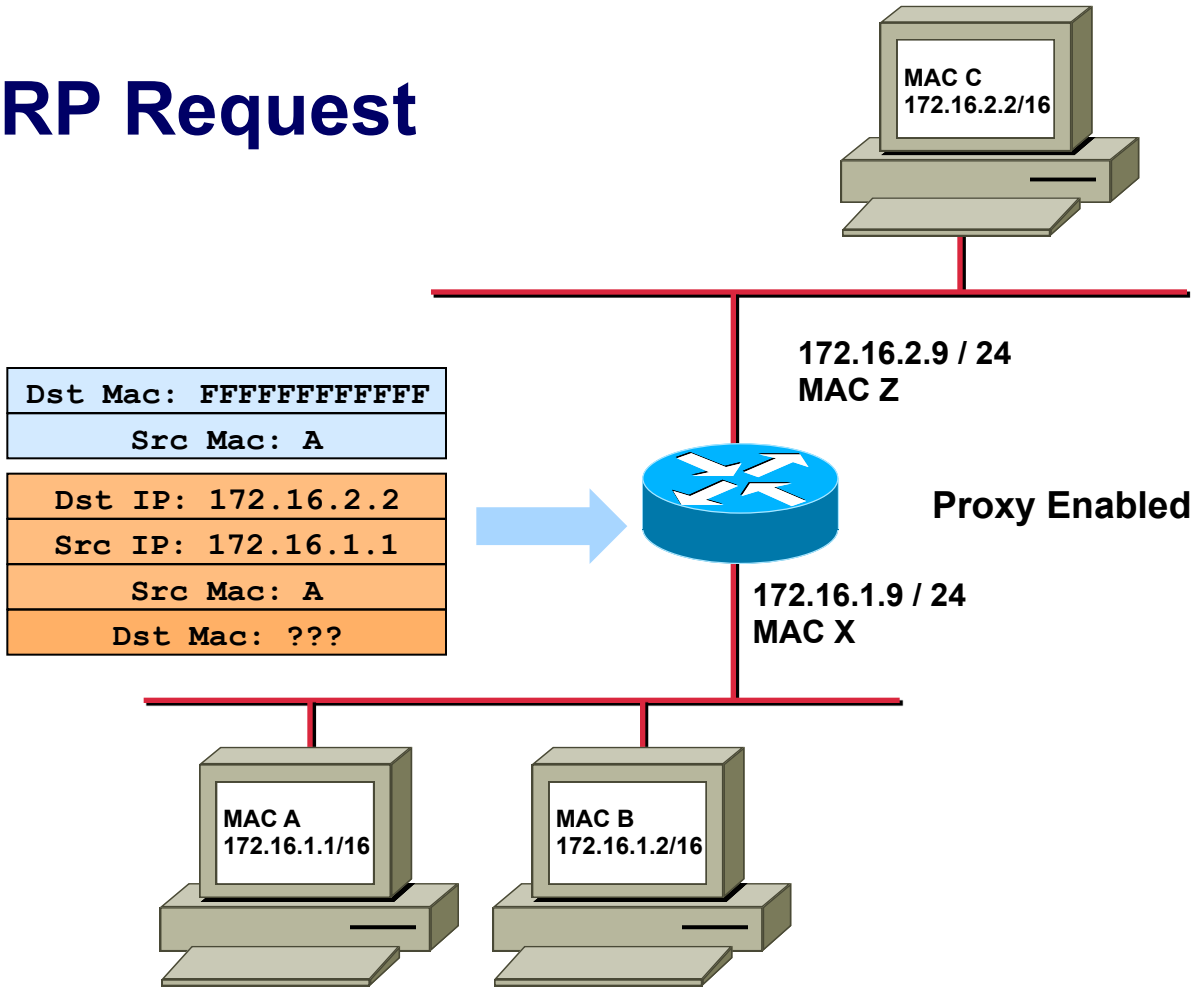
- **Methods for solving it at the IP host level:**
  - Proxy ARP
  - IRDP (ICMP Router Discovery Protocol)
  - DHCP (Dynamic Host Configuration Protocol)
  - IP Routing (RIPv2, OSPF)
- **Methods for solving it at the IP router level:**
  - HSRP (Hot Standby Router Protocol)
    - Cisco proprietary
  - VRRP (Virtual Router Redundancy Protocol)
    - Same as HSRP but open RFC
  - GLBP (Gateway Load Balancing Protocol)
    - Cisco proprietary
    - Not handled in this lecture

# Old Proxy ARP Usage

- **Old method for migration from transparent bridging to IP routing**
  - Two LANs connected by a transparent bridge (=broadcast domain) using a given IP Net-ID should be decoupled by a router
  - IP address were already assigned to the LAN segments in such a way that IP subnets can be built by the replacing router
  - Now by enabling proxy ARP gateway functionality on the router the host can still use their old subnet mask in order to communicate with all other stations
  - The proxy ARP gateway of the router will answer ARP requests
  - Term “proxy” means “instead of”
    - Some system is doing some function instead of the expected system
- **Replaced nowadays by usage of IP subnetting**
  - on all systems

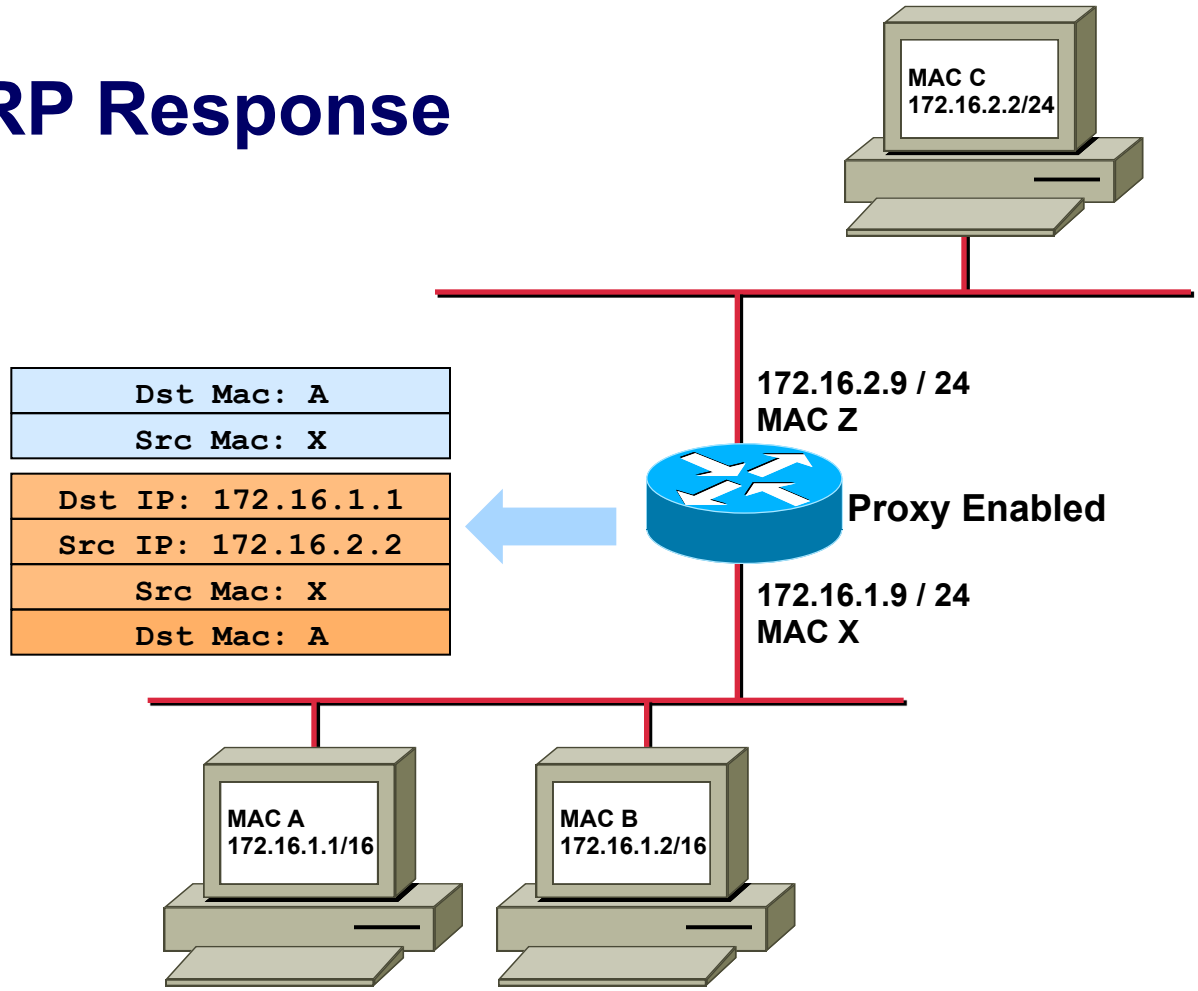
# Old Proxy in Action (1)

## Proxy ARP Request



# Old Proxy in Action (2)

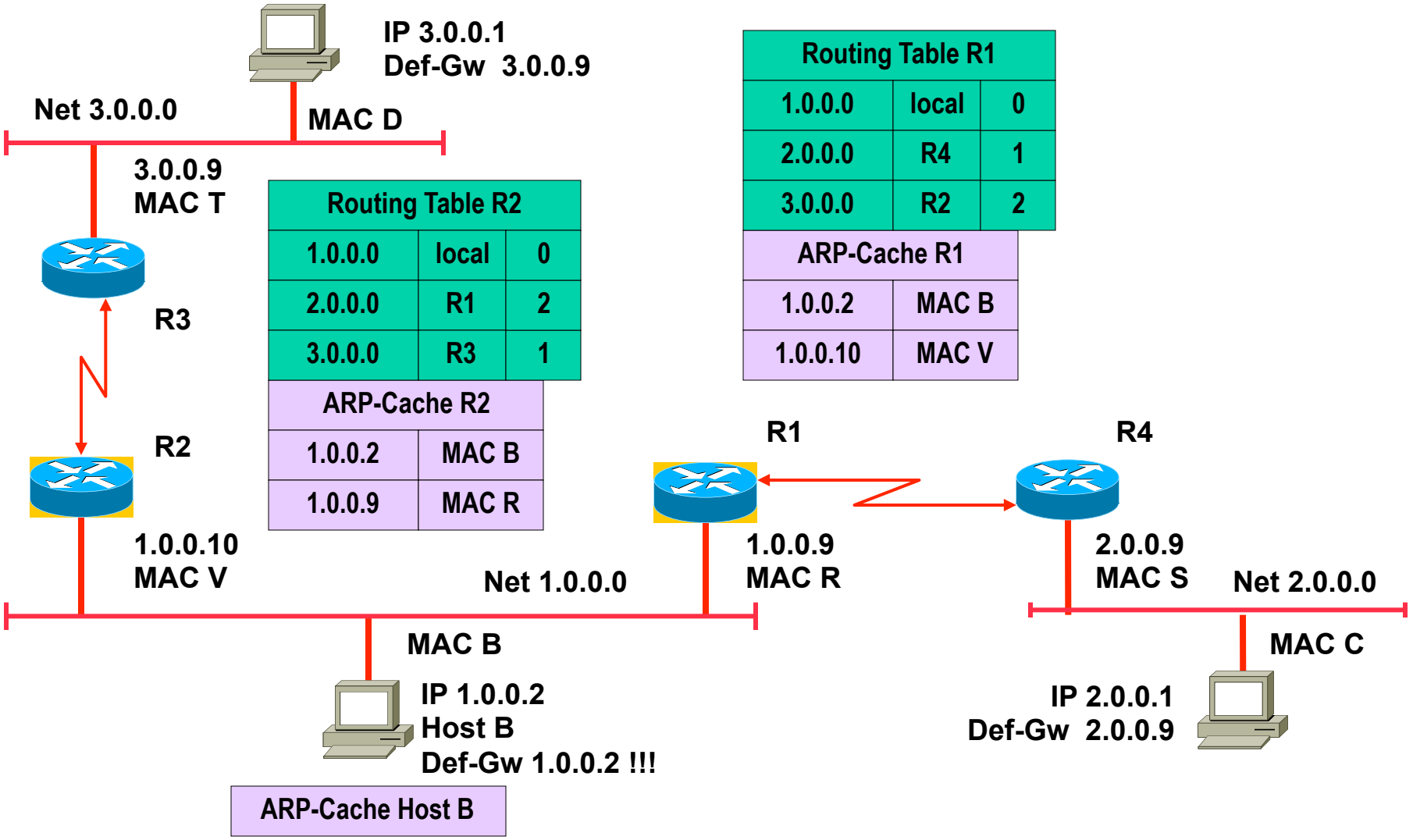
## Proxy ARP Response



# Proxy ARP Usage Nowadays

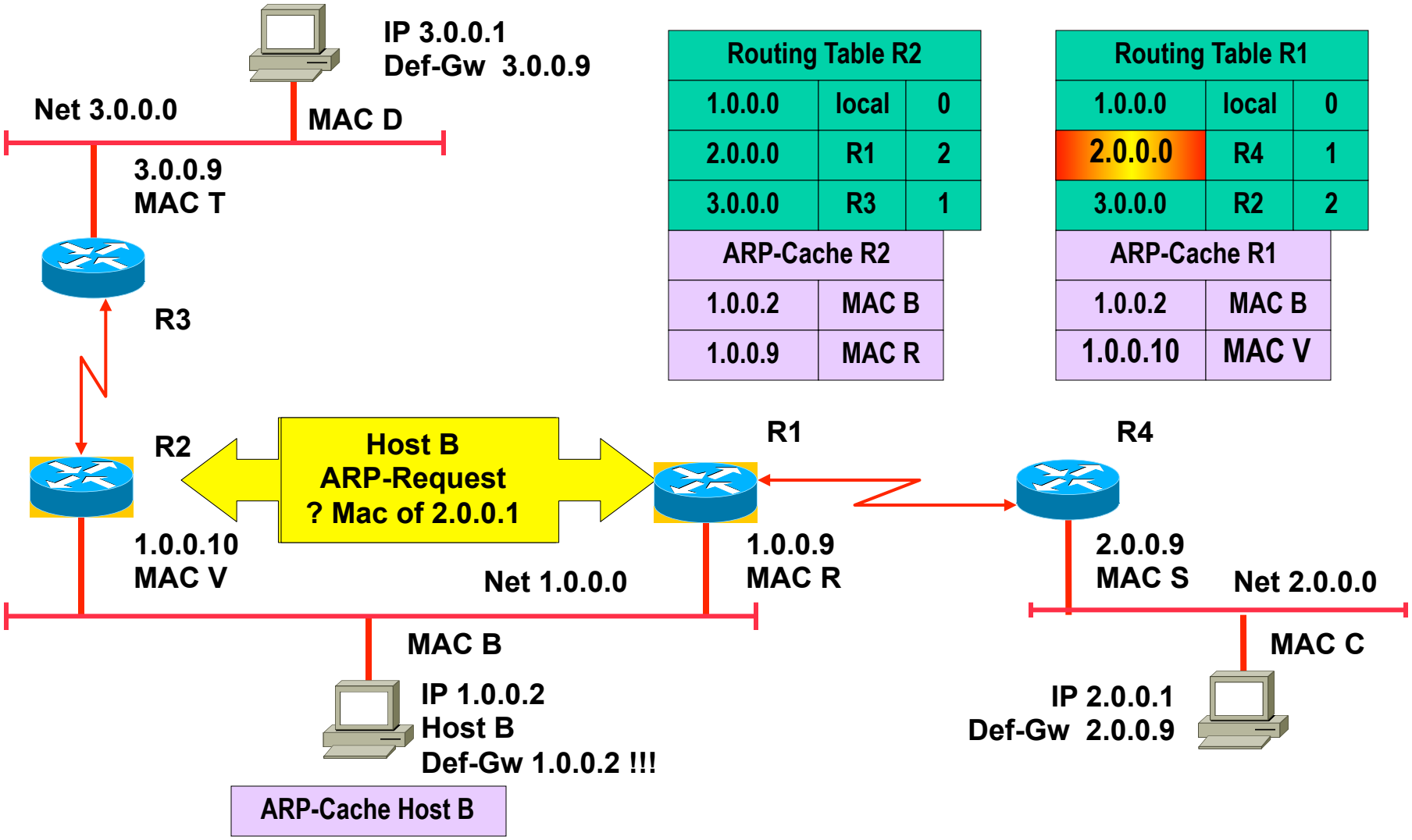
- **Proxy ARP is can be used if an IP host didn't know the address of the default gateway or want to find it dynamically:**
  - Normally in an IP host a static entry will tell the IP address of the router
    - If an IP datagram has to be sent to a non-local Net-ID, an ARP request will find the MAC address of the default gateway
  - With proxy ARP extensions in the IP host and with proxy ARP support enabled 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
  - 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)

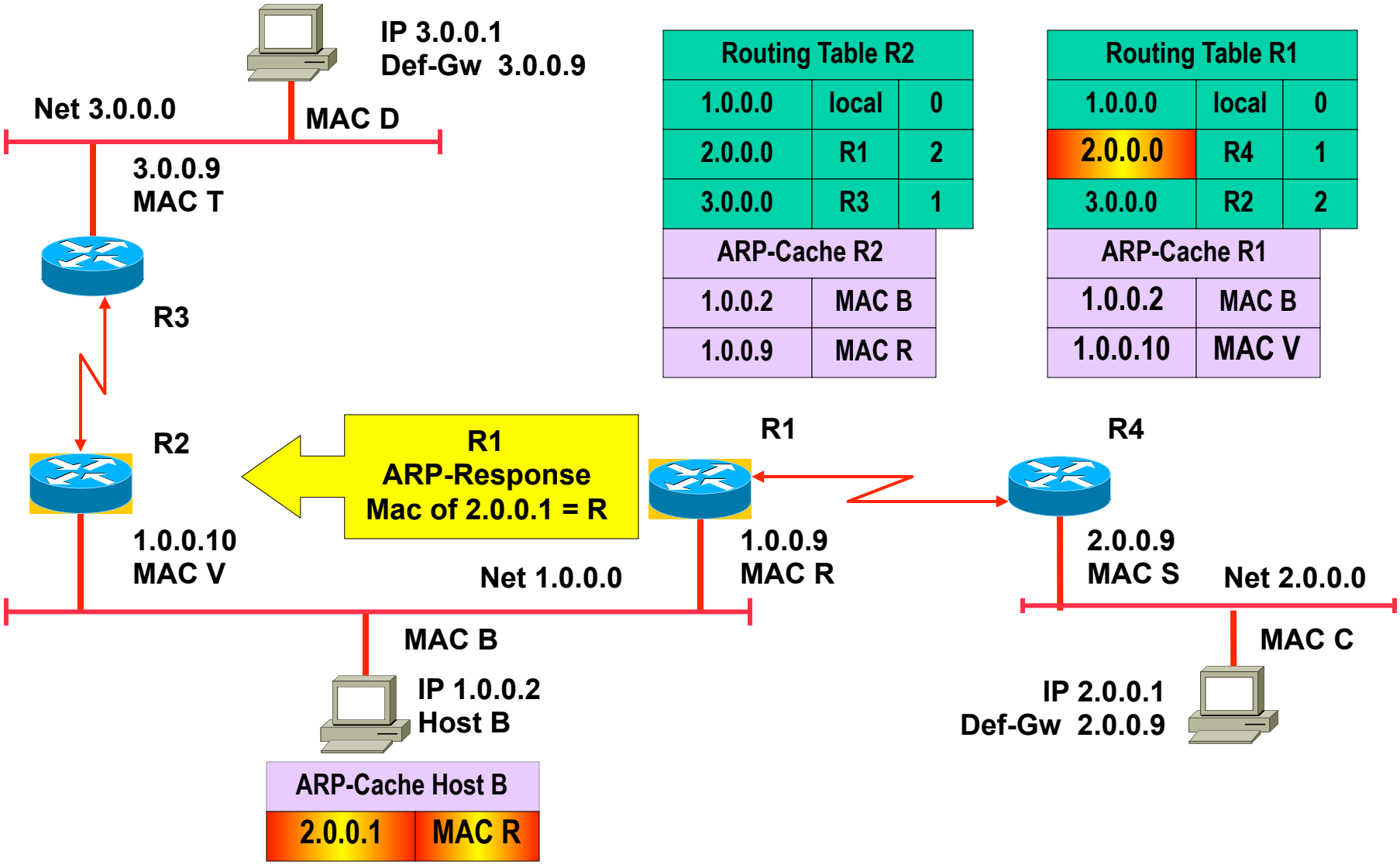



R1 and R2 are proxy ARP enabled; Host B sends ARP also for net-ID unequal own net-ID

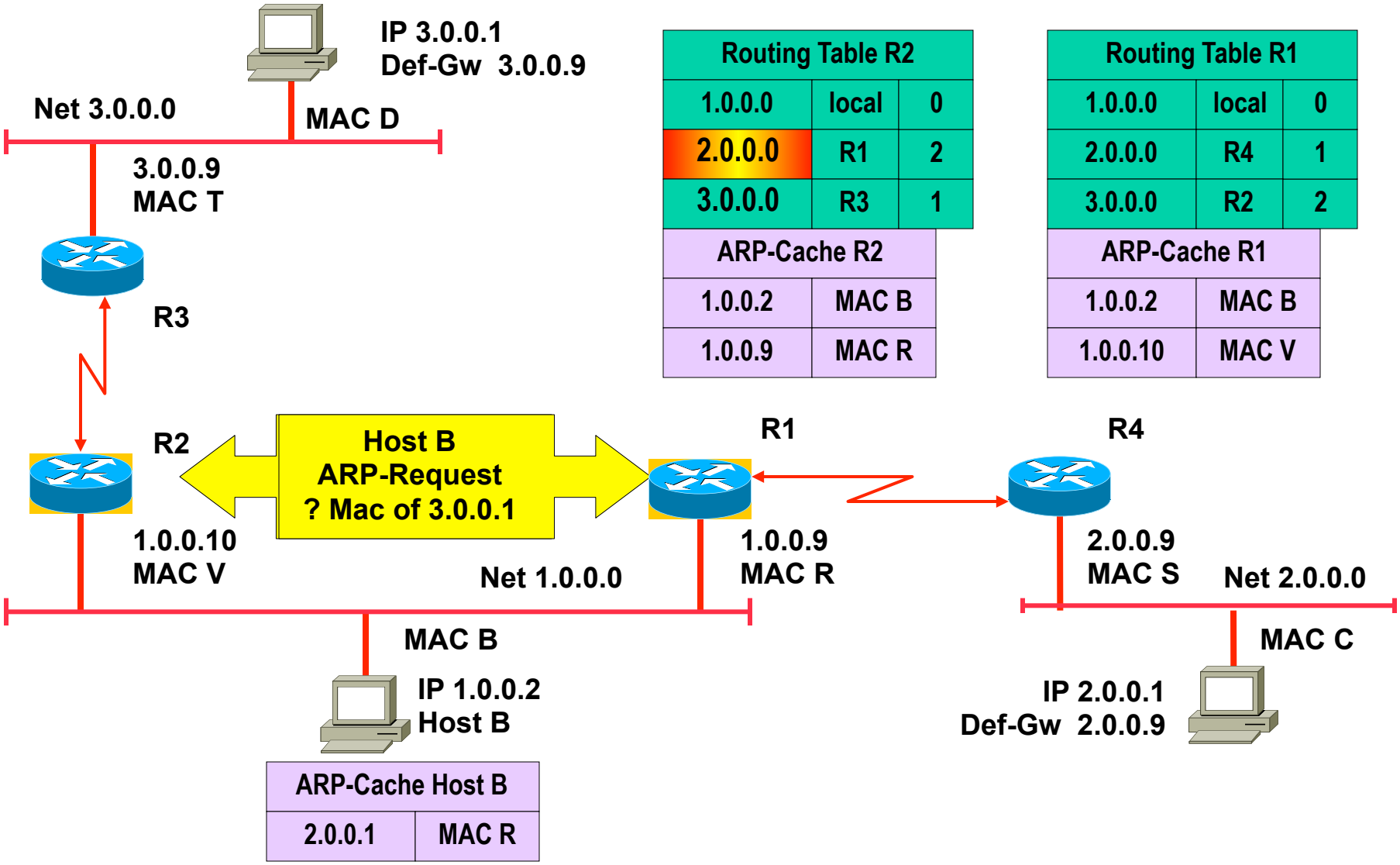
# 1.0.0.2 -> 3.0.0.1 / 2.0.0.1 with proxy ARP (2)



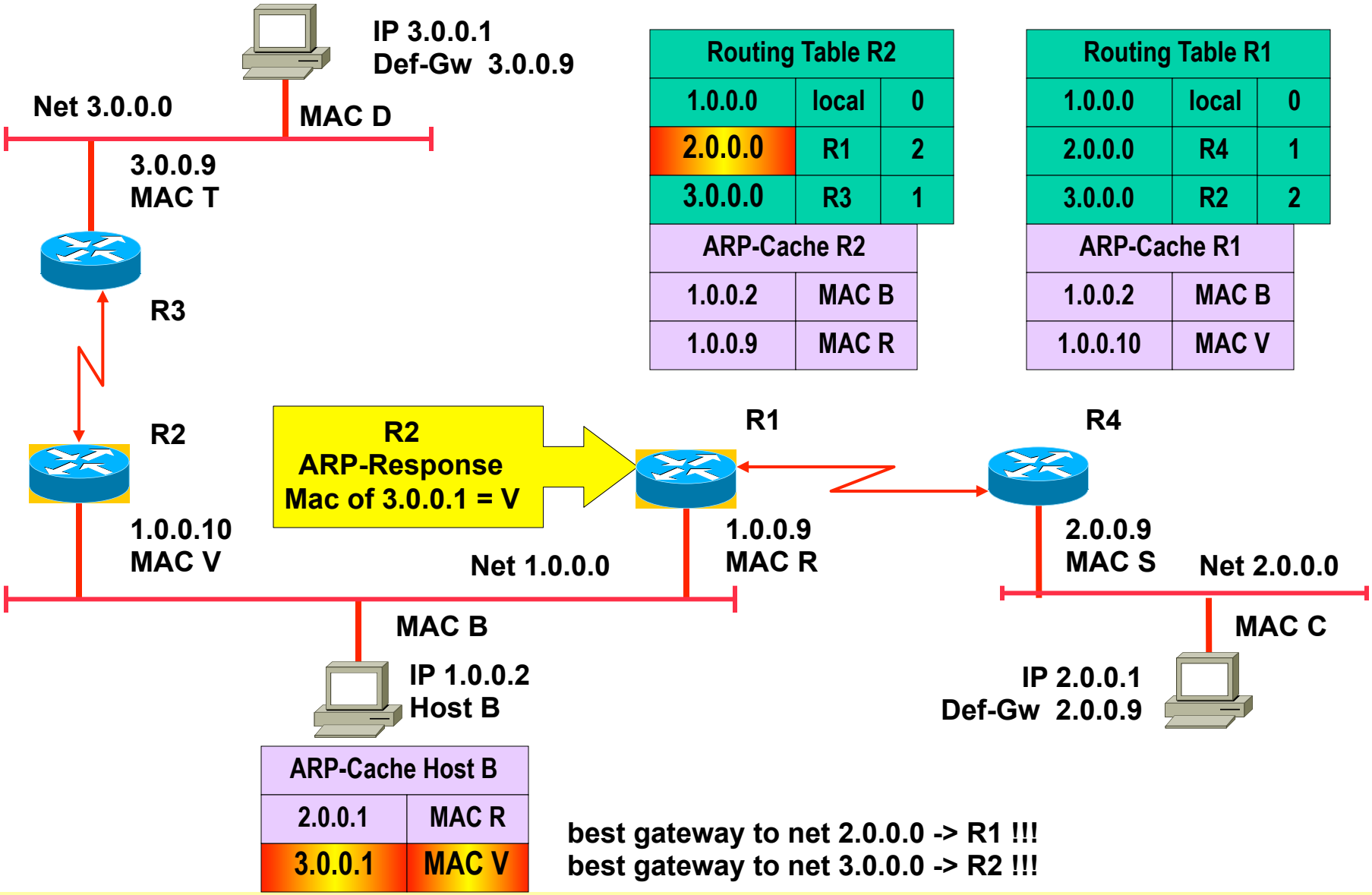
# 1.0.0.2 -> 3.0.0.1 / 2.0.0.1 with proxy ARP (3)



# 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)




| 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 |

| ARP-Cache Host B | |
|---|---|
| 2.0.0.1 | MAC R |
| 3.0.0.1 | MAC V |

best gateway to net 2.0.0.0 -> R1 !!!
best gateway to net 3.0.0.0 -> R2 !!!

# Other Techniques to Solve the Problem 1

- **IRDP**
  - ICMP Router Discovery Messages (RFC 1256)
  - Routers periodically advertise their IP address on a shared media together with an preference value and a lifetime
    - ICMP Router Advertisement Message
  - Hosts may listen to these messages to find out all possible Default Gateways
    - Or may ask by sending an ICMP Router Solicitation Message
- **DHCP**
  - Dynamic Host Configuration Protocol (RFC 2131)
  - More than one Default Gateway can be specified
  - Every Default Gateway has a preference value

# Other Techniques to Solve the Problem 2

- **With IDRP and DHCP**
  - You still depend on OS functionality in order to trigger switchover between redundant local routers
    - How often the currently selected router will be tested for reachability? What is if the currently selected router is reachable via LAN but networks behind are not reachable?
- **Therefore running a classical IP routing protocol on the IP host would be optimal**
  - RIPv2
    - But slow convergence if the currently selected router fails, no hello messages hence 180 seconds for recognizing that event
  - OSPF
    - Fast convergence because of hello messages, the best but the most complex solution
  - But IP routing on an IP host for that reason is seldom done

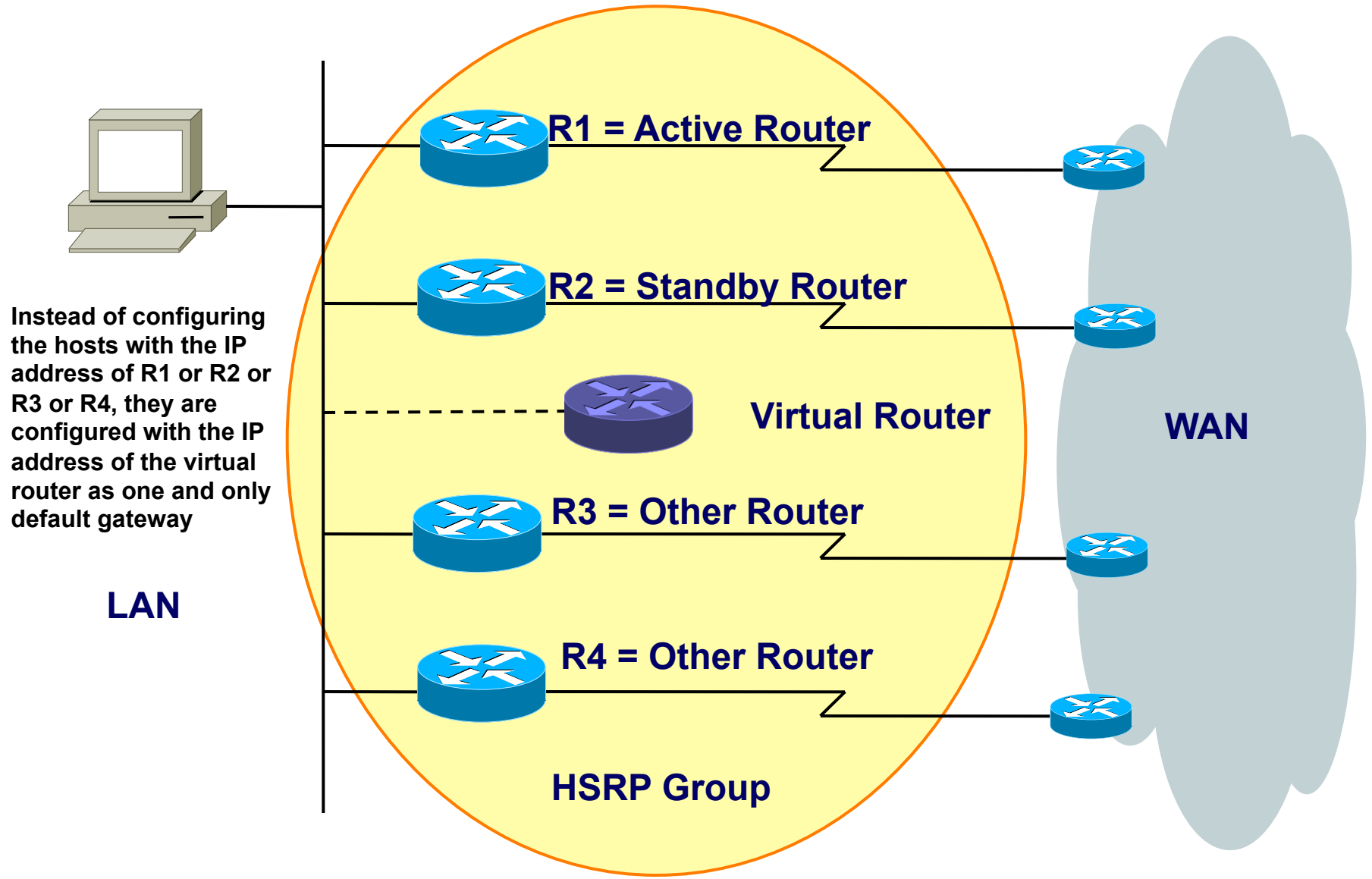
# Agenda

- **Introduction**
  - Short History of the Internet (not part of the exam!)
  - Basic Principles
- **IP**
  - IP Protocol
  - IP QoS
  - Addressing
  - Classful  versus Classless (not part of the exam!)
- **IP Forwarding**
  - Principles
  - ARP
  - ICMP
  - PPP
- **First Hop Redundancy**
  - Proxy ARP, IDRP
  - HSRP
  - VRRP (not part of the exam!)

# HSRP – Hot Standby Router Protocol

- **HSRP (Hot Standby Router Protocol)**
  - Proprietary protocol invented by Cisco
  - RFC 2281 (Informational)
- **Basic idea: a set of routers pretend a single (virtual) router to the IP hosts on a LAN**
  - Active router
    - One router is responsible for forwarding the datagrams that hosts send to the virtual router
  - Standby router
    - If active router fails, the standby takes over the datagram forwarding duties of the active router
  - Conspiring routers form a so called HSRP group

# HSRP Overview



# HSRP Principles (1)

- **Basics:**
  - A group of routers forms a HSRP group
  - The group is represented by a virtual router
    - With a virtual IP address and virtual MAC address for that group
  - IP hosts are configured with the virtual IP address as default gateway
  - One router is elected by HSRP as the active router, one router is elected as the standby router of that group
    - HSRP messages are UDP messages to port 1985, addressed to IP multicast 224.0.0.2 using Ethernet multicast frames
      - Note HSRP version 1
  - Active router responds to ARP request directed to the virtual IP address with the virtual MAC address
  - Standby router supervises if the active router is alive
    - By listening to HSRP messages sent by the active

# HSRP Principles (2)

- **Roles:**
  - Active router
    - Is responsible for the virtual IP address hence attracts any IP traffic which should leave the subnet
  - Standby router
    - Takes over the role of the active router in case the active router fails for the subnet
  - Additional HSRP member routers - Other
    - Other routers are neither active nor standby. They just monitor the messages of the current active and standby routers and transition into one of those roles if the current router fails for the subnet
  - Virtual router
    - The virtual router is not an actual router
    - Rather, it is a concept of the entire HSRP group acting as one virtual router for the IP hosts of the given subnet

# HSRP Principles (3)

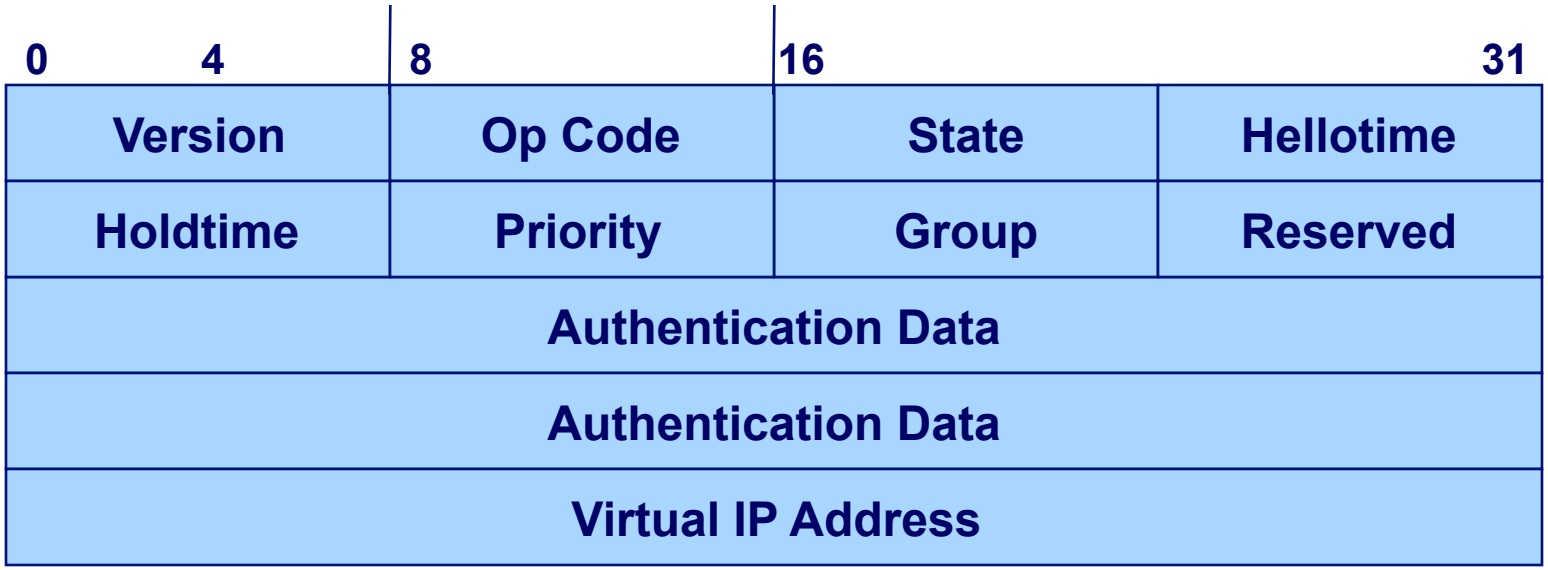
- **Roles (cont.):**
  - Active, Standby, Other defined by HSRP priority
  - Priority value can be configured
    - Default value is 100
  - The higher the better
    - Will become the active router after initialization
    - If priority is equal than the higher IP address decides
  - Preemption allows to give up the role of the active router
    - When a router with higher priority is reported by HSRP messages
  - Preemption happens
    - Either when the failed router comes back, a better router is activated or object tracking has changed priority

# HSRP Principles (4)

- **Two basic failover scenarios:**
  - 1) Active router is not reachable via LAN
    - Standby router will take over active role
    - A new standby router is elected from the remaining routers of a HSRP group
    - Timing depends on HSRP hello message interval and hold-time
      - Default hello-time = 3 seconds, default hold-time = 10 seconds
      - Note HSRP version 1
  - 2) Active router losses connectivity either to a WAN interface or losses connectivity to a given IP route
    - Tracking will lower the priority of the active router
    - If preemption is configured on all routers the standby router will take over
    - Remember: Preemption allows another router to take over the role of the active router even if the current active router does not fail

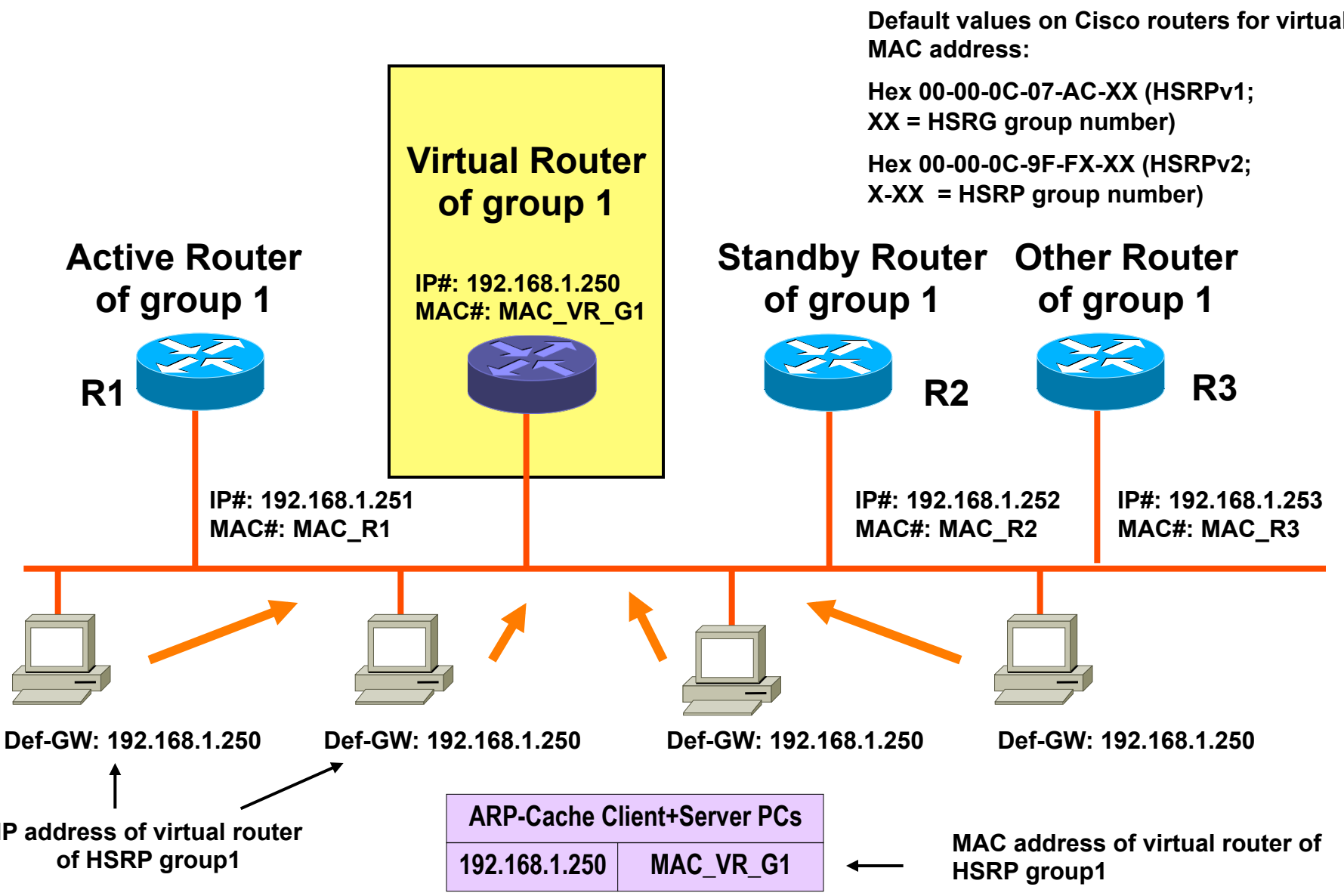
# HSRP Protocol Fields

- **Standby protocol runs on top of UDP (port 1985)**
  - IP packets are sent to IP multicast address 224.0.0.2 (HSRPv1) or 224.0.0.102 (HSRPv2) with a IP TTL = 1

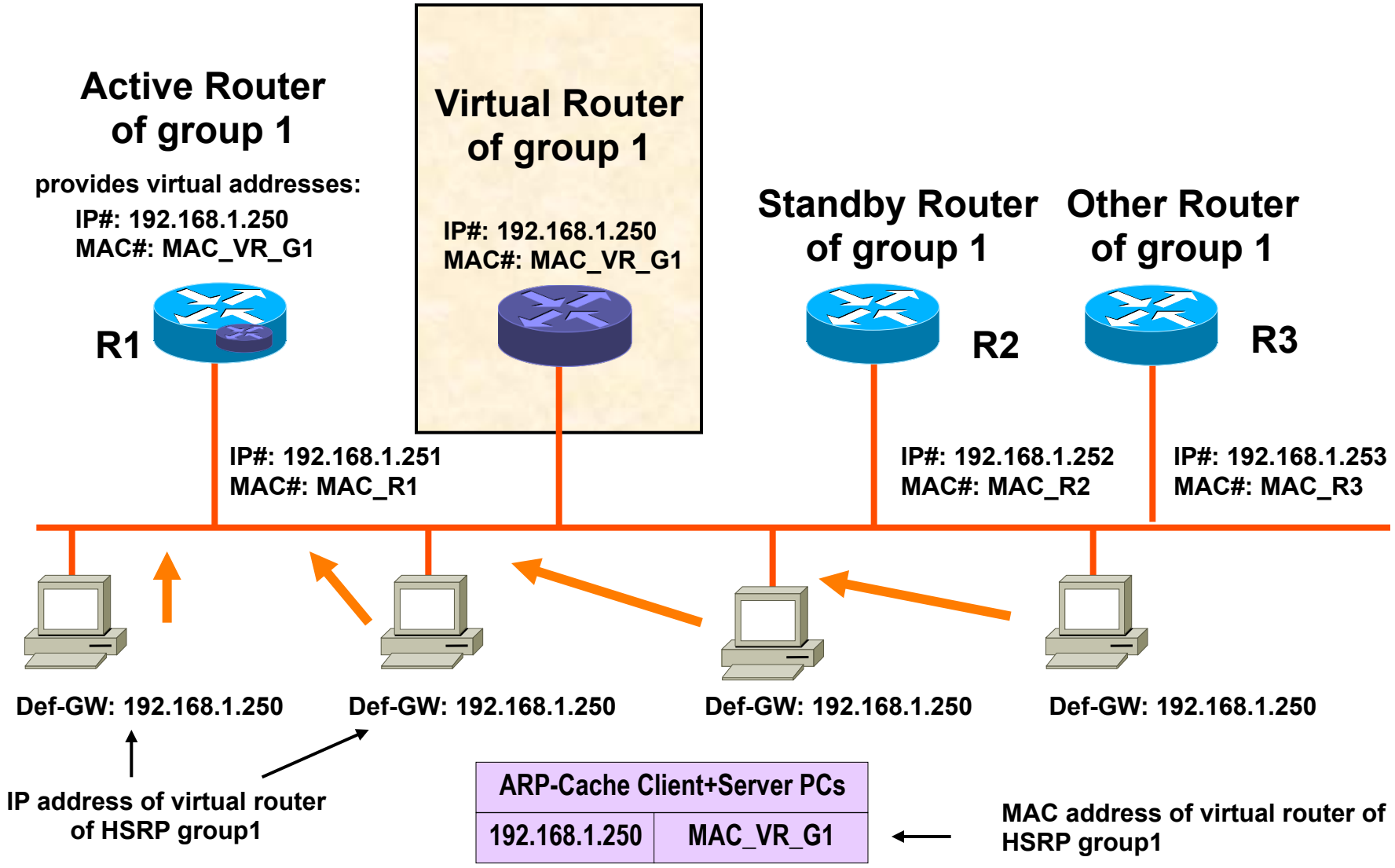



- **Version**: Version of the HSRP messages
- **Op code**: 4 types
  - **Hello**: Indicates that a router is running and is capable of becoming the active or standby router
  - **Coup**: When a router wishes to become the active router
  - **Resign**: When a router no longer wishes to be the active router
  - **Advertise**: Announce state of own HSRP interface
- **States**: Initial, learn, listen, speak, standby, active
- **Hellotime**: Contains the period between the hello messages that the router sends
- **Holdtime**: Amount of time the current hello message is valid
- **Priority**: Compares priorities of 2 different routers
- **Group**: Identifies standby group (0...255)
- **Authentication data**: Cleartext or MD5 signed hash

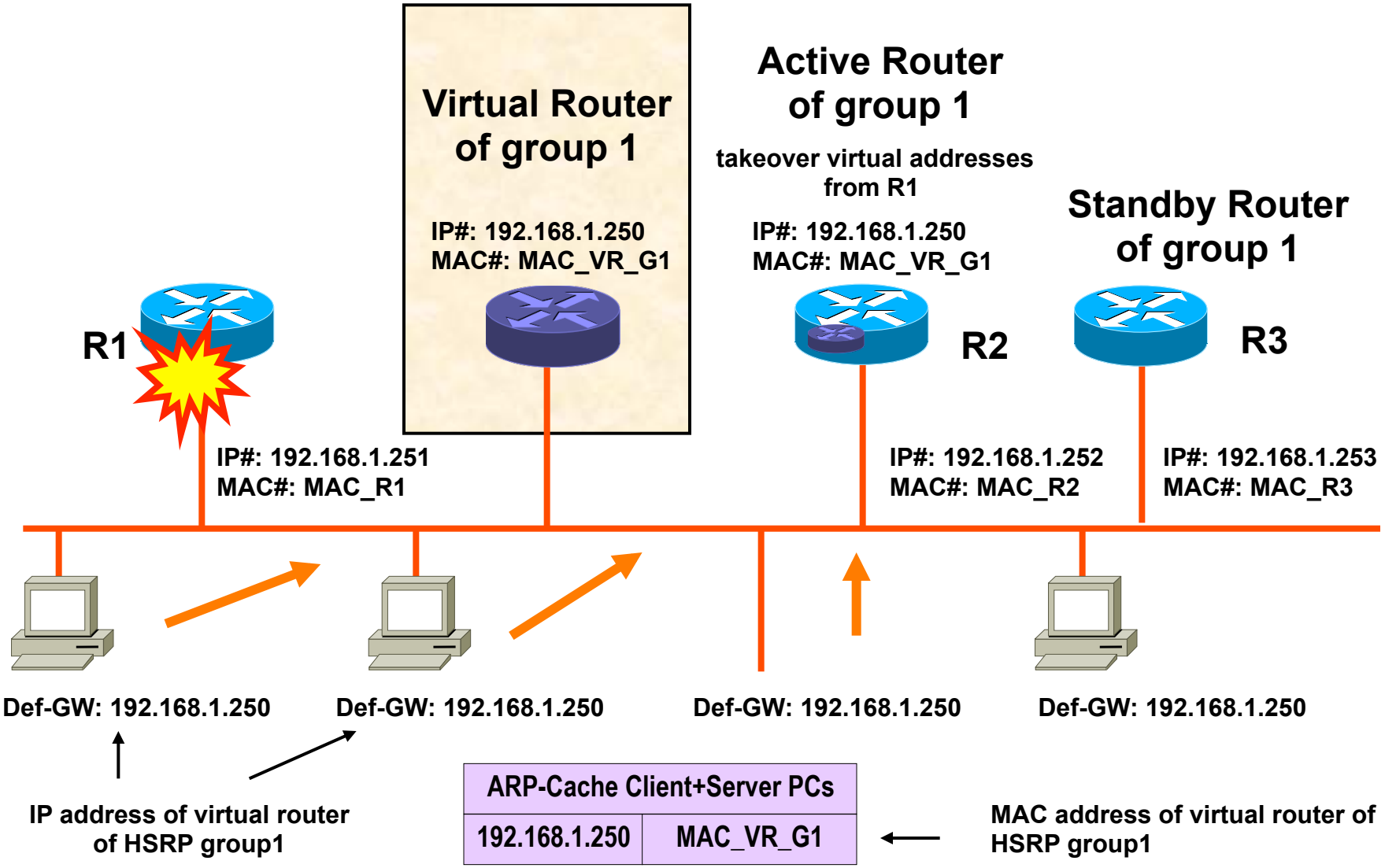
# HSRP:
# Real and Virtual IP Addresses / MAC Addresses



# HSRP in Action (1)



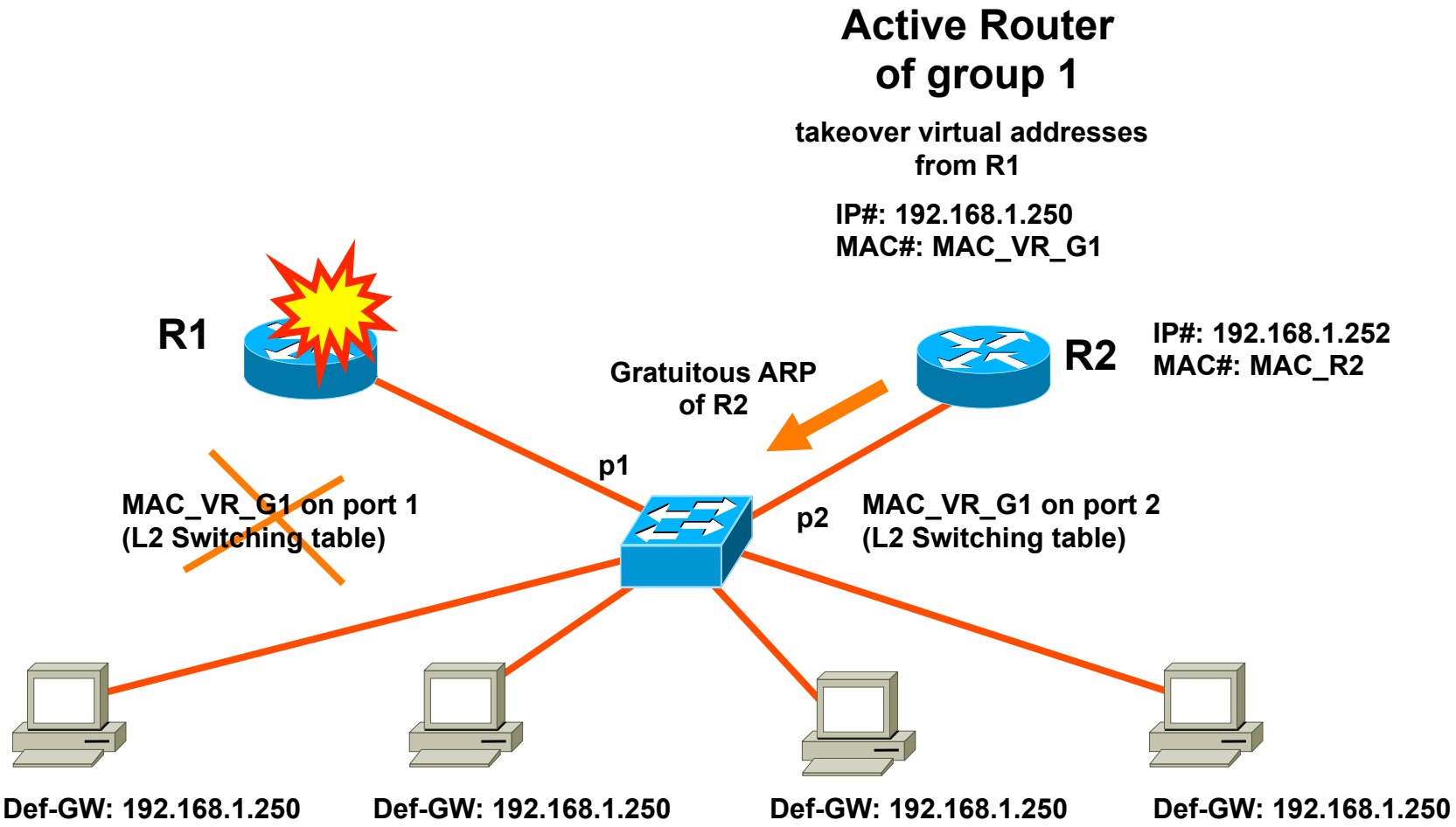
# HSRP in Action (2)



# HSRP Additional Aspects

- **L2 Ethernet Switching Table Refresh:**
  - Done by gratuitous ARP in case of switchover
- **Load Balancing:**
  - You can achieve this by specifying at least two different HSRP groups with complementary roles
- **HSRP Security**
  - Authentication of messages by generation of fingerprints and checking this fingerprints
    - Based on keyed MD5
  - Against HSRP spoofing

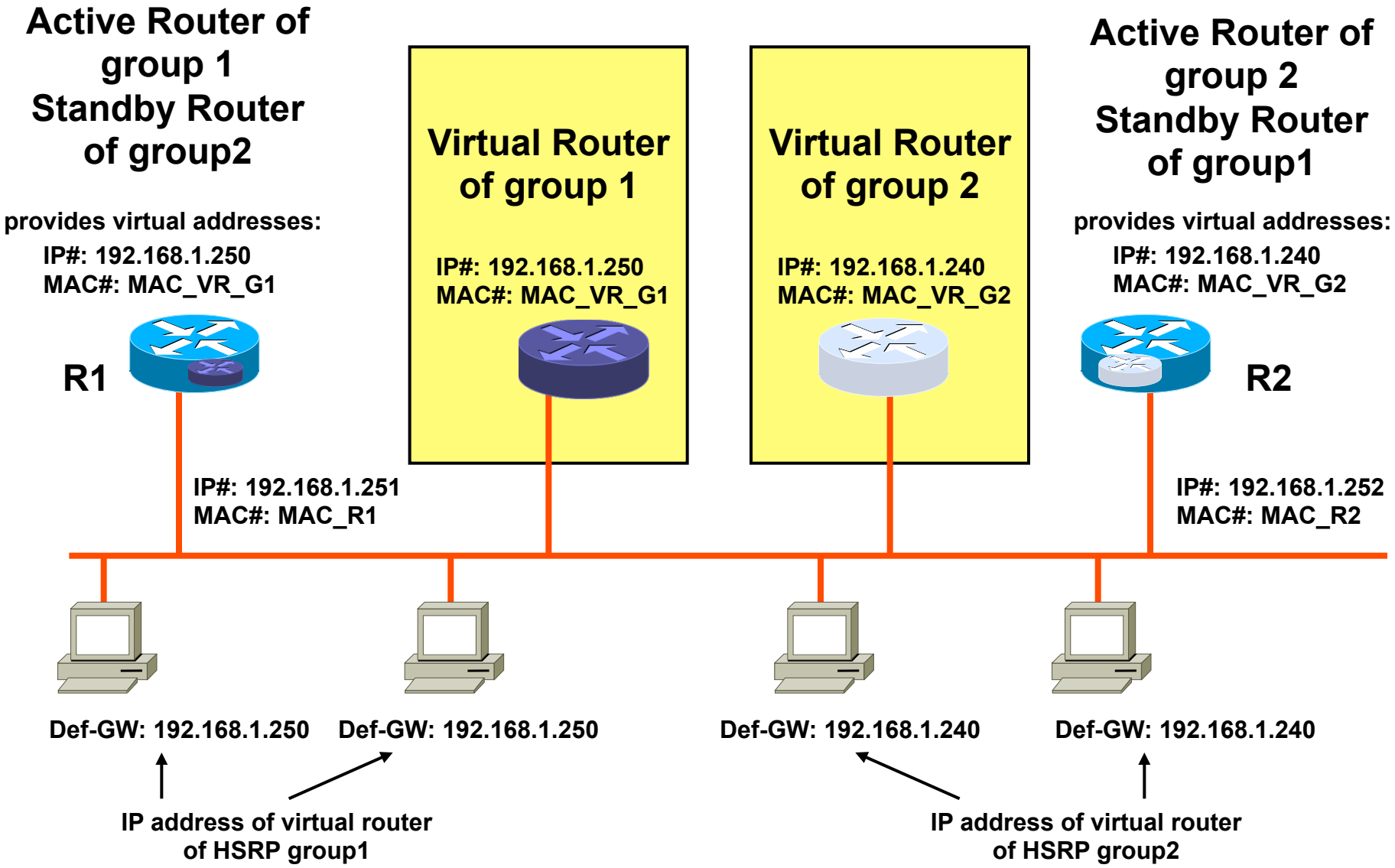
# HSRP – Gratuitous ARP



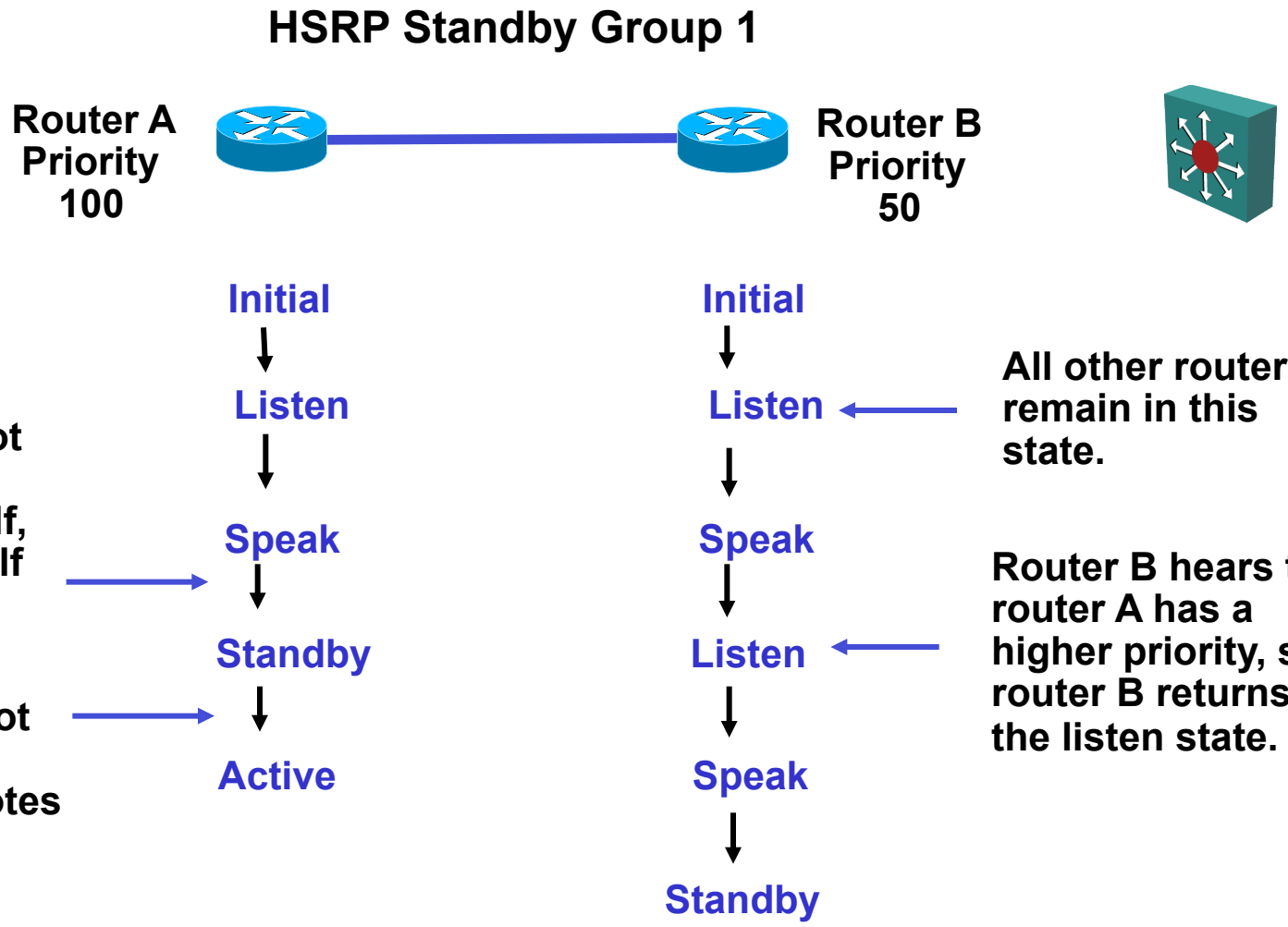

| ARP-Cache Client+Server PCs | |
|---|---|
| 192.168.1.250 | MAC_VR_G1 |

MAC address of virtual router of HSRP group1

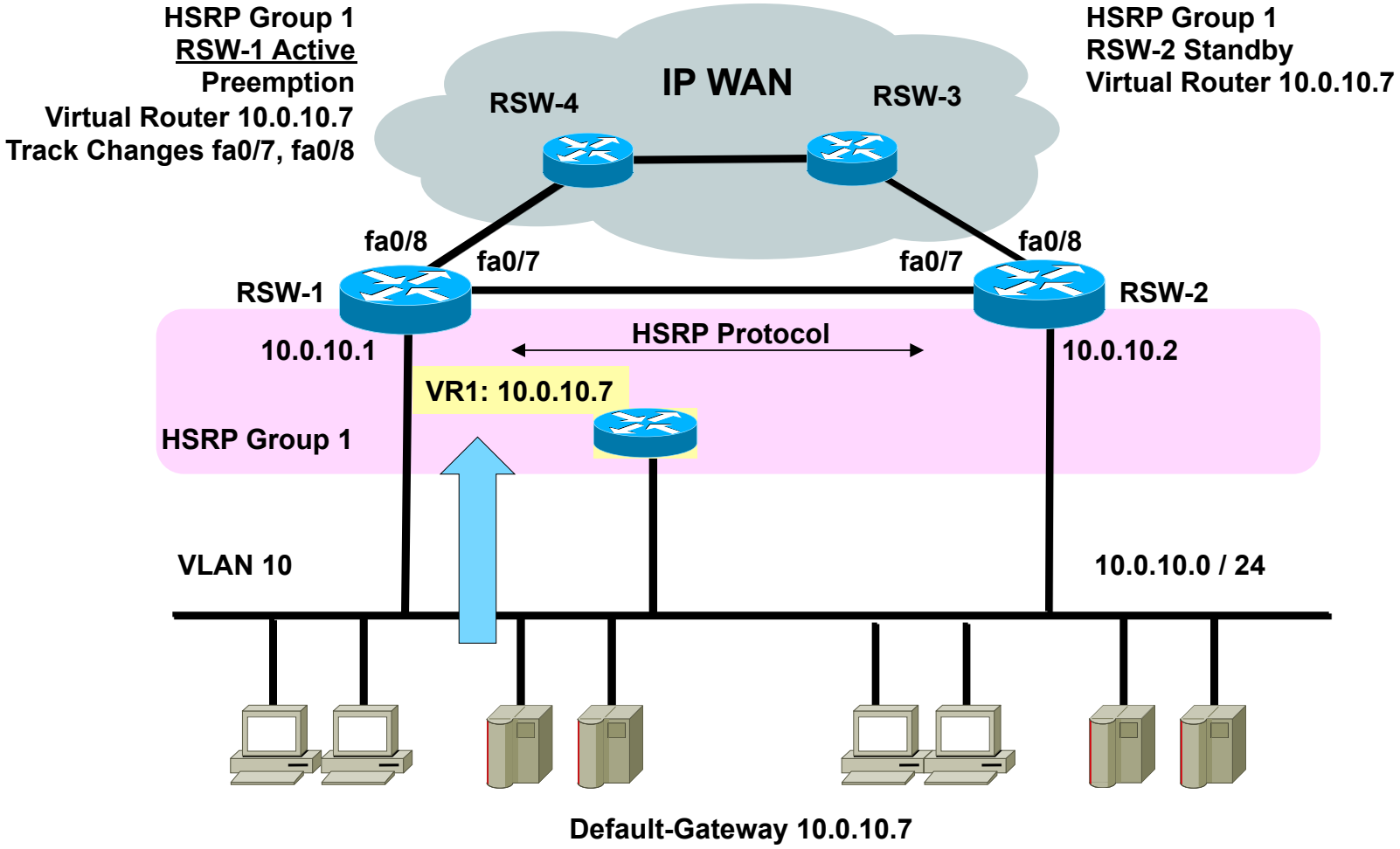
# HSRP Load Balancing



# HSRP States Details



# Basic HSRP Scenario (Cisco Example)

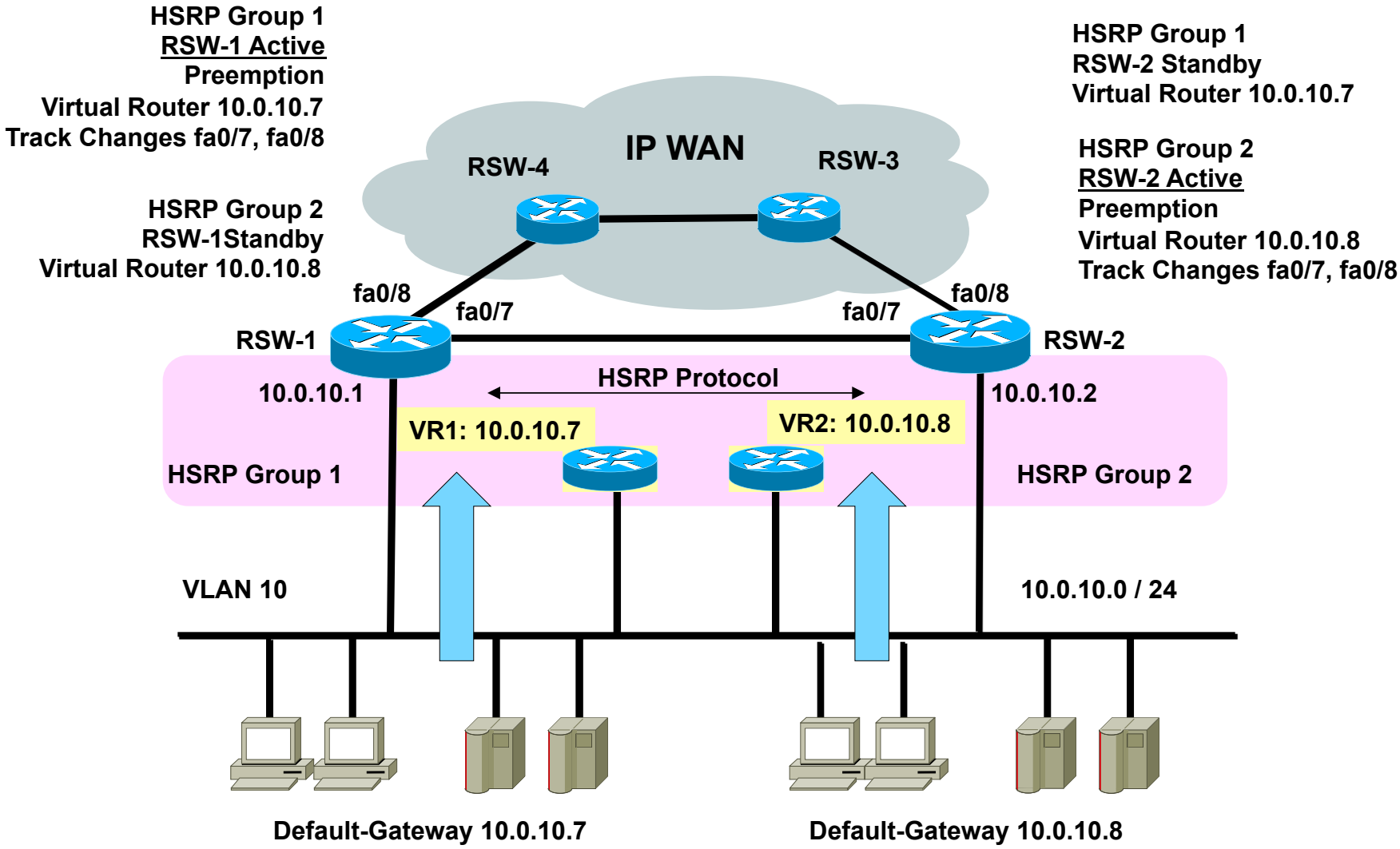



HSRP … Hot Standby Router Protocol

# Cisco IOS Configuration – Basic Scenario

- On RSW-1:
  - RSW-1(config)# track 101 interface fa0/7 line-protocol
  - RSW-1(config)# track 102 interface fa0/8 line-protocol
  - RSW-1(config)#  interface vlan10
  - RSW-1(config-if)# standby 1 ip 10.0.10.7
  - RSW-1(config-if)# standby 1 priority 150
  - RSW-1(config-if)# standby 1 timers 2 7
    - Tuning HSRP timers: hello = 2 seconds, dead-time = 7 seconds
  - RSW-1(config-if)# standby 1 preempt delay minimum 30 reload 60
    - Preemption: wait for 30 seconds (in case of reload wait 60 seconds) before taking back active role from RSW-2
  - RSW-1(config-if)# standby 1 track 101 decrement 30
  - RSW-1(config-if)# standby 1 track 102 decrement 30
- On RSW-2
  - RSW-2(config)#  interface vlan10
  - RSW-2(config-if)# standby 1 ip 10.0.10.7
  - RSW-2(config-if)# standby 1 priority 110
  - RSW-2(config-if)# standby 1 timers 2 7
  - RSW-2(config-if)# standby 1 preempt
    - Preemption: RSW-2 will immediately take over active role from RSW-1  after dead-time reached

# Advanced HSRP Scenario (Cisco Example)




HSRP … Hot Standby Router Protocol

# Cisco IOS Configuration – Adv. Scenario

- On RSW-1:
  - RSW-1(config)# track 101 interface fa0/7 line-protocol
  - RSW-1(config)# track 102 interface fa0/8 line-protocol
  - RSW-1(config)#  interface vlan10
  - RSW-1(config)#  standby version 2
  - RSW-1(config-if)# standby 1 ip 10.0.10.7
  - RSW-1(config-if)# standby 1 priority 150
  - RSW-1(config-if)# standby 1 timers msec 300 msec 950
    - Tuning HSRP timers: hello = 300 milliseconds, dead-time = 950 milliseconds
  - RSW-1(config-if)# standby 1 preempt delay minimum 30 reload 60
  - RSW-1(config-if)# standby 1 track 101 decrement 30
  - RSW-1(config-if)# standby 1 track 102 decrement 30
  - RSW-1(config-if)# standby 2 ip 10.0.10.8
  - RSW-1(config-if)# standby 2 priority 110
  - RSW-1(config-if)# standby 2 timers msec 300 msec 950
  - RSW-1(config-if)# standby 2 preempt
- On RSW-2
  - RSW-2(config)# track 101 interface fa0/7 line-protocol
  - RSW-2(config)# track 102 interface fa0/8 line-protocol
  - RSW-2(config)#  interface vlan10
  - RSW-2(config)#  standby version 2
  - RSW-2(config-if)# standby 1 ip 10.0.10.7
  - RSW-2(config-if)# standby 1 priority 110
  - RSW-2(config-if)# standby 1 timers msec 300 msec 950
  - RSW-2(config-if)# standby 1 preempt
  - RSW-2(config-if)# standby 2 ip 10.0.10.8
  - RSW-2(config-if)# standby 2 priority 150
  - RSW-2(config-if)# standby 2 timers msec 300 msec 950
  - RSW-2(config-if)# standby 2 preempt delay minimum 30 reload 60
  - RSW-2(config-if)# standby 2 track 101 decrement 30
  - RSW-2(config-if)# standby 2 track 102 decrement 30

# Agenda

- **Introduction**
  - Short History of the Internet (not part of the exam!)
  - Basic Principles
- **IP**
  - IP Protocol
  - IP QoS
  - Addressing
  - Classful versus Classless (not part of the exam!)
- **IP Forwarding**
  - Principles
  - ARP
  - ICMP
  - PPP
- **First Hop Redundancy**
  - Proxy ARP, IDRP
  - HSRP
  - VRRP (not part of the exam!)

# VRRP Operation 1

- **VRRP (Virtual Router Redundancy Protocol)**
  - RFC 2338 (Standards Track)
- **Principle:**
  - A group of routers forms a VRRP group
  - The group is represented by a virtual router
    - With is identified by a VRID (Virtual Router ID) and a virtual MAC address
  - One router is elected as the **virtual router master**, all other routers get the role of **virtual router backup** routers
  - The real IP address of the virtual router master become the IP address of the virtual router for a given VRRP group
    - IP address owner
  - Default Gateway of IP hosts is configured with the IP address of the virtual router for a given VRRP group
  - Virtual router master responds to ARP request directed to the IP address of the virtual router with the virtual MAC address
  - Backup routers supervise if master router is alive and take over the role of the master in case of failure
    - VRRP protocol using IP protocol number 112, IP multicast 224.0.0.18, and Ethernet multicast as destination address
  - Router must be able to support more than one unicast MAC address on an Ethernet interface

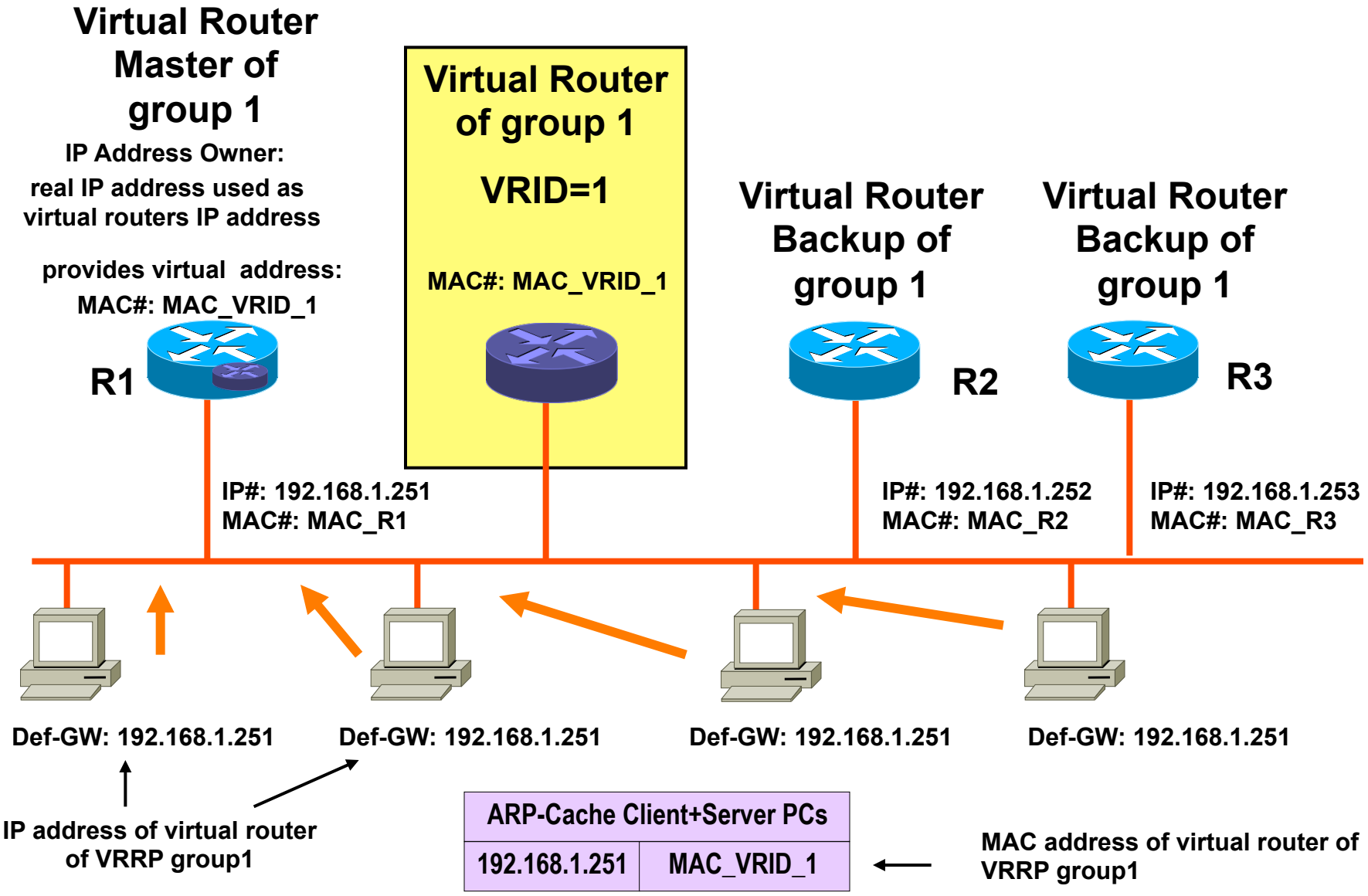
# VRRP Operation 2

- **Roles of router:**
  - Virtual router master, virtual router backup defined by VRRP priority
  - Priority value can be configured
    - Default value is 100
  - The higher the better
    - Will become the master after initialization
    - If priority is equal than the higher IP address decides
  - Preempt allows to give up the role of the master router when a router with higher priority is activated or reported
    - e.g. a failed router comes back or tracking has changed priority
- **Load Balancing:**
  - Specify at least two different VRRP groups with complementary roles
- **VRRP authentication:**
  - Based on keyed MD5
  - Against VRRP spoofing

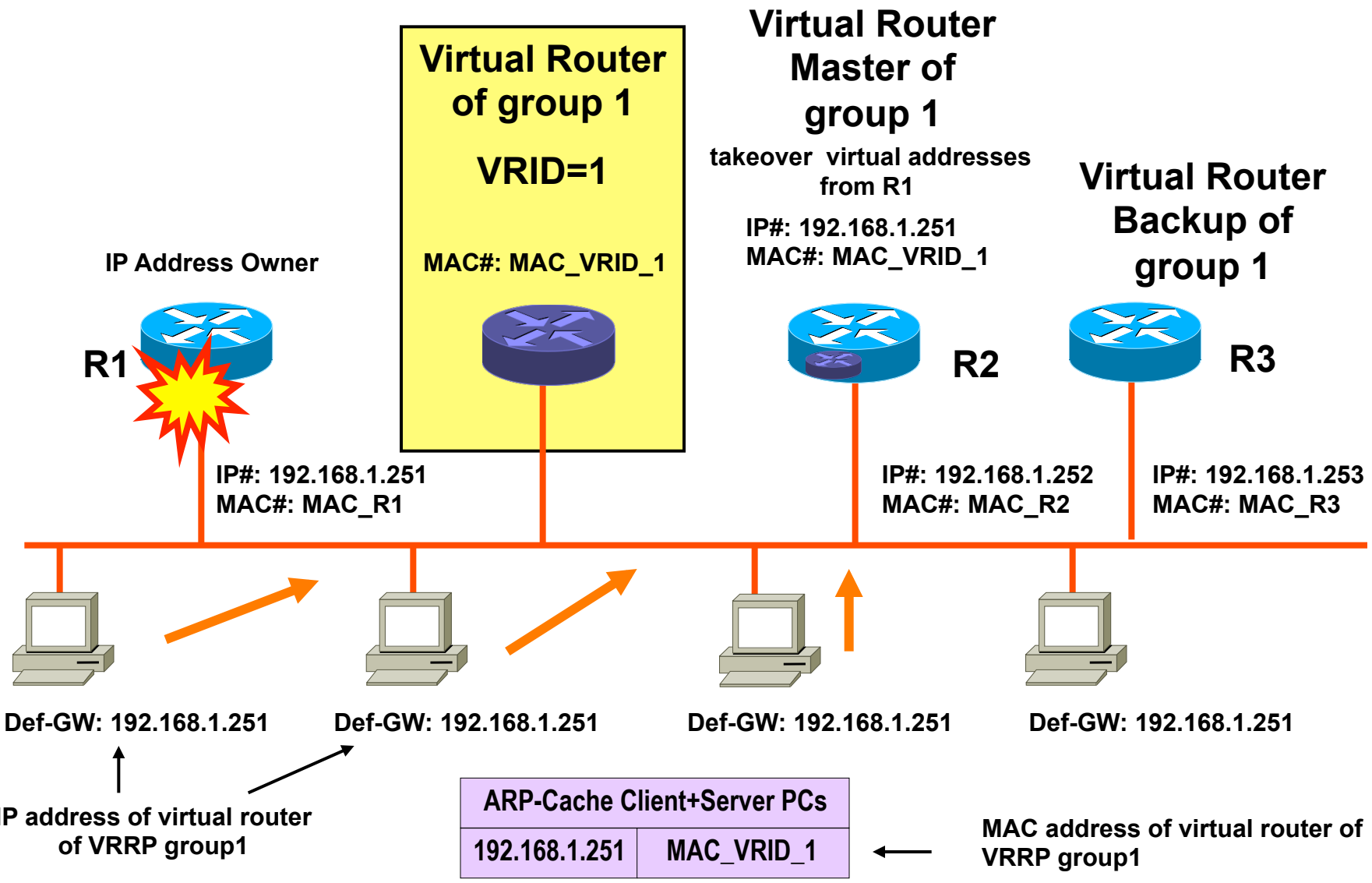
# VRRP Operation 3

- **Failover scenarios:**
  - Master router not reachable via LAN
    - Backup router with highest priority will take over master role
    - Timing depends on VRRP advertisements interval and master down interval
      - Default advert-interval = 1 seconds
      - Default master-down-interval = 3 * advert-interval + skew-time
  - Master router losses connectivity to a WAN interface (basic tracking options) or losses connectivity to an IP route (enhanced tracking options)
    - If tracking and preempt is configured backup router will take over
      - Tracking will lower the priority
      - Preempt allows another router to take over the role of the master router even if the current master router does not fail
  - Enhanced tracking options depend on IOS version

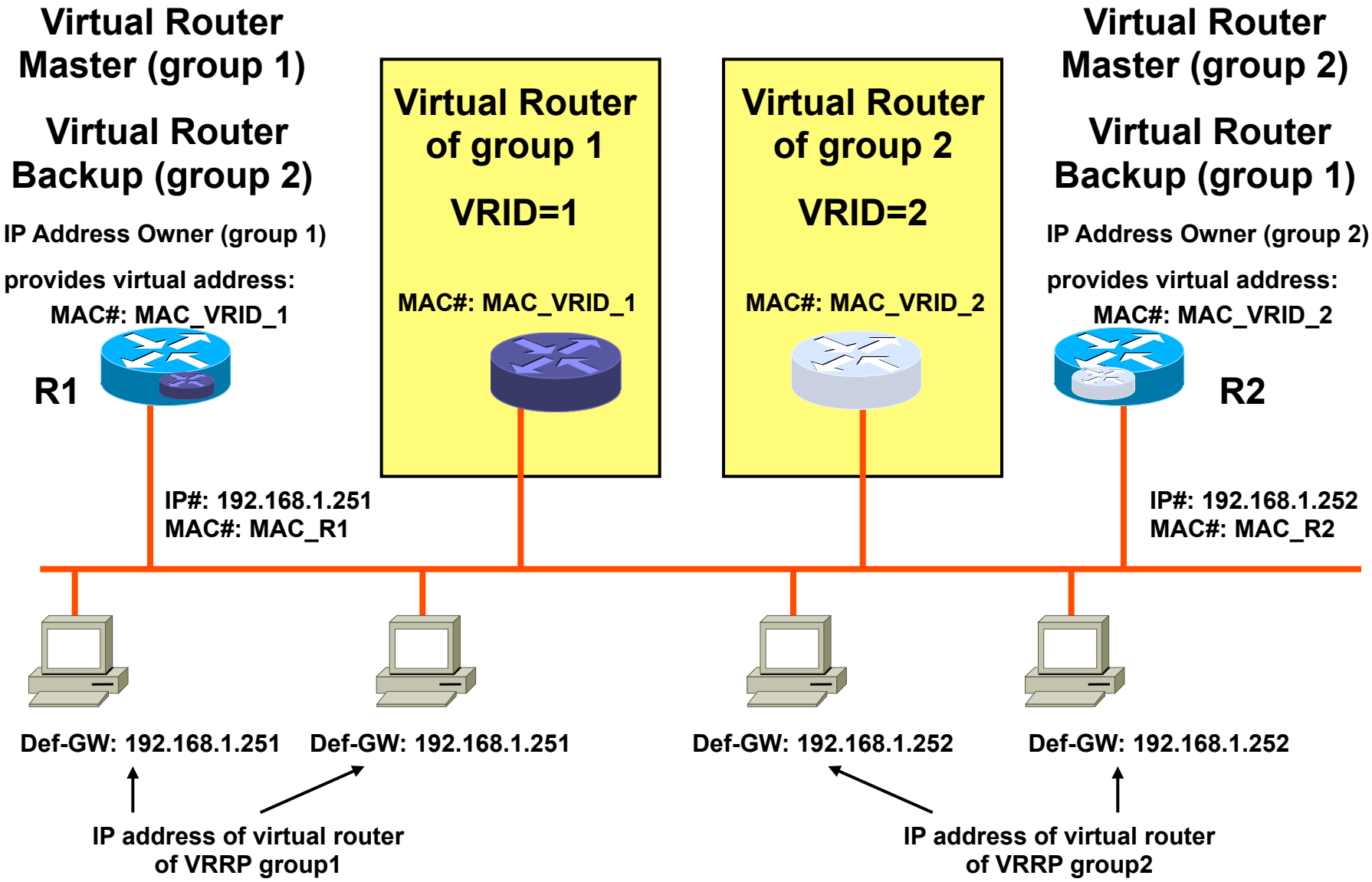
# VRRP


Virtual Router Master of group 1
IP Address Owner:
real IP address used as virtual routers IP address
provides virtual address:
MAC#: MAC_VRID_1
R1
Virtual Router of group 1
VRID=1
MAC#: MAC_VRID_1
Virtual Router Backup of group 1
R2
Virtual Router Backup of group 1
R3
IP#: 192.168.1.251
MAC#: MAC_R1
IP#: 192.168.1.252
MAC#: MAC_R2
IP#: 192.168.1.253
MAC#: MAC_R3
Def-GW: 192.168.1.251
Def-GW: 192.168.1.251
Def-GW: 192.168.1.251
Def-GW: 192.168.1.251
IP address of virtual router of VRRP group1
ARP-Cache Client+Server PCs
192.168.1.251
MAC_VRID_1
MAC address of virtual router of VRRP group1

# VRRP


Virtual Router of group 1
VRID=1
MAC#: MAC_VRID_1
Virtual Router Master of group 1
takeover virtual addresses from R1
IP#: 192.168.1.251
MAC#: MAC_VRID_1
Virtual Router Backup of group 1
IP Address Owner
R1
R2
R3
IP#: 192.168.1.251
MAC#: MAC_R1
IP#: 192.168.1.252
MAC#: MAC_R2
IP#: 192.168.1.253
MAC#: MAC_R3
Def-GW: 192.168.1.251
Def-GW: 192.168.1.251
Def-GW: 192.168.1.251
Def-GW: 192.168.1.251
IP address of virtual router of VRRP group1
ARP-Cache Client+Server PCs
192.168.1.251
MAC_VRID_1
MAC address of virtual router of VRRP group1

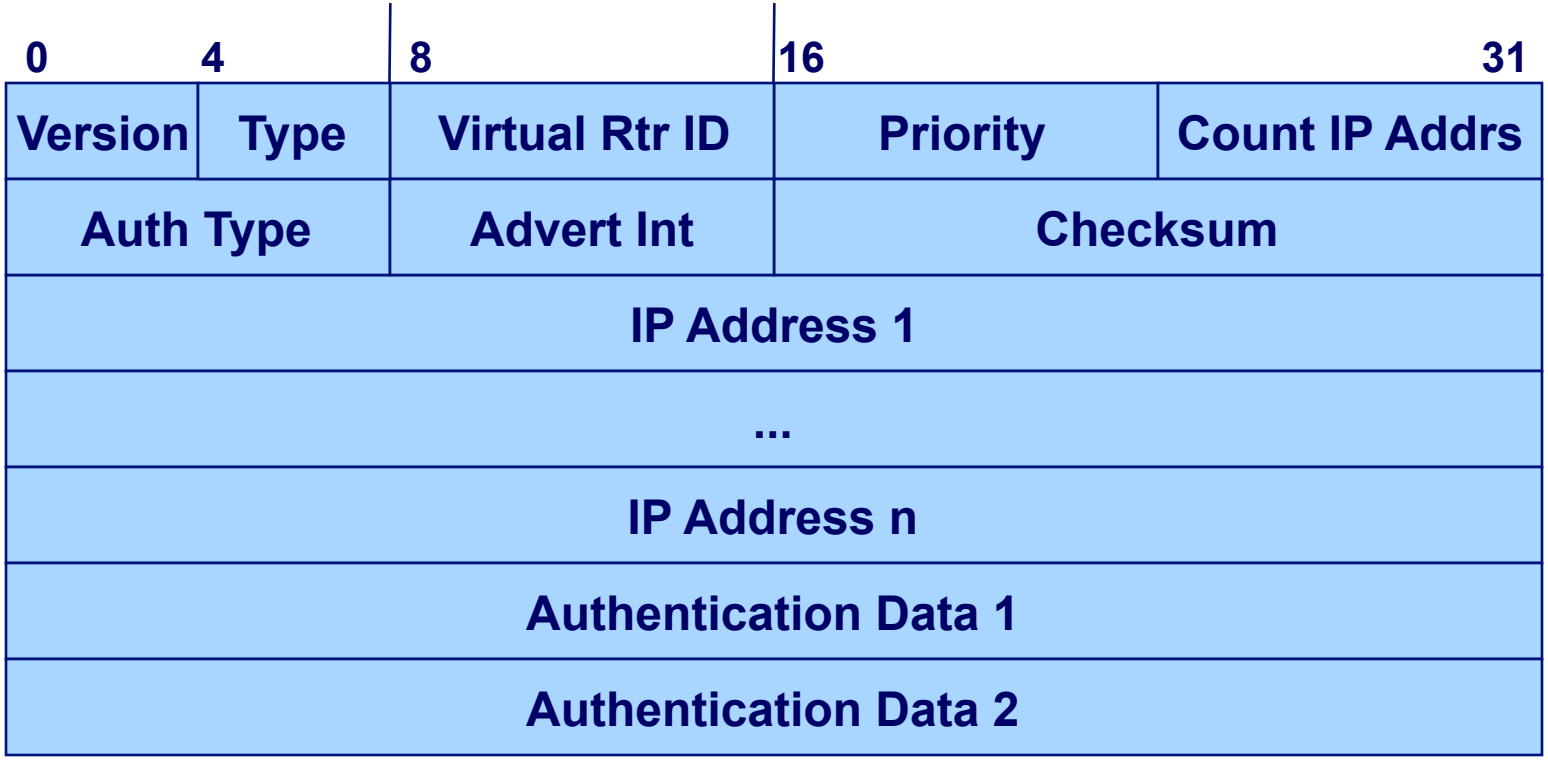
# VRRP Load Balancing



# Some VRRP Details

- **VRRP:**
  - Second or milliseconds timers
  - VRID range
    - 1 – 255
    - Maximum 255 groups
  - Virtual Mac Address: 00-00-5E-00-01-VRID
    - VRID value = group number
  - IP multicast 224.0.0.18

# VRRP Protocol Fields




- Version - This version is version 2.
- Type - The only packet type defined in this version of the protocol is: 1 ADVERTISEMENT.
- Virtual Rtr ID - The Virtual Router Identifier (VRID) field identifies the virtual router this packet is reporting status for.
- Priority - VRRP routers backing up a virtual router MUST use priority values between 1-254 (decimal).
- Count IP Addresses -The number of IP addresses
- Auth Type - Identifies the authentication method being utilized.
- Advertisement Interval - Indicates the time interval (in seconds) between advertisements.
- Checksum - used to detect data corruption
- IP Address(es) - One or more IP addresses that are associated with the virtual router.
- Authentication Data - The authentication string is currently only utilized for simple text authentication