

L08 - IP Technology

IP Technology

Introduction, IP Protocol Details
IP Addressing and IP Forwarding
ARP, ICMP, PPP

Agenda

- **Introduction**
- **IP**
 - IP Protocol
 - Addressing
- **IP Forwarding**
 - Principles
 - ARP
 - ICMP
 - PPP

© 2007, D.I. Manfred LindnerIP Technology, v4.72

L08 - IP Technology

IP Technology

- **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

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

3

TCP Technology

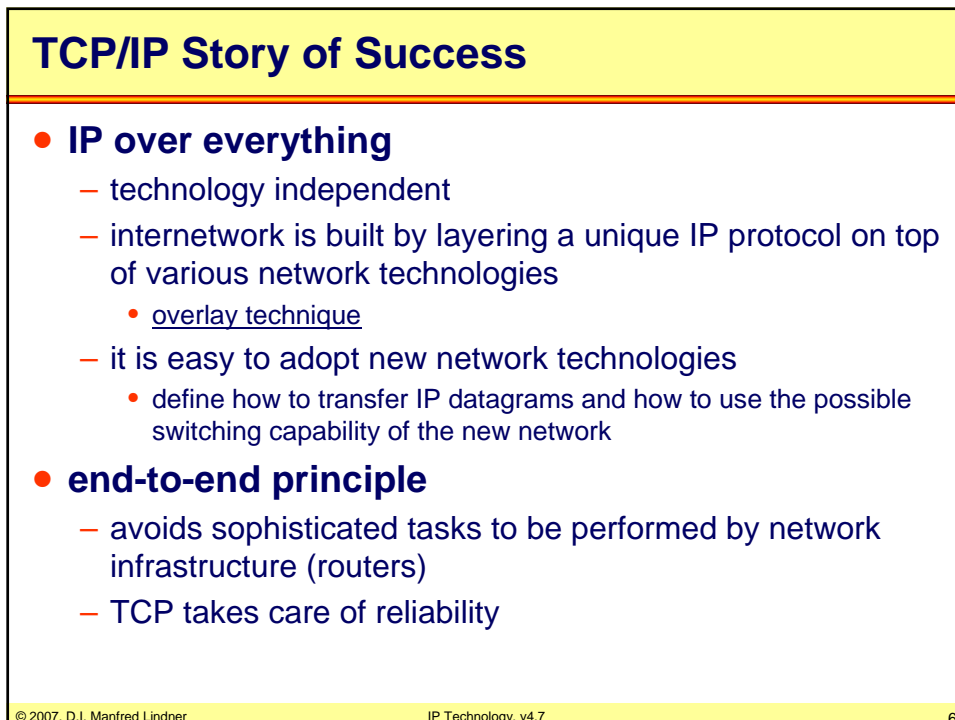
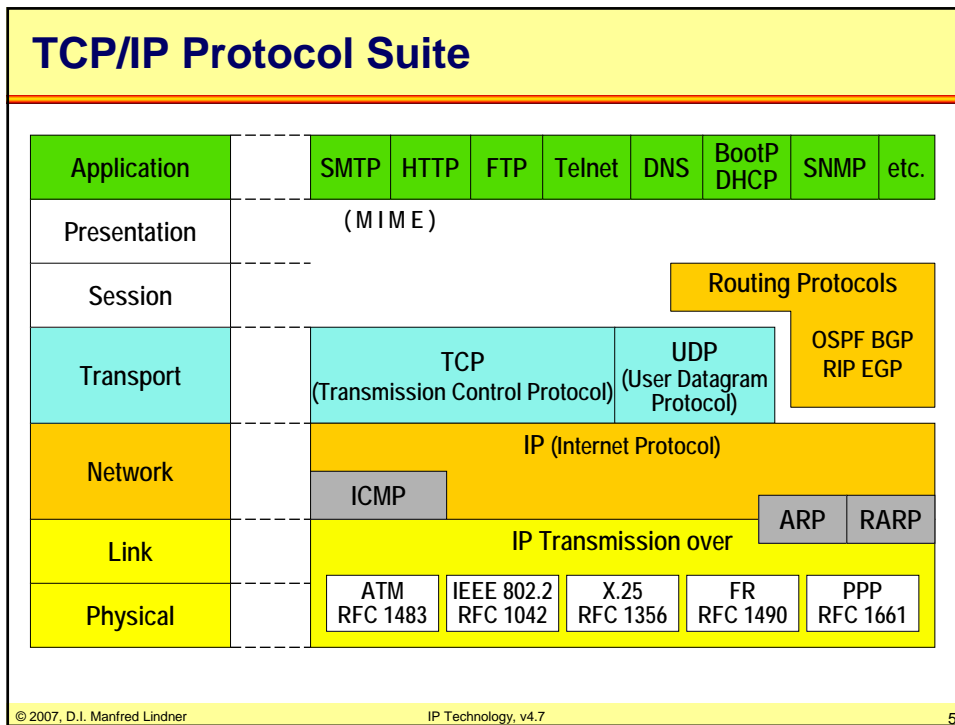
- **shared responsibility between network and end systems**
 - routers responsible for delivering datagrams to remote networks based on structured IP address
 - IP hosts responsible for end-to-end control
- **end to end control**
 - is implemented in upper layers of IP hosts
 - TCP (Transmission Control Protocol)
 - connection oriented
 - sequencing, windowing
 - error recovery by retransmission
 - flow control

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

4

L08 - IP Technology



L08 - IP Technology

TCP/IP Story of Success

- **TCP**

- tolerant and adaptive to network operational conditions
 - robust against network failures
 - adapts to varying network delays
 - adapts to varying network load

- **right functionality partition between**

- IP

- knows nothing about end systems applications
- makes best effort to route packets through the network

- and TCP

- takes care of end-to-end issues
- end users know nothing about network internals

- **WWW**

© 2007, D.I. Manfred Lindner

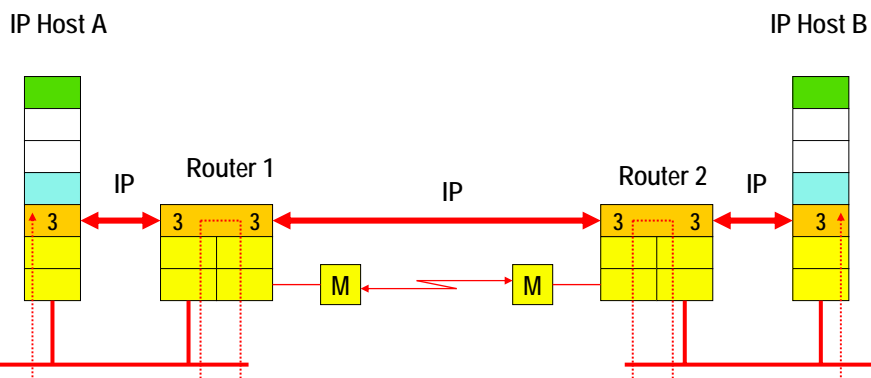
IP Technology, v4.7

7

IP and OSI Network Layer 3

Layer 3 Protocol = IP

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

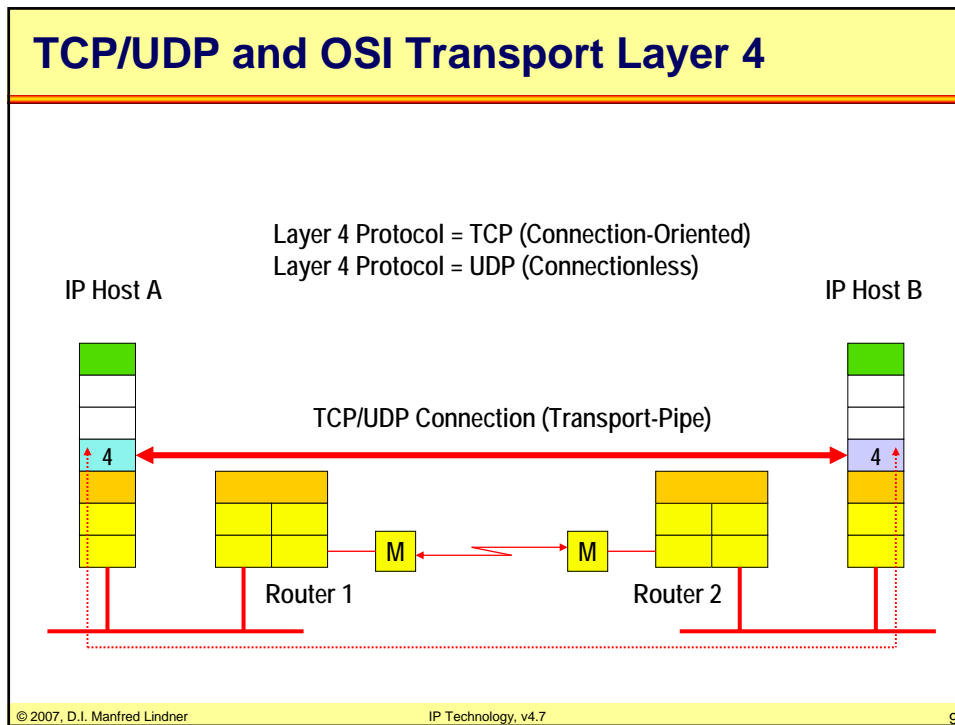


© 2007, D.I. Manfred Lindner

IP Technology, v4.7

8

L08 - IP Technology



- ### Key Players of Internet Technology
- **IAB (Internet Architecture Board)**
 - responsible for technical directions, coordination and standardization of the TCP/IP technology
 - the "Board" is highest authority and controls IETF, IRTF
 - **IETF (Internet Engineering Task Force)**
 - provides solutions and extensions for TCP/IP
 - working groups organized in areas
 - area manager and IETF chairman form the IESG (Internet Engineering Steering Group)
 - **IRTF (Internet Research Task Force)**
 - coordinates and prioritize research
 - research groups controlled by the IRSG (Internet Research Steering Group)
- © 2007, D.I. Manfred Lindner IP Technology, v4.7 10

L08 - IP Technology

Internet in Europe

- **RIPE NCC (Reséaux 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>

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

11

Standardization by RFCs

- **all documentation, standards, proposals for new protocols and enhancements for the Internet**
 - are published as "Requests for Comments" (RFC)
 - RFCs were the initial approach of engineers to discuss questions, suggestions via e-mail to speed up development
 - part of the success story of TCP/IP
 - IETF (Internet Engineering Task Force) decides, which RFCs will be adopted as a standard after rigorous review (e.g. two different implementations have to exist)
 - RFCs are numbered in sequence of publishing
 - adopted enhancements or changes to a protocol will result in a new RFC number

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

12

L08 - IP Technology

Standardization by RFCs

- **today's standardization process is best described**
 - in RFC-2026
 - The Internet Standards Process Revision3
- **not every RFC is an Internet Standard**
 - categories
 - Informational, Experimental, Historic
 - Proposed Standard
 - Draft Standard
 - Standard
- **IAB (Internet Architecture Board) publishes periodically a status list of all protocols:**
 - Official Protocol Standard RFC (currently RFC 3300).

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

13

Agenda

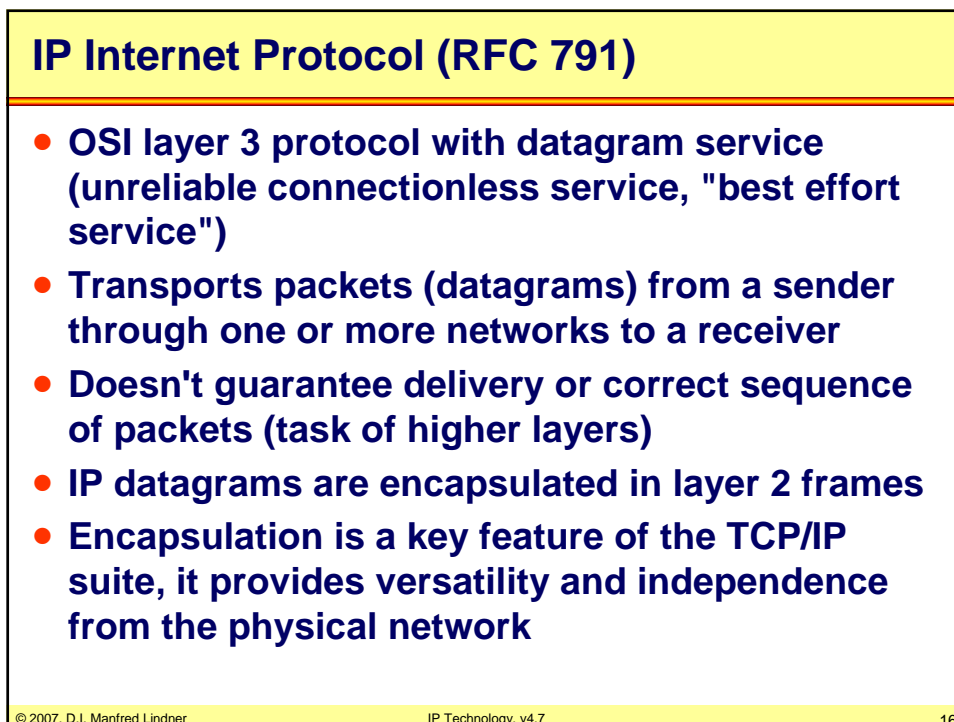
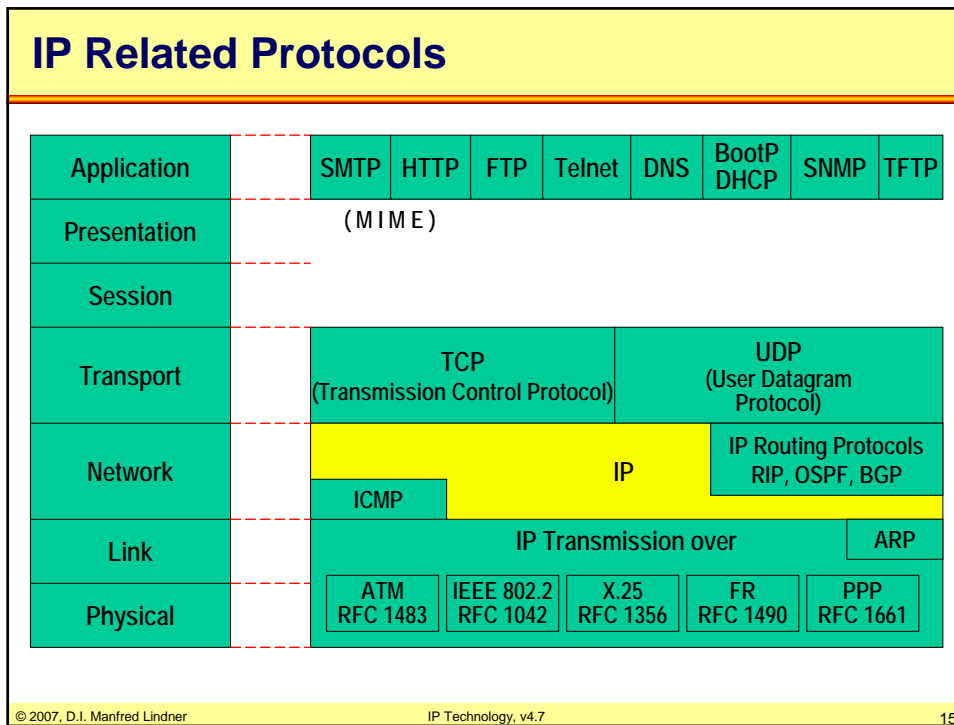
- **Introduction**
- **IP**
 - IP Protocol
 - Addressing
- **IP Forwarding**
 - Principles
 - ARP
 - ICMP
 - PPP

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

14

L08 - IP Technology



L08 - IP Technology

IP Protocol Functions

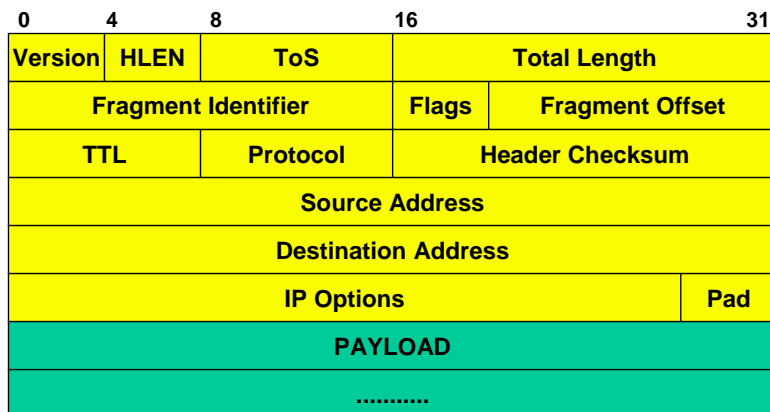
- **Mechanisms for packet forwarding, based on network addressing (Net-IDs)**
- **Error detection (only packet header)**
- **Fragmentation and reassembly of datagram's**
 - Necessary, if a datagram has to pass a network with a small max. frame size.
 - Reassembly by receiver
- **Mechanisms to limit the lifetime of a datagram**
 - To omit an endless circulating of datagrams if routing errors occur

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

17

IP Header



© 2007, D.I. Manfred Lindner

IP Technology, v4.7

18

L08 - IP Technology

IP Header Entries

1

- **Version**

- Version of the IP protocol
- Current version is 4
- Useful for testing or for migration to a new version, e.g. "IP next generation" (IPv6)

- **HLEN**

- Length of the header in 32 bit words
- Different header lengths result from IP options
 - HLEN 5 to 15 = 20 to 60 octets

IP Header Entries

2

- **Total Length**

- Total length of the IP datagram (header + data) in octets
- If fragmented: length of fragment
- Datagram size max. = 65535 octets
- Each host has to accept datagram's of at least 576 octets
 - either as a complete datagram or for reassembly

L08 - IP Technology

IP Header Entries

3

- **Protocol**

- Indicates the higher layer protocols
 - Examples are: 1 (ICMP), 6 (TCP), 8 (EGP), 17 (UDP), 89 (OSPF) etc.
- 100 different IP protocol types are registered so far

- **Source IP Address**

- IP address of the source (sender) of a datagram

- **Destination IP Address**

- IP address of the receiver (destination) of a datagram

- **Pad**

- "0"-octets to fill the header to a 32 bit boundary

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

21

IP Header Entries

4

- **TTL Time To Live**

- Limits the lifetime of a datagram in the network (Units are seconds, range 0-255)
- Is set by the source to a starting value. 32 to 64 are common values, the current recommended value is 64 (RFC1700)
- Every router decrements the TTL by the processing/waiting time. If the time is less than one second, TTL is decremented by one ("TTL = hop count").
- If TTL reaches 0, the datagram (fragment) is discarded.
- An end system can use the remaining TTL value of the first arriving fragment to set the reassembly timer.

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

22

L08 - IP Technology

IP Header Entries

5

- **Identification (for fragmentation)**
 - Unique identification of a datagram, used for fragmentation and reassembly
 - In praxis a hidden sequence number although not used because of connectionless behavior of IP
- **Flags (for fragmentation).**
 - DF (don't fragment)
 - If set: fragmentation is not allowed
 - Datagram's must be discarded by router if MTU (maximum transmission unit) size of next link is too small
 - MF (more fragments)
 - If set: more fragments of the same original datagram will follow

"0"	DF	MF	Fragment Offset
-----	----	----	-----------------

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

23

IP Header Entries

6

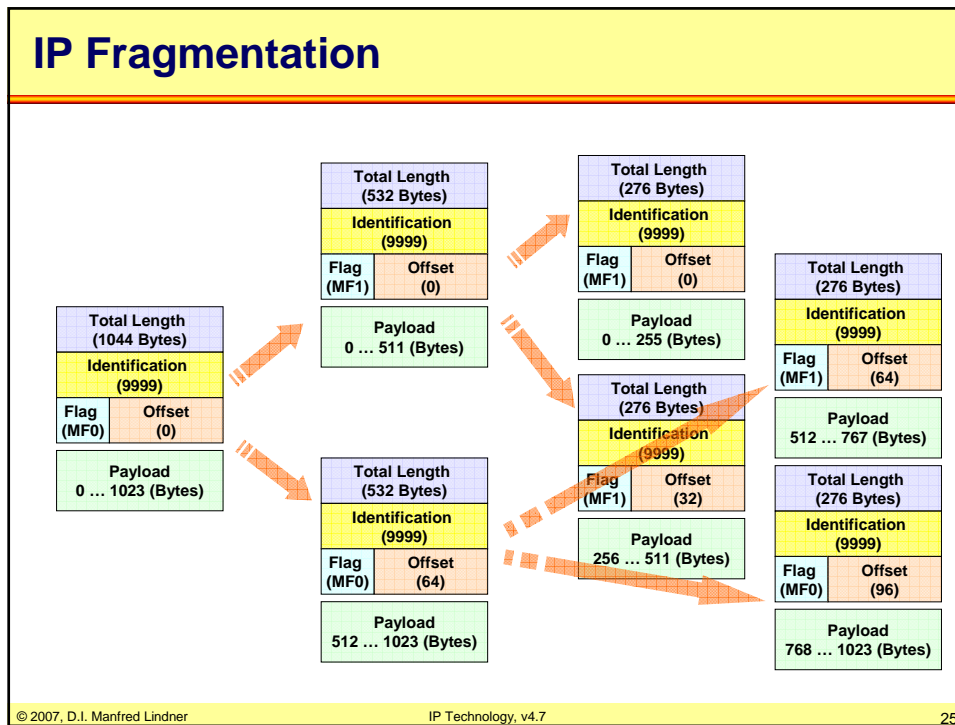
- **Fragment Offset**
 - Indicates the position of a fragment relative to the beginning of the original datagram
 - Offset is measured in multiples of 8 octets (64 bits)
 - The first fragment and unfragmented packets have an offset of 0
 - Fragments (except the last) must be a multiple of 8 octets
 - Fragments with the same combination of source address / destination address / protocol / identification will be reassembled to the original datagram

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

24

L08 - IP Technology



Reassembly

- Reassembly is done at the destination, because fragments can take different paths
- Buffer space has to be provided at the receiver
- Some fragments may not arrive (unreliable nature of IP)
- Measures must be taken to free buffers if a packet can't be reconstructed in a timely manner
- The first arriving fragment of an IP packet (with MF=1 and/or Offset \neq 0) starts a reassembly timer
- If the timer expires before the packet was reconstructed, all fragments will be discarded and the buffer is set free
- The reassembly timer limits the lifetime of an incomplete datagram and allows better use of buffer resources.

L08 - IP Technology

IP Header Entries

7

- **TOS field (Type Of Service)**
- **Old Meaning (RFC 1349)**
 - Tells the priority of a datagram (precedence bits) and the preferred network characteristics (low delay, high throughput, high reliability, low monetary cost.)
 - Precedence bits:
 - Define the handling of a datagram within the router
 - e.g. priority within the input / output queues
 - D, T, R and C bits:
 - Can be used to take a path decision for routing if multiple paths with different characteristics exist to the destination
 - needs one routing table per characteristic
 - TOS bits may be ignored by routers but may never lead to discarding a packet if the preferred service can't be provided

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

27

TOS Field Old Meaning (RFC 1349)

Precedence	D	T	R	C	"0"
------------	---	---	---	---	-----

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

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

28

L08 - IP Technology

IPv4 TOS Recycling

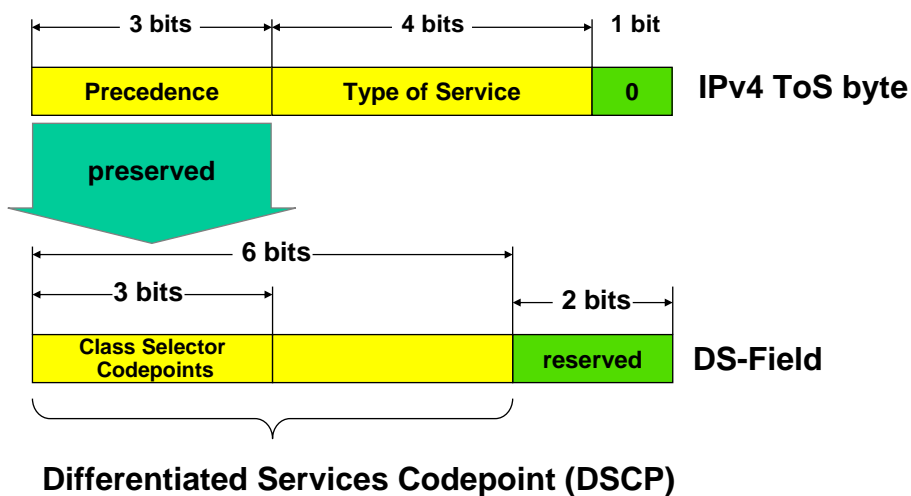
- IPv4 TOS field was redefined by the IETF to become the "Differentiated Service CodePoint" (DSCP)
- Now the DSCP field is used to label the traffic class of a flow
 - a flow is a given communication relationship (session) between two IP hosts
 - IP datagram's of a flow have the same
 - Source IP Address
 - Destination IP Address
 - Protocol Number
 - TCP/UDP Source Port
 - TCP/UDP Destination Port

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

29

IPv4 TOS Recycling



© 2007, D.I. Manfred Lindner

IP Technology, v4.7

30

L08 - IP Technology

DSCP Usage

- **Important for IP QoS (Quality of Service)**
 - IP QoS Differentiated Services Model
 - RFC 2474: "Definition of the Differentiated Service Field in the IPv4 and IPv6 Headers"
 - RFC 2475: "An Architecture for Differentiated Services"
 - Remember
 - IP is basically a Best Effort Service, therefore not suited for interactive real-time traffic like voice and video
 - Using DSCP a IP datagram can be labelled at the border of IP QoS domain
 - with a certain traffic class
 - Traffic class will receive a defined handling within in IP QoS Domain
 - e.g. limited delay, guaranteed throughput

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

31

IP Header Entries

8

- **IP Options**
 - IP options have to be implemented by every IP station
 - The only thing optional is their presence in an IP header
 - Options include provisions for timestamps, security and special routing aspects
 - Some options may, others must be copied to all fragments
- **Today most IP Options are blocked by firewalls because of inherent security flaws**
 - e.g. source routing could divert an IP stream to a hacker's network station

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

32

L08 - IP Technology

IP Options

- **Record Route**
 - Records the route of a packet through the network
 - Each router, which forwards the packet, enters its IP address into the provided space
- **Loose Source Route**
 - A datagram or fragment has to pass the routers in the sequence provided in the list
 - Other intermediate routers not listed may also be passed
- **Strict Source Route**
 - A datagram or fragment has to pass the routers in the sequence listed in the source route
 - No other router or network may be passed

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

33

Agenda

- **Introduction**
- **IP**
 - IP Protocol
 - Addressing
- **IP Forwarding**
 - Principles
 - ARP
 - ICMP
 - PPP

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

34

L08 - IP Technology

IP Address

- **IP address**

- 32 bit , dotted decimal notation
- identifies access to a network (network interface)
- basic structure
 - network number (net-id)
 - host number (host-id)
- two level hierarchy
- net-id must be unique when a physical network with IP hosts is connected to the Internet
 - assignment controlled by Internet Registry
- host-id is assigned by each local network manager

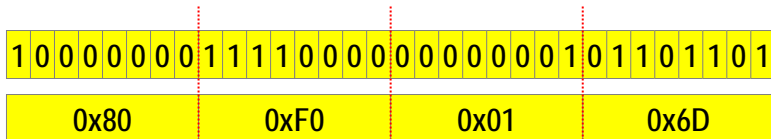
© 2007, D.I. Manfred Lindner

IP Technology, v4.7

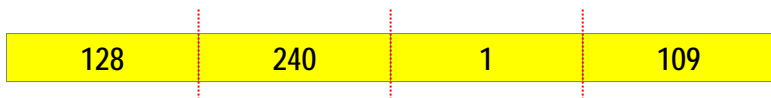
35

Address notation

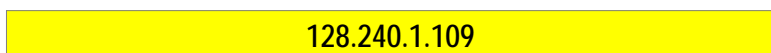
IP address (example):



each octet of an IP address is written as the decimal equivalent:



The resulting four numbers are delimited with dots (dotted decimal notation):



© 2007, D.I. Manfred Lindner

IP Technology, v4.7

36

L08 - IP Technology

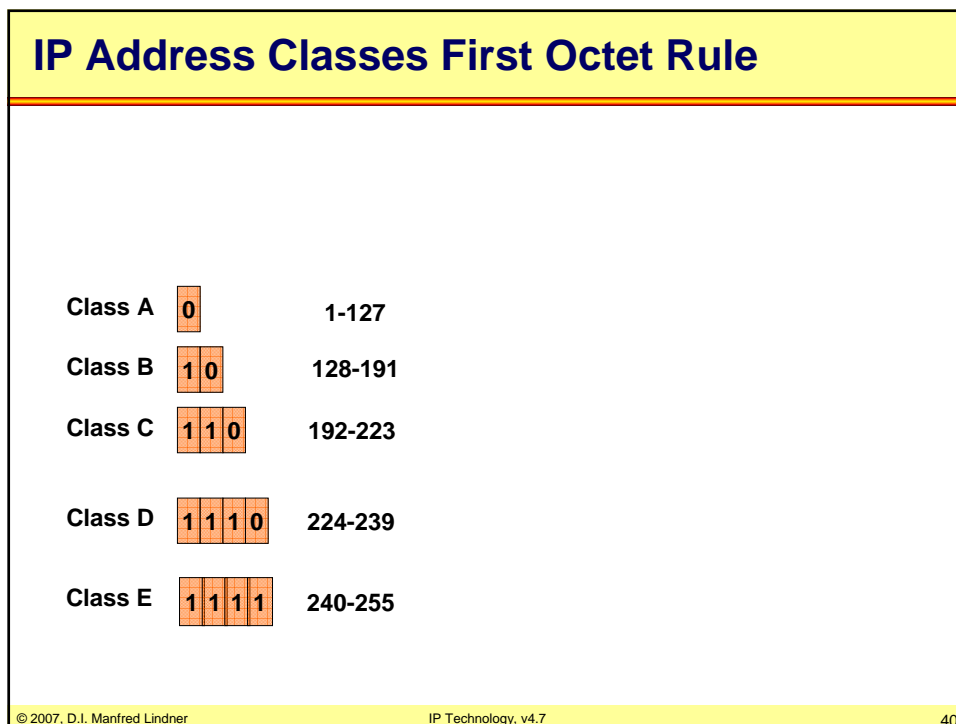
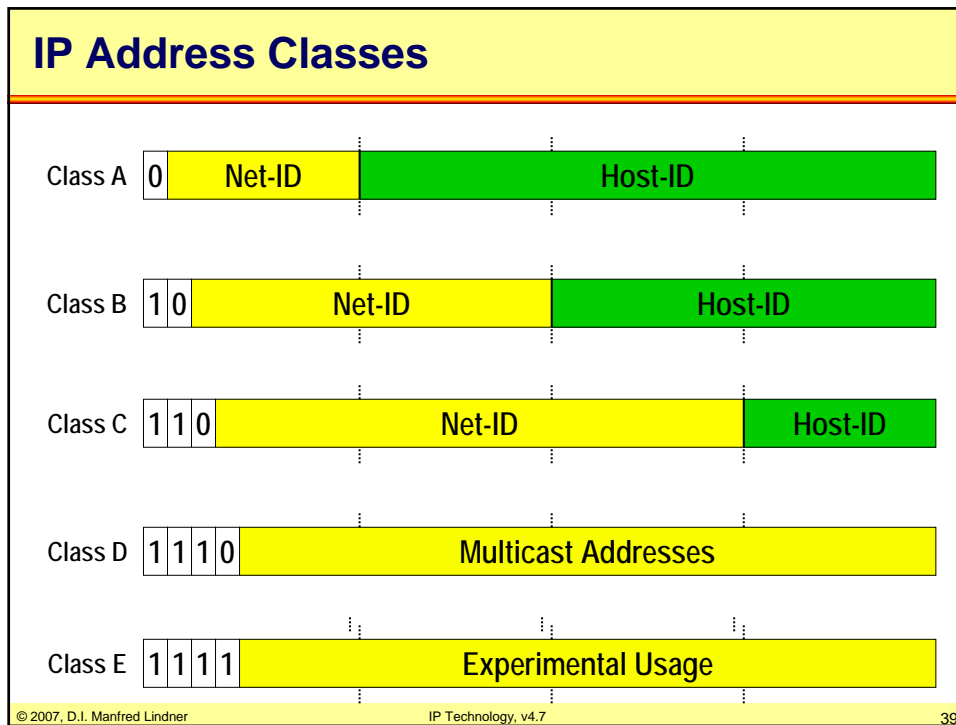
Binary vs Decimal Notation								
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
1	0	0	0	0	0	0	0	128
0	1	0	0	0	0	0	0	64
0	0	1	0	0	0	0	0	32
0	0	0	1	0	0	0	0	16
0	0	0	0	1	0	0	0	8
0	0	0	0	0	1	0	0	4
0	0	0	0	0	0	1	0	2
0	0	0	0	0	0	0	1	1
1	1	1	1	1	1	1	1	255

© 2007, D.I. Manfred Lindner IP Technology, v4.7 37

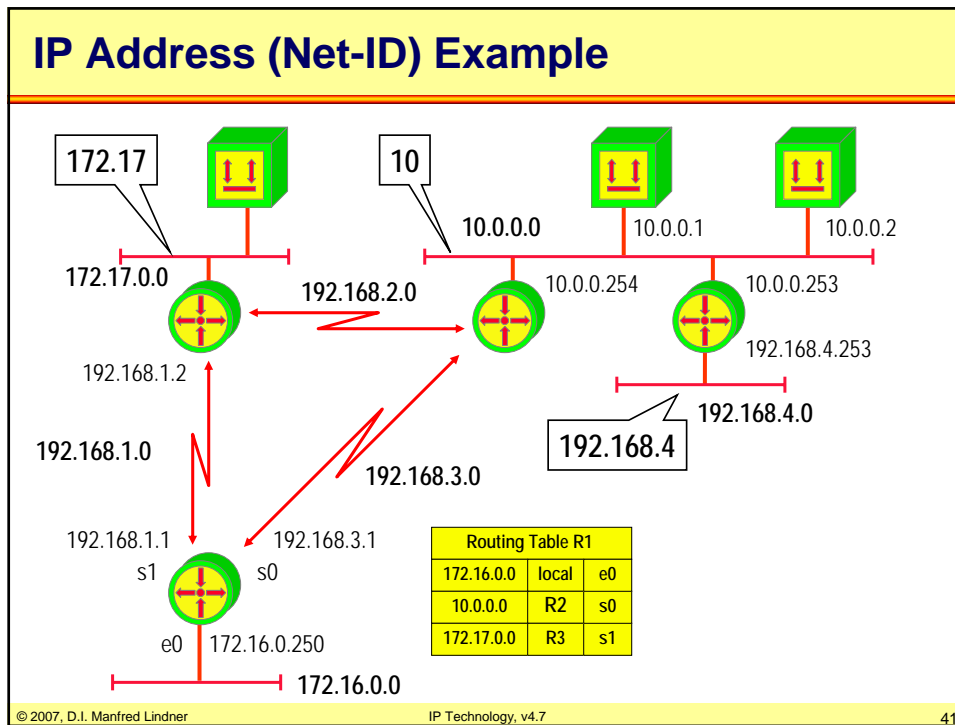
Classes	
<ul style="list-style-type: none"> • several classes of IP addresses <ul style="list-style-type: none"> – A, B, C (unicast), D (multicast), E (experimental) – class defines numbers of address-bits to be used for net-id <ul style="list-style-type: none"> • class A 7 bits of net-id, 24 bits of host-id 126 nets / 16.777.214 hosts • class B 14 bits of net-id, 16 bits of host-id 16.384 nets / 65.534 hosts • class C 21 bits of net-id, 8 bits of host-id 2.097.512 nets / 254 hosts • class D 28 bits multicast group number – first octet rule <ul style="list-style-type: none"> • class A range: 1 - 126 • class B range: 128 - 191 • class C range: 192 - 223 • class D range: 224 - 239 	

© 2007, D.I. Manfred Lindner IP Technology, v4.7 38

L08 - IP Technology



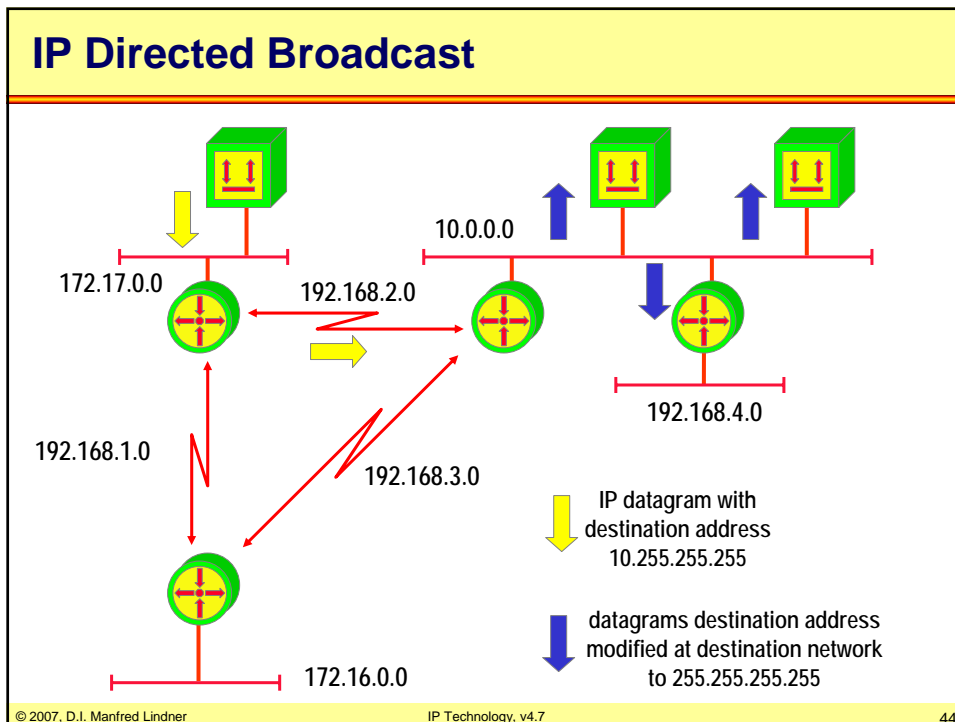
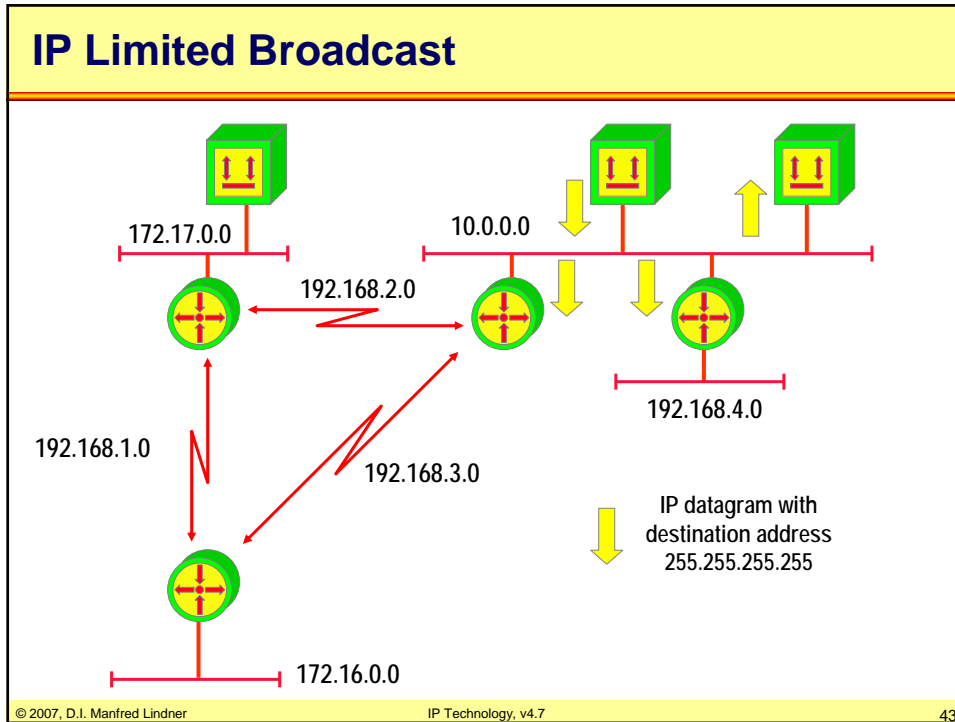
L08 - IP Technology



Special Addresses

- **basic IP address format**
 - { net-id, host-id }
- **special purpose addresses and rules**
 - { 0, 0 } this host on this network (0.0.0.0)
 - { 0, <host-id> } specified host on this network
 - { <net-id>, -1 } directed broadcast to specified network
 - { -1, -1 } limited broadcast on this network (255.255.255.255)
 - { 127, <any> } loopback address
 - { <net-id>, 0 } never used for a host number, identifies network itself
 - note:
 - 0 ... means all corresponding bits = 0
 - 1 ... means all corresponding bits = 1

L08 - IP Technology



L08 - IP Technology

Subnetting

- **two level hierarchy was sufficient in the early days of the Internet**
- **with local area networks a third hierarchical level was introduced by subnetting**
- **subnetting**
 - some bits of the host-id can be used as subnet-id
 - subnet-id extends classful net-id meaning
 - subnet-id bits are only locally interpreted inside subnetted area
 - net-id bits are still globally seen outside the subnetted area
 - number of bits to be used for network identification are specified by subnet mask (written in dotted decimal notation)
 - ones portion represents network part (must be contiguous)
 - zeros portion represent the host part

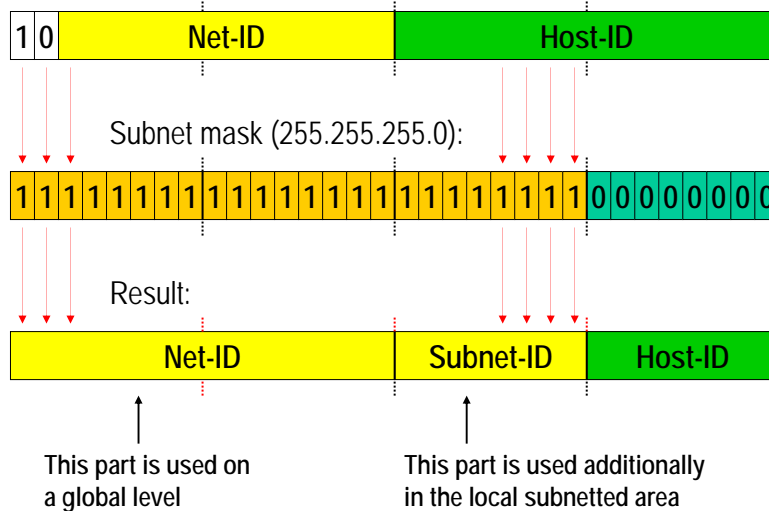
© 2007, D.I. Manfred Lindner

IP Technology, v4.7

45

Subnet addressing

Example of a subnetted class B address:



© 2007, D.I. Manfred Lindner

IP Technology, v4.7

46

L08 - IP Technology

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

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

47

Subnet Mask

- **natural subnet mask**
 - address classes without subnetting
 - class A ... 255.0.0.0
 - class B ... 255.255.0.0
 - class C ... 255.255.255.0
- **old notation of IP addresses**
 - with subnetmask
 - 10.0.0.0 255.0.0.0 (Class A)
 - 176.16.0.0 255.255.0.0 (Class B)
- **new notation of IP addresses**
 - with prefix/length
 - 10.0.0.0 / 8 (Class A)
 - 176.16.0.0 / 16 (Class B)

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

48

L08 - IP Technology

Rules with Subnetting

- **IP address format with subnetting**
 - { net-id, subnet-id, host-id }
- **additional special purpose addresses and rules**
 - { <net-id>, <subnet-id>, -1 }
 - directed broadcast to specified subnet
 - { <net-id>, -1, -1 }
 - directed broadcast to all subnets of specified subnetted network
 - { <net-id>, 0, <host-id> }
 - subnet zero never used for a subnet number for classful routing (see RFC 950)
 - { <net-id>, -1, <host-id> }
 - subnet broadcast never used for a subnet number for classful routing (see RFC 950)

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

49

Subnet Mask Examples 1

- **class A ⇔ pseudo class B (8 bit subnetting)**
 - 10.0.0.0 with 255.255.0.0 (10.0.0.0 / 16)
 - subnetworks:
 - 10.0.0.0 subnet zero
 - 10.1.0.0
 - 10.1.0.1 first IP host in net 10.1.0.0
 - 10.1.255.254 last IP host in net 10.1.0.0
 - 10.1.255.255 directed broadcast in net 10.1.0.0
 - 10.2.0.0
 - 10.3.0.0
 -
 - 10.254.0.0
 - 10.255.0.0 subnet broadcast
 - 254 subnets / 65534 hosts

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

50

L08 - IP Technology

Subnet Zero / Subnet Broadcast

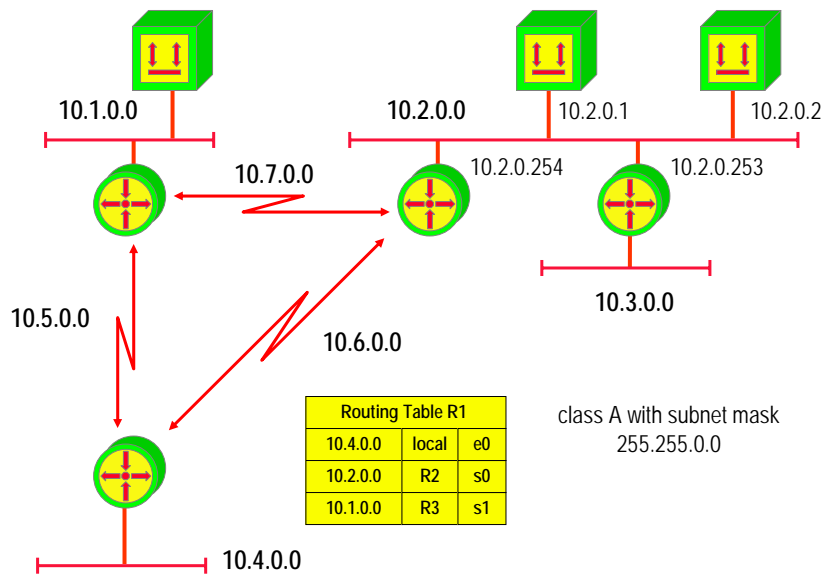
- **What is the problem?**
 - Does 10.0.0.0 mean net-ID of net 10 or of subnet 10.0 ?
 - Does 10.255.255.255 mean directed broadcast for the whole net 10 or for the subnet 10.255 ?
 - subnet zero and subnet broadcast are ambiguous

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

51

IP Address Example with Subnetting

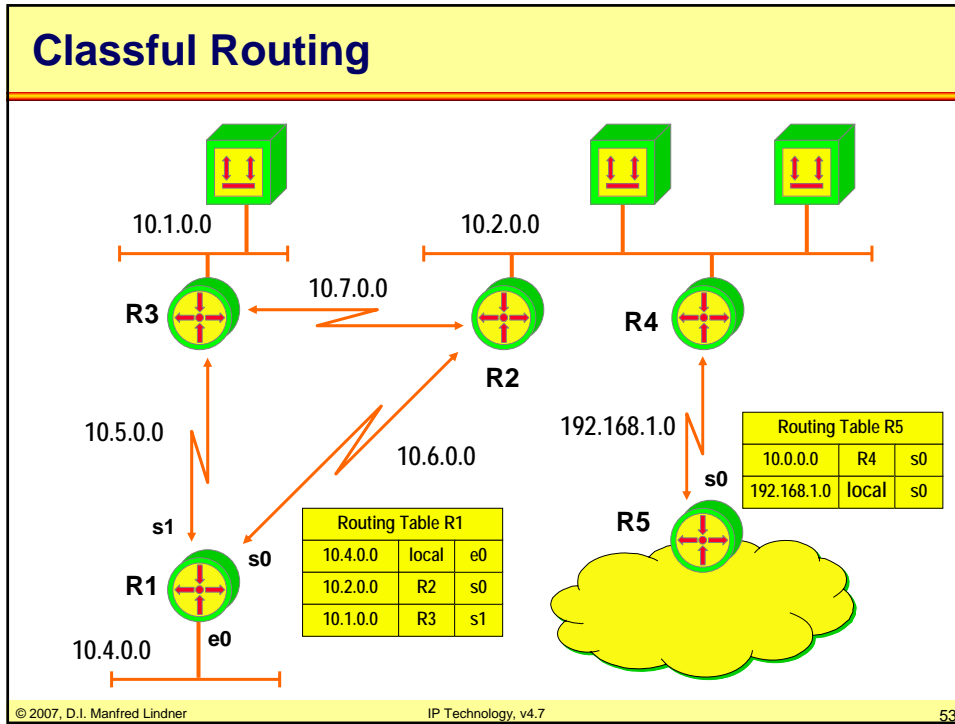


© 2007, D.I. Manfred Lindner

IP Technology, v4.7

52

L08 - IP Technology



Subnet Mask Examples 2

- **class A ⇒ pseudo class C (16 bit subnetting)**
 - 10.0.0.0 with 255.255.255.0 (10.0.0.0 / 24)
 - subnetworks:
 - 10.0.0.0 subnet zero
 - 10.0.1.0
 - 10.0.2.0
 -
 - 10.0.255.0
 - 10.1.0.0
 - 10.1.2.0
 -
 - 10.255.254.0
 - 10.255.255.0 subnet broadcast
 - 65534 subnets / 254 hosts

© 2007, D.I. Manfred Lindner IP Technology, v4.7 54

L08 - IP Technology

Subnet Mask Examples 3

- **class B ⇒ pseudo class C (8 bit subnetting)**
 - 172.16.0.0 with 255.255.255.0 (172.16.0.0 / 24)
 - subnetworks:
 - 172.16.0.0 subnet zero
 - 172.16.1.0
 - 172.16.2.0
 -
 -
 - 172.16.254.0
 - 172.16.255.0 subnet broadcast
 - 254 subnets / 254 hosts

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

55

Subnet Mask -> Net-ID, Host-ID

- **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

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

56

L08 - IP Technology

Subnet Mask Examples 4

- **class B address**

subnet mask 255.255.255.192

IP- Address 172.16.3.144

? net-id, ? host-id

address binary 1010 1100 . 0001 0000 . 0000 0011 . 1001 0000

mask (binary) 1111 1111 . 1111 1111 . 1111 1111 . 1100 0000

logical AND (bit by bit)

net-id 1010 1100 . 0001 0000 . 0000 0011 . 1000 0000

net-id = 172.16.3.128

host-id = 0.0.0.16

Subnet Mask Examples 5

- **class B ⇒ 10 bit subnetting**

– 172.16.0.0 with 255.255.255.192 (172.16.0.0 / 26)

– subnetworks:

	net-ID	host-ID
• 172.16.0.0 subnet zero	172.16.0. 00	xx xxxx
• 172.16.0.64	172.16.0. 01	xx xxxx
– 172.16.0.65 first IP host	172.16.0. 01	00 0001
– 172.16.0.66 second IP host	172.16.0. 01	00 0010
.....		
– 172.16.0.126 last IP host	172.16.0. 01	11 1110
– 172.16.0.127 directed broadcast	172.16.0. 01	11 1111
• 172.16.0.128	172.16.0. 10	xx xxxx
• 172.16.0.192	172.16.0. 11	xx xxxx

L08 - IP Technology

Subnet Mask Examples 5

– subnetworks (cont.):

• 172.16.1.0	172.16.1. 00 xx xxxx
• 172.16.1.64	172.16.1. 01 xx xxxx
• 172.16.1.128	172.16.1. 10 xx xxxx
• 172.16.1.192	172.16.1. 11 xx xxxx
• 172.16.2.0	172.16.2. 00 xx xxxx
• 172.16.2.64	172.16.2. 01 xx xxxx
.....	
• 172.16.255.0	172.16.255. 00 xx xxxx
• 172.16.255.64	172.16.255. 01 xx xxxx
• 172.16.255.128	172.16.255. 10 xx xxxx
• 172.16.255.192 subnet broadcast	172.16.255. 11 xx xxxx

– 1022 subnets / 62 hosts

Subnet Mask Examples 6

• **class C** ⇒ **2 bit subnetting**

– 192.168.16.0 with 255.255.255.192 (192.168.16.0 / 26)

– subnetworks:

	net-ID	host-ID
• 192.168.16.0 subnet zero	192.168.16. 00 xxxxxx	
• 192.168.16.64	192.168.16. 01 xxxxxx	
• 192.168.16.128	192.168.16. 10 xxxxxx	
• 192.168.16.192 subnet broadcast	192.168.16. 11 xxxxxx	

– 2 subnets / 62 hosts

L08 - IP Technology

Subnet Mask Examples 7

- **class C ⇒ 3 bit subnetting**

- 192.168.16.0 with 255.255.255.224 (192.168.16.0 / 27)
- subnetworks:

	net-ID	host-ID
• 192.168.16.0 subnet zero	192.168.16. 000	xxxxx
• 192.168.16.32	192.168.16. 001	xxxxx
• 192.168.16.64	192.168.16. 010	xxxxx
• 192.168.16.96	192.168.16. 011	xxxxx
• 192.168.16.128	192.168.16. 100	xxxxx
• 192.168.16.160	192.168.16. 101	xxxxx
• 192.168.16.192	192.168.16. 110	xxxxx
• 192.168.16.224 subnet broadcast	192.168.16. 111	xxxxx
- 6 subnets / 30 hosts

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

61

Subnet Mask Examples 8

- **class C ⇒ 4 bit subnetting**

- 192.168.16.0 with 255.255.255.240 (192.168.16.0 / 28)
- subnetworks:

	net-ID	host-ID
• 192.168.16.0 subnet zero	192.168.16. 0000	xxxx
• 192.168.16.16	192.168.16. 0001	xxxx
– 192.168.16.17 1st IP host	192.168.16. 0001	0001
– 192.168.16.18 2nd IP host	192.168.16. 0001	0010
–		
– 192.168.16.30 14th IP host	192.168.16. 0001	1110
– 192.168.16.31 directed broadcast	192.168.16. 0001	1111
• 192.168.16.32	192.168.16. 0010	xxxx
• 192.168.16.48	192.168.16. 0011	xxxx

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

62

L08 - IP Technology

Subnet Mask Examples 8

– subnetworks (cont.):	net-ID	host-ID
• 192.168.16.64	192.168.16. 0100	xxxx
• 192.168.16.80	192.168.16. 0101	xxxx
• 192.168.16.96	192.168.16. 0110	xxxx
• 192.168.16.112	192.168.16. 0111	xxxx
• 192.168.16.128	192.168.16. 1000	xxxx
• 192.168.16.144	192.168.16. 1001	xxxx
• 192.168.16.160	192.168.16. 1010	xxxx
• 192.168.16.176	192.168.16. 1011	xxxx
• 192.168.16.192	192.168.16. 1100	xxxx
• 192.168.16.208	192.168.16. 1101	xxxx
• 192.168.16.224	192.168.16. 1110	xxxx
• 192.168.16.240 subnet broadcast	192.168.16. 1111	xxxx
– 14 subnets / 14 hosts		

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

63

Subnet Mask Examples 9

• class C ⇒ 5 bit subnetting		
– 192.168.16.0 with 255.255.255.248 (192.168.16.0 / 29)		
– subnetworks:	net-ID	host-ID
• 192.168.16.0 subnet zero	192.168.16. 00000	xxx
• 192.168.16.8	192.168.16. 00001	xxx
• 192.168.16.16	192.168.16. 00010	xxx
• 192.168.16.24	192.168.16. 00011	xxx
•		
• 192.168.16.240	192.168.16. 11110	xxx
• 192.168.16.248 subnet broadcast	192.168.16. 11111	xxx
– 30 subnets / 6 hosts		

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

64

L08 - IP Technology**Subnet Mask Examples 10**

- **class C ⇒ 6 bit subnetting**

- 192.168.16.0 with 255.255.255.252 (192.168.16.0 / 30)
- subnetworks:

	net-ID	host-ID
● 192.168.16.0 subnet zero	192.168.16. 000000	xx
● 192.168.16.4	192.168.16. 000001	xx
– 192.168.16.5 1st IP host	192.168.16. 000001	01
– 192.168.16.6 2nd IP host	192.168.16. 000001	10
– 192.168.16.7 directed broadcast	192.168.16. 000001	11
● 192.168.16.8	192.168.16. 000010	xx
.....		
● 192.168.16.248	192.168.16. 111110	xx
● 192.168.16.252 subnet broadcast	192.168.16. 111111	xx
- 62 subnets / 2 hosts

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

65

Agenda

- **Introduction**
- **IP**
 - IP Protocol
 - Addressing
- **IP Forwarding**
 - Principles
 - ARP
 - ICMP
 - PPP

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

66

L08 - IP Technology

IP Forwarding Responsibilities

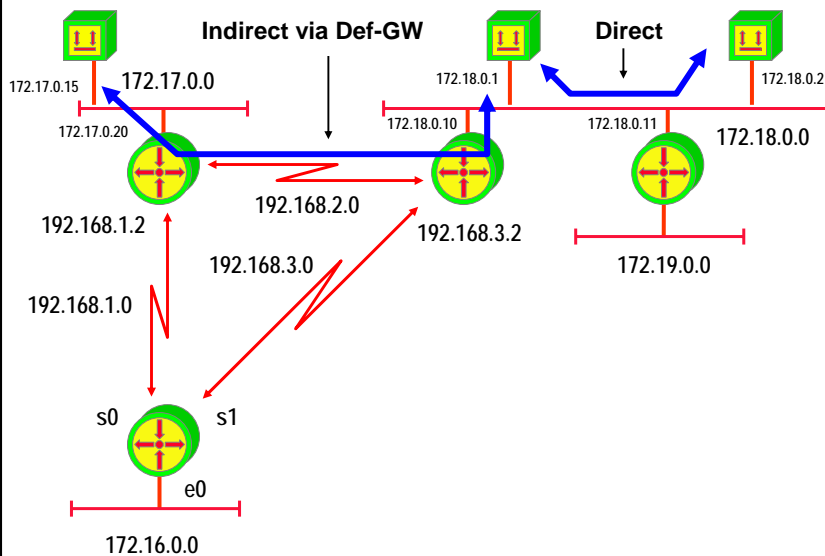
- **IP hosts and IP routers take part in this process**
 - IP hosts responsible for direct delivery of IP datagram's
 - IP routers responsible for selecting the best path in a meshed network in case of indirect delivery of IP datagram's
 - decision based on current state of routing table
- **direct versus 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

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

67

Direct versus Indirect Delivery



© 2007, D.I. Manfred Lindner

IP Technology, v4.7

68

L08 - IP Technology

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)

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

69

IP Routing Paradigm

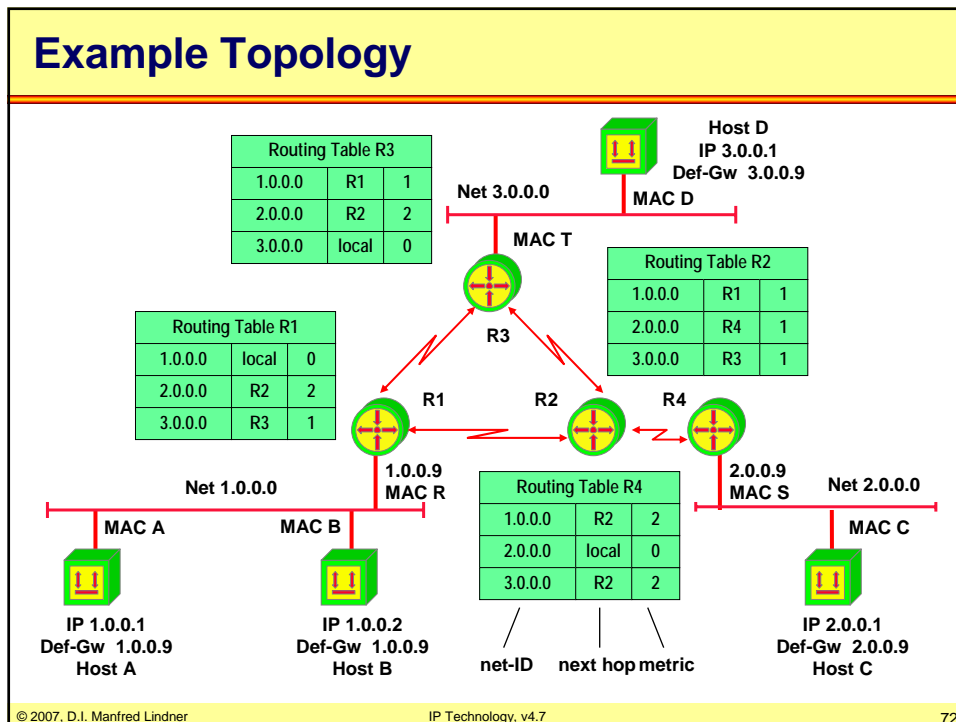
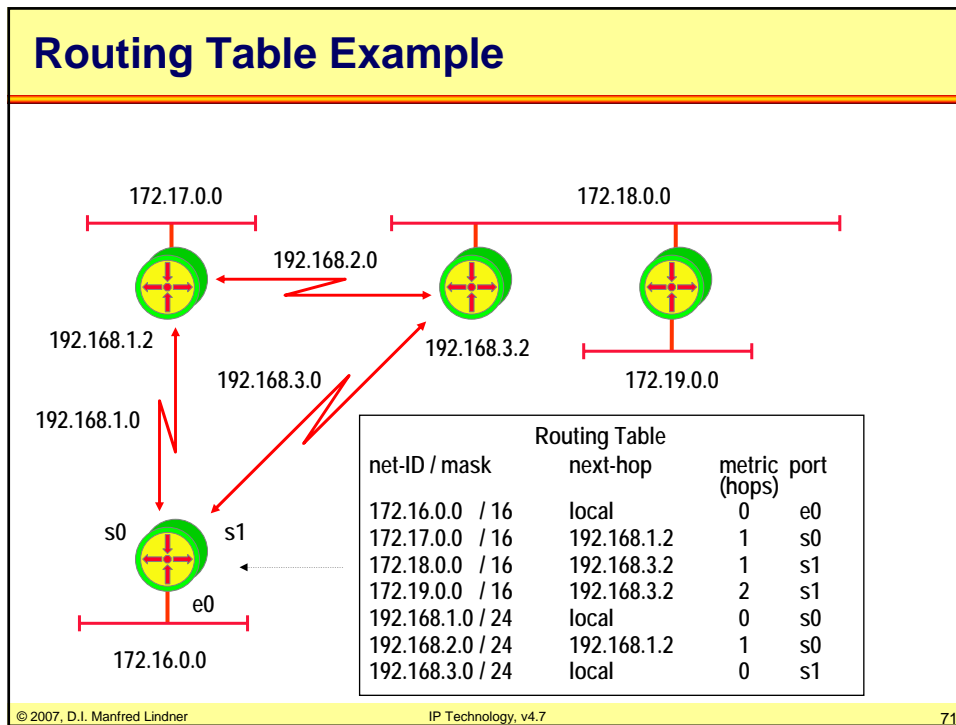
- **Destination Based Routing**
 - source address is not taken into account for the forward decision
- **Hop by Hop Routing**
 - IP datagram's follow the path, which is pointed by the current state of the routing tables
- **Least Cost Routing**
 - normally only the best path is considered for forwarding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

© 2007, D.I. Manfred Lindner

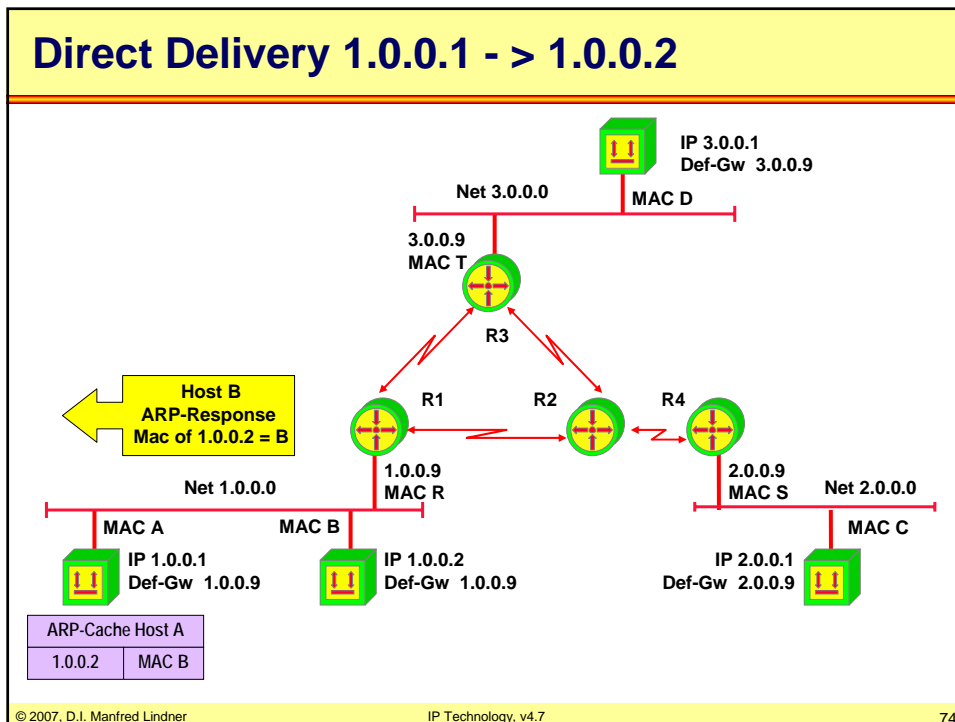
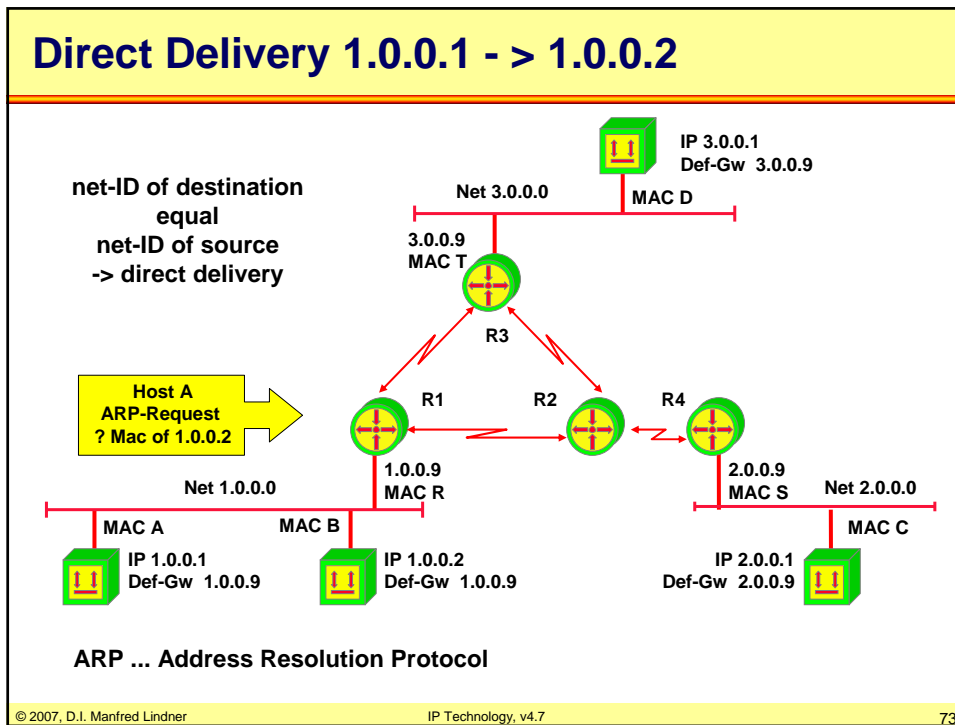
IP Technology, v4.7

70

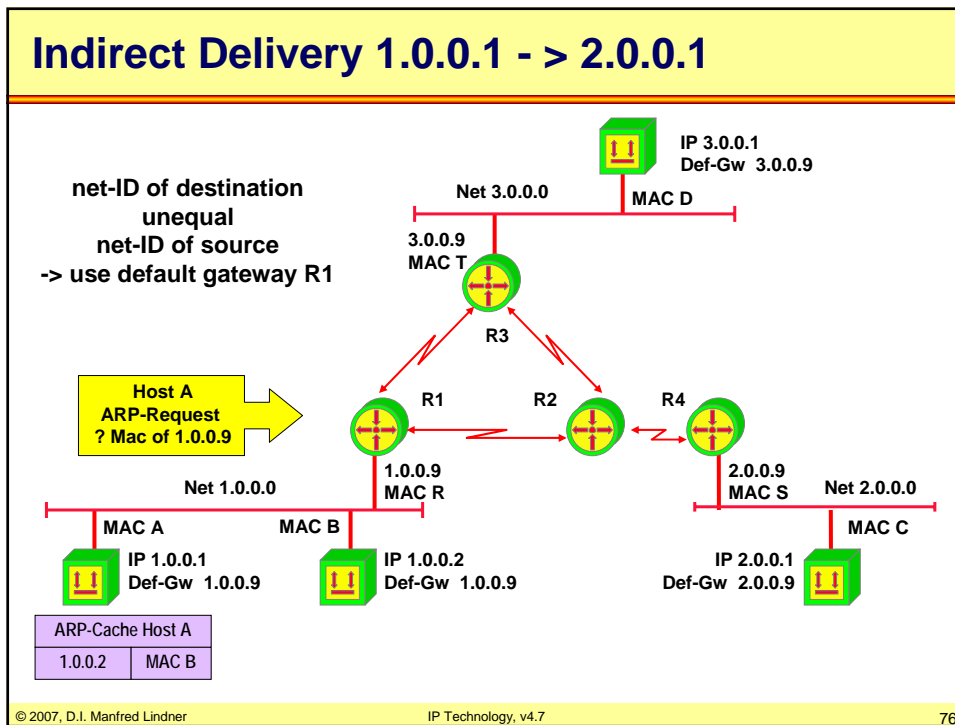
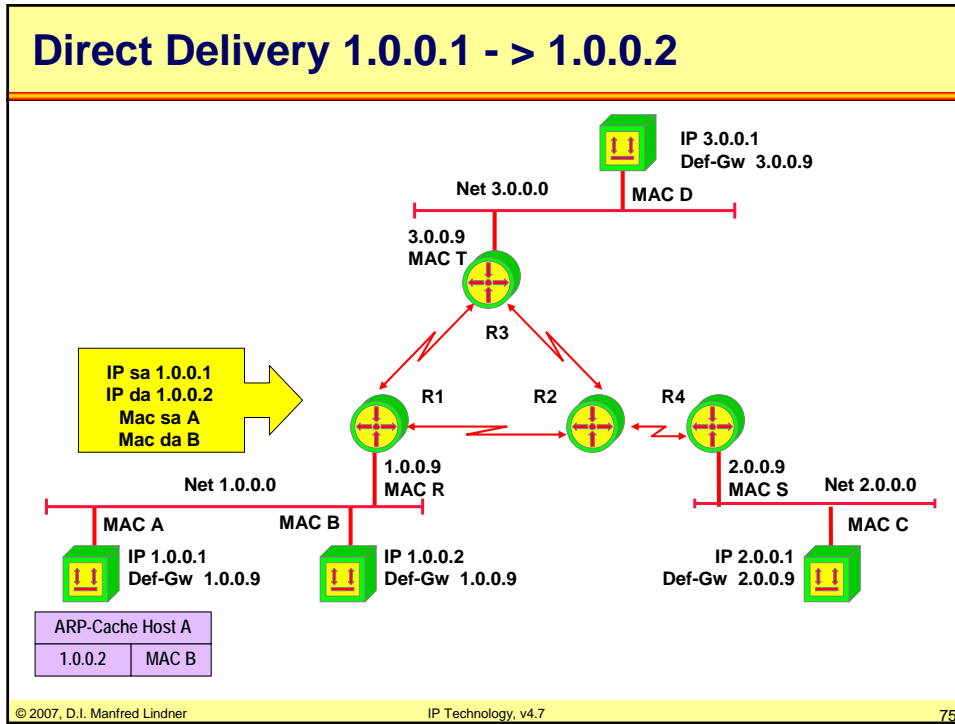
L08 - IP Technology



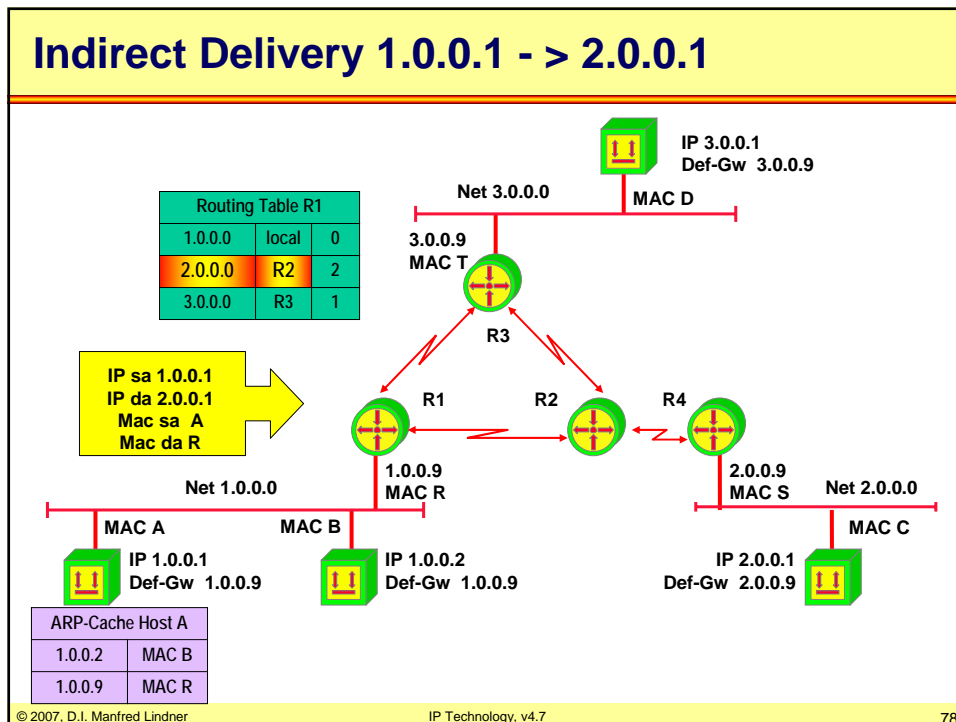
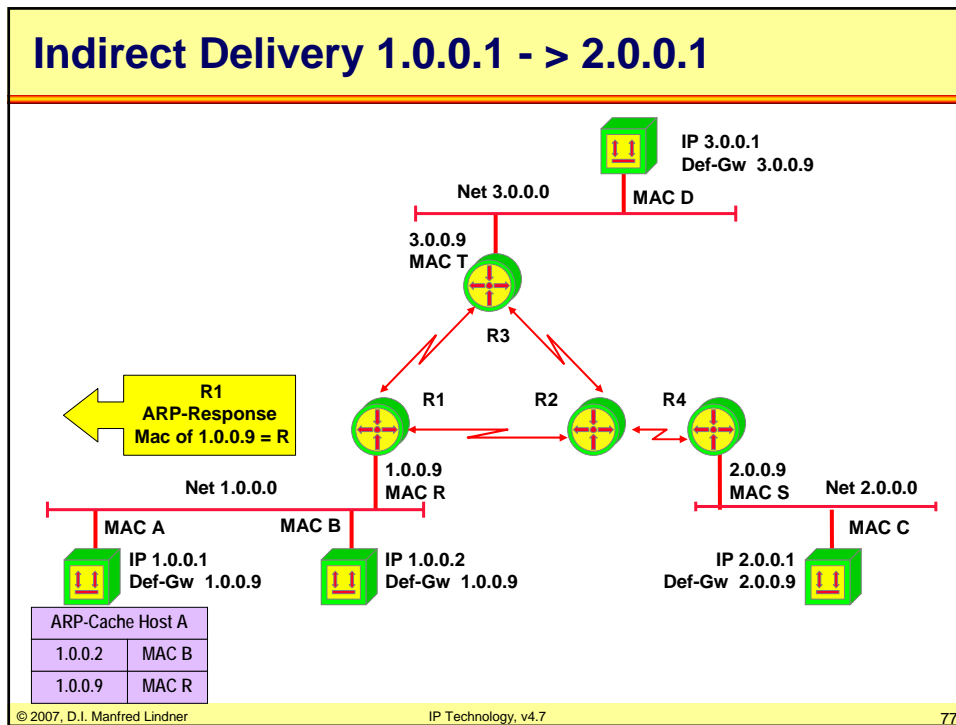
L08 - IP Technology



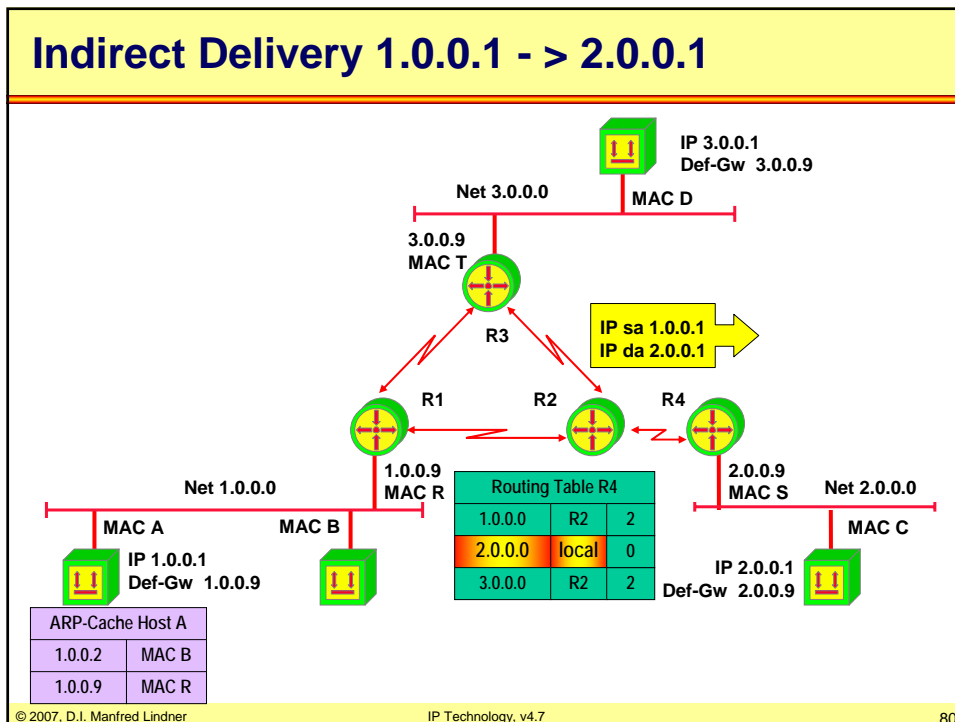
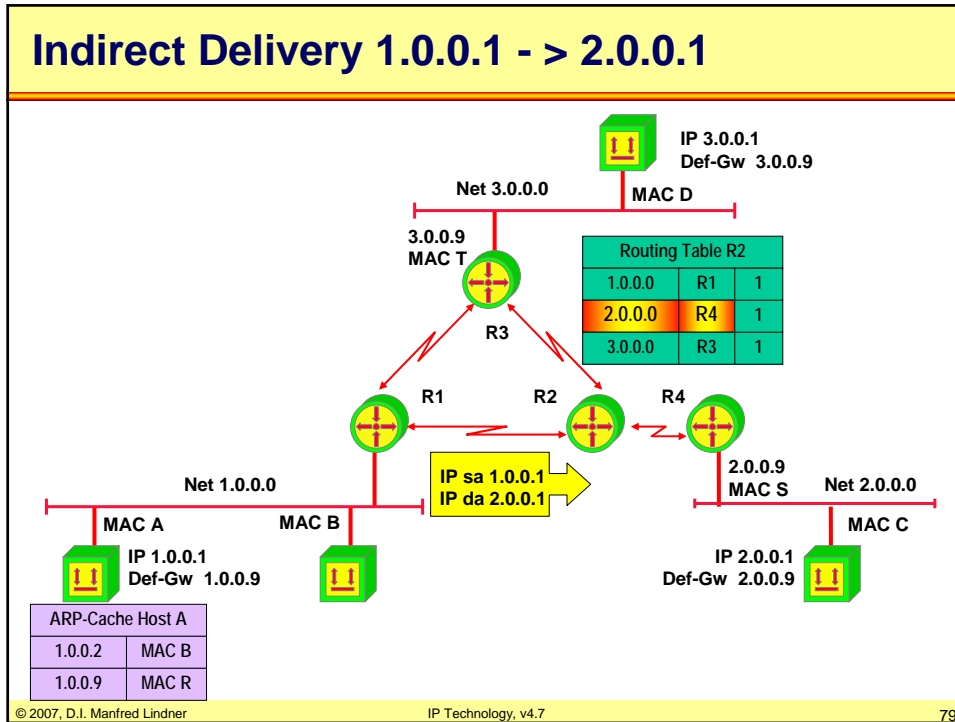
L08 - IP Technology



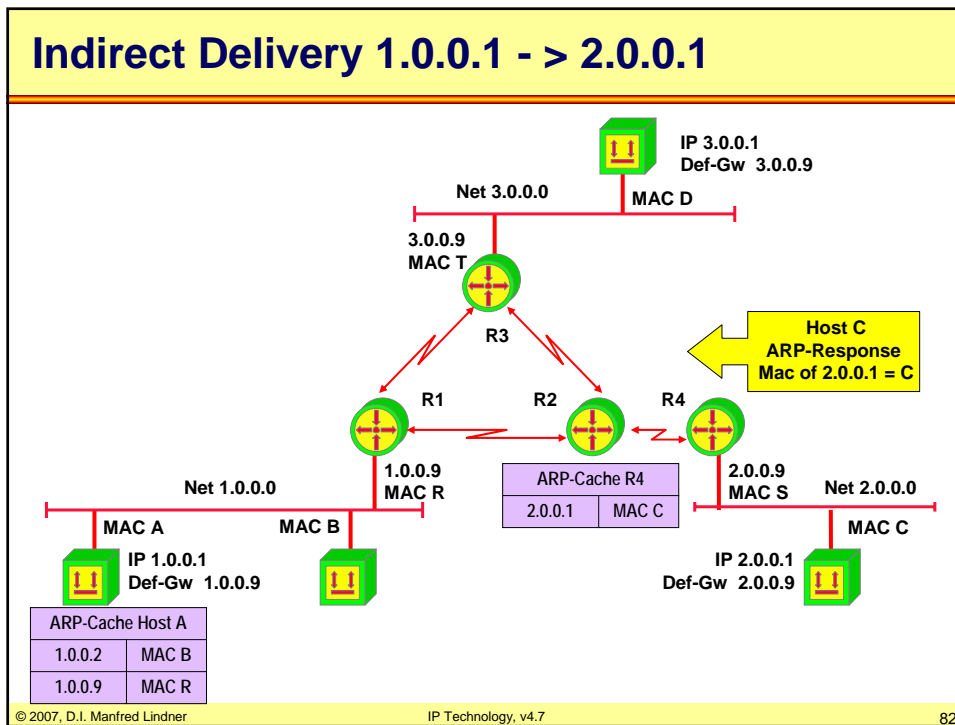
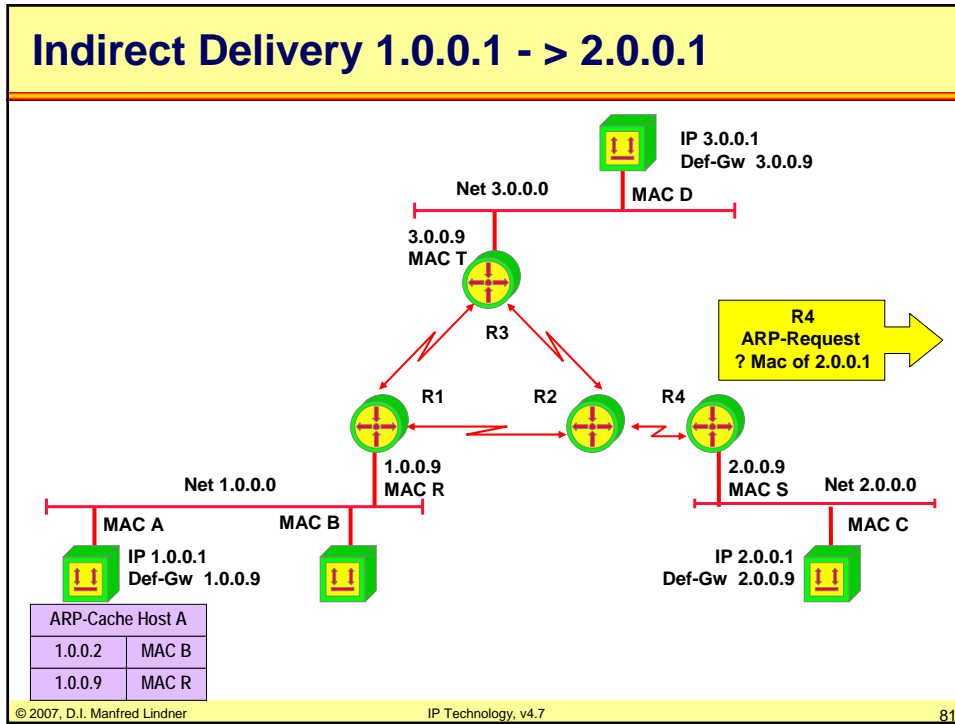
L08 - IP Technology



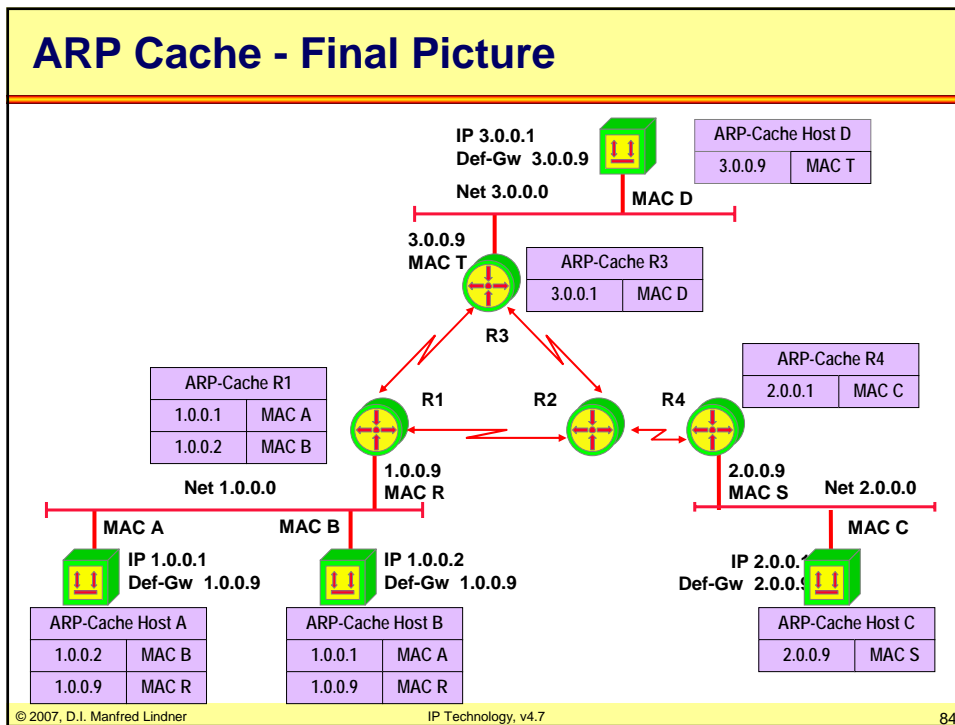
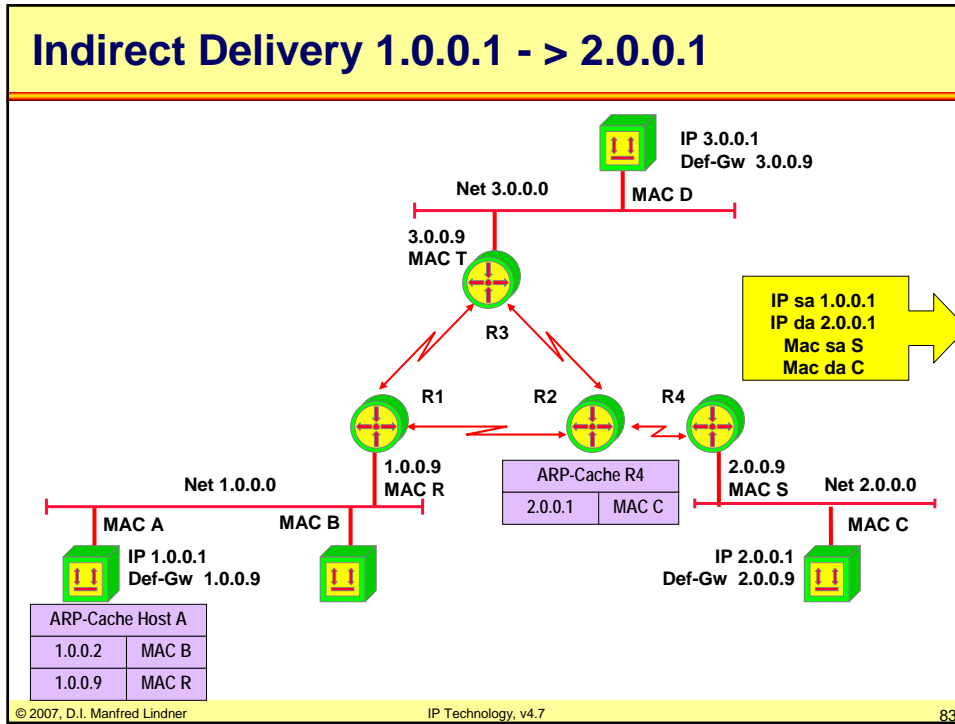
L08 - IP Technology



L08 - IP Technology



L08 - IP Technology



L08 - IP Technology

Agenda

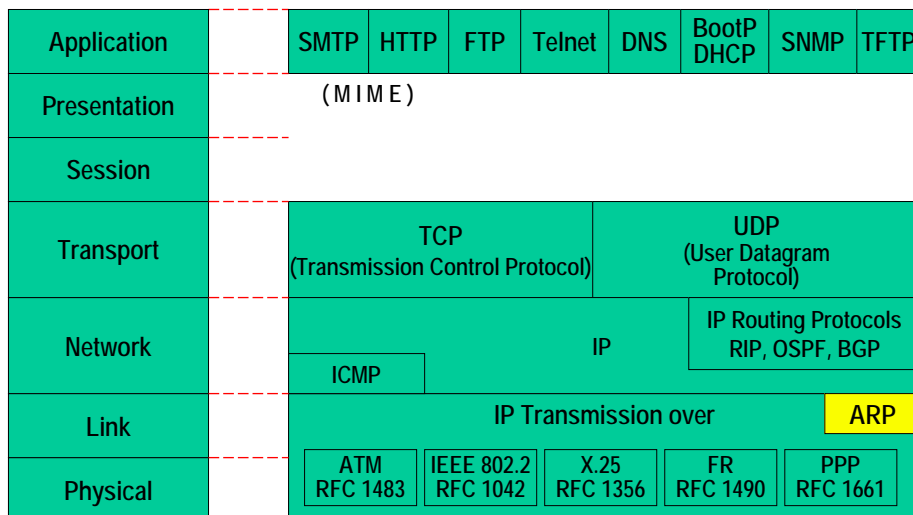
- **Introduction**
- **IP**
 - IP Protocol
 - Addressing
- **IP Forwarding**
 - Principles
 - ARP
 - ICMP
 - PPP

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

85

IP Related Protocols



© 2007, D.I. Manfred Lindner

IP Technology, v4.7

86

L08 - IP Technology

ARP (Address Resolution Protocol)

- An IP address identifies the logical access to an IP network
- The station can be reached without any further addressing, if the physical network consists only of a point-to-point connection
- On a shared media LAN MAC addresses are used to deliver packets to a specific station
- A mapping between IP address and MAC address is needed
- RFC 826

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

87

ARP Operation

1

- The mapping between MAC- and protocol-address on a LAN can be static (table entries) or dynamic (ARP protocol and ARP cache)
- Operation of ARP:
 - Station A wants to send to station B and doesn't know the MAC address (both are connected to the same LAN)
 - A sends an ARP request in form of a MAC broadcast (dest. = FF, source = Mac_A), ARP request holds IP address of B
 - Station B sees the ARP request with its IP address and sends an ARP response as a MAC frame (SA=Mac_B, DA=Mac_A), B puts the newly learned mapping (source MAC- and IP-address of A) into its ARP cache

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

88

L08 - IP Technology

ARP Operation

2

- The ARP response holds MAC address of station B
- A stores the MAC- / IP-address mapping for station B in its ARP cache
- For subsequent packets from A to B or from B to A the MAC addresses are taken from the ARP cache (no further ARP request / response)
- Entries in the ARP cache are deleted if they aren't used for a defined period (usually 5 min), this aging mechanism allows for changes in the network and saves table space
- ARP requests / responses are sent in Ethernet II or SNAP frames (Type field 0x0806)
- ARP has been designed to support different layer 3 protocols

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

89

ARP Request/Response Format

Hardware		Protocol (IP = 0x0800)
hIn	pIn	Operation
Source Hardware Address (byte 0 - 3)		
Source HW Addr. (byte 4 - 5)		Source IP Addr. (byte 0 - 1)
Source IP Addr. (byte 2 - 3)		Dest. HW Addr. (byte 0 - 1)*
Destination Hardware Address (byte 2 - 5)*		
Destination IP Address (byte 0 - 3)		

*) Destination hardware address is left empty (hex FF FF FF FF FF) for ARP request.

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

90

L08 - IP Technology

ARP Request/Response Fields

- **Hardware**

- Defines the type of network hardware, e.g.:
 - 1 Ethernet DIX
 - 6 802.x-LAN
 - 7 ARCNET
 - 11 LocalTalk

- **Protocol**

- Selects the layer 3 protocol (uses the values which are defined for the Ethernet type field, e.g. 0x800 for IP)

- **hln**

- Length of hardware address in bytes

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

91

ARP Request/Response Fields

- **pln**

- Length of layer 3 address in bytes

- **Operation**

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

- **Addresses**

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

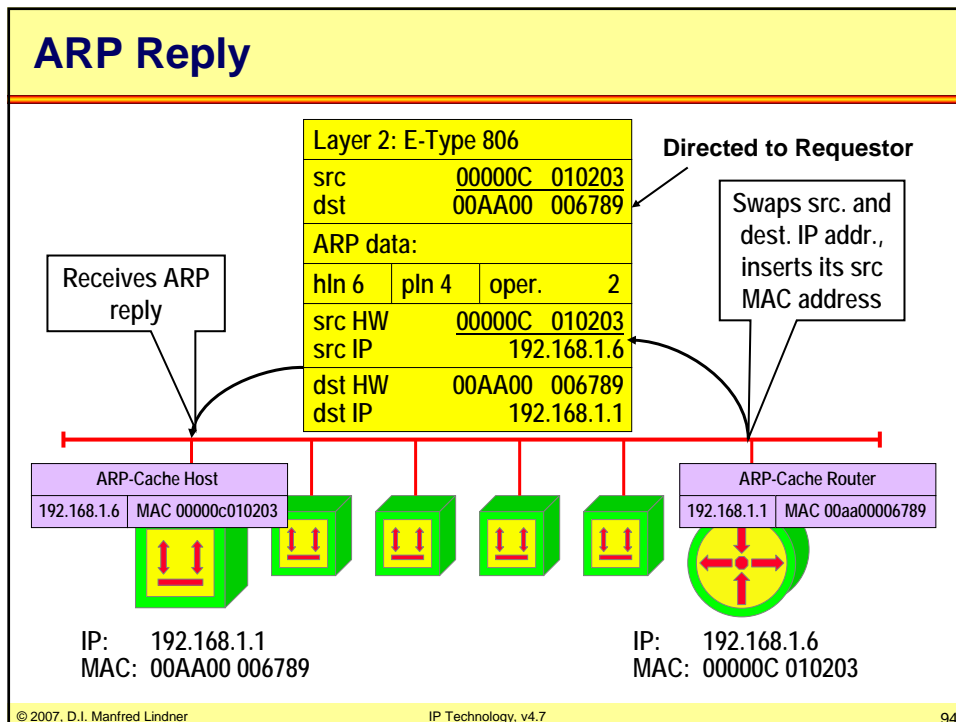
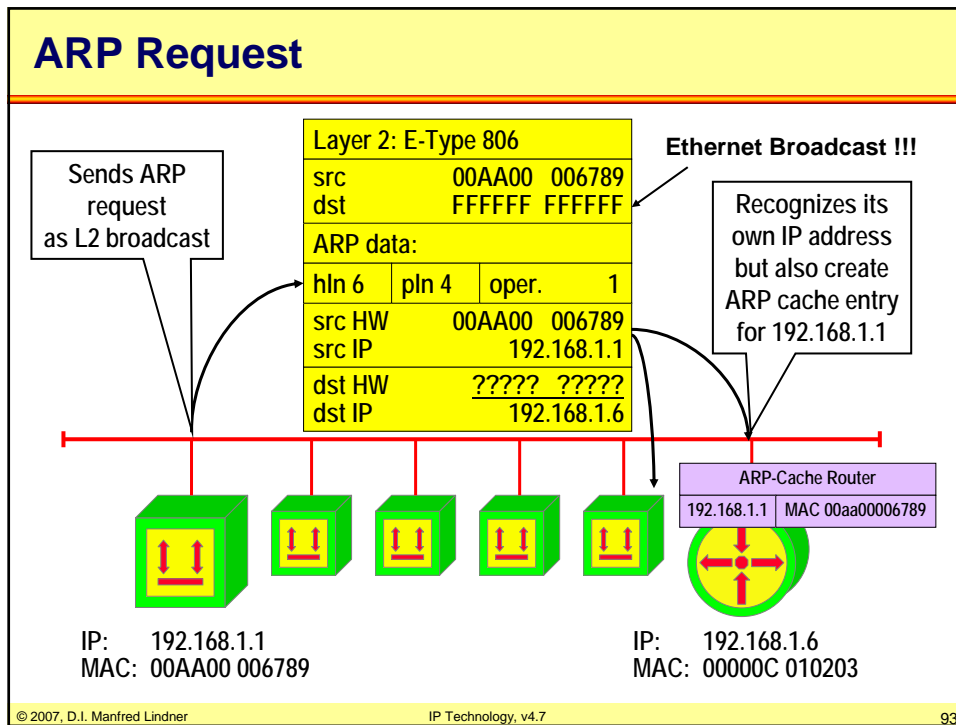
- **ARP request and responses are not forwarded by routers (LAN broadcast only!!!)**

© 2007, D.I. Manfred Lindner

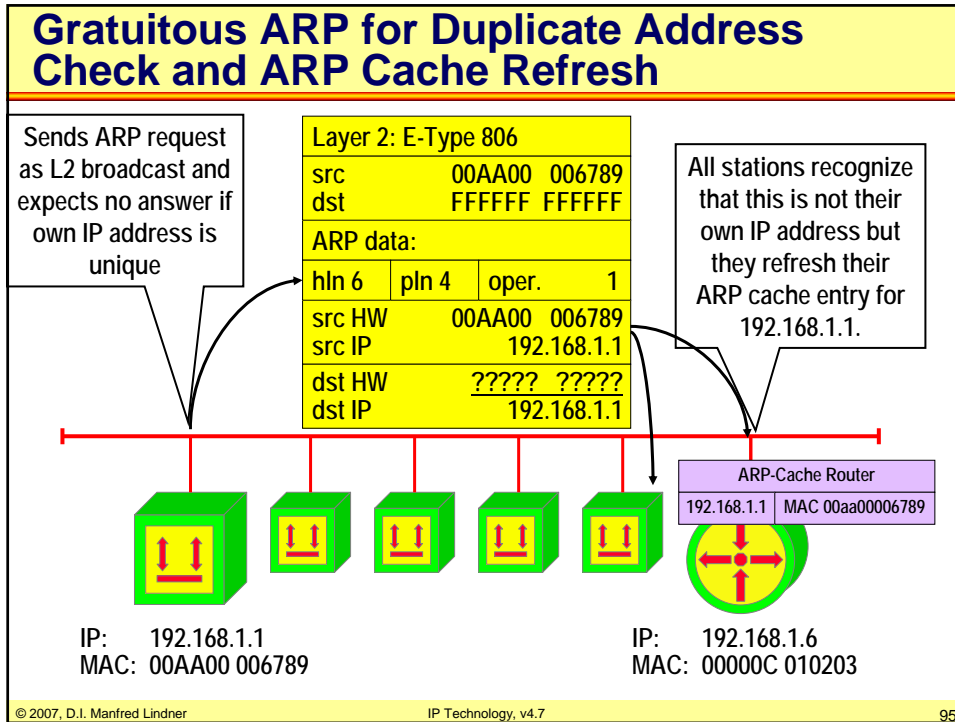
IP Technology, v4.7

92

L08 - IP Technology



L08 - IP Technology

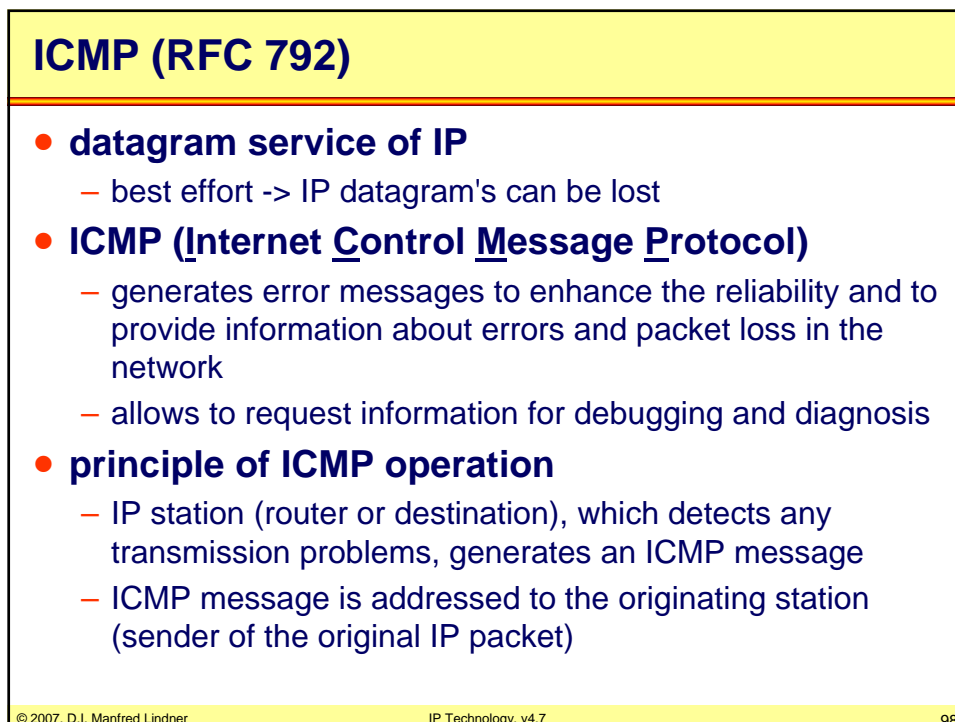
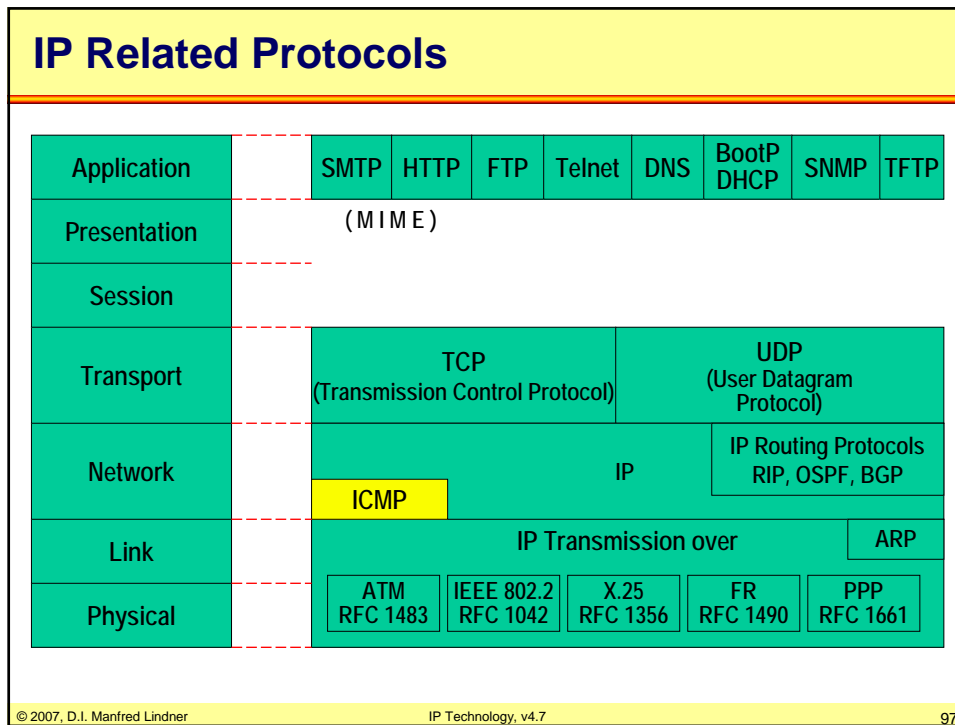


Agenda

- **Introduction**
- **IP**
 - IP Protocol
 - Addressing
- **IP Forwarding**
 - Principles
 - ARP
 - ICMP
 - PPP

© 2007, D.I. Manfred Lindner IP Technology, v4.7 96

L08 - IP Technology



L08 - IP Technology

ICMP

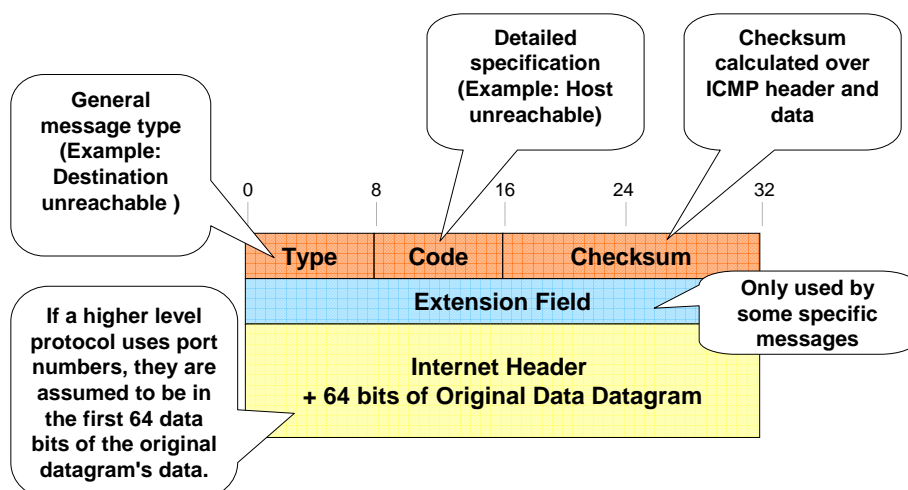
- **ICMP messages are sent as IP packets**
 - protocol field = 1, ICMP header and code in the IP data area
- **If a IP datagram carrying an ICMP message cannot be delivered**
 - No additional ICMP error message is generated to avoid an ICMP avalanche
 - "ICMP must not invoke ICMP"
 - Exception: PING command (Echo request and echo response)
- **Analysis of ICMP messages**
 - through network management systems or statistic programs can give valuable hints for network administrators

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

99

ICMP Message Format



© 2007, D.I. Manfred Lindner

IP Technology, v4.7

100

L08 - IP Technology**Type Field**

0	Echo reply ("Ping")
3	Destination Unreachable Reason specified in Code
4	Source Quench (decrease data rate of sender) Theoretical Flow Control Possibility of IP
5	Redirect (use different router) More information in Code
8	Echo Request ("PING")
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 (finding the Net-ID of the network; e.g. SLIP)
17/18	Address Mask Request / Reply

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

101

Using ICMP Types

0, 8	"PING" testing whether an IP station (router or end system) can be reached and is operational
3, 11, 12	Signaling errors concerning reachability, TTL / reassembly timeouts and errors in the IP header
4	Flow control (only possibility to signal a possible buffer overflow)
5	Signaling of alternative (shorter) routes to a target
13 - 18	Diagnosis or management

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

102

L08 - IP Technology

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

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

103

Code Field for Type 3 (destination unreachable)

See RFC1122 (Host Requirements) page 38:

The following additional codes are hereby defined:

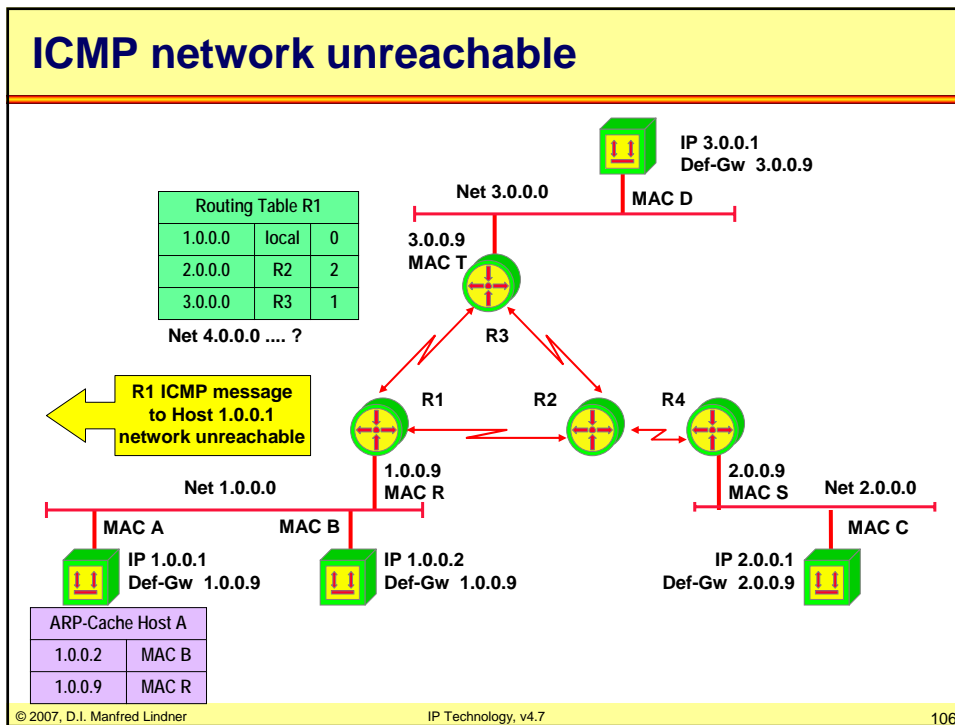
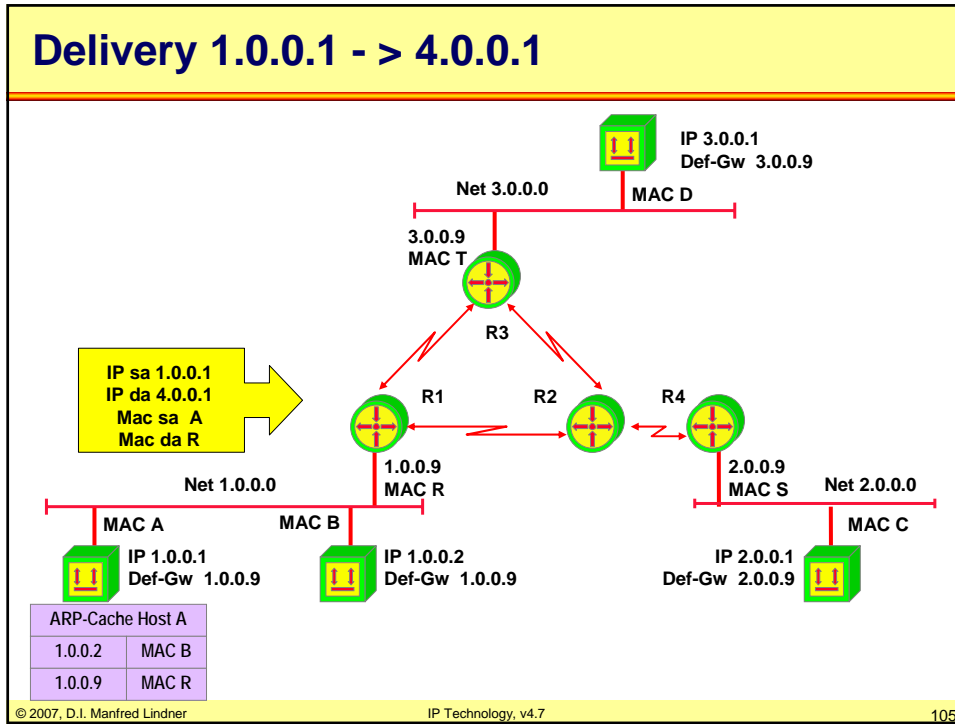
- 6 ... destination network unknown
- 7 ... destination host unknown
- 8 ... source host isolated
- 9 ... communication with destination network administratively prohibited
- 10 ... communication with destination host administratively prohibited
- 11 ... network unreachable for type of service
- 12 ... host unreachable for type of service

© 2007, D.I. Manfred Lindner

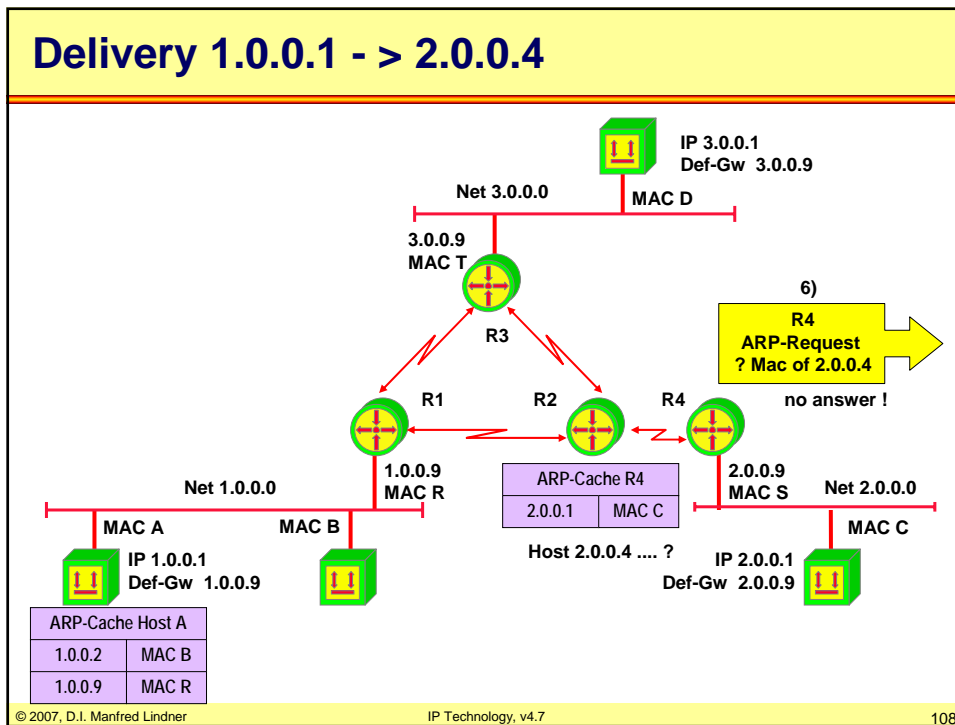
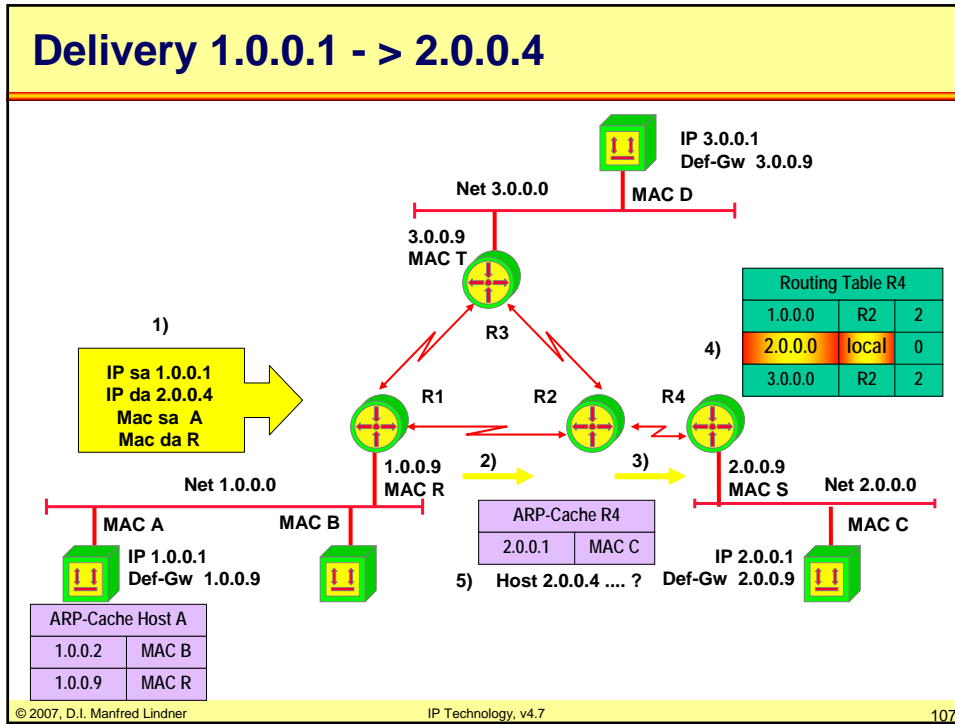
IP Technology, v4.7

104

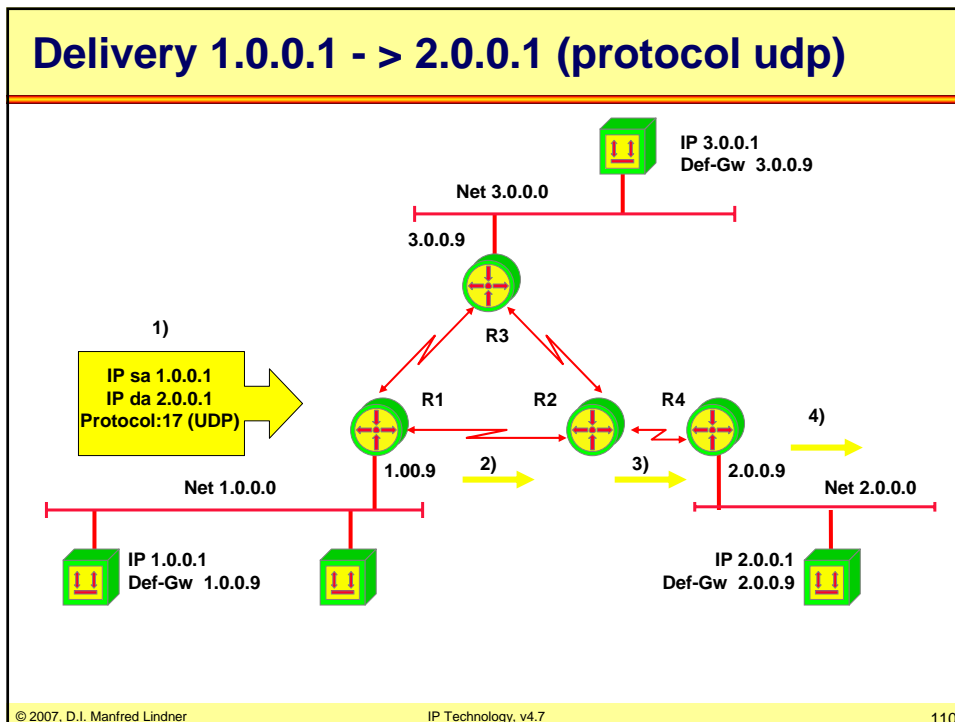
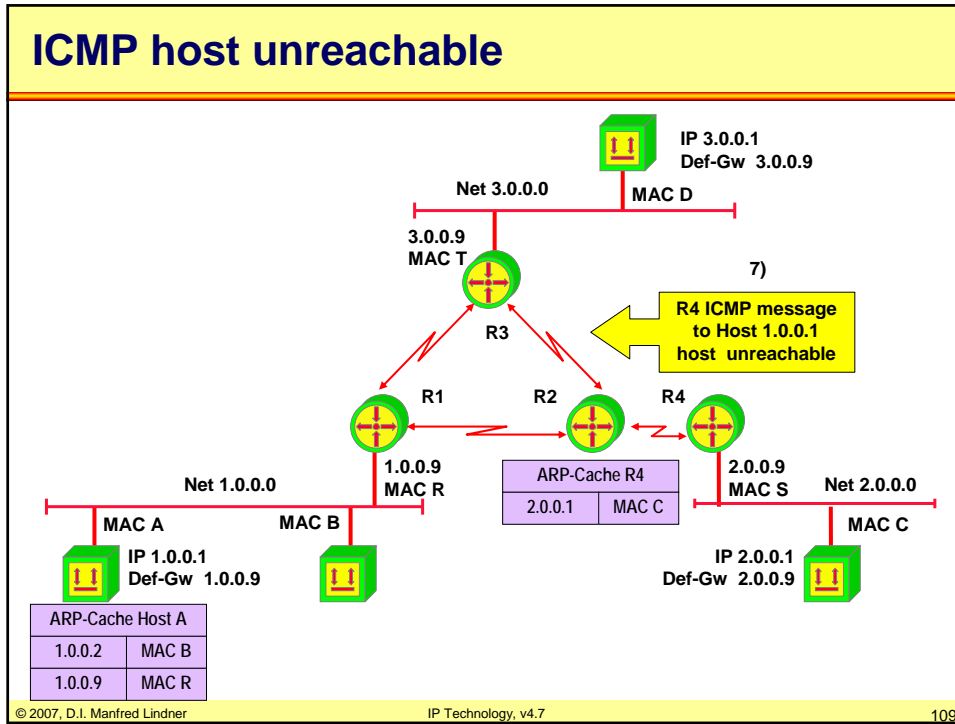
L08 - IP Technology



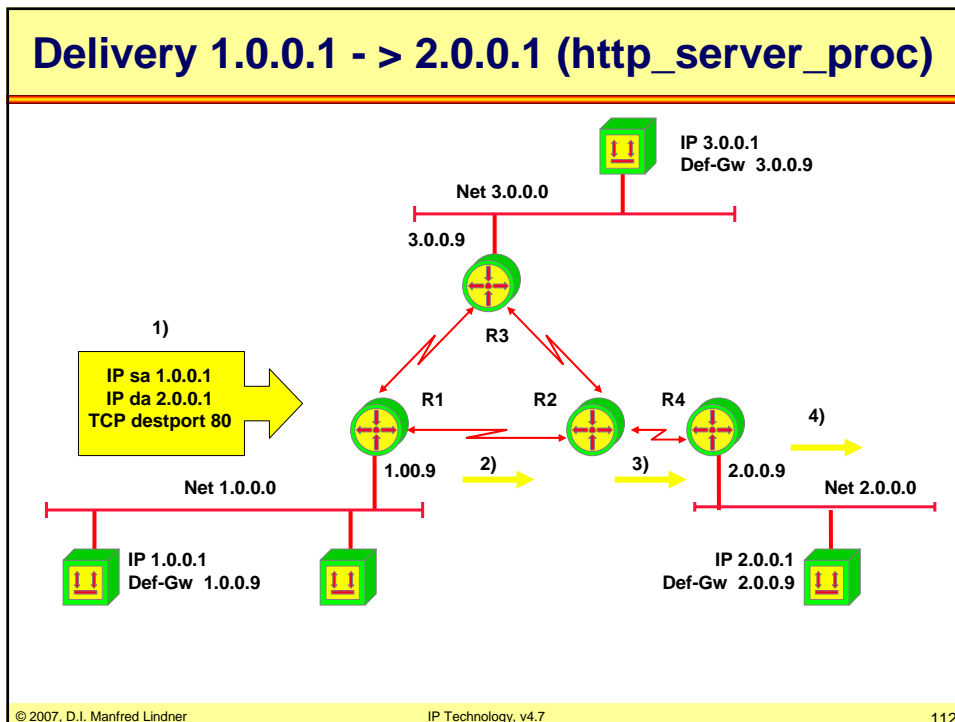
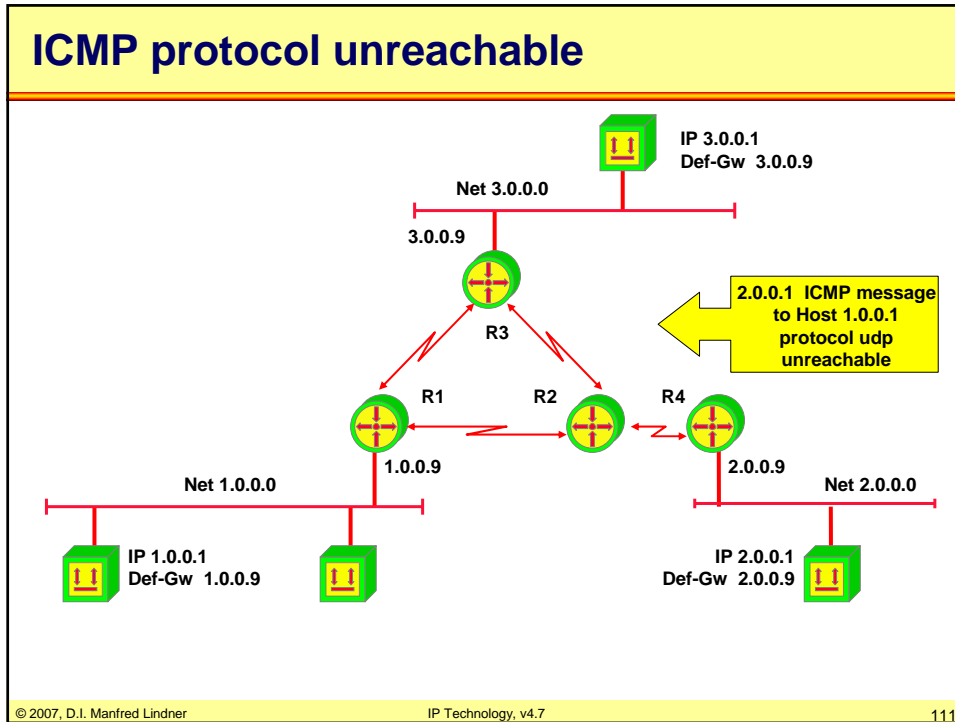
L08 - IP Technology



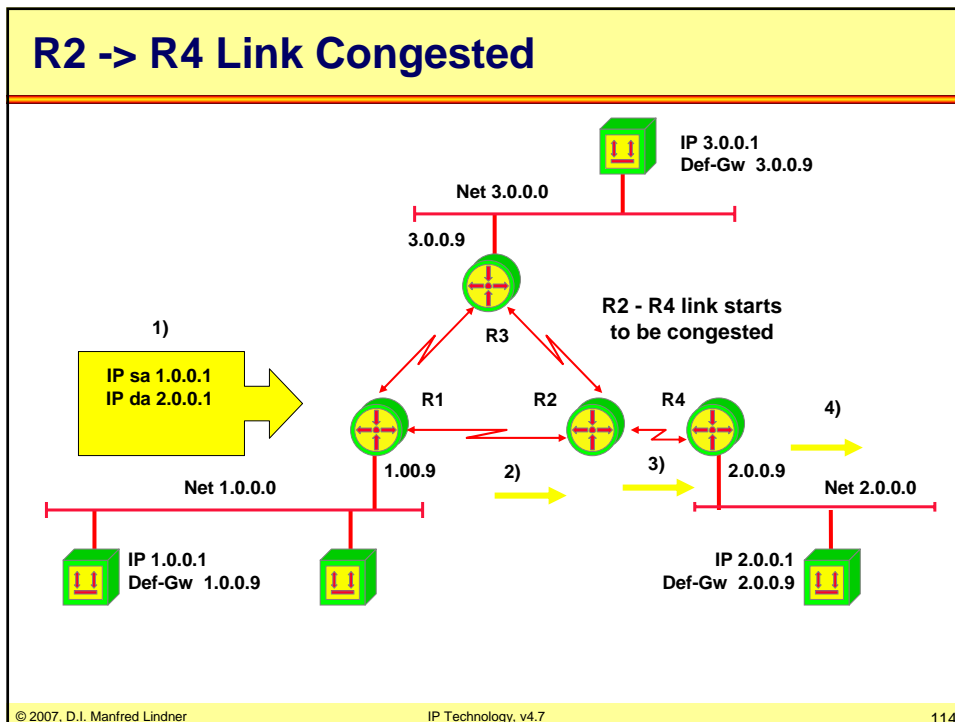
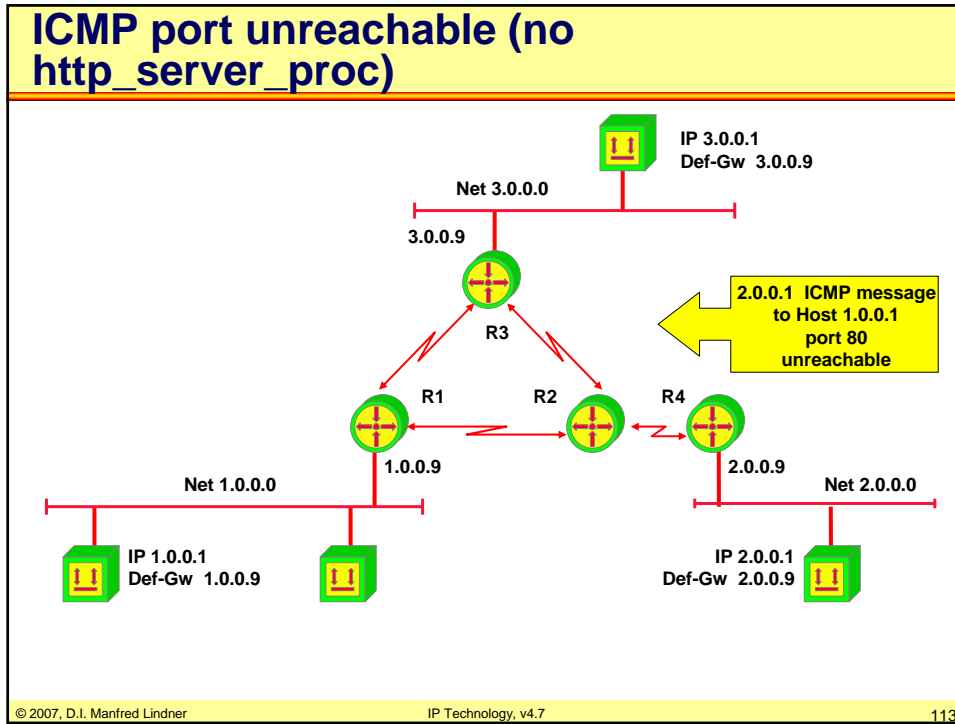
L08 - IP Technology



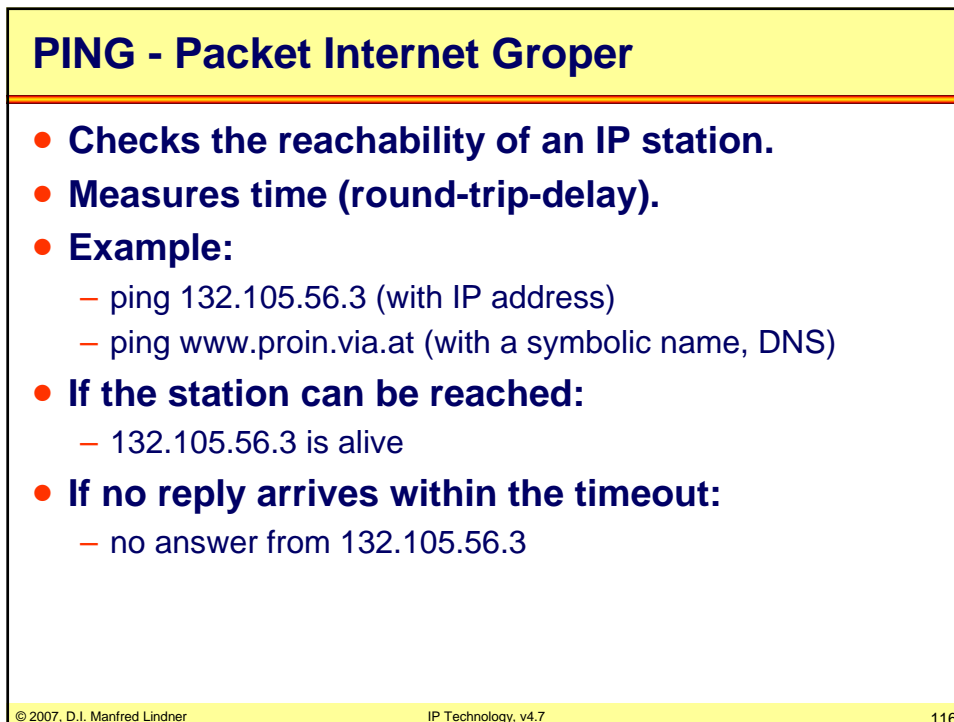
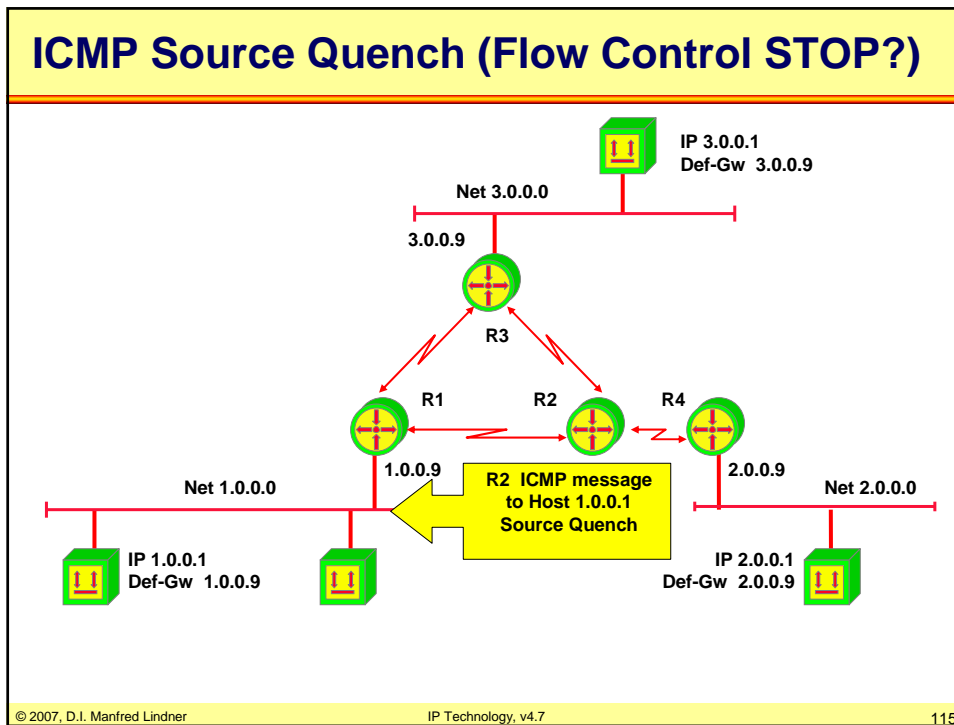
L08 - IP Technology



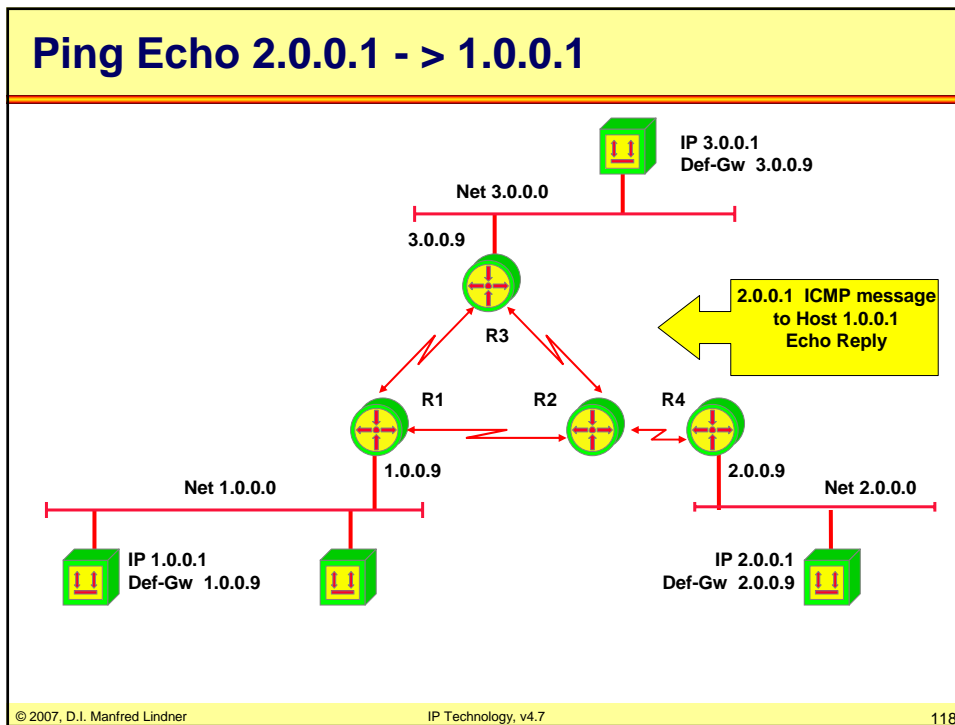
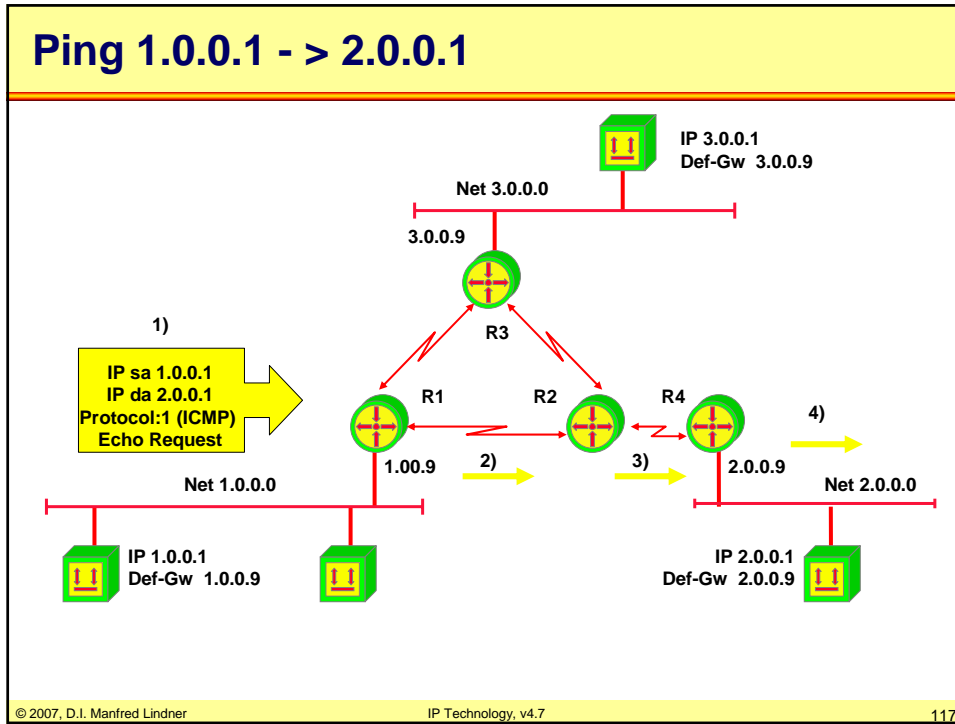
L08 - IP Technology



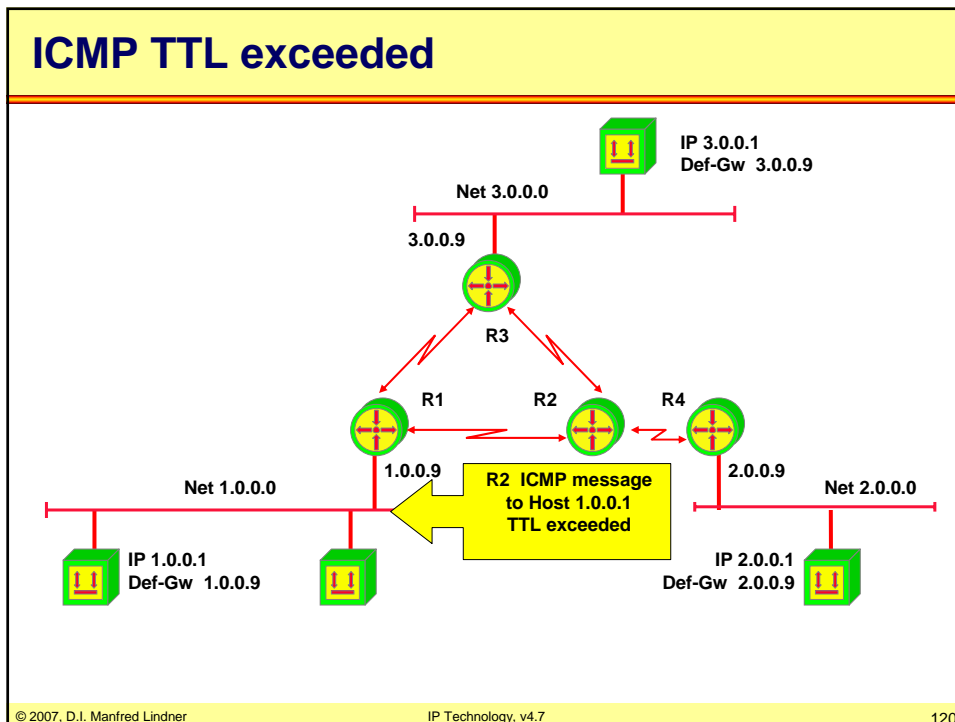
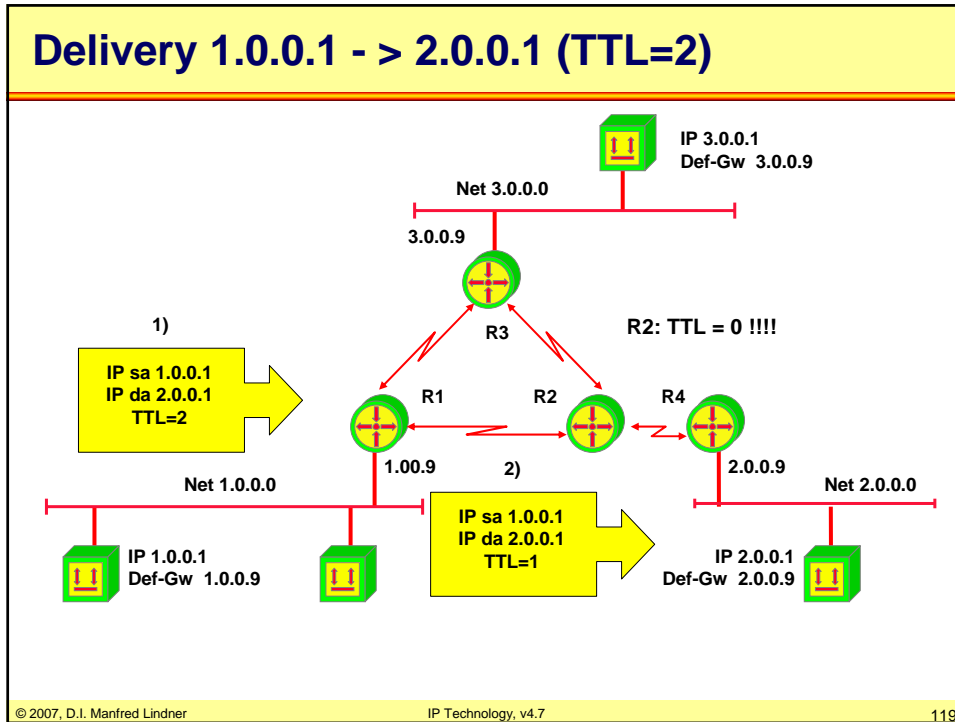
L08 - IP Technology



L08 - IP Technology



L08 - IP Technology



L08 - IP Technology

Traceroute

- Lists the exact route, a packet will take through the network
- UDP segment and manipulation of the TTL field (time to live) of the corresponding IP header is used
 - to generate ICMP error messages
 - TTL exceeded
 - port not reachable
- UDP segments with undefined port number (> 30000)
 - Echo requests with TTL manipulation only can't be used because after reaching the final IP host no TTL exceeded message will be generated (done by routers only)

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

121

Traceroute - Operation

- UDP datagram with TTL=1 is sent
- UDP datagram with TTL=2 is sent
-
- The routers in the path generate ICMP time exceeded messages because TTL reaches 0
- If the UDP datagram arrives at the destination, an ICMP port unreachable message is generated
- From the source addresses in the ICMP messages the path can be reconstructed
- The IP addresses are resolved to names through DNS

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

122

L08 - IP Technology

Traceroute - Sample Output

tracert 140.252.13.65

```

1 bsdi (140.252.13.35)  20ms  10ms  10ms
2 slip (140.252.13.65) * 120ms 120ms
    
```

3 Packets are sent for each TTL value.
Output of "*", if no answer arrives within 5 seconds.

© 2007, D.I. Manfred Lindner

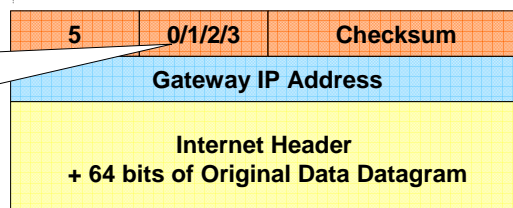
IP Technology, v4.7

123

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
 - Datagram's will be sent twice through a LAN, if the sender ignores the redirect message

0 = Redirect datagram's for the Network.
1 = Redirect datagram's for the Host.
2 = Redirect datagram's for the Type of Service (ToS) and Network.
3 = Redirect datagram's for the Type of Service (ToS) and Host.

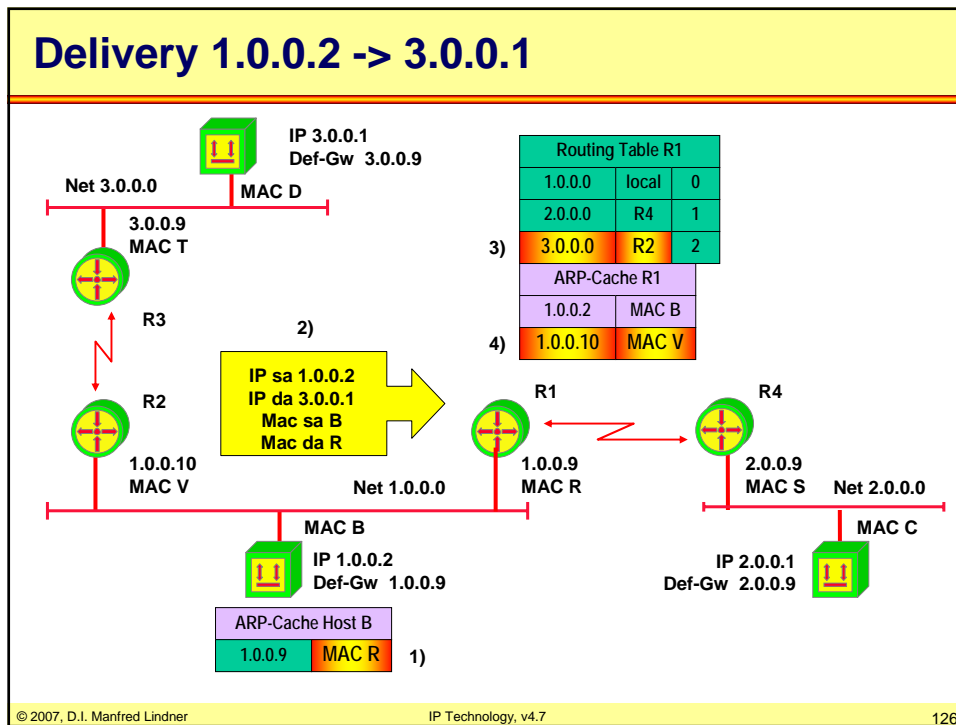
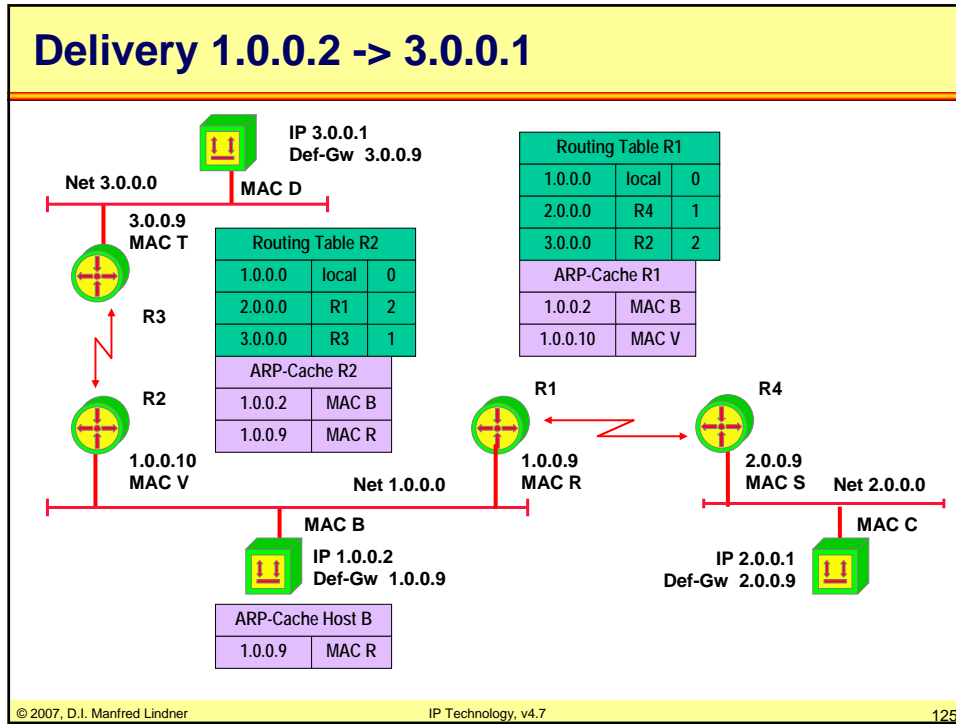


© 2007, D.I. Manfred Lindner

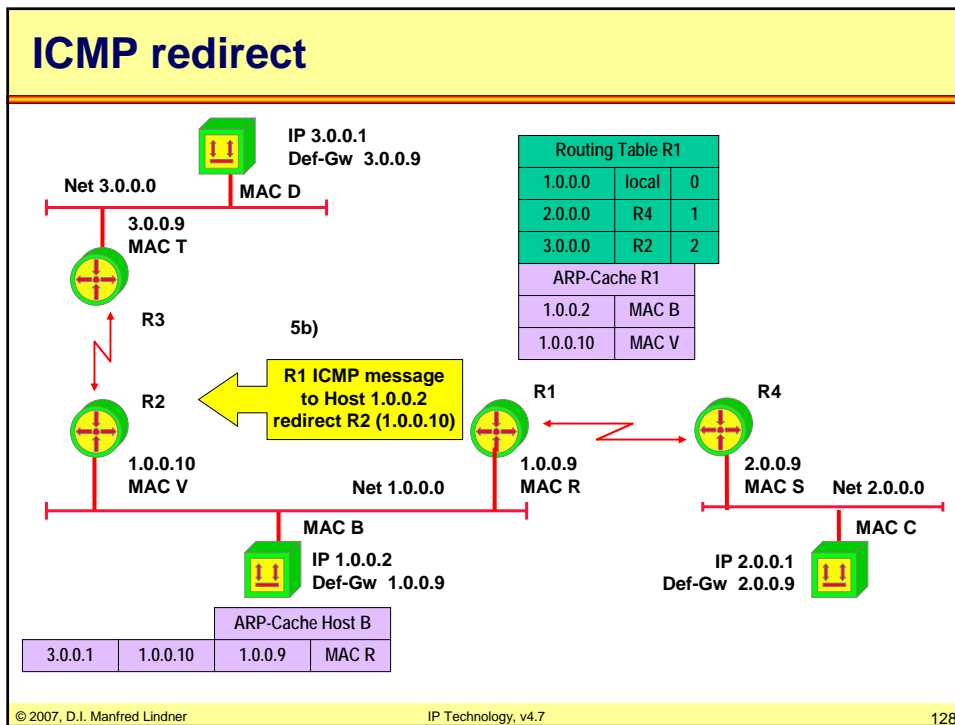
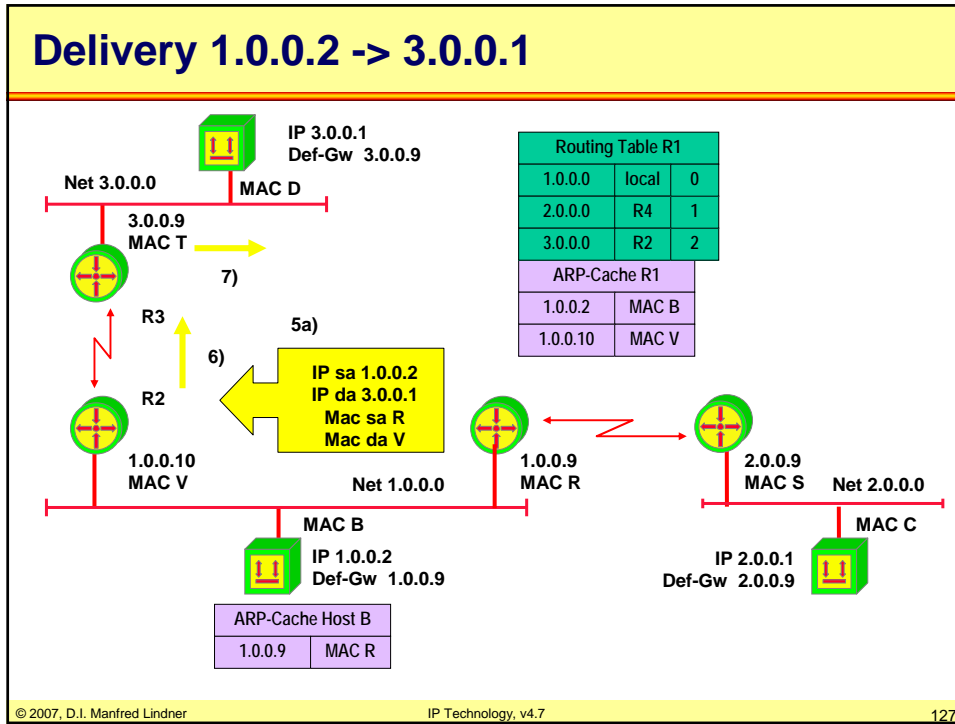
IP Technology, v4.7

124

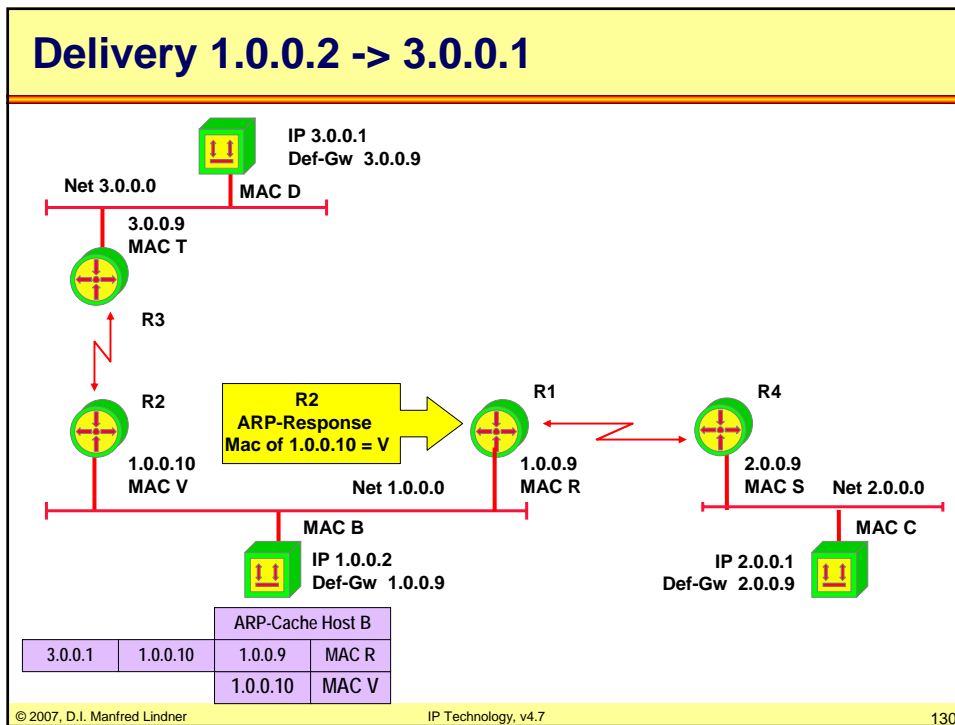
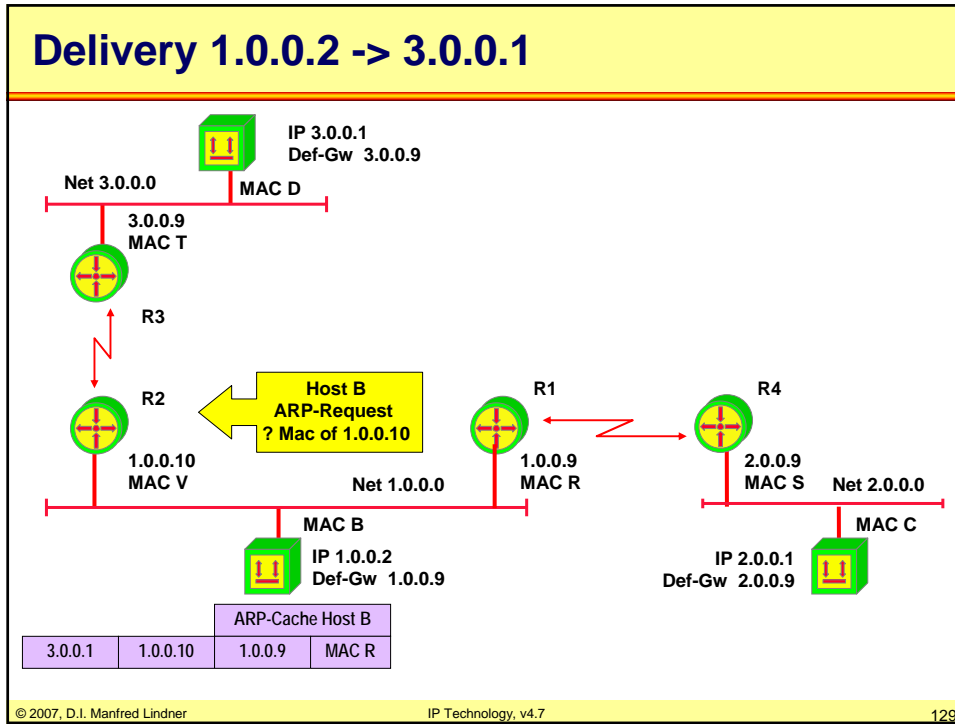
L08 - IP Technology



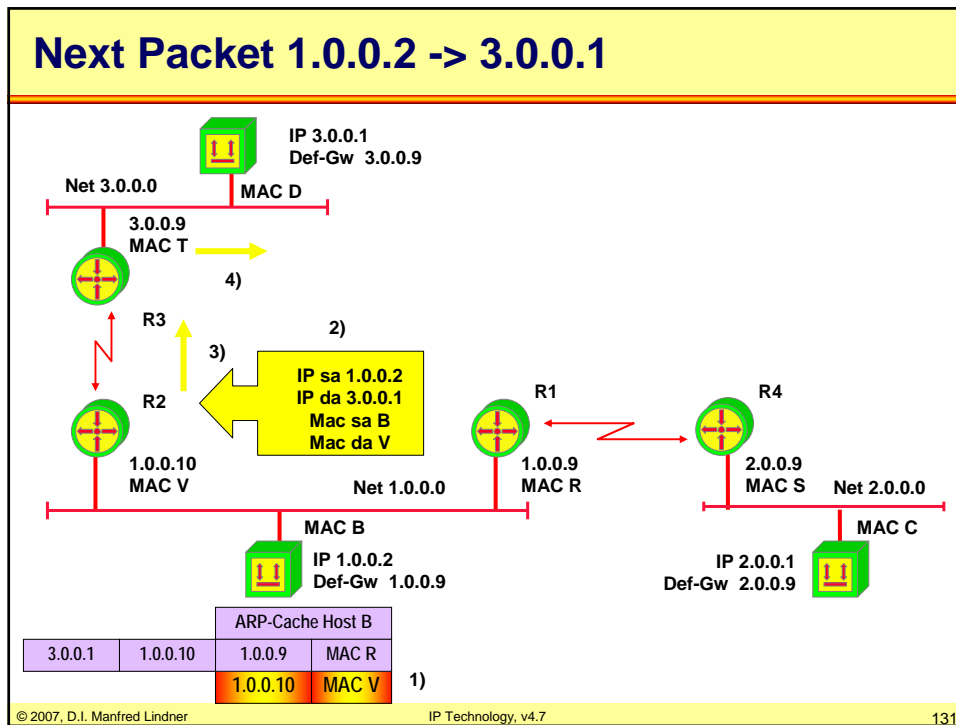
L08 - IP Technology



L08 - IP Technology



L08 - IP Technology



Agenda

- **Introduction**
- **IP**
 - IP Protocol
 - Addressing
- **IP Forwarding**
 - Principles
 - ARP
 - ICMP
 - PPP

© 2007, D.I. Manfred Lindner IP Technology, v4.7 132

L08 - IP Technology

Reasons for Point-to-Point Protocol (PPP)

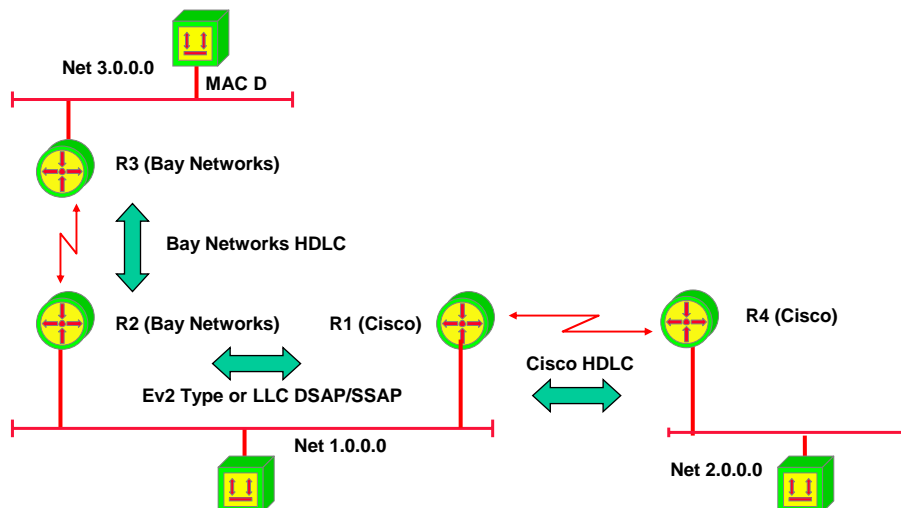
- **Communication between router of different vendors on a LAN was possible**
 - from the very beginning
 - Remember: Ethernet V2 Protocol Type field or LLC-DSAP/SSAP fields carry information about the protocol stack (e.g. IP or IPX or SAN or NetBEUI or AppleTalk)
- **Communication between router of different vendors on a serial line was not possible**
 - because of the proprietary “kind of HDLC” encapsulation method used by different vendors
- **PPP standardizes multiprotocol encapsulation on a serial line**
 - hence interoperability is the main focus

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

133

Interoperability without PPP

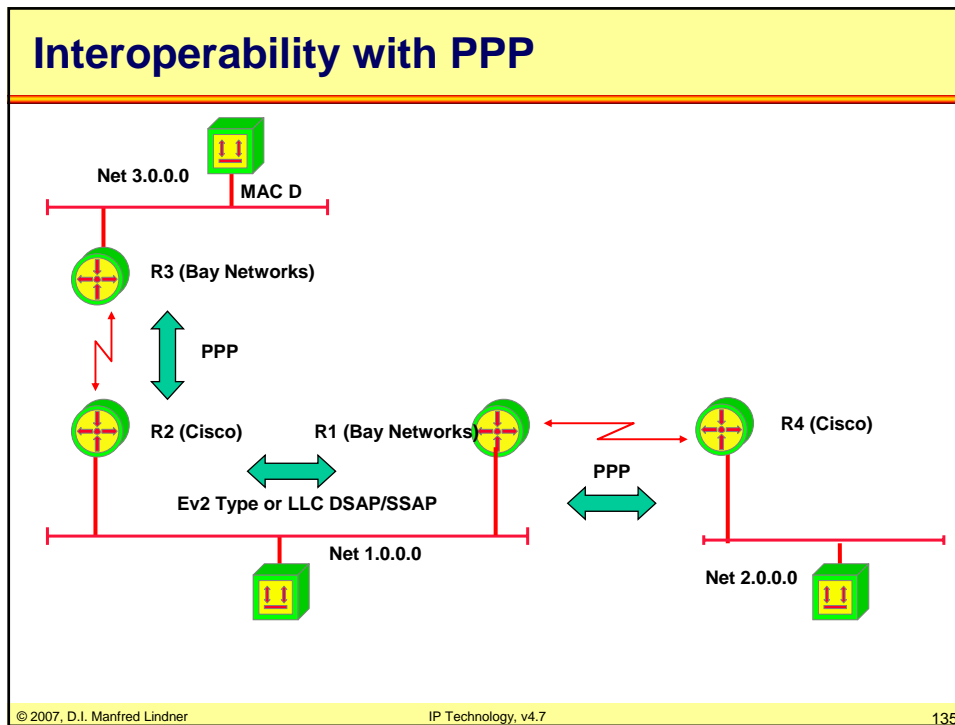


© 2007, D.I. Manfred Lindner

IP Technology, v4.7

134

L08 - IP Technology



- ### Today's Main Focus of PPP
- **Providing Dial-In connectivity for IP systems**
 - using modems and Plain Old Telephone Network (POTS)
 - PPP
 - using ISDN
 - PPP over transparent B-channel
 - using ADSL (Asymmetric Digital Subscriber Line)
 - PPPoE (PPP over Ethernet)
 - PPPoA (PPP over ATM)
 - using Dial-In VPN technology
 - Microsoft PPTP (Point-to-Point Tunneling Protocol)
 - Cisco L2F (L2 Forwarding Protocol)
 - L2TP (Layer2 Tunneling Protocol), IETF-RFC
- © 2007, D.I. Manfred Lindner IP Technology, v4.7 136

L08 - IP Technology

PPP Overview

- **data link protocol (L2)**
- **used to encapsulate network layer datagram's 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**

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

137

PPP Components

- **three major 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 (NCP, div. RFCs)
 - Configures and maintains network layer protocols
 - NCP's exist for IP, OSI, DECnet, AppleTalk, Novell
 - NCP's are started after PPP link establishment through LCP

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

138

L08 - IP Technology

PPP Frame Format



Flag = 01111110 Protocol = see RFC 1700 (assigned numbers)
 Address = 11111111 Information = Network Layer PDU
 Control = 00000011 (UI frame) FCS = 16 bit

- **some protocol fields**

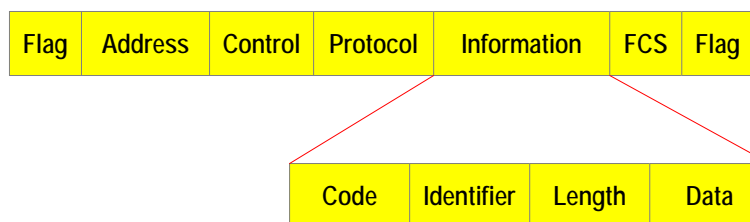
- 0021 Internet Protocol 0027 DECnet Phase 4
- 0029 AppleTalk 002b Novell IPX
- 8021 IP Control Protocol 8027 DECnet Control Protocol
- 8029 AppleTalk Control Prot. 802b IPX Control Protocol
- c021 Link Control Protocol C023 Authentication Protocol
- C223 Authentication CHAP

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

139

Link Control Protocol (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)

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

140

L08 - IP Technology

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)

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

141

LCP and PPP Connection

- **LCP**
 - supports the establishment of the PPP connection and allows certain configuration options to be negotiated
- **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, ...
 - phase 4: link termination

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

142

L08 - IP Technology

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
 - authentication protocol
 - quality protocol
 - Protocol-Field-Compression
 - Address-and-Control-Field-Compression
 - these options are described in RFC 1661 (except authentication protocols)

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

143

PPP Phases

- **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

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

144

L08 - IP Technology

PPP Phases

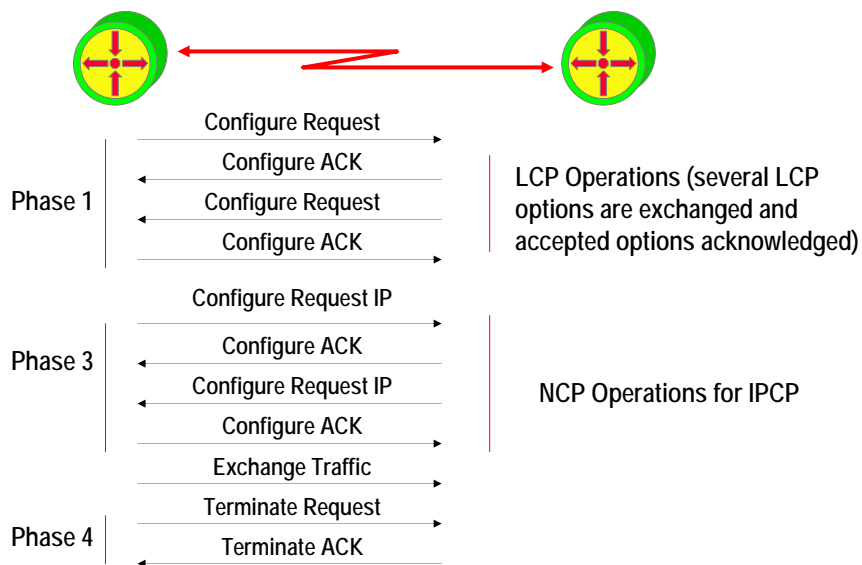
- **task of phase 2**
 - providing of optional facilities
 - authentication, compression initialization, multilink, etc.
- **task of phase 3**
 - network layer protocol configuration negotiation
 - after link establishment, stations negotiate/configure the protocols that will be used at the network layer; 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

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

145

PPP Link Operation Example



© 2007, D.I. Manfred Lindner

IP Technology, v4.7

146

L08 - IP Technology

Network Control Protocol

- one per upper layer protocol (IP, IPX...)
- each NCP negotiates parameters appropriate for that protocol
- NCP for IP (IPCP)
 - IP address, Def. Gateway, DNS Server, TTL, TCP header compression can be negotiated
 - Similar functionality as DHCP for LAN

IPCP addr = 10.0.2.1 compr = 0	IPXCP net = 5a node = 1234.7623.1111
LCP	
Link	

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

147

CHAP Authentication RFC 1994

- **Challenge Authentication Protocol**
- **follows establishment of LCP**
- **identifies user**
- **three way handshake**
- **one way authentication only**
 - station which starts the three way handshake proofs authentication of other station
 - must be configured on both sides if two way authentication is necessary
- **snooping does not discover password**

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

148

L08 - IP Technology

CHAP Operation

- **three way handshake**

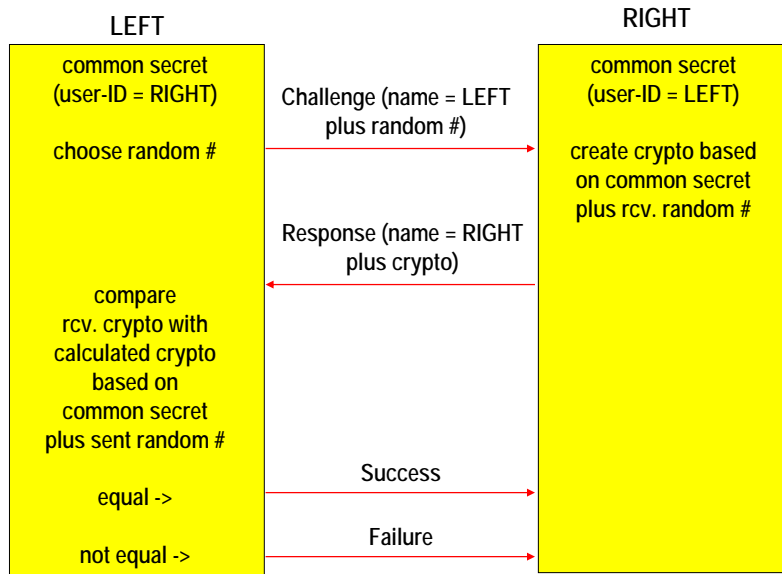
- PPP link successfully installed by LCP
- local station sends a challenge message to remote station
- challenge contain random number and own user-id
- remote station replies with value using one way hash function based on crypto negotiated for this user-id
- response is compared with stations own calculation of random number with same crypto
- if equal success messages is sent to remote station
- if unequal failure message is sent

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

149

CHAP Authentication Procedure



© 2007, D.I. Manfred Lindner

IP Technology, v4.7

150

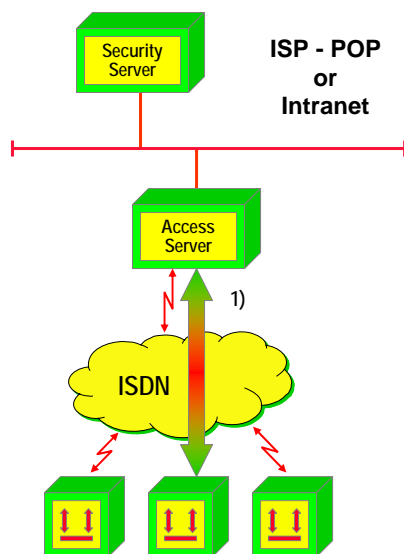
L08 - IP Technology

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

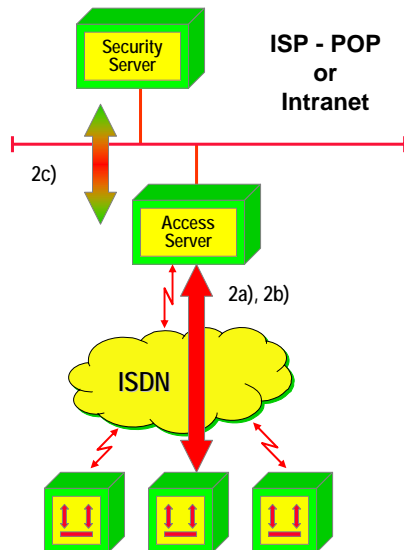
RAS Operation 1



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

L08 - IP Technology

RAS Operation 2



- **PPP link (multiprotocol over serial line) is established**

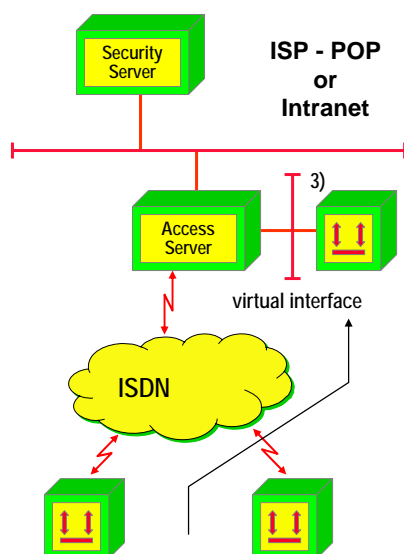
- LCP Link Control Protocol (2a)
 - establishes PPP link plus negotiates parameters like authentication CHAP
- authentication
 - CHAP Challenge Authentication Protocol to transport passwords (2b)
 - verification maybe done by central security server (2c) -> Radius, TACACS, TACACS+

© 2007, D.I. Manfred Lindner

IP Technology, v4.7

153

RAS Operation 3



- **PPP NCP (Network Control Protocol) IPCP**

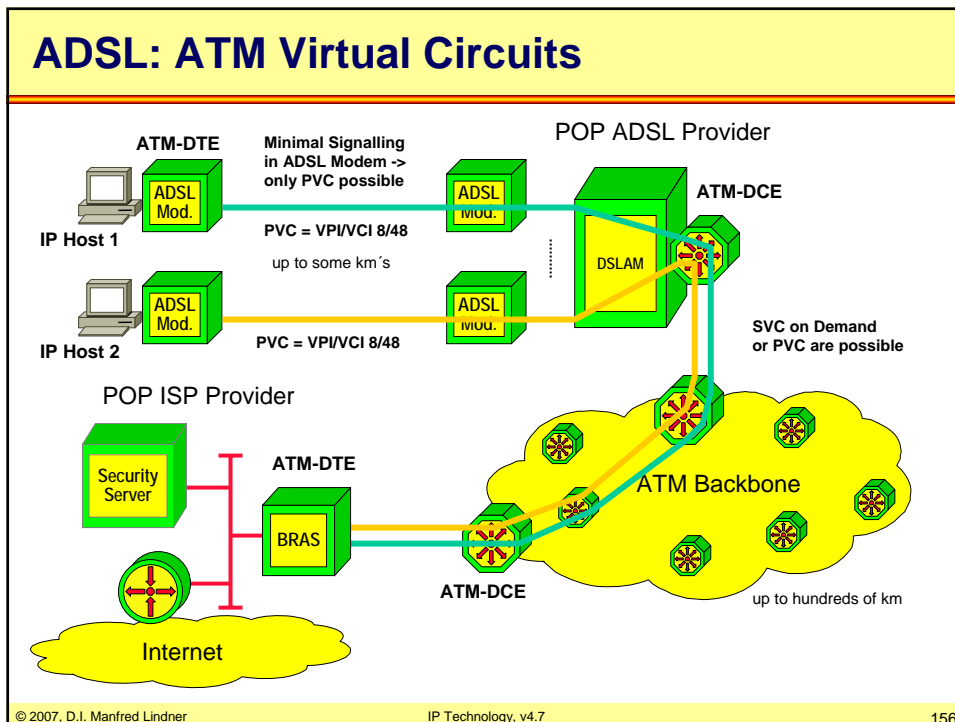
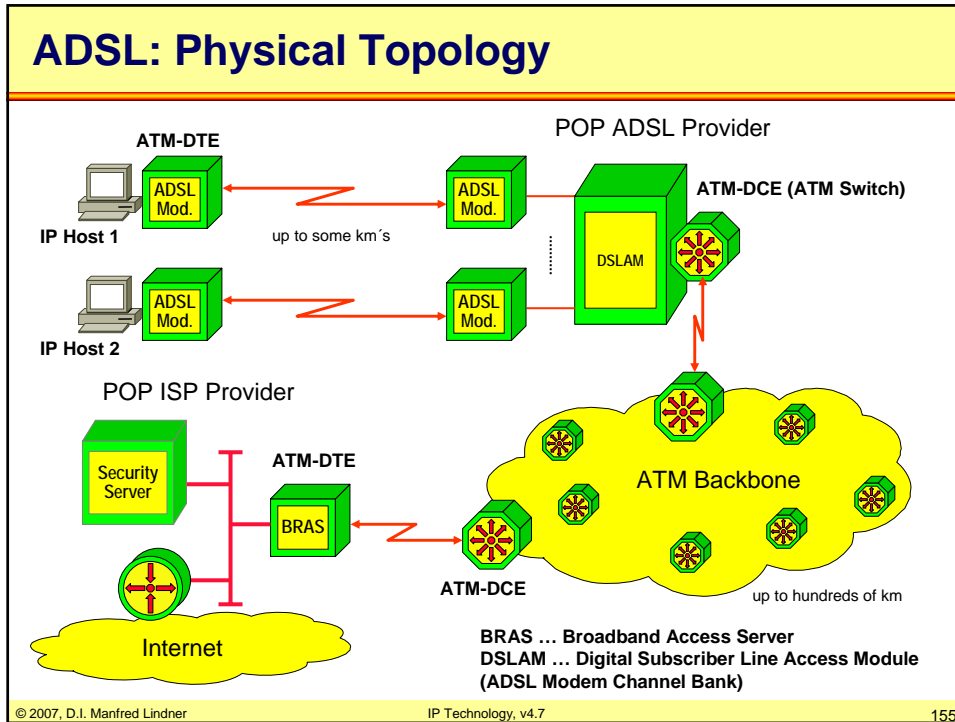
- assigns IP address, Def. GW, DNS to remote PC
- **remote PC appears as**
 - device reachable via virtual interface (3), IP host Route
- **optionally**
 - filter could be established on that virtual interface
 - authorization
 - accounting can be performed
 - actually done by security server (AAA server)
 - TACACS, Radius

© 2007, D.I. Manfred Lindner

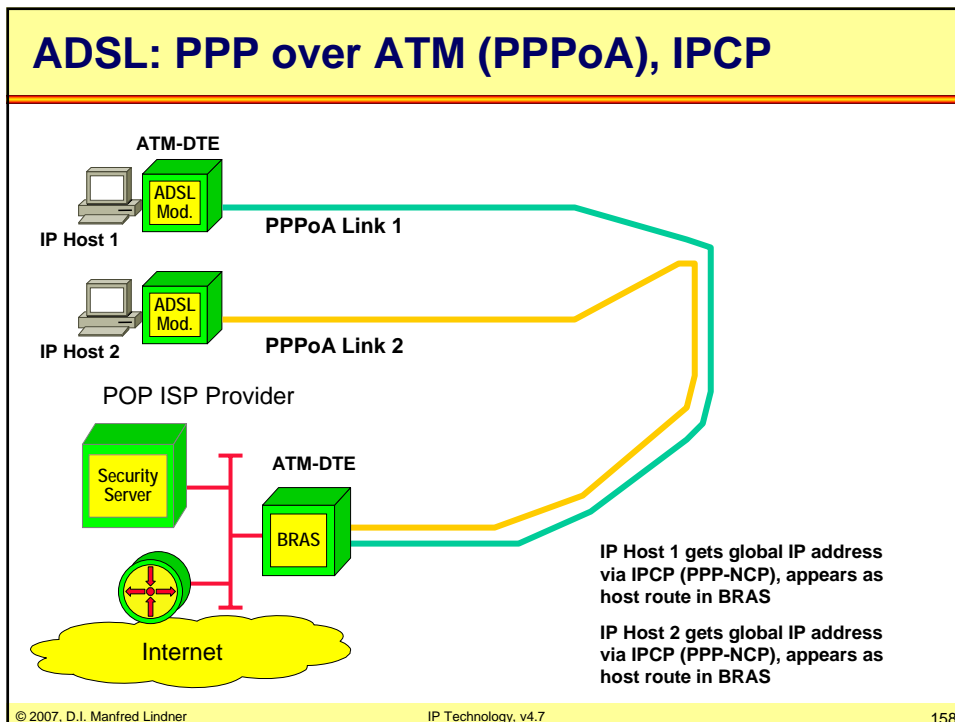
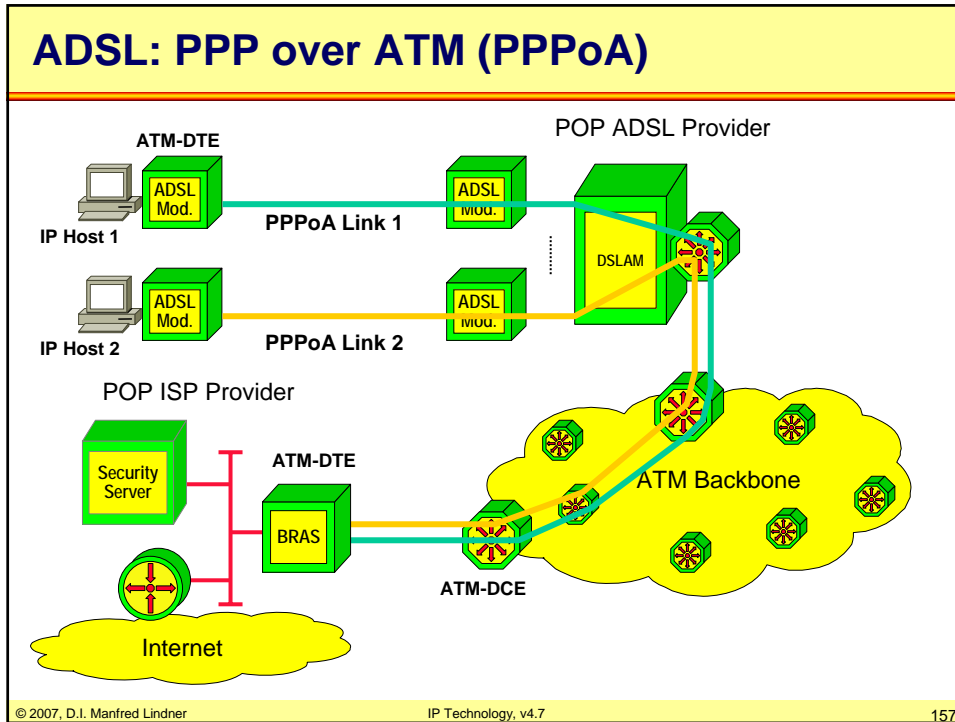
IP Technology, v4.7

154

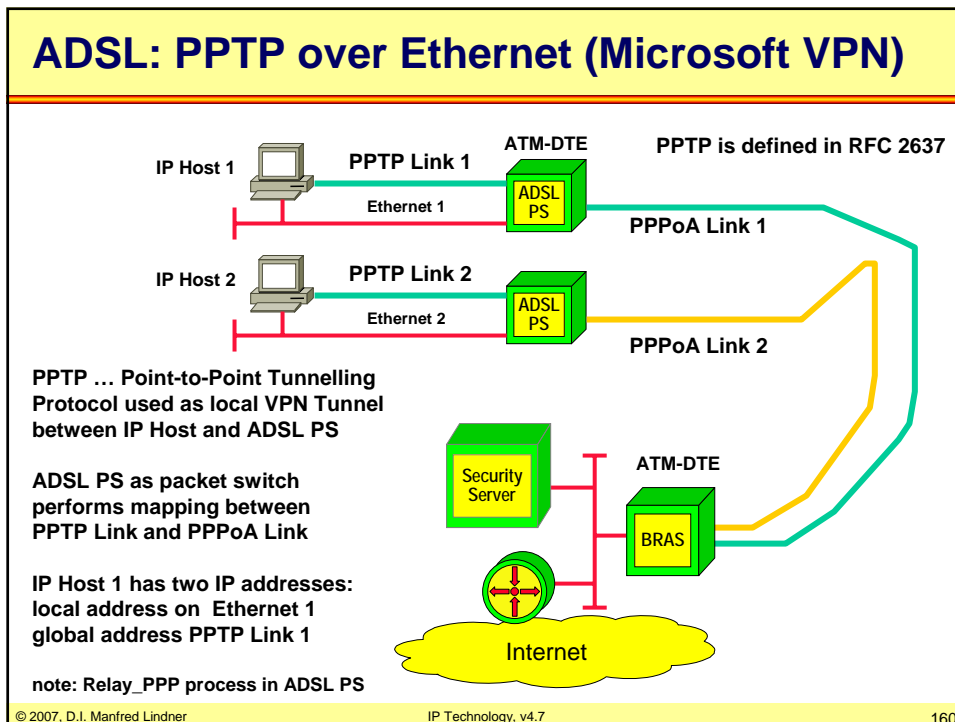
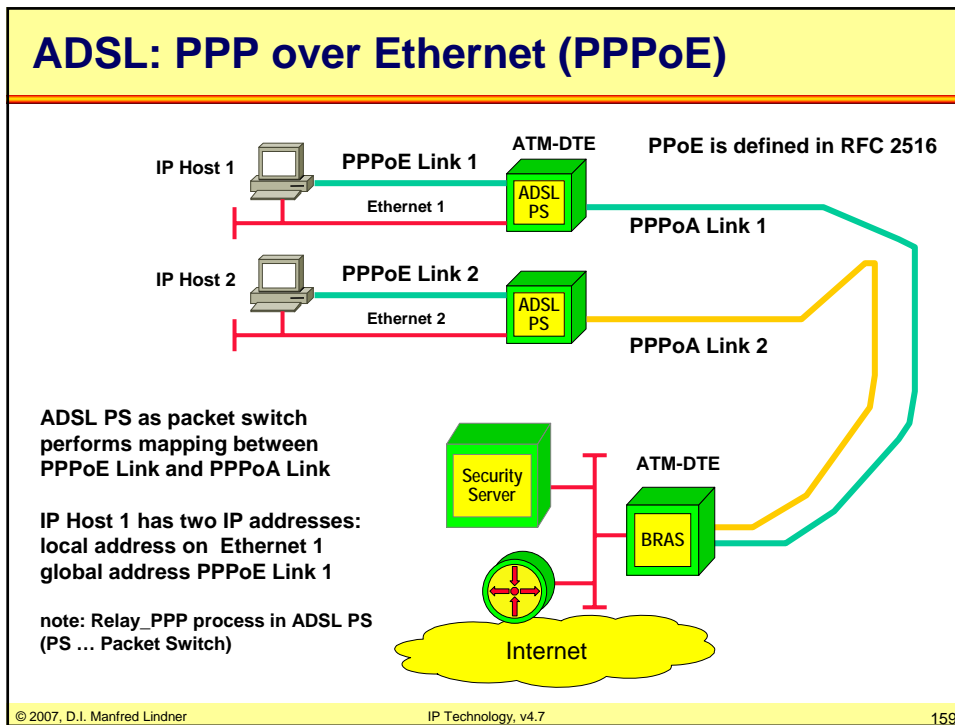
L08 - IP Technology



L08 - IP Technology



L08 - IP Technology



L08 - IP Technology

