Student Online Teaching Advice Notice

The materials and content presented within this session are intended solely for use in a context of teaching and learning at Trinity.

Any session recorded for subsequent review is made available solely for the purpose of enhancing student learning.

Students should not edit or modify the recording in any way, nor disseminate it for use outside of a context of teaching and learning at Trinity.

Please be mindful of your physical environment and conscious of what may be captured by the device camera and microphone during videoconferencing calls.

Recorded materials will be handled in compliance with Trinity's statutory duties under the Universities Act, 1997 and in accordance with the University's policies and procedures.

Further information on data protection and best practice when using videoconferencing software is available at https://www.tcd.ie/info_compliance/data-protection/.

Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

CSU33031 Computer Networks

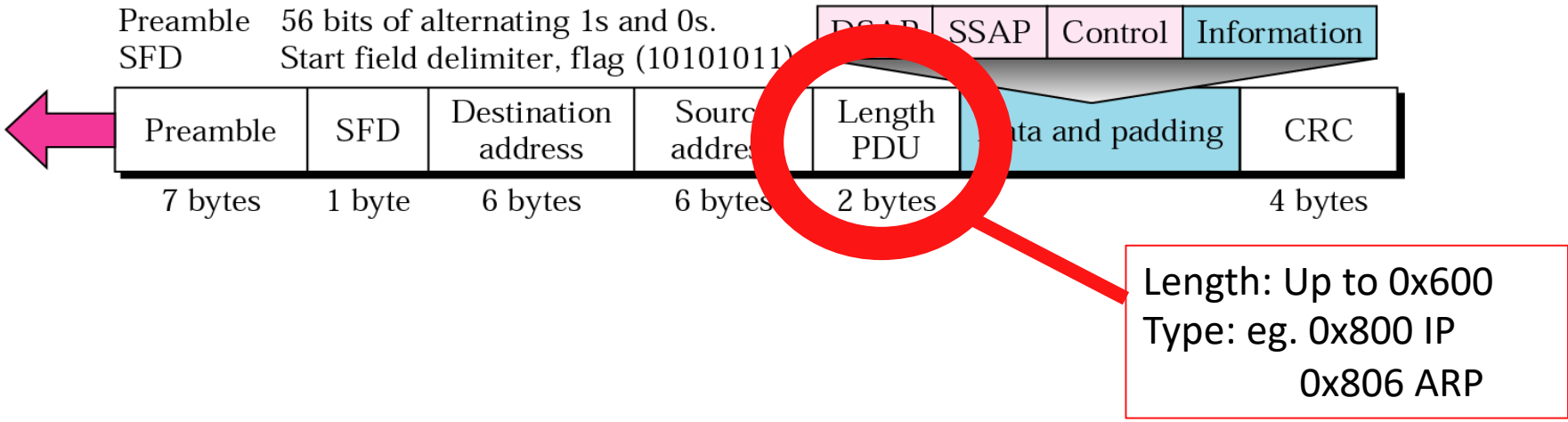
Ethernet & IPv4

Stefan Weber

email: sweber@tcd.ie

Office: Lloyd 1.41

802.3 Ethernet



- Types of Addresses:
  - Unicast – delivered to one station
    - 00-10-4B 3Com 3C905-TX PCI
    - 00-A0-C9 Intel (PRO100B and PRO100+)

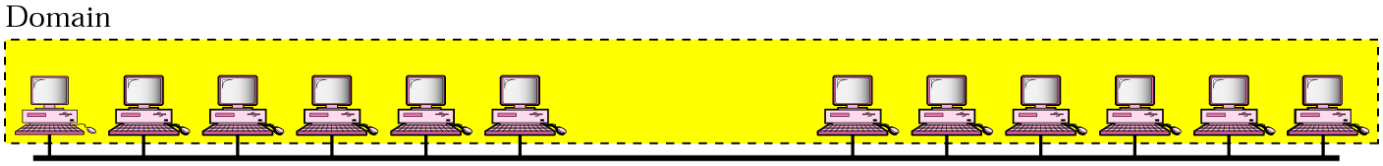
    (omitted Ethernet Multicast)
  - Broadcast – delivered to all stations
    - FF-FF-FF-FF-FF-FF

06-01-02-01-2C-4B

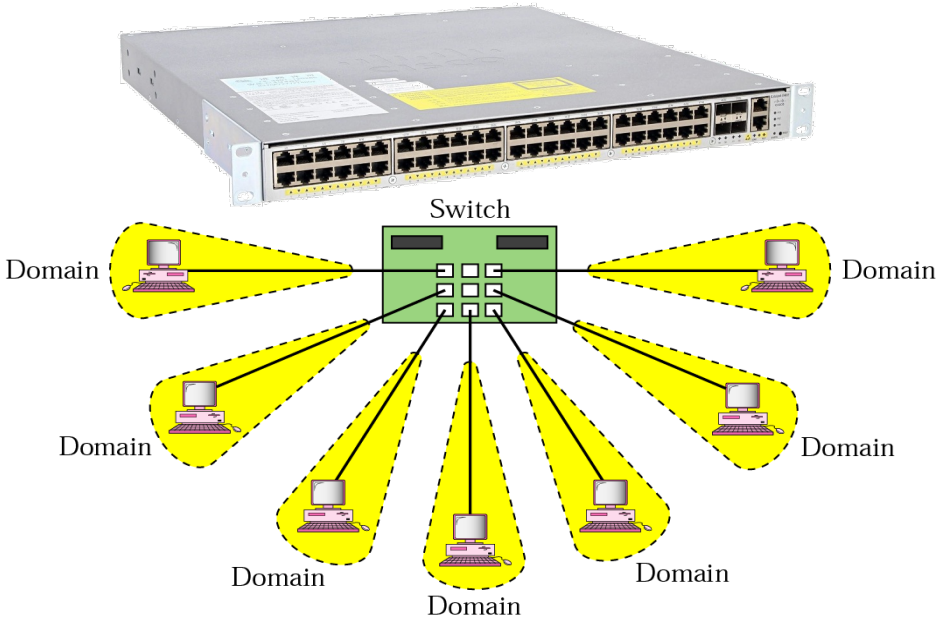
vendor-specific

* Figure is courtesy of B. Forouzan

From Shared Media to Switched Networks

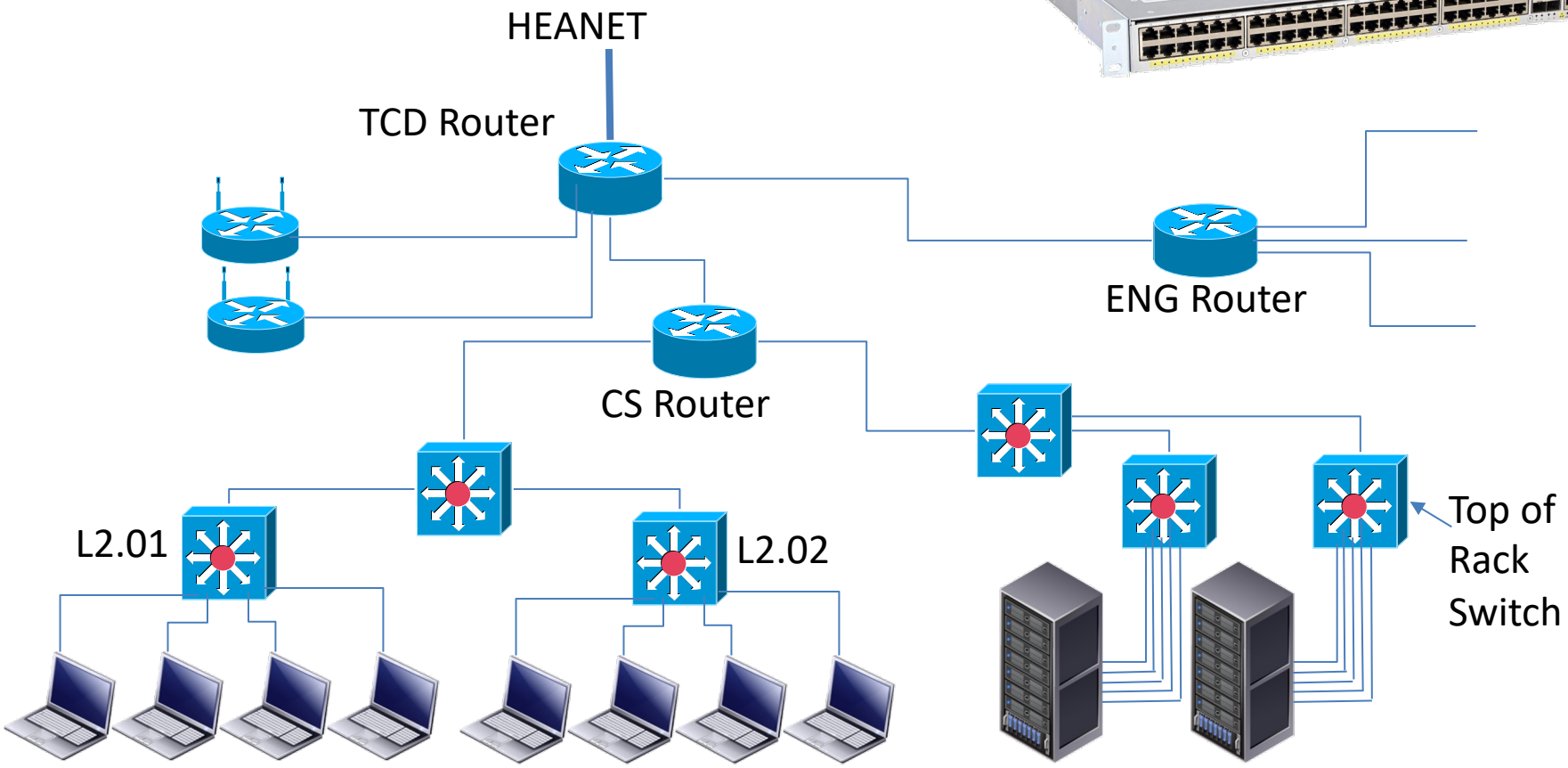


a. Without bridging



* Figure is courtesy of B. Forouzan

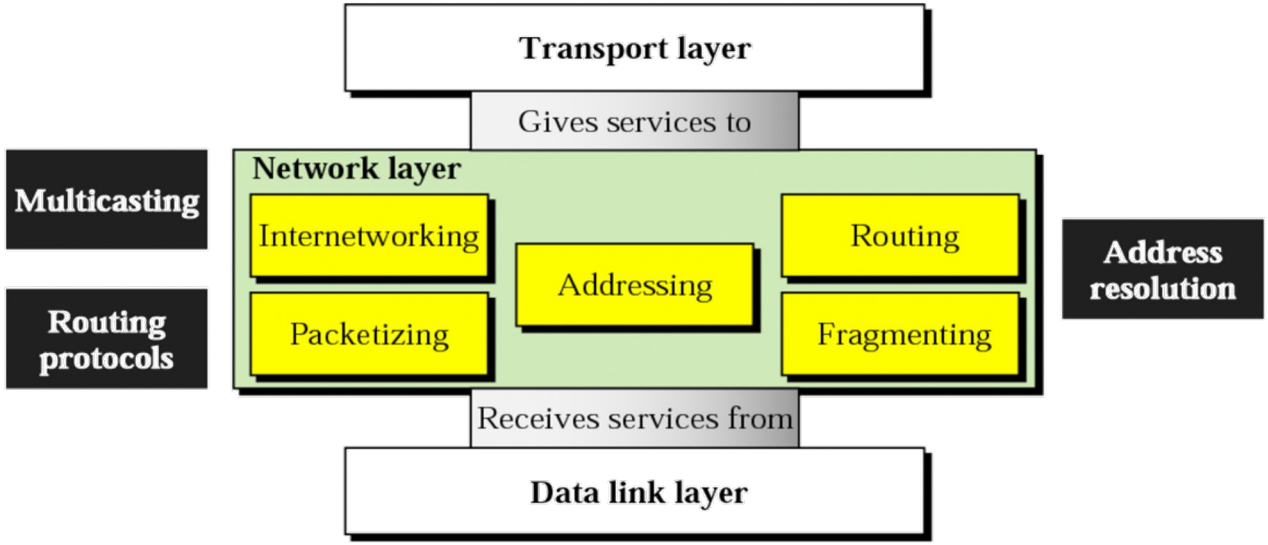
College's Switched Network

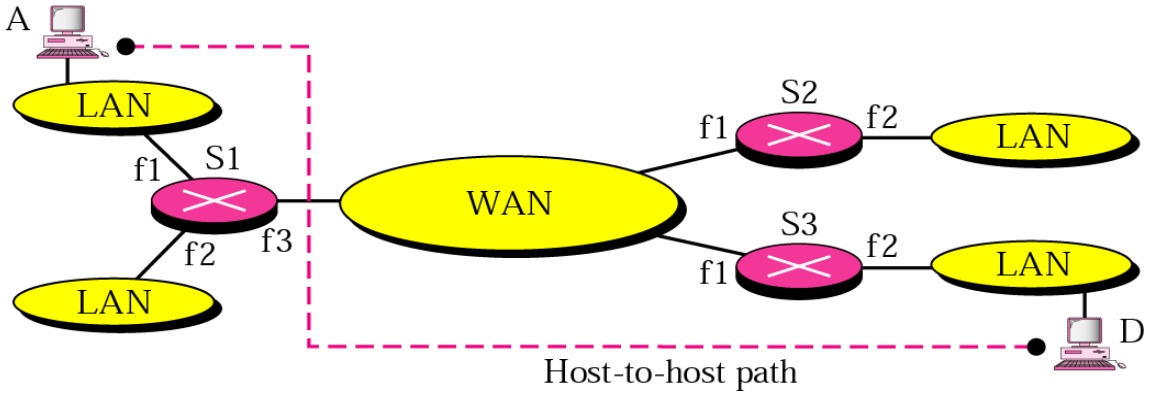


At the switch level = Hardware Addresses i.e. Ethernet Addresses

Potential topology of College; may or may not reflect the reality of our setup

Network Layer





* Figure is courtesy of B. Forouzan

Building a Network of Networks...

- Paul Barran, On Distributed Communication Networks, IEEE Transactions on Communication Systems, Volume 12, No. 1, March 1964

- Introduced Concepts of
  - Distributed Networks
  - Routing (hot-potato-routing)
  - Packet-Switching (message-block)

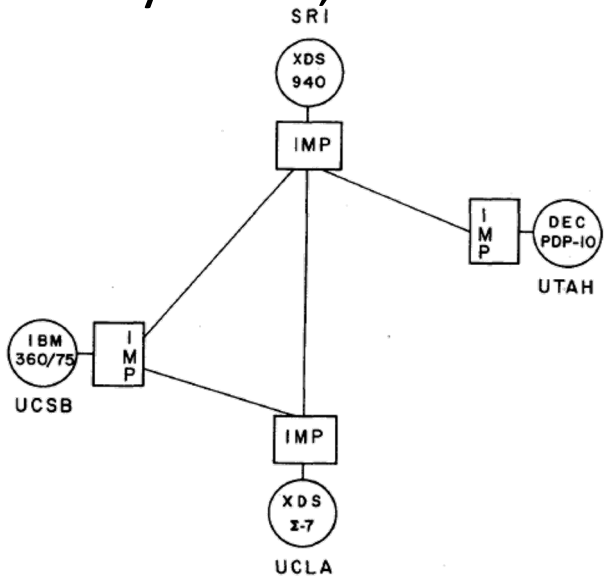
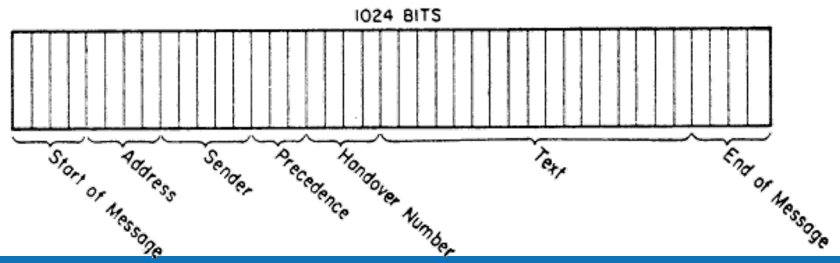


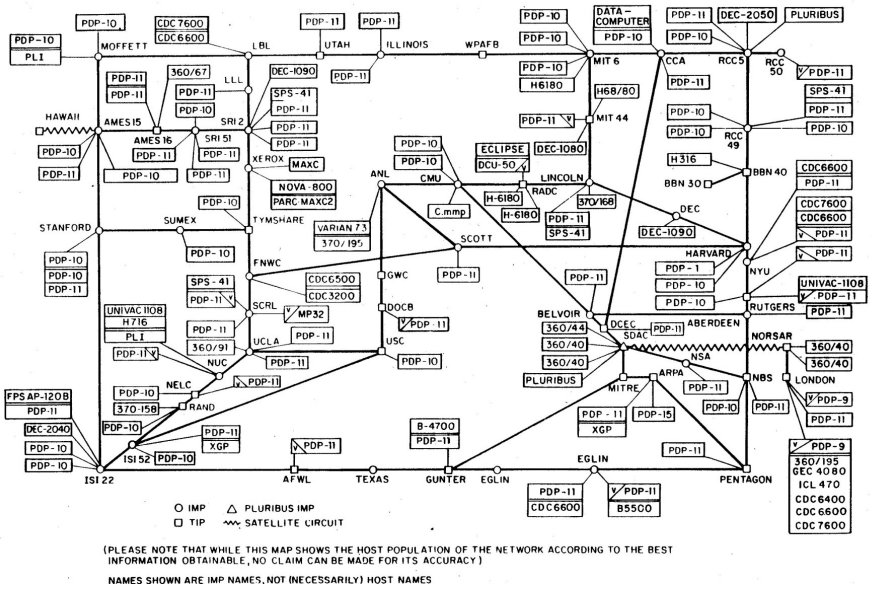
Figure 1—Initial network configuration



AT&T's comment in the 1960s:

Packet-switching will never be useful.

From ARPANET to IPv4



- 32-bit number
  - 4.294.967.296 addresses

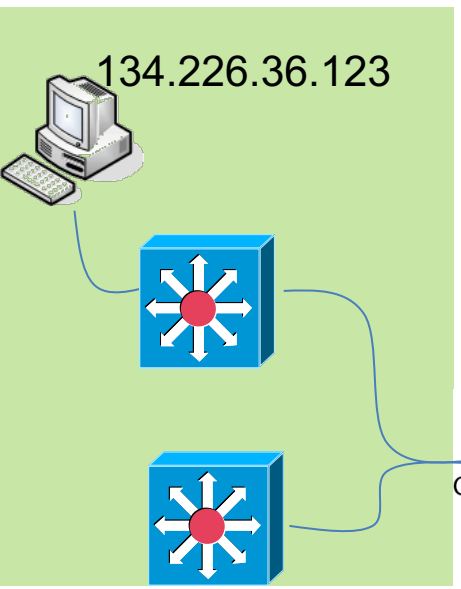
10000000 00001011 00000011 00011111

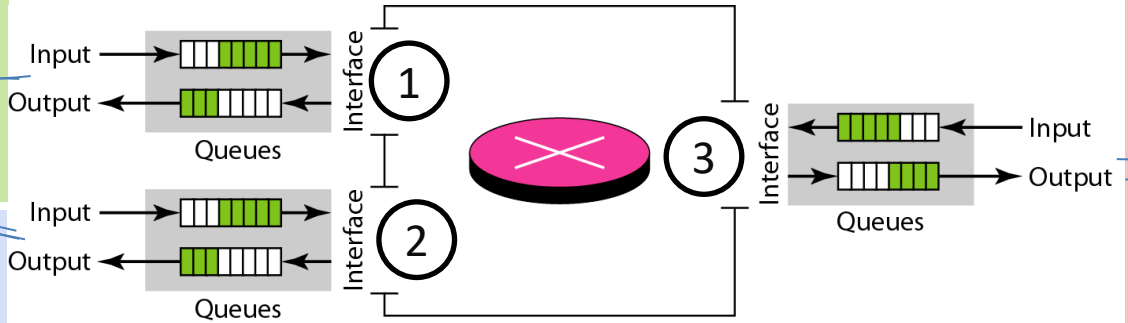
128.11.3.31

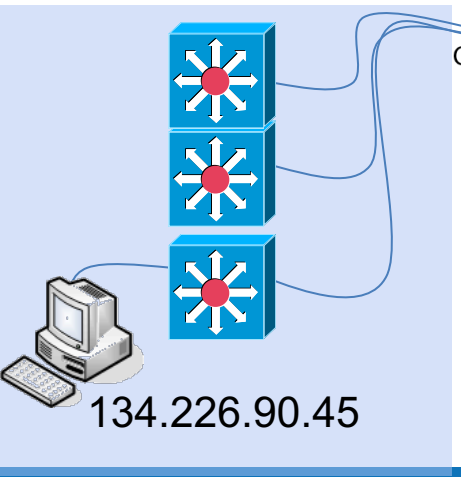
- IP addresses are unique and universal
  - with some exceptions

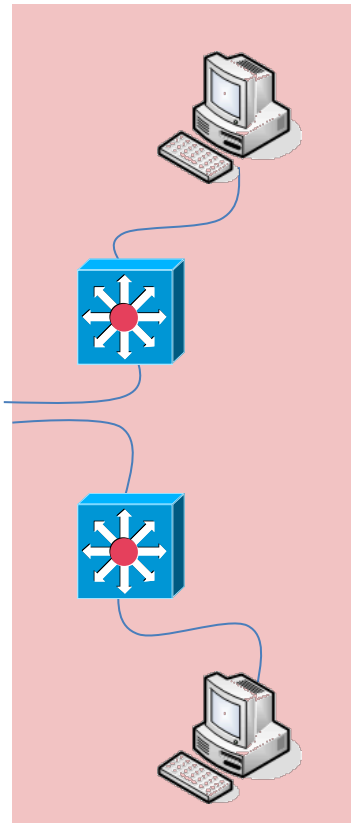
- Dotted decimal notation:
  - Bytes of binary notation represented as decimal separated by dot

Routers (or Network Elements)



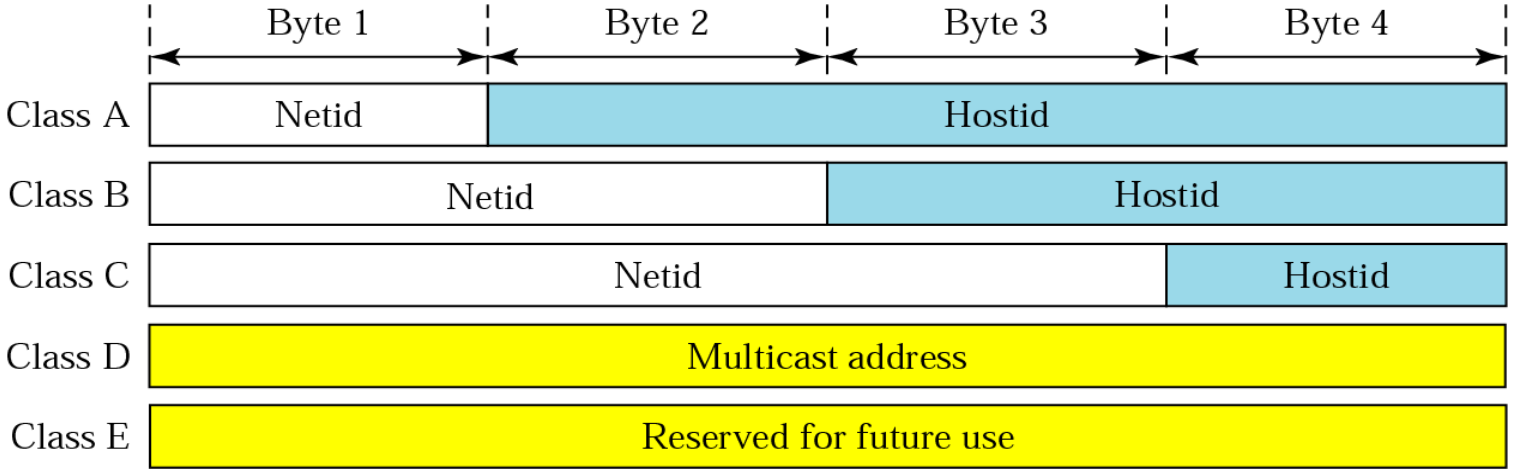






Forwarding Table or Routing Table	
Network Address	Next Hop
134.226.36.123	interface 1
134.226.90.45	interface 2

Classful Addresses – Making routing manageable



- Class A (international organisations)
  - 126 networks with 16,277,214 hosts each
- Class B (large companies)
  - 16,384 networks with 65,354 hosts each
- Class C (smaller companies)
  - 2,097,152 networks with 254 hosts each

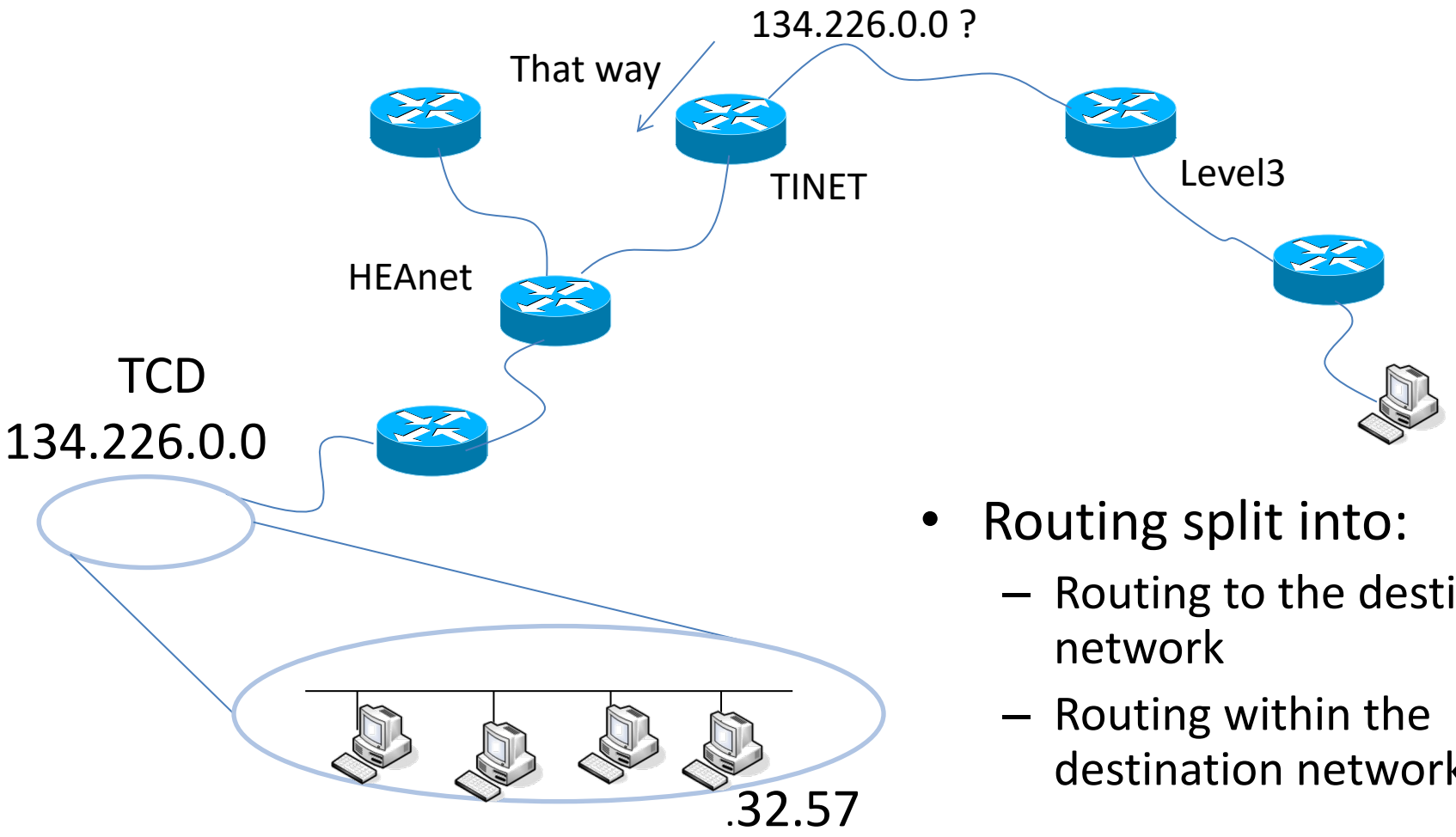
Private Address Ranges:

Not unique but also not on the Internet

Range			*Total*
10.0.0.0	to	10.255.255.255	2^{24}
172.16.0.0	to	172.31.255.255	2^{20}
192.168.0.0	to	192.168.255.255	2^{16}

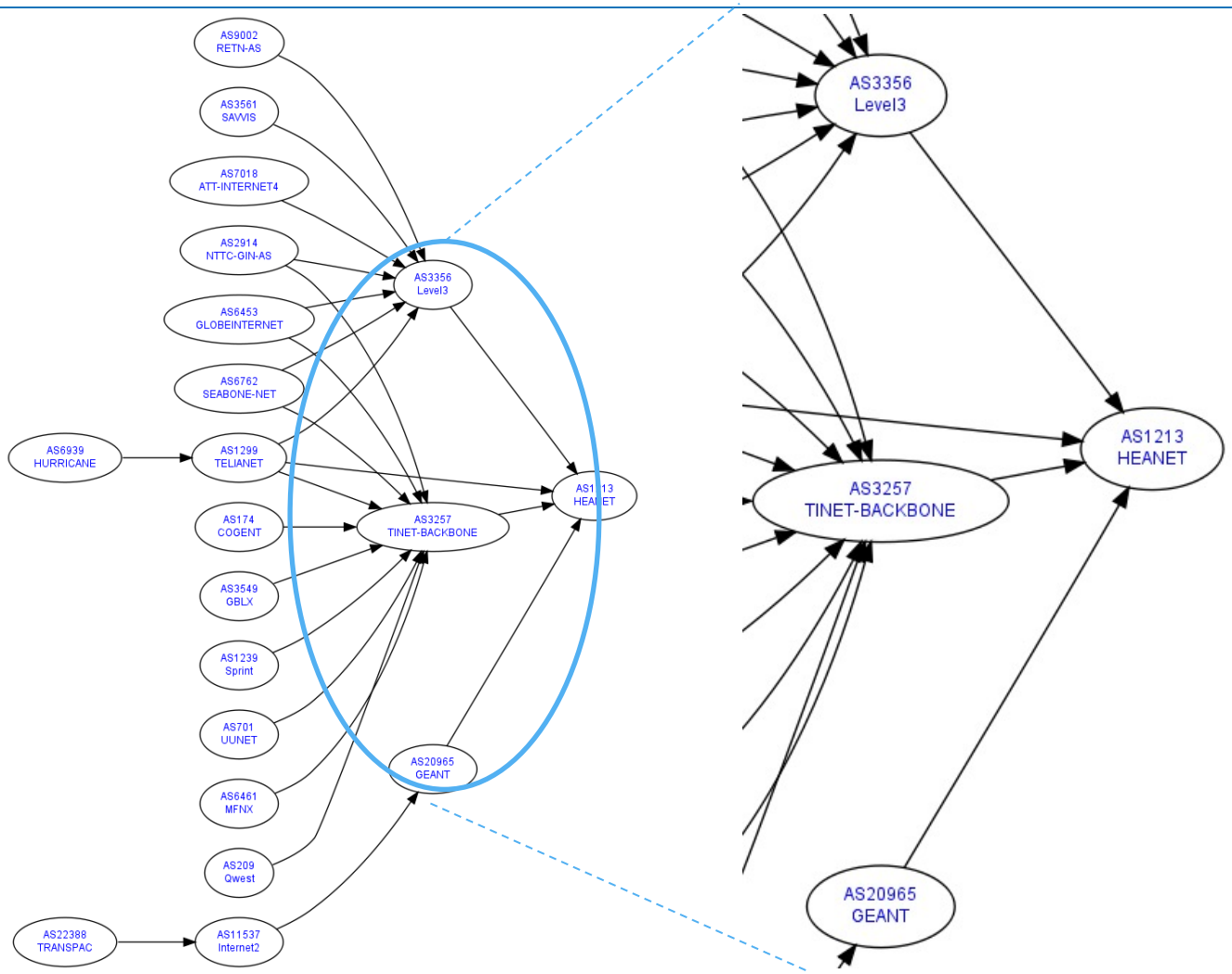
* Figure is courtesy of B. Forouzan

Network IDs and Host IDs



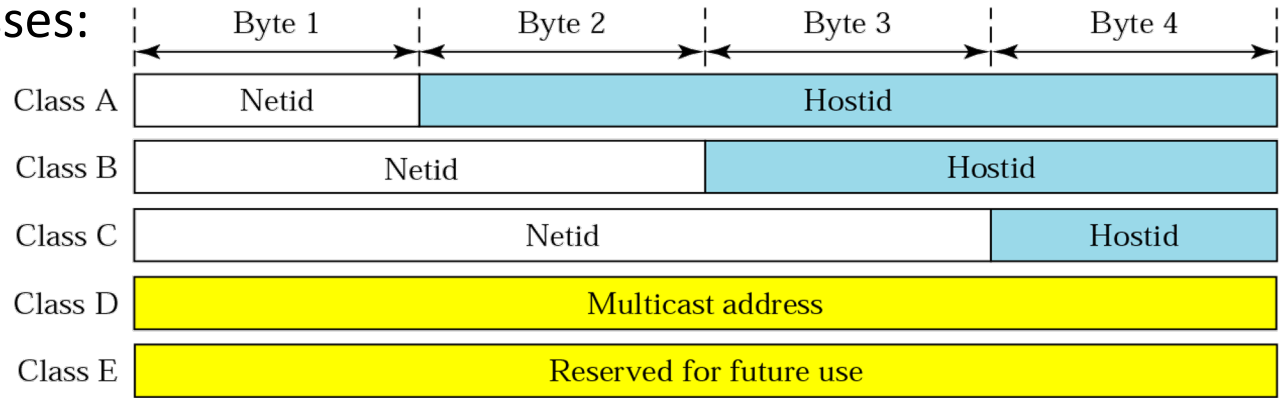
- Routing split into:
  - Routing to the destination network
  - Routing within the destination network

AS1213 - HEANET



Inefficiency of Classful Addresses

- Classful Addresses:



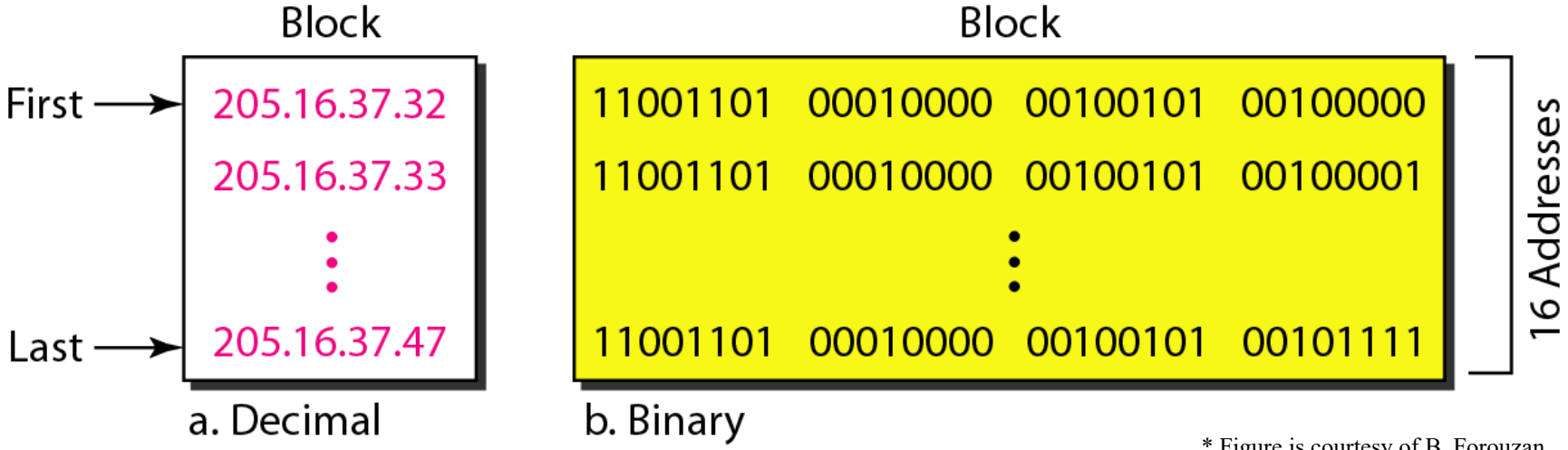
- Inefficient use of Hierarchical Address Space
  - Class C with 2 hosts (2/254 = 0.78% efficient)
  - Class B with 256 hosts (256/65534 = 0.39% efficient)

Class	Networks	Addresses
A	126	16,777,214
B	16,382	65,534
C	2,097,152	254

* Figure is courtesy of B. Forouzan

Classless Inter-Domain Routing(CIDR)

- Allow address space to be divided into blocks of addresses
  - only limited to the power of 2
- Notation as decimal number of the significant bits e.g. 134.226.36.0 /29
- 205.16.37.32/28
  - 32 bits – 28 bits are static - 4 bits are varied



* Figure is courtesy of B. Forouzan

Classless Inter-Domain Routing(CIDR)

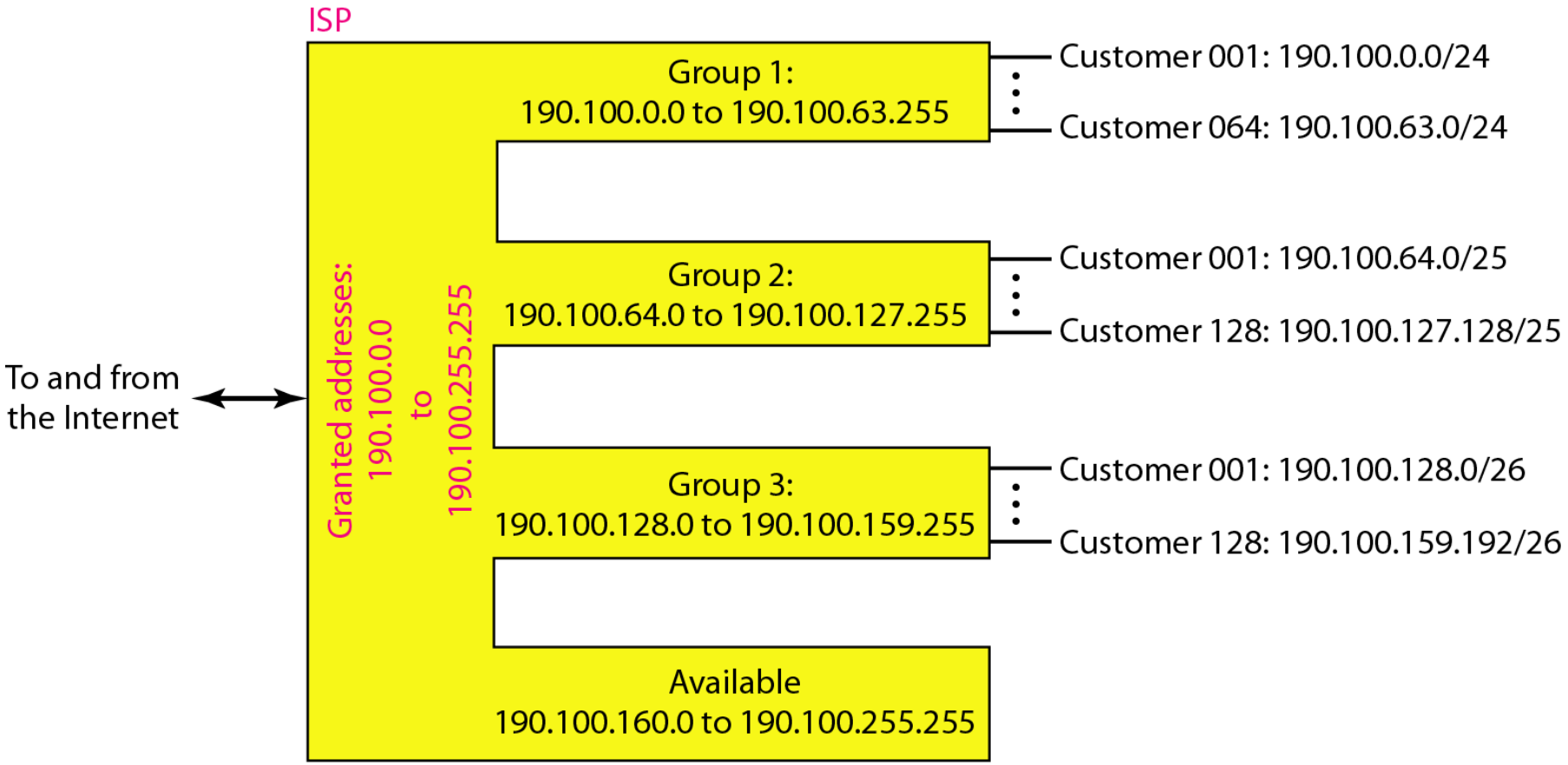
- Aggregation: For example, class C networks can be combined to larger networks
- /21 = 8 class C = 8 * 256 addresses = 2048 addresses

	Dotted Decimal	32-bit binary equivalent
Lowest	128.211.168.0	10000000 11010011 10101000 00000000
Highest	128.211.175.255	10000000 11010011 10101111 11111111

= 128.211.168.0/21

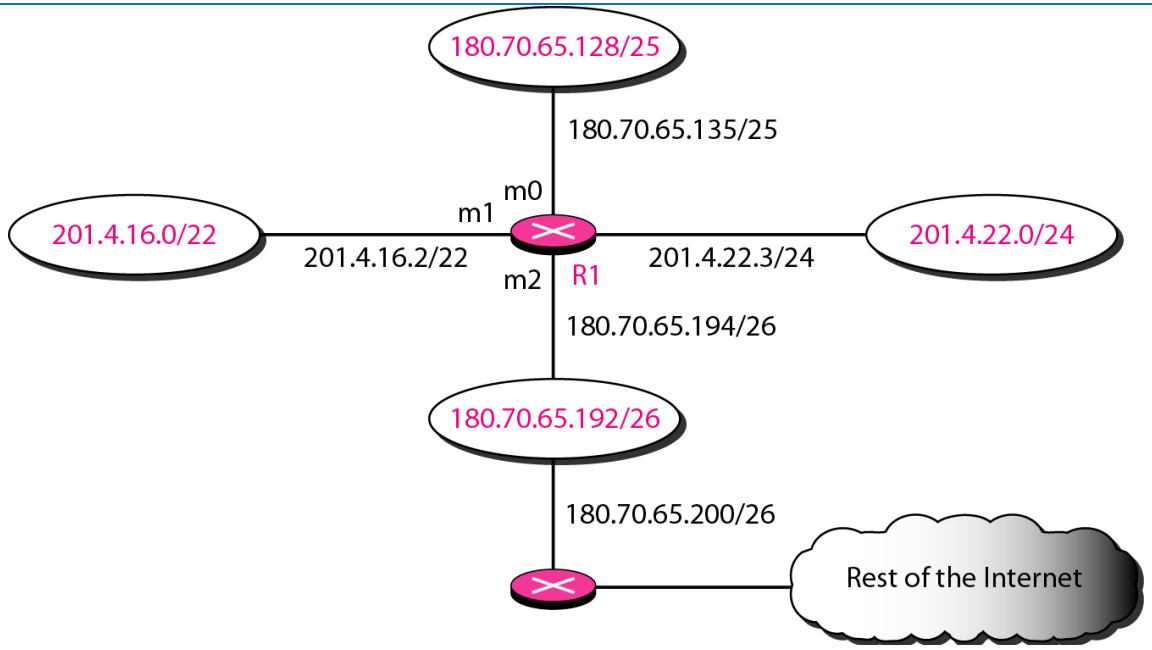
* Figure is courtesy of B. Forouzan

ISPs & Classless Addresses



* Figure is courtesy of B. Forouzan

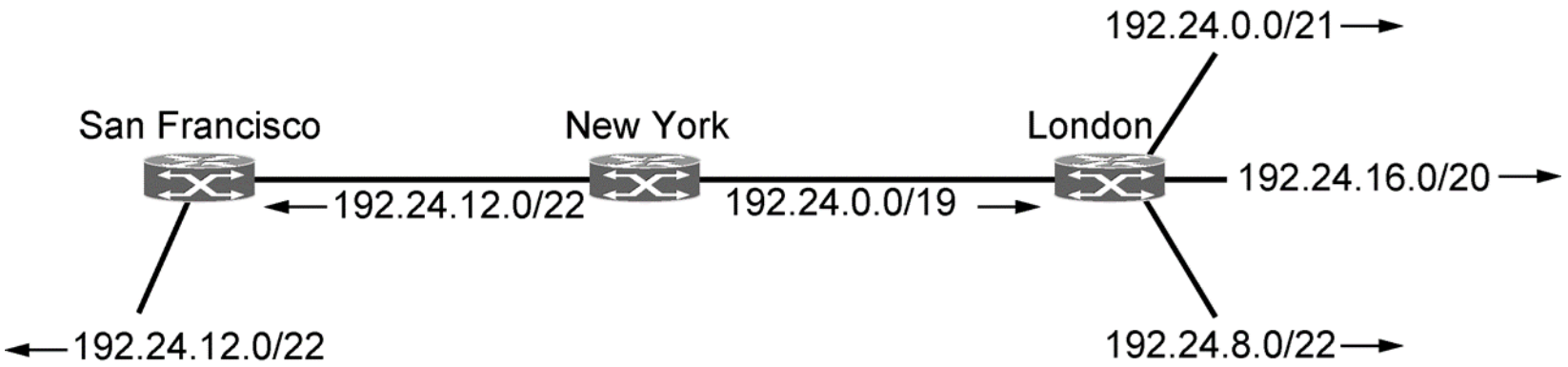
CIDR & Router



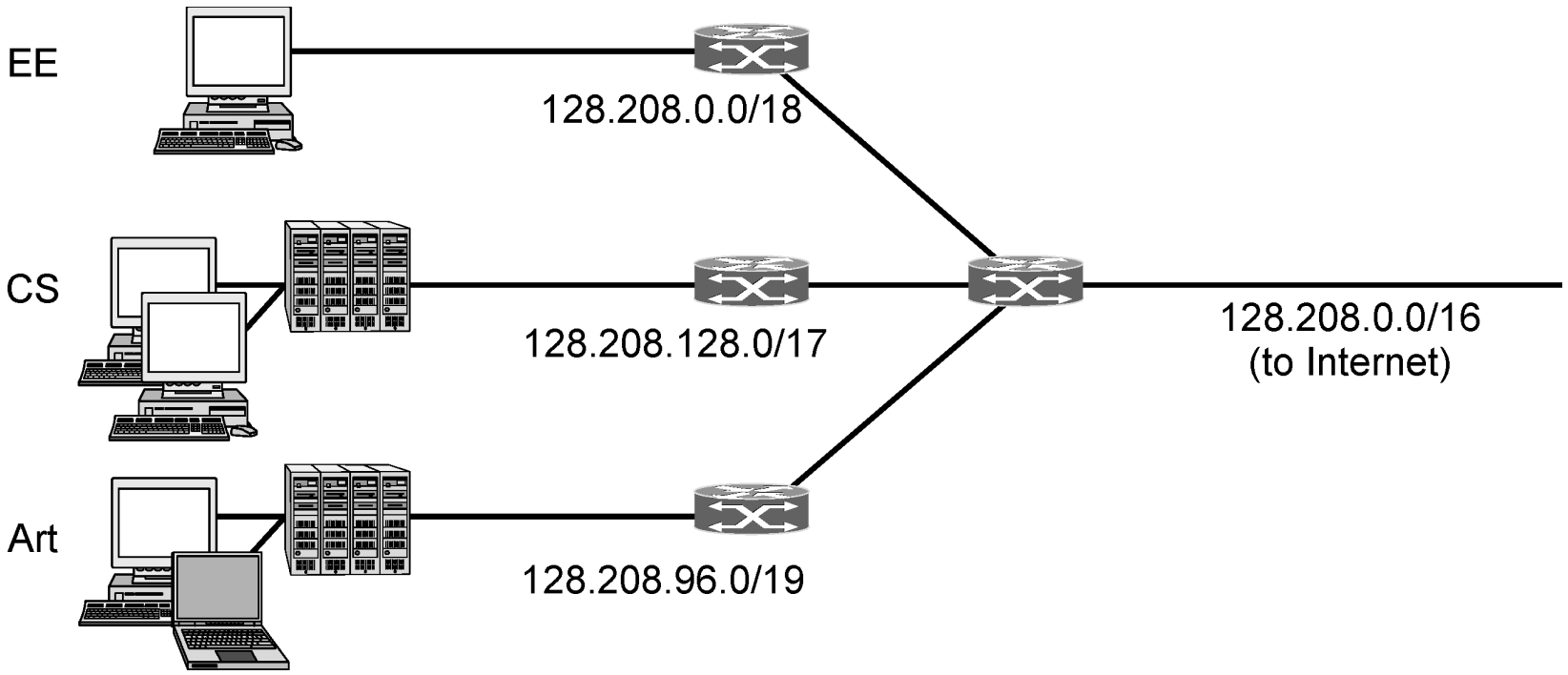
Mask	*Network Address*	*Next Hop*	*Interface*
/26	180.70.65.192	—	m2
/25	180.70.65.128	—	m0
/24	201.4.22.0	—	m3
/22	201.4.16.0	....	m1
Any	Any	180.70.65.200	m2

* Figure is courtesy of B. Forouzan

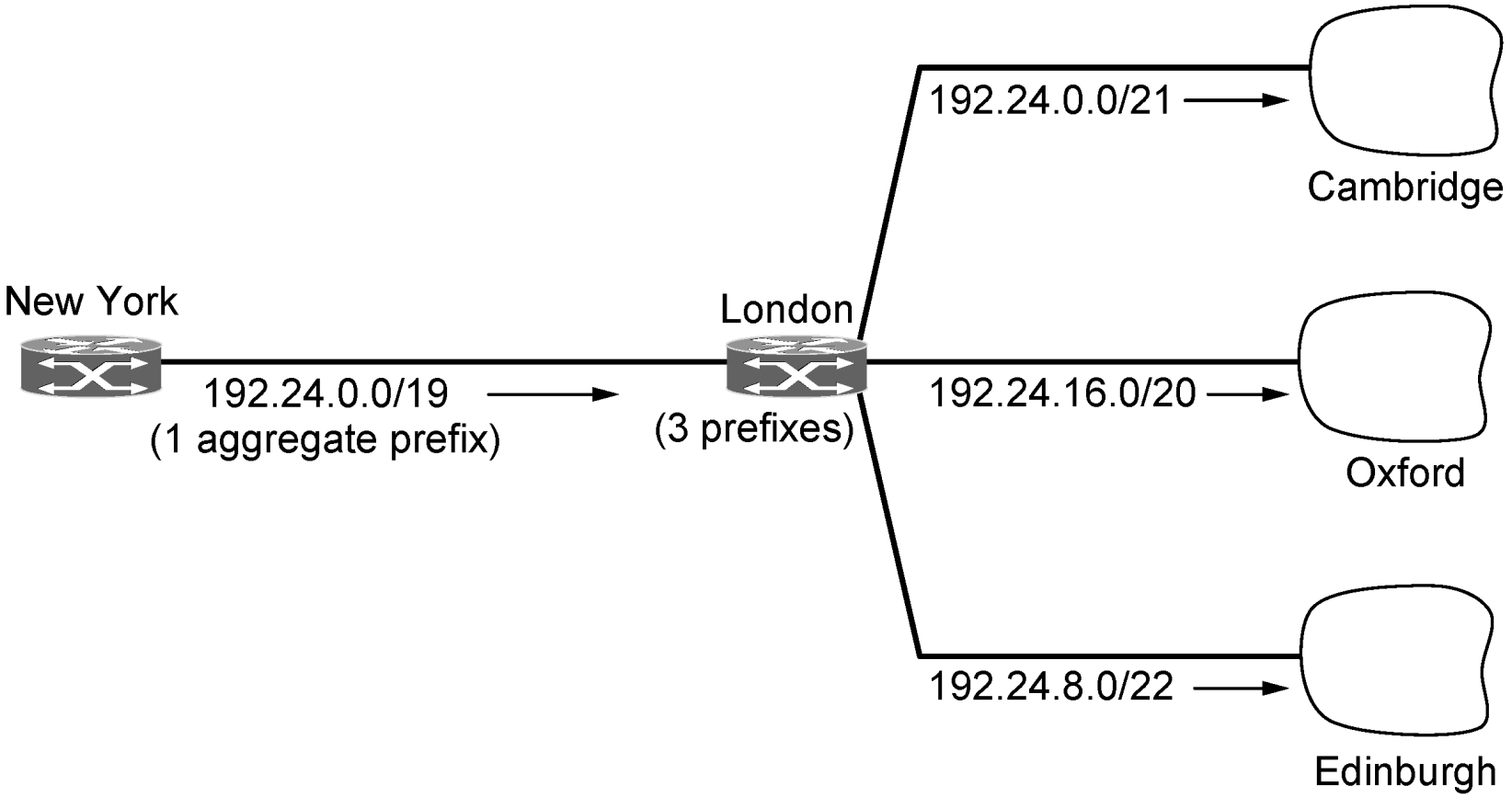
Longest matching Prefix



IP Prefix & Subnets

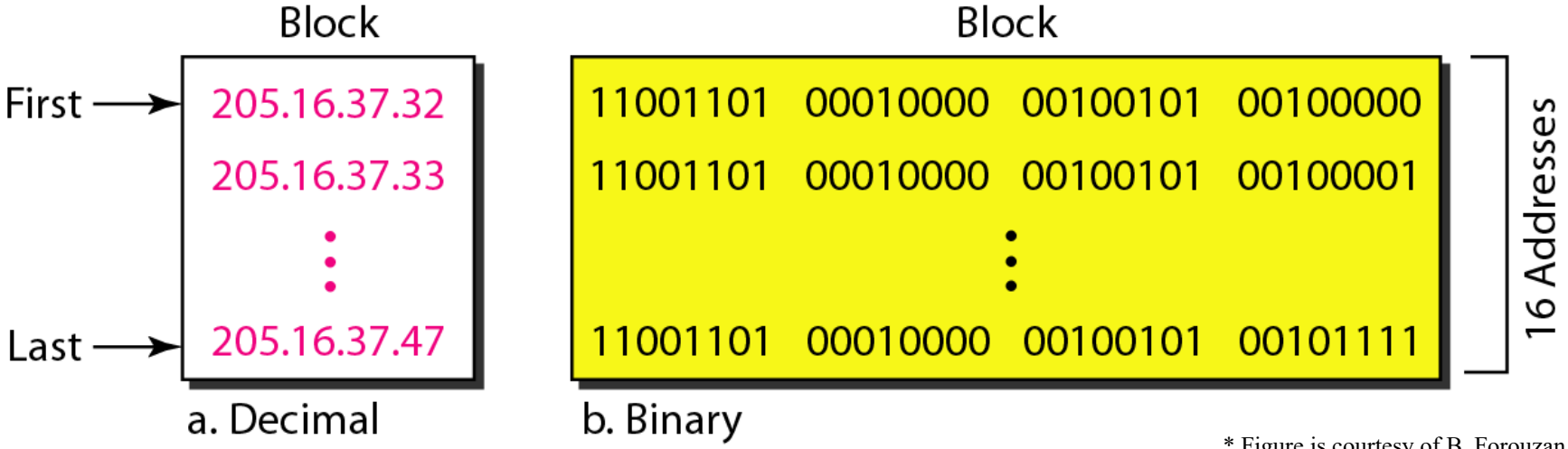


Aggregate Prefix



Classless Inter-Domain Routing(CIDR)

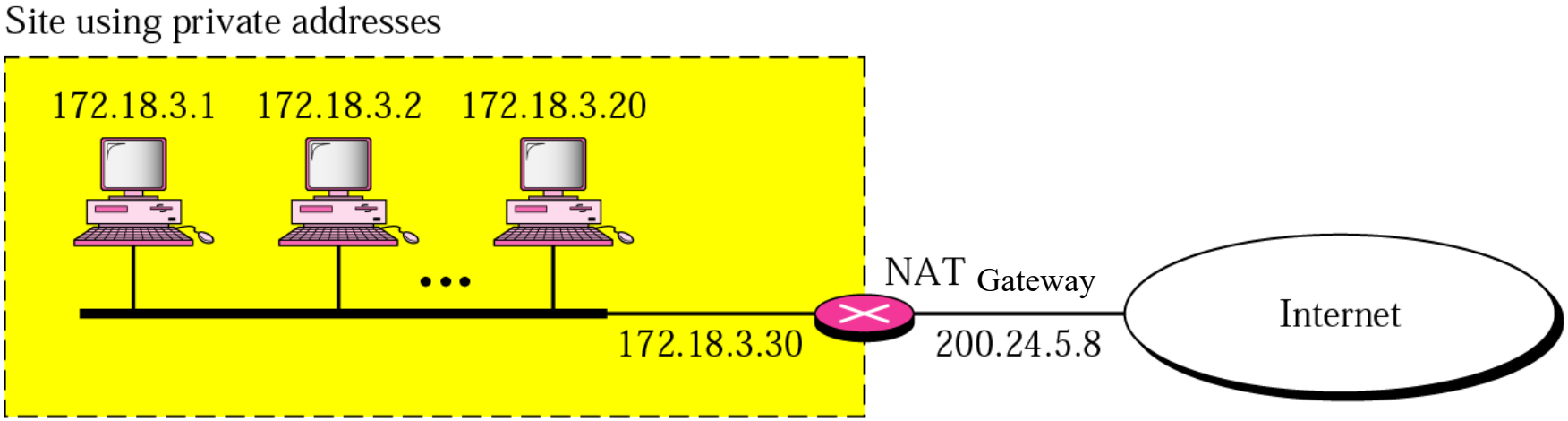
- Allow address space to be divided into blocks of addresses
  - only limited to the power of 2
- Notation as decimal number of the significant bits e.g. 134.226.36.0 /29
- 205.16.37.32/28
  - 32 bits – 28 bits are static - 4 bits are varied



* Figure is courtesy of B. Forouzan

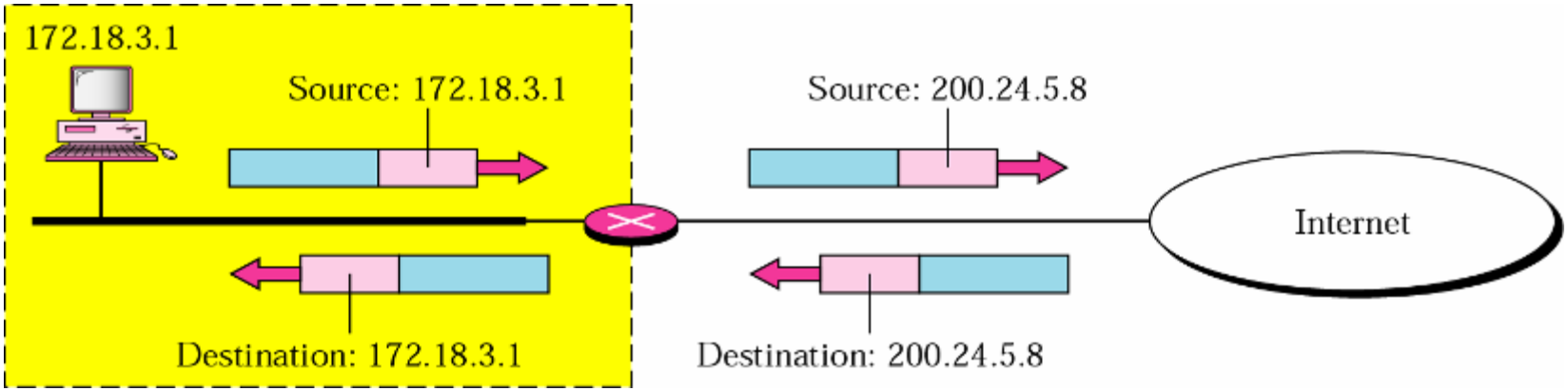
Network Address Translation (NAT)

- NAT gateway translates traffic from the local network to the IP address of the gateway



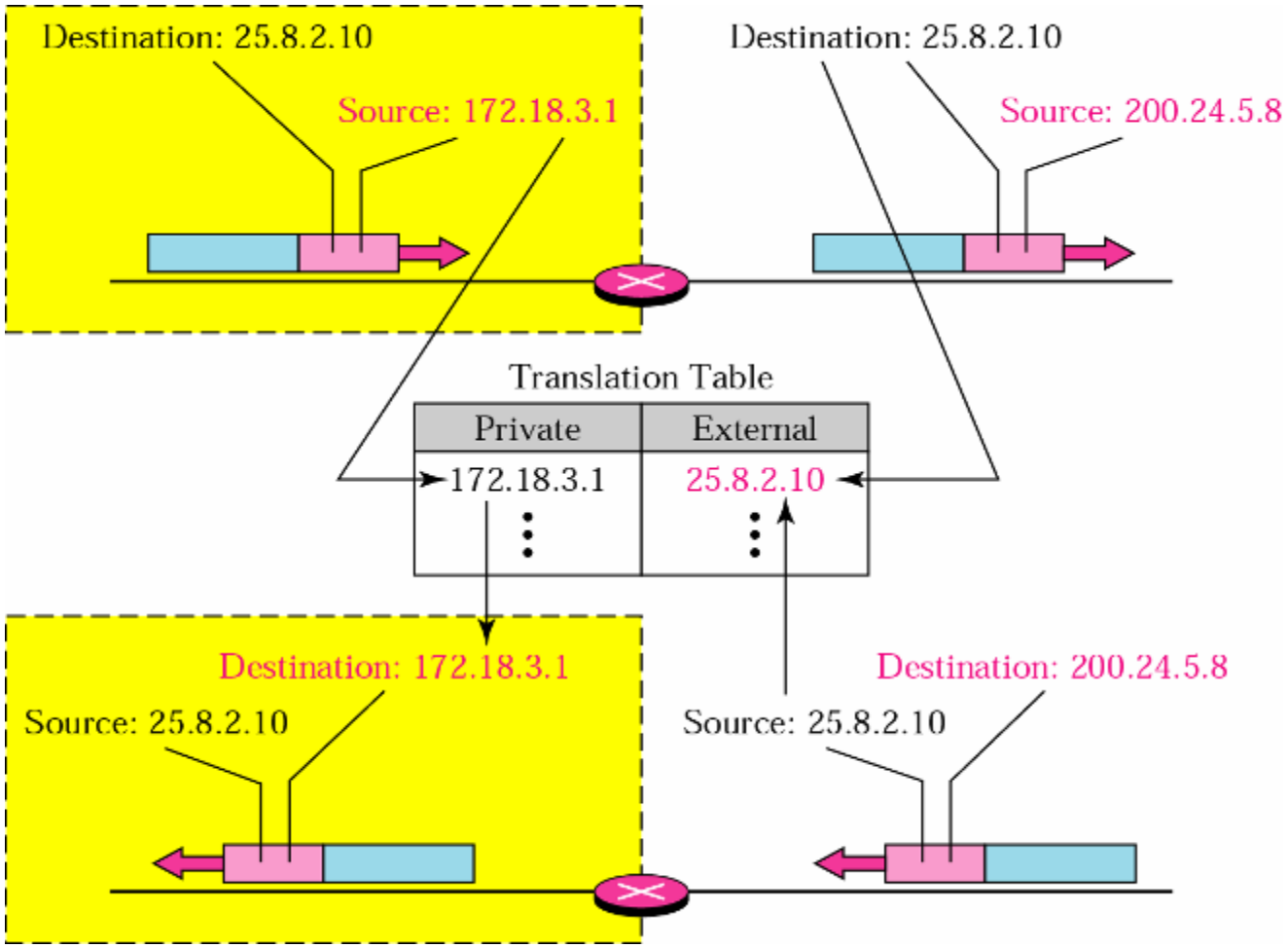
- Involves processing of outgoing & incoming packet e.g. translation between addresses, recalculation of checksums, etc

Address Translation

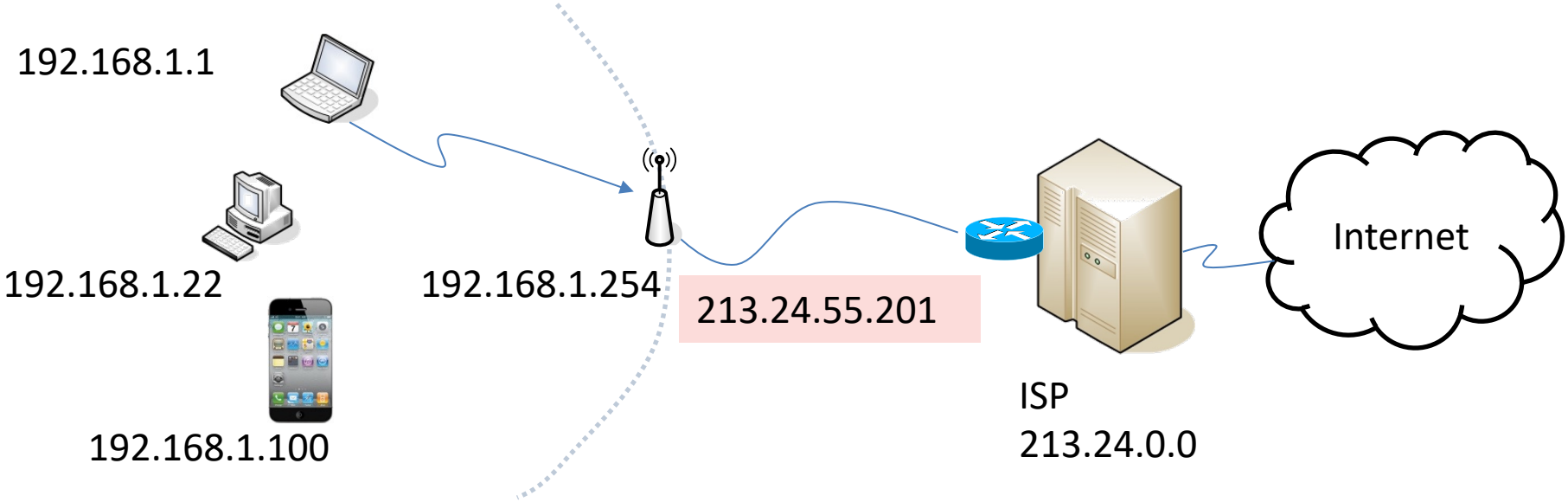


Private Address	Private Port	External Address	External Port	Transport Protocol
172.18.3.1	1400	25.8.3.2	80	TCP
172.18.3.2	1401	25.8.3.2	80	TCP
...	...	...	...	...

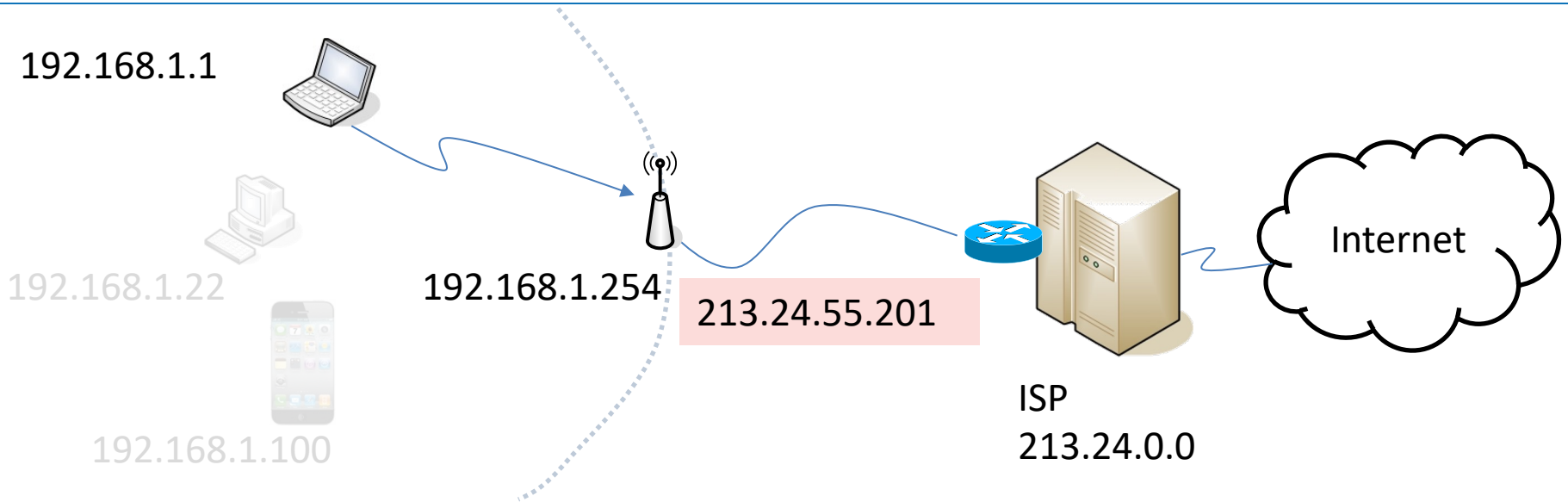
Example for NAT



NAT Example


192.168.1.1
192.168.1.22
192.168.1.100
192.168.1.254
213.24.55.201
ISP
213.24.0.0
Internet

NAT Example

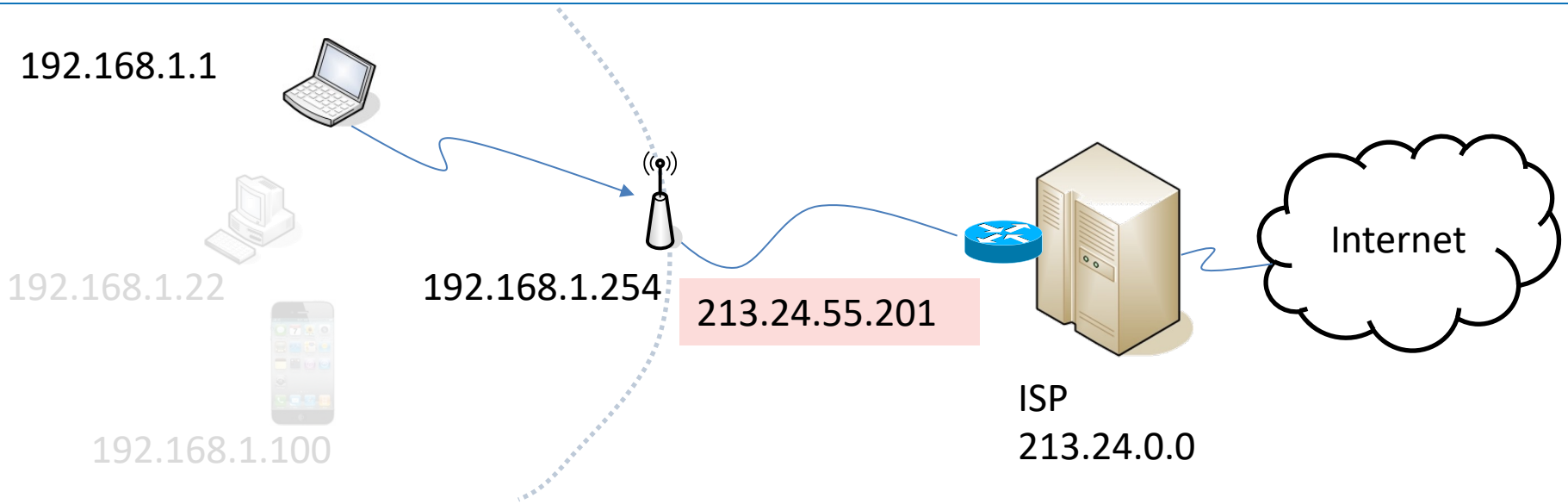


Src 192.168.1.1
Dst 134.226.36.14

NAT Table

Source	Destination
192.169.1.1:55612	134.226.36.14:80

NAT Example

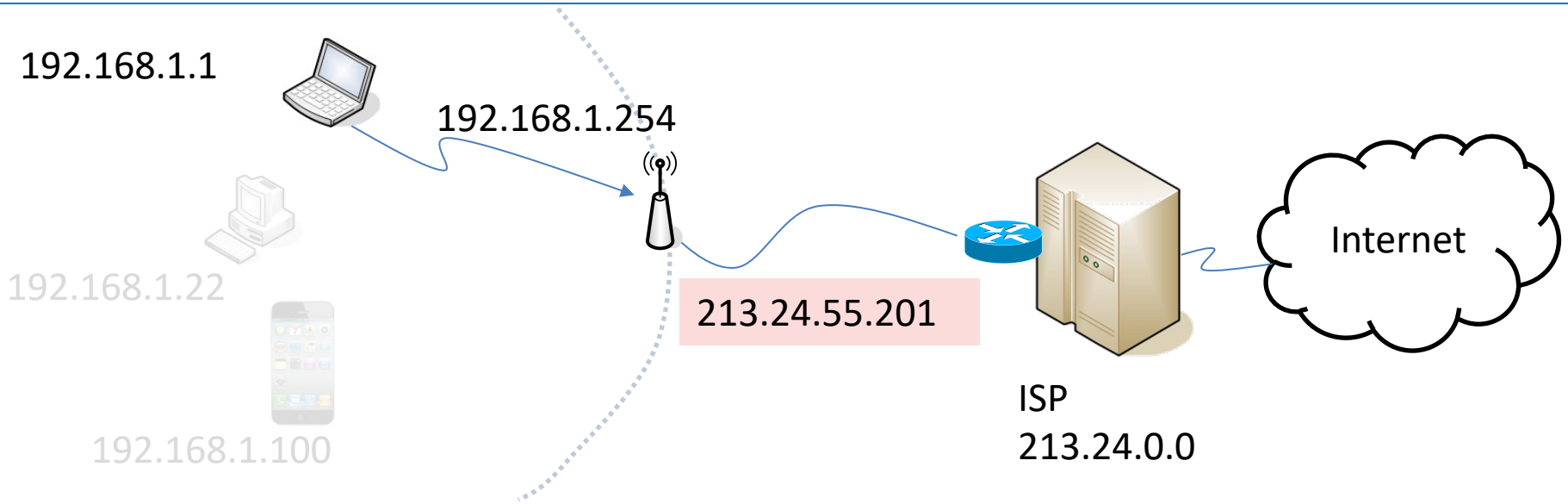


Src 213.24.55.201
Dst 134.226.36.14

NAT Table

Source	Destination
192.169.1.1:55612	134.226.36.14:80

NAT Example

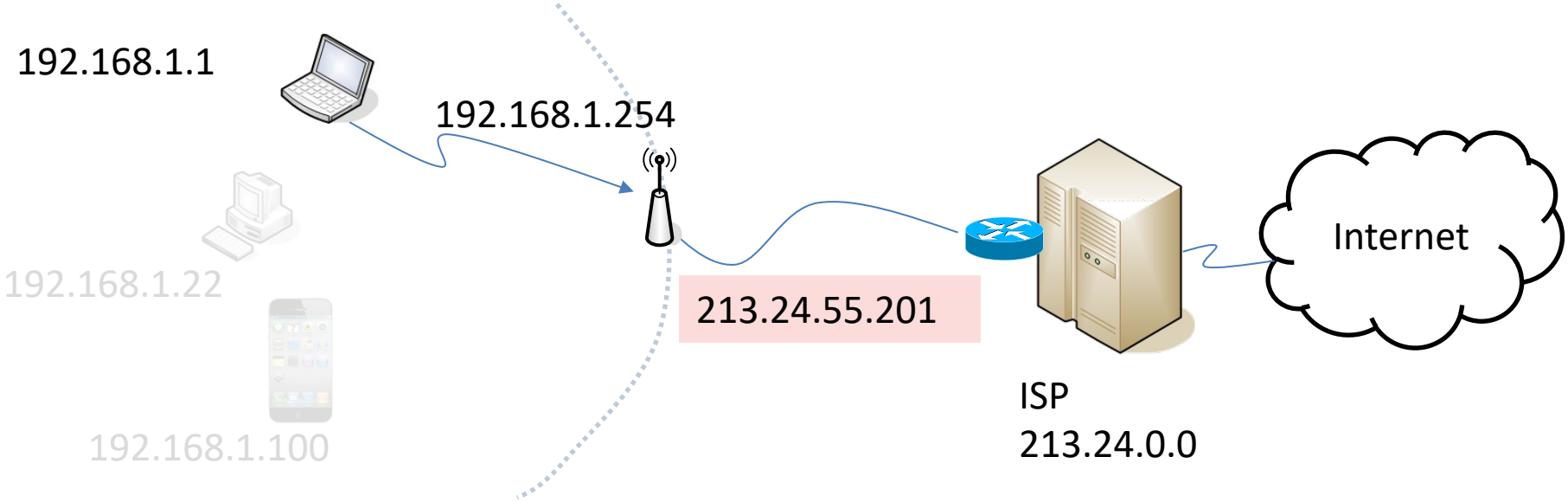


Src 134.226.36.14
Dst 213.24.55.201

NAT Table

Source	Destination
192.169.1.1:55612	134.226.36.14:80

NAT Example



Src 134.226.36.14
Dst 192.168.1.1

NAT Table

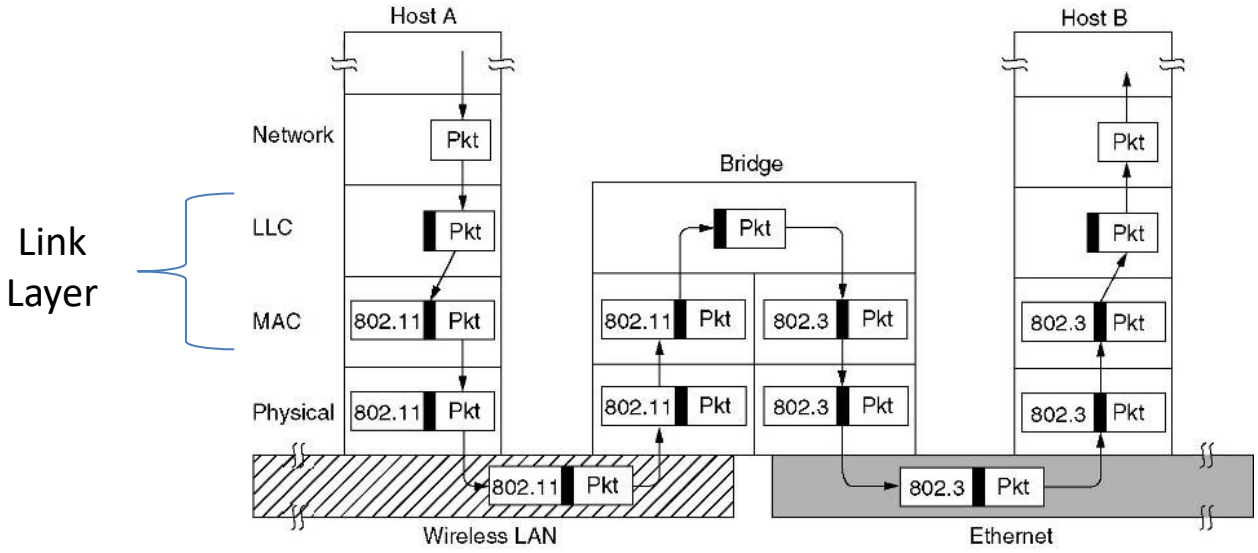
Source	Destination
192.169.1.1:55612	134.226.36.14:80

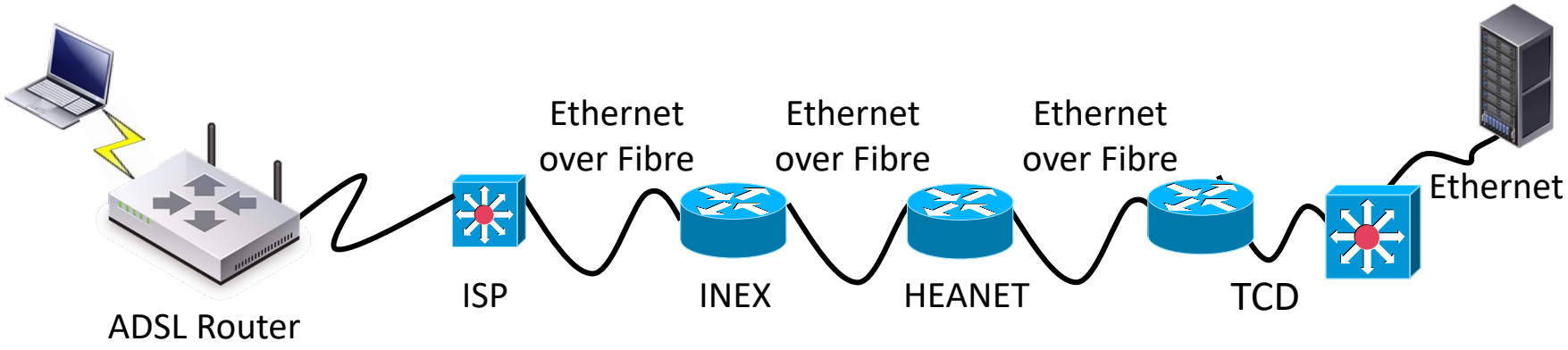
Everything's a Router

```
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.192.1   192.168.192.37      25
        127.0.0.0        255.0.0.0         On-link        127.0.0.1     306
        127.0.0.1  255.255.255.255         On-link        127.0.0.1     306
  127.255.255.255  255.255.255.255         On-link        127.0.0.1     306
     192.168.21.0    255.255.255.0         On-link     192.168.21.1     276
     192.168.21.1  255.255.255.255         On-link     192.168.21.1     276
   192.168.21.255  255.255.255.255         On-link     192.168.21.1     276
    192.168.111.0    255.255.255.0         On-link    192.168.111.1     276
    192.168.111.1  255.255.255.255         On-link    192.168.111.1     276
  192.168.111.255  255.255.255.255         On-link    192.168.111.1     276
    192.168.150.0    255.255.255.0         On-link    192.168.150.1     276
    192.168.150.1  255.255.255.255         On-link    192.168.150.1     276
  192.168.150.255  255.255.255.255         On-link    192.168.150.1     276
    192.168.192.0    255.255.255.0         On-link   192.168.192.37     281
   192.168.192.37  255.255.255.255         On-link   192.168.192.37     281
  192.168.192.255  255.255.255.255         On-link   192.168.192.37     281
```

Networks don’t talk IP

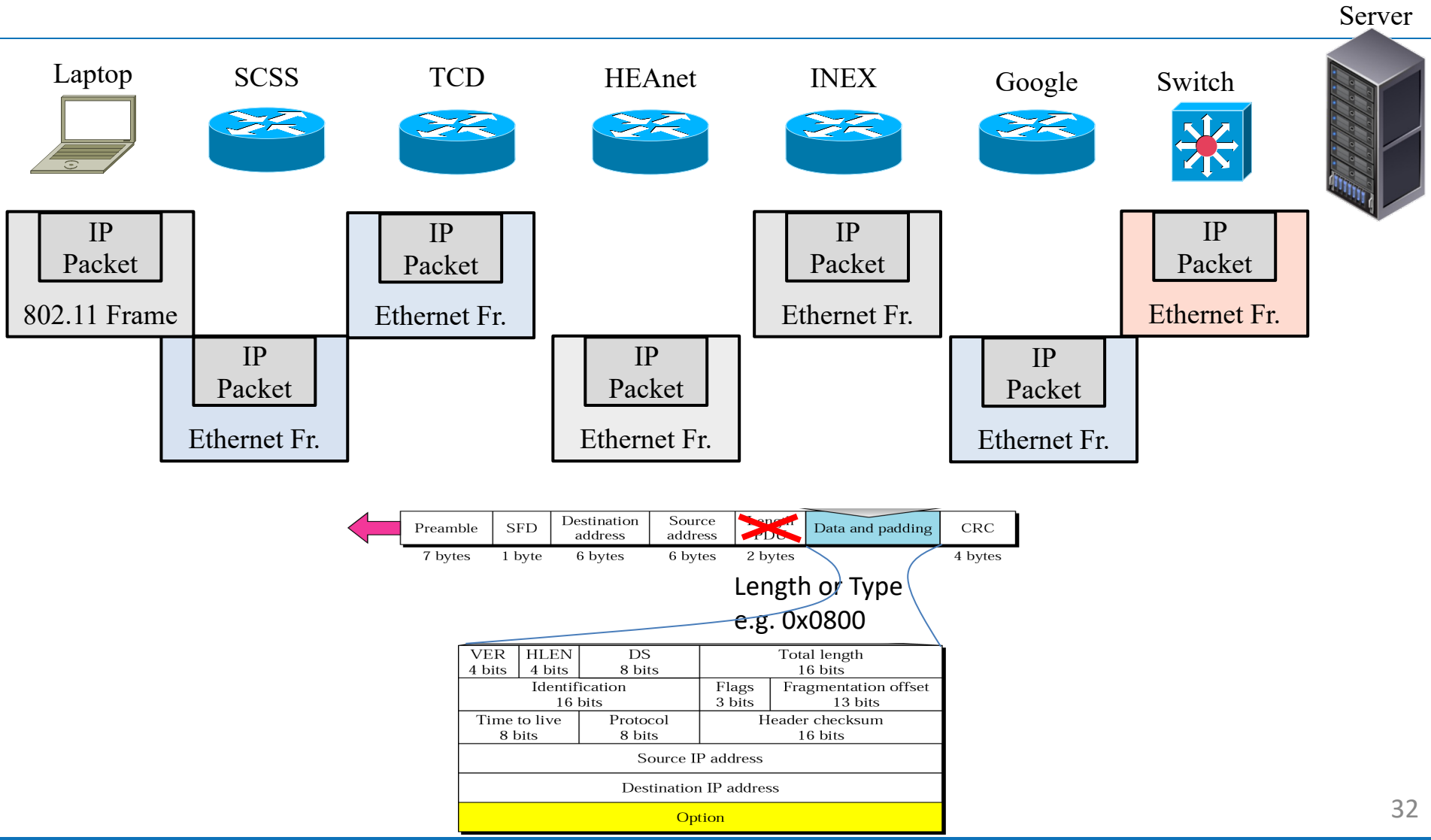
Ethernet all the way



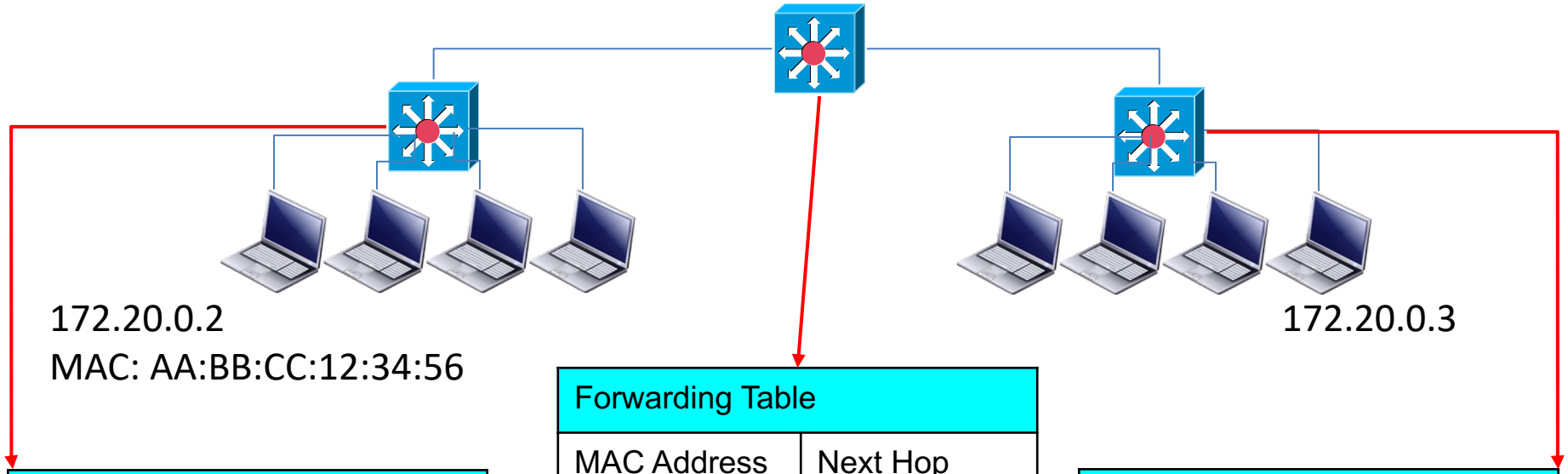


* Figure is courtesy of A. Tanenbaum

IP Packet Encapsulation in Ethernet



ARP Request: Broadcast through local net



172.20.0.2
MAC: AA:BB:CC:12:34:56

172.20.0.3

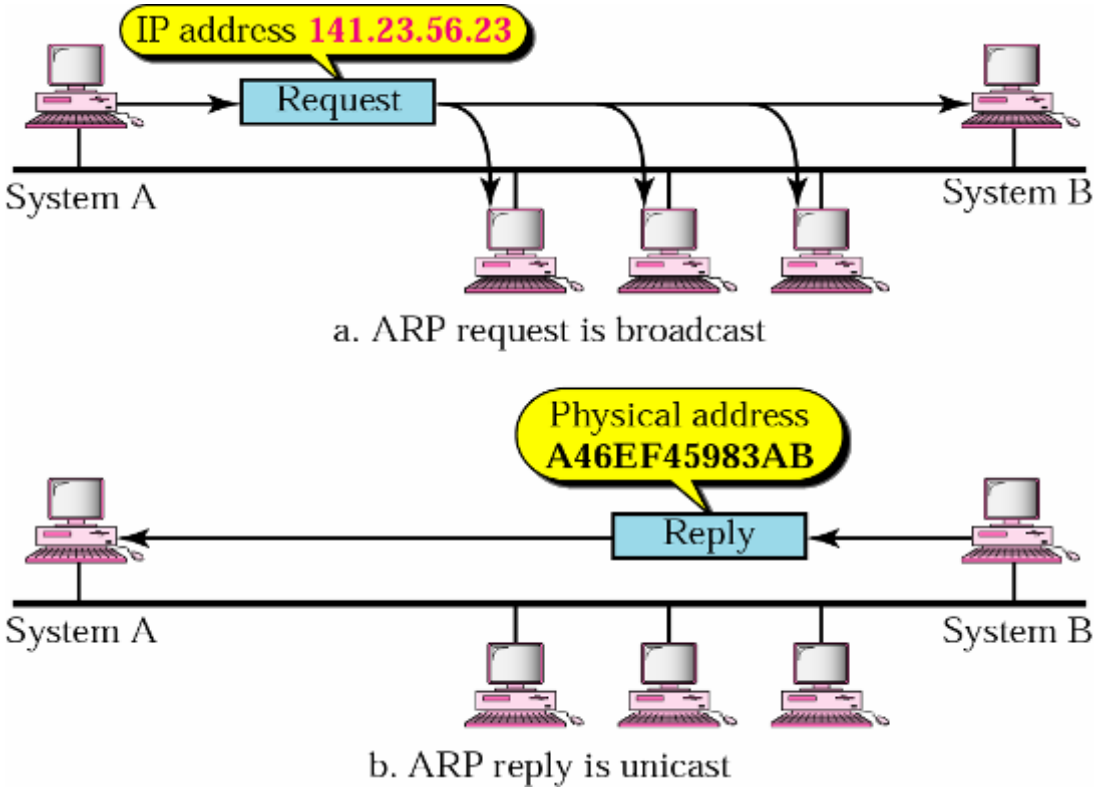
Forwarding Table	
MAC Address	Next Hop
AA:BB…34:56	Port 1
AA:BB…45:44	Port 2

Forwarding Table	
MAC Address	Next Hop
AA:BB…34:56	Port 7

Forwarding Table	
MAC Address	Next Hop
AA:BB:…:34:33	Port 13
CC:FF:…:55:66	Port 5

Address Resolution Protocol (ARP)

Ethernet all the way

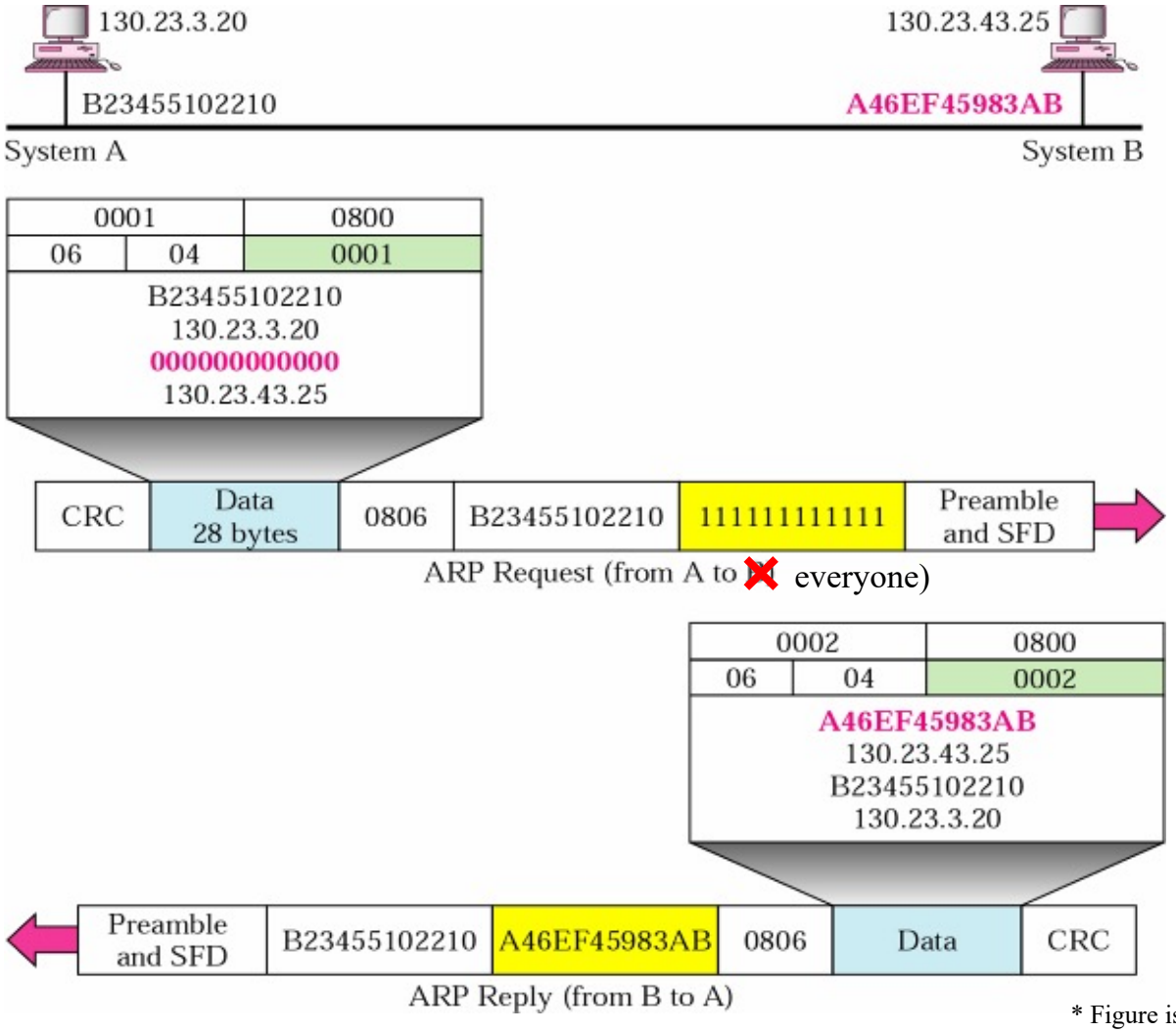


- Association between hardware address and IP address

* Figure is courtesy of B. Forouzan

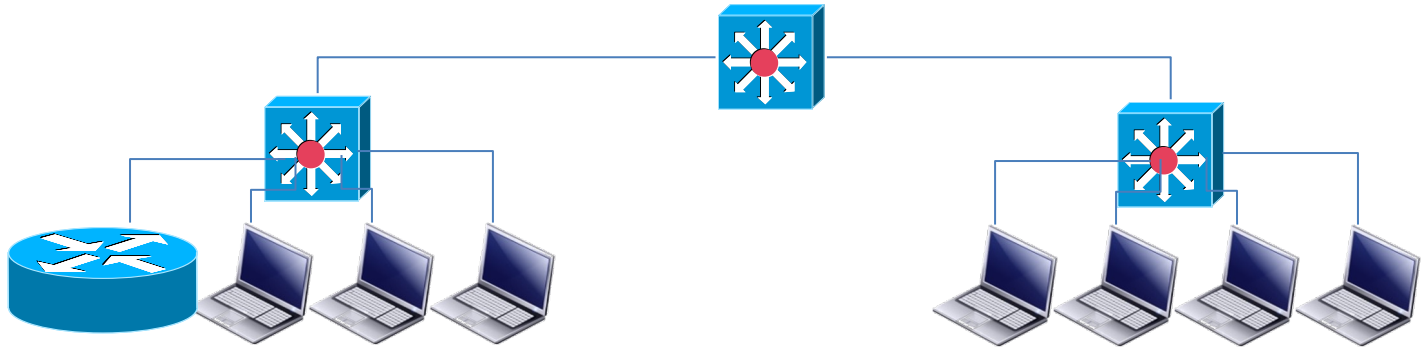
Address Resolution Protocol (ARP)

ARP Request & Reply



* Figure is courtesy of B. Forouzan

.0.2 trying to find .0.3



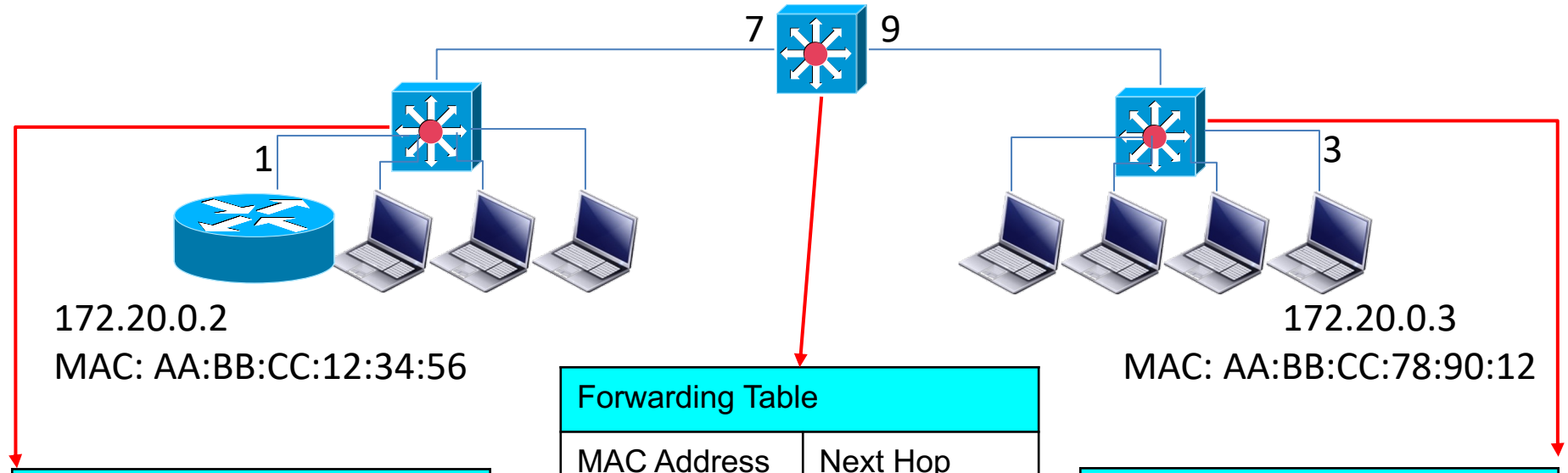
IP: 172.20.0.2
MAC: AA:BB:CC:12:34:56

172.20.0.3
MAC: AA:BB:CC:78:90:12

- ARP broadcast to everyone: Who has “172.20.0.3”?

- ARP reply from 172.20.0.3: Me, I’m AA:BB:CC:78:90:12

Packet from .0.2 to .0.3

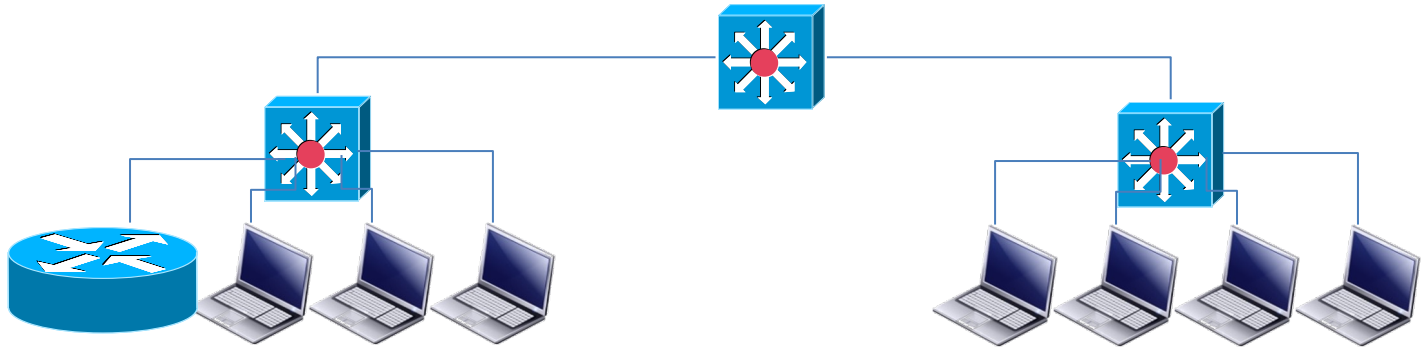


Forwarding Table	
MAC Address	Next Hop
AA:BB…34:56	Port 1
AA:BB…45:44	Port 2

Forwarding Table	
MAC Address	Next Hop
AA:BB…34:56	Port 7
AA:BB:..:90:12	Port 9

Forwarding Table	
MAC Address	Next Hop
AA:BB:…:34:33	Port 13
AA:BB:..:90:12	Port 3

Packet from .0.2 to .0.3



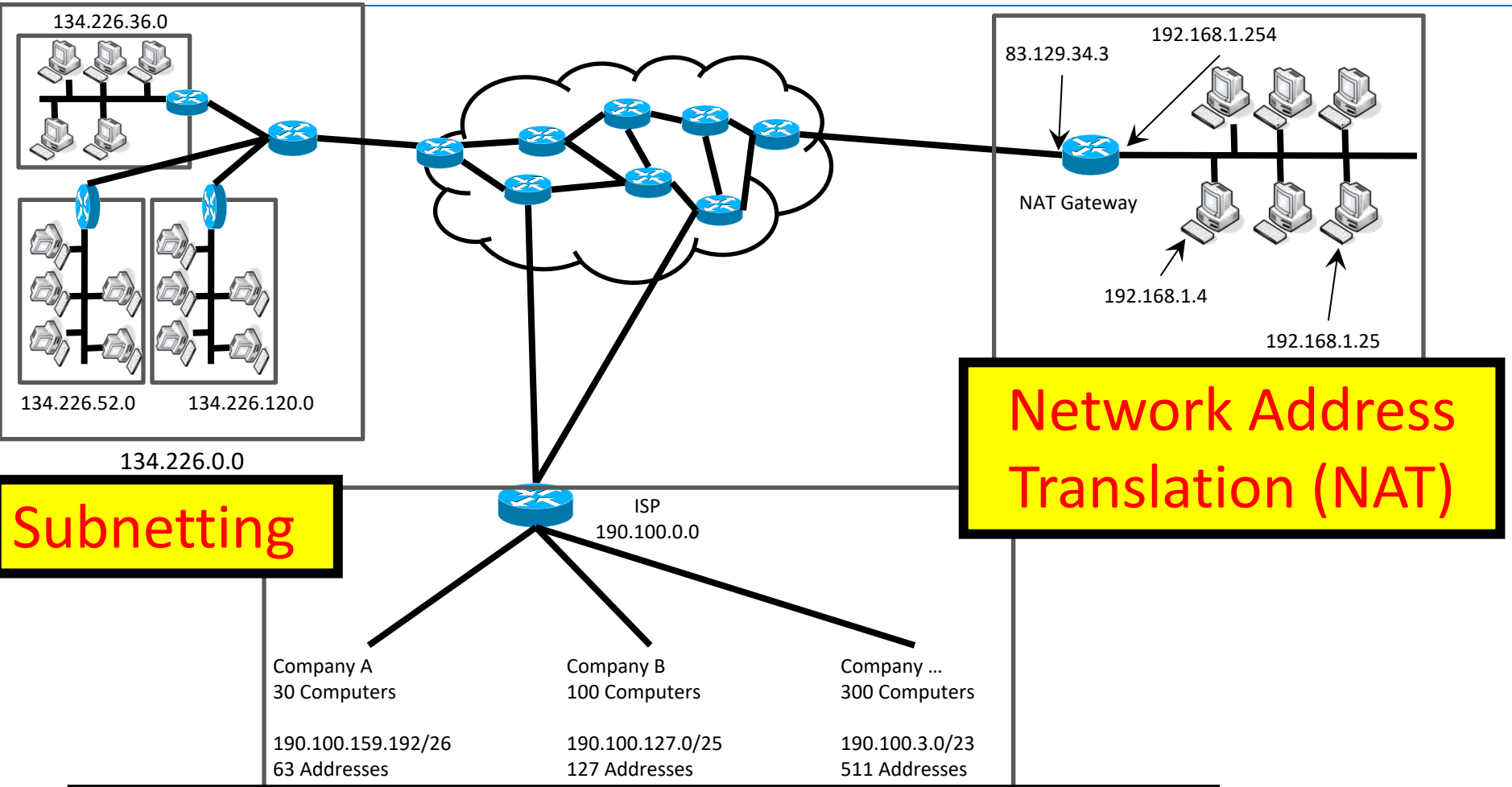
IP: 172.20.0.2
MAC: AA:BB:CC:12:34:56

172.20.0.3
MAC: AA:BB:CC:78:90:12

Ethernet Frame
From: AA:BB:CC:12:34:56
To: AA:BB:CC:78:90:12

IP Packet
From: 172.20.0.2
To: 172.20.0.3

Summary IP Addresses

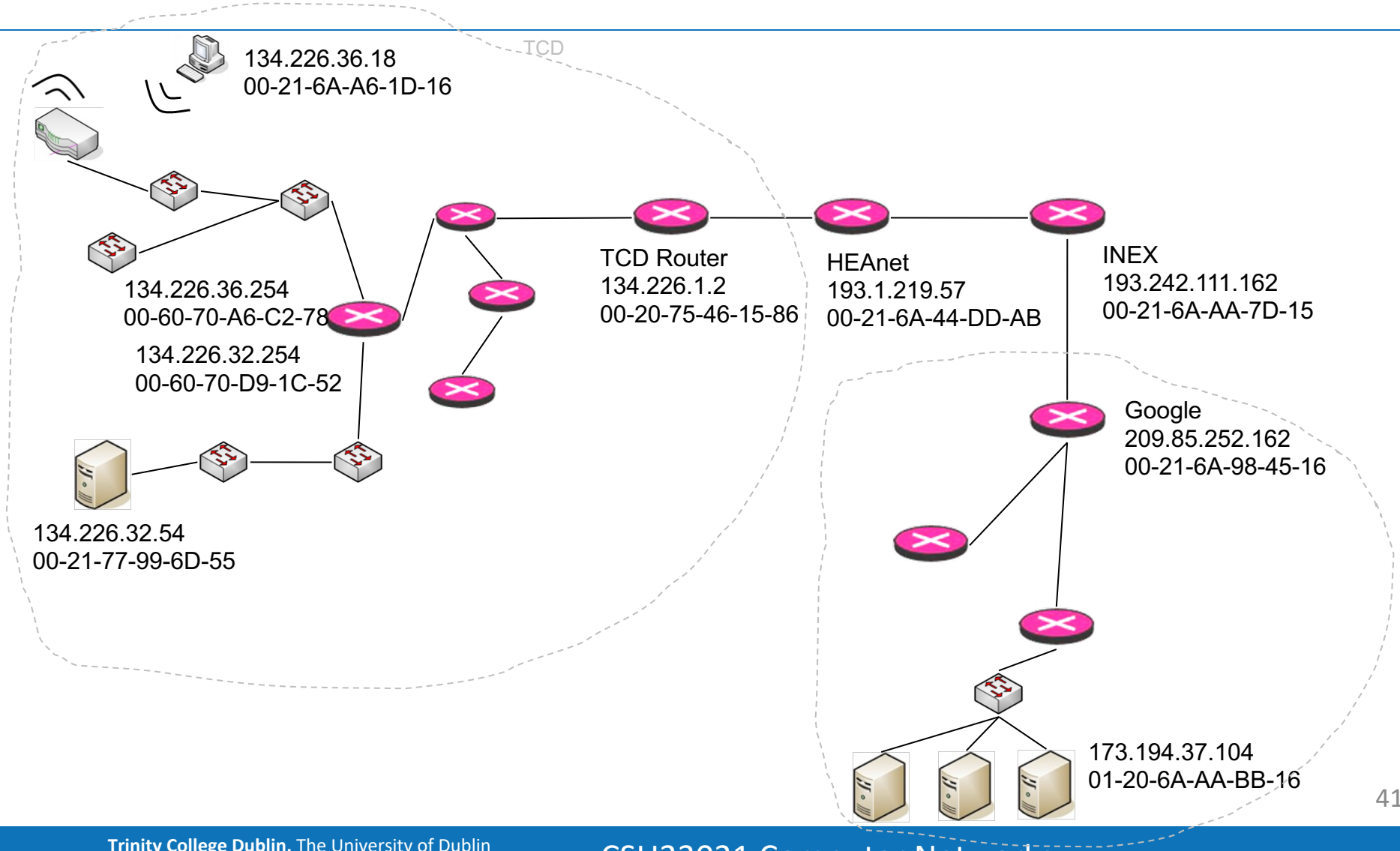


Summary: Addresses

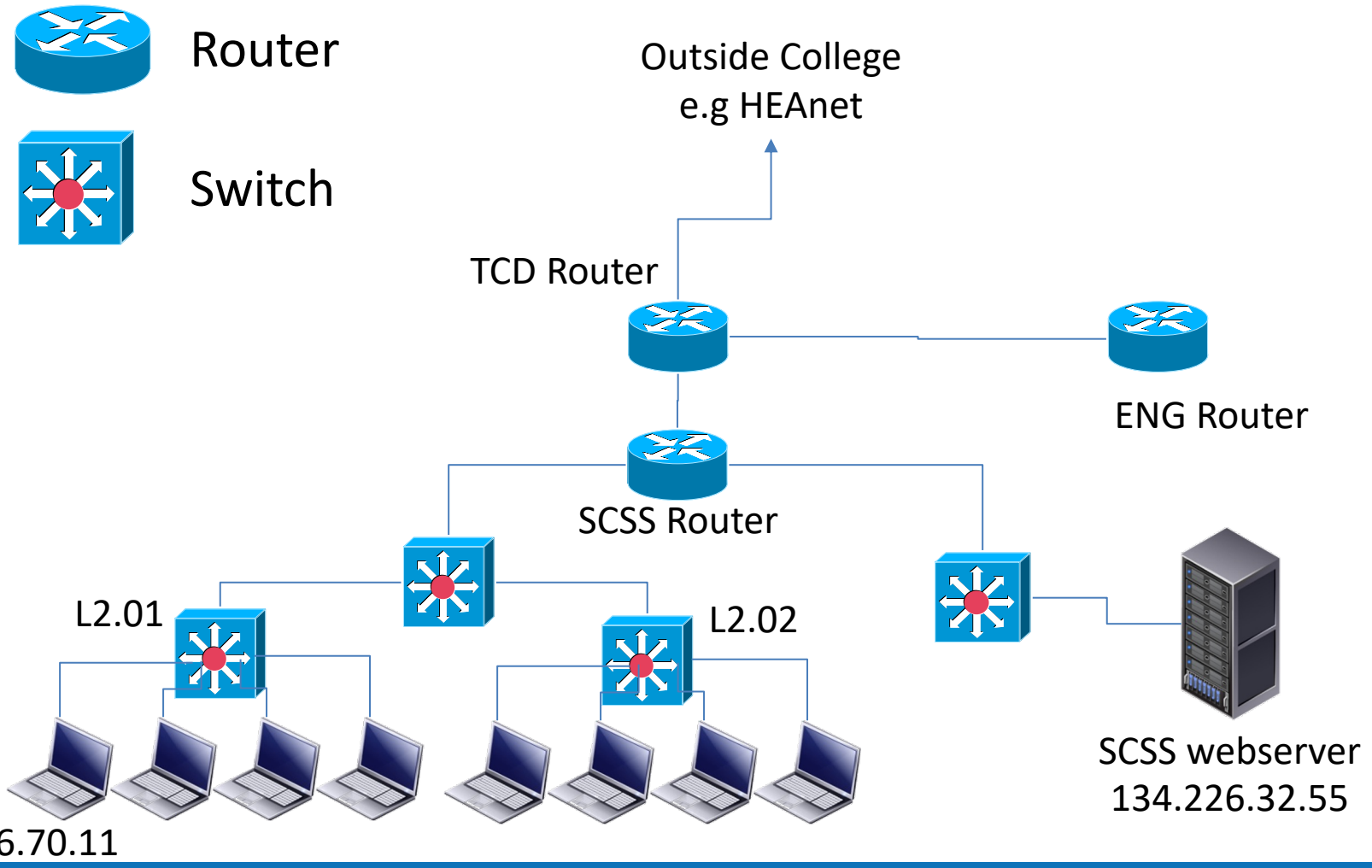
- 32-bit number / Dotted decimal notation
- IP addresses are unique and universal
  - Exception: Private Addresses

- Classful addresses
  - Classes A, B, and C for networks, D for multicast
  - Routing on Network IDs
- Subnetting + Netmasks
  - Dealing with scale in local networks
- Classless Inter-Domain Routing (CIDR)
  - / notation – significant bits of address
- Network Address Translation (NAT)

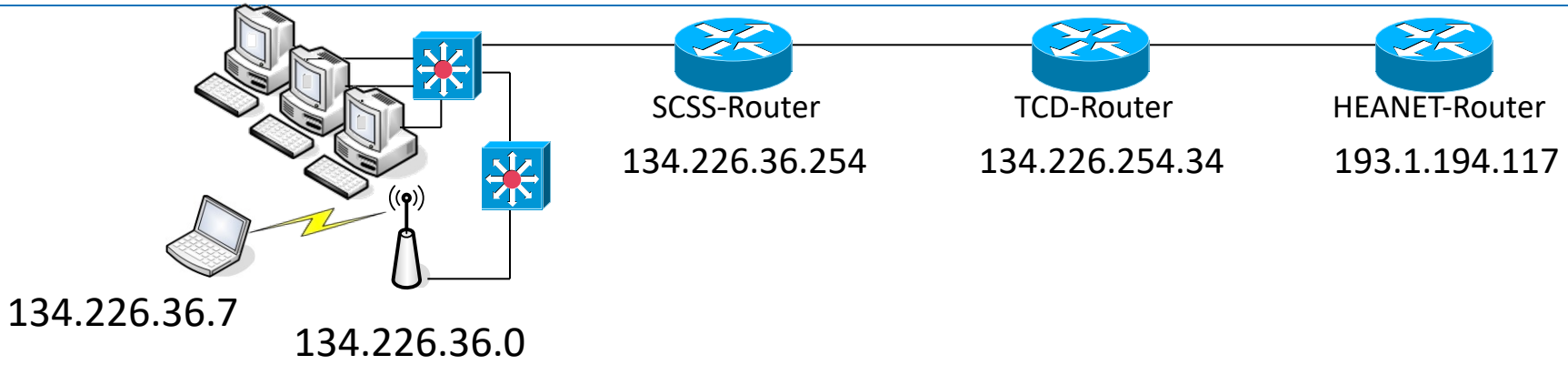
Network Layer Scenario I



Network Layer Scenario II



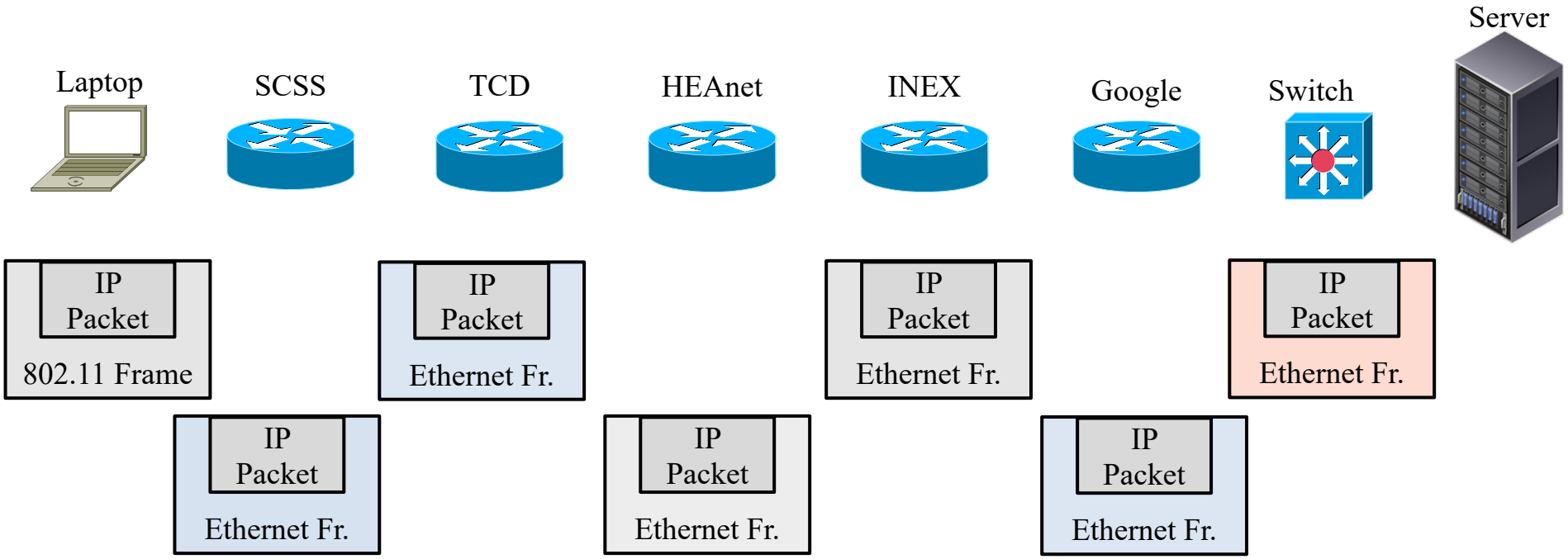
Default Gateway



Subnet	Gateway	Netmask	Interface
134.226.36.0	0.0.0.0	255.255.255.0	eth1
0.0.0.0	134.226.36.254	0.0.0.0	eth1

- All nodes within the subnet can communicate directly with each other
- All communication with nodes in other networks passes through the default gateway e.g. router 134.226.36.254

Encapsulation



Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

CSU33031 Computer Networks

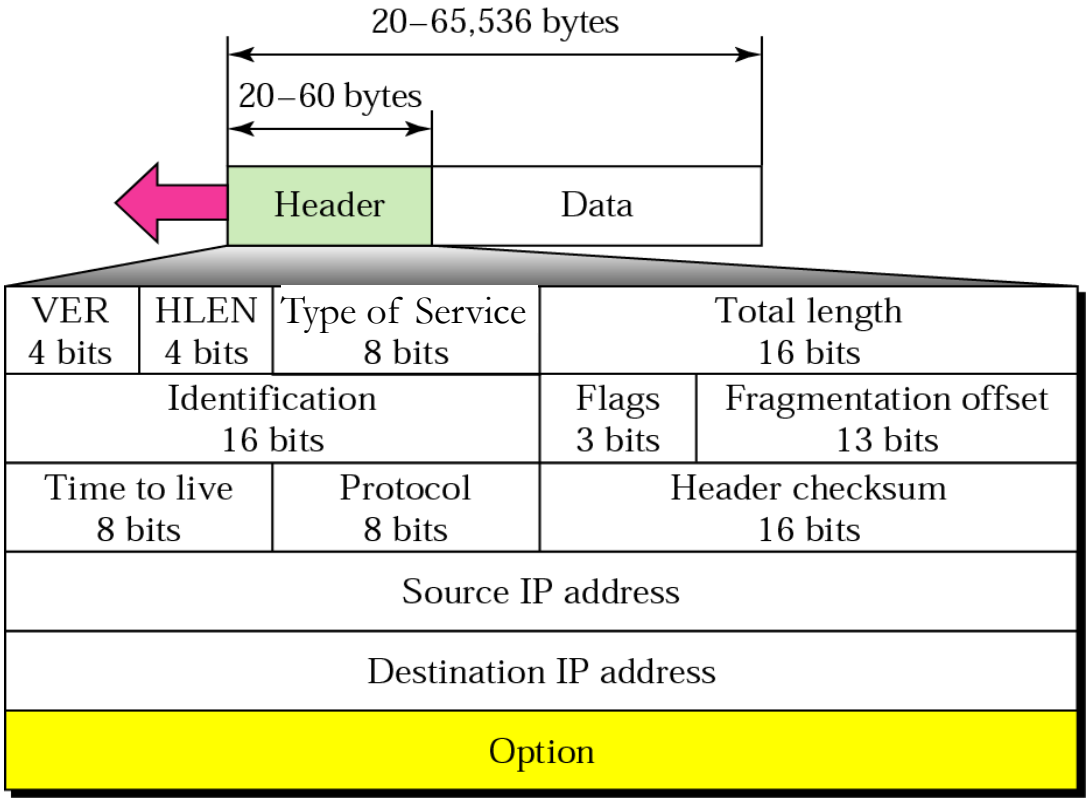
IPv4 Fragmentation

Stefan Weber

email: sweber@tcd.ie

Office: Lloyd 1.41

IP Packet



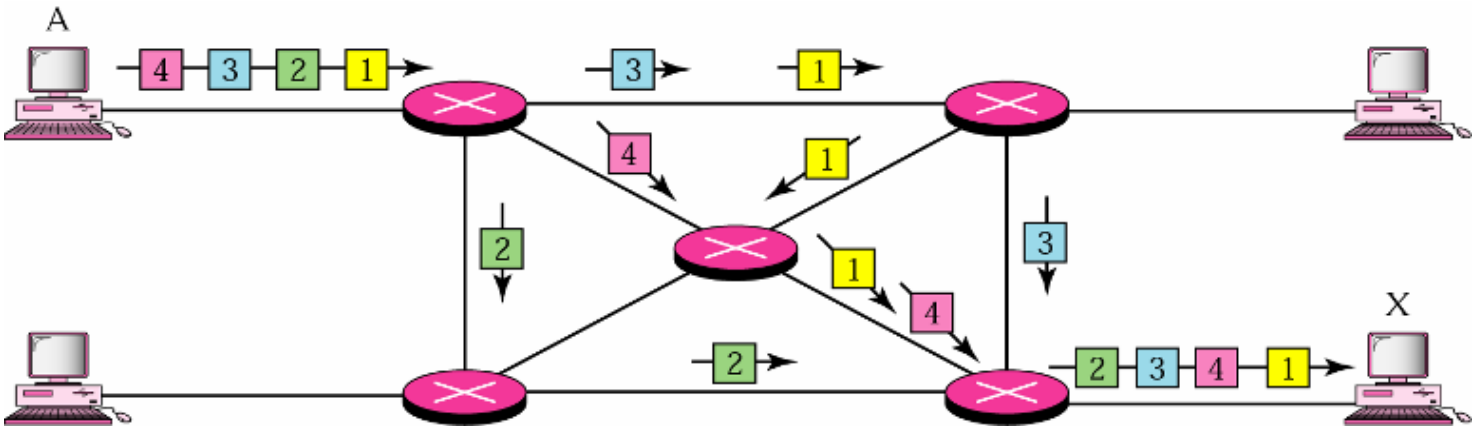
- The total length field defines the total length of the packet including the header.

* Figure is courtesy of B. Forouzan

IP Packet Header Fields

Length in bit	Name	Description
4	Version	Version of IP (4, 6)
4	HLEN	Length of the header
8	Service Type	Sender's preference for services e.g. low latency, etc
16	Total Length	Total length of datagram in bytes/octects
16	Identification	Unique identification for each datagram
4	Flags	Control fragmentation of datagrams
12	Fragment Offset	Used in fragmentation of datagrams
8	TTL	Time to live; decremented at each hop it passes
8	Protocol	Higher-layer protocol such as TCP, UDP, etc
16	Header Checksum	Checksum to verify correctness of header information
32	Source address	IP address of the sender
32	Dest. address	IP address of the destination

IP Service Model



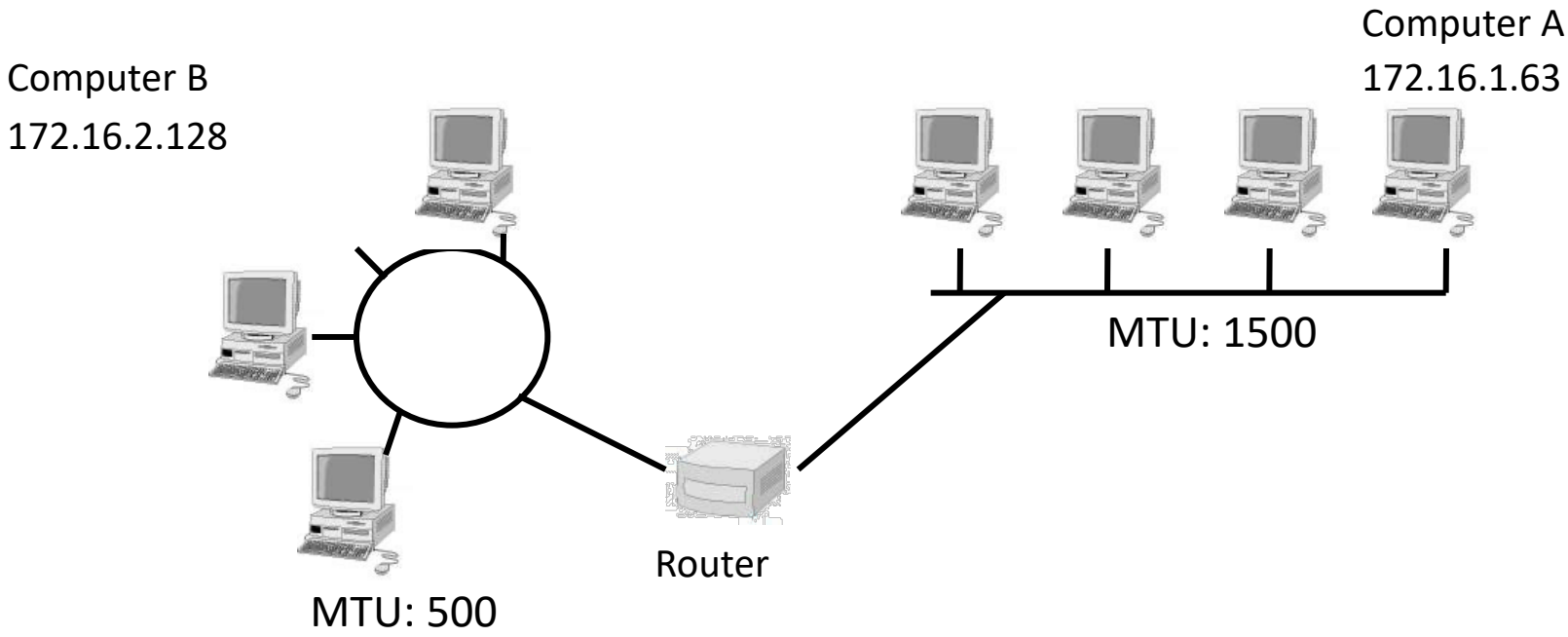
- Best-effort delivery (unreliable service)
  - Packets may be lost
  - Packets may be delivered out of order
  - Duplicate copies of a packet may be delivered
  - Packets can be delayed for a long time

Maximum Transmission Unit (MTU)

- Maximum size of a data unit depends on underlying hardware architecture
- Maximum frame size determines *Maximum Transmission Unit (MTU)*

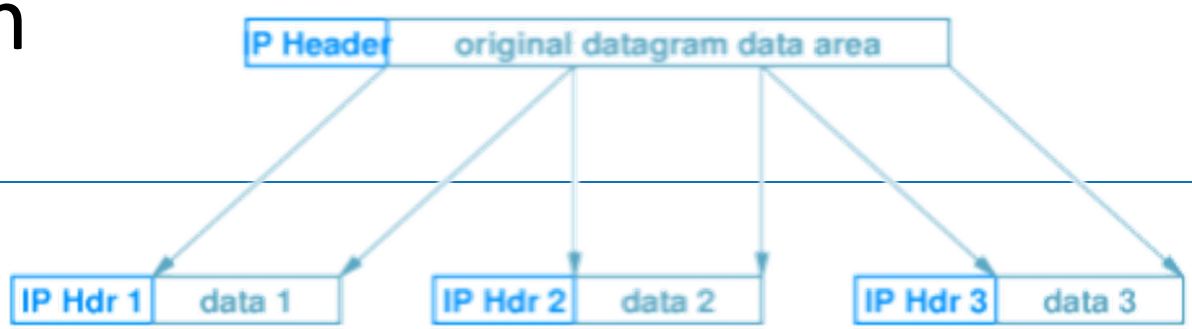
Protocol	*MTU*
Hyperchannel	65,535
Token Ring (16 Mbps)	17,914
Token Ring (4 Mbps)	4,464
FDDI	4,352
Ethernet	1,500
X.25	576
PPP	296

IP & Network Architectures



- IP packets may be larger than most MTUs of underlying network architectures
- Maximum frame size limits maximum size of an IP packet for a network

Fragmentation

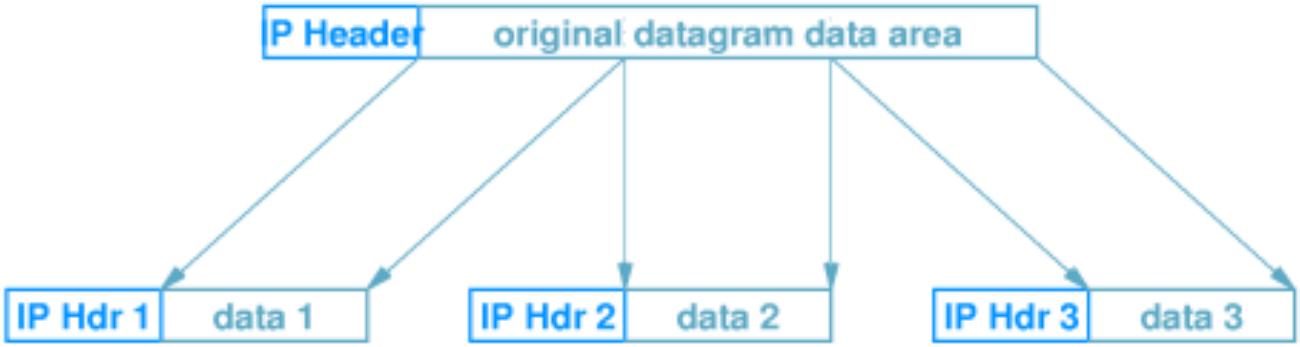


- Possible techniques
  - Limit packet size to smallest MTU of any network
  - Adjust packet size as packet progresses through networks
    - Router detects packet larger than network MTU and splits into fragments

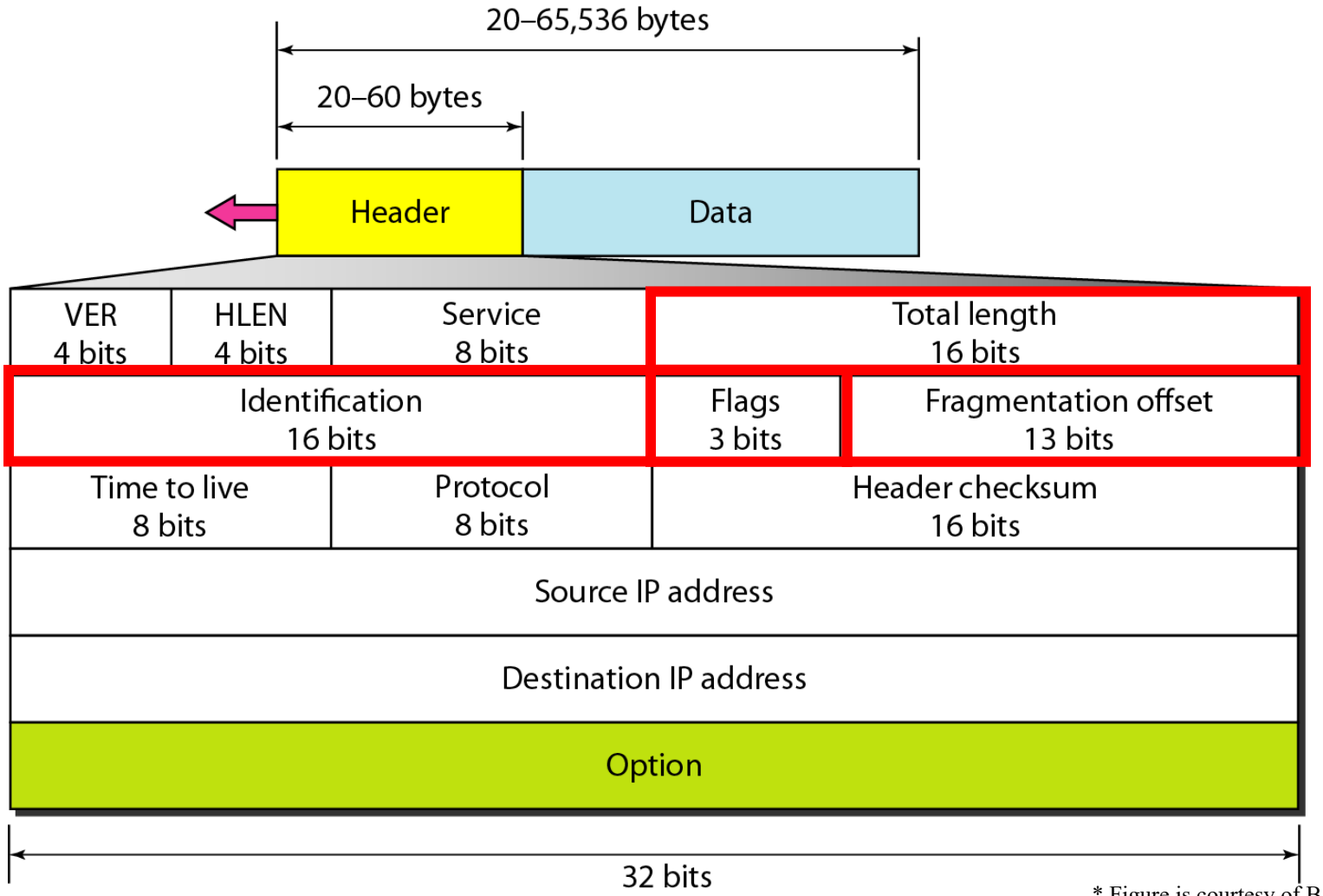
- IP Strategy
  - Fragment when necessary (Datagram > MTU)
  - Try to avoid fragmentation at source host
  - Re-fragmentation is possible
  - Delay reassembly until destination host
  - Do not recover from lost fragments
    - If one fragment is lost all fragments are discarded

Fragmentation (details)

- Each fragment is an independent packet
  - Includes all header fields
  - Bit in header indicates packet is a fragment
  - Other fields have information for reconstructing original packet
  - FRAGMENT OFFSET gives original location of fragment



Fragmentation & IPv4 Header

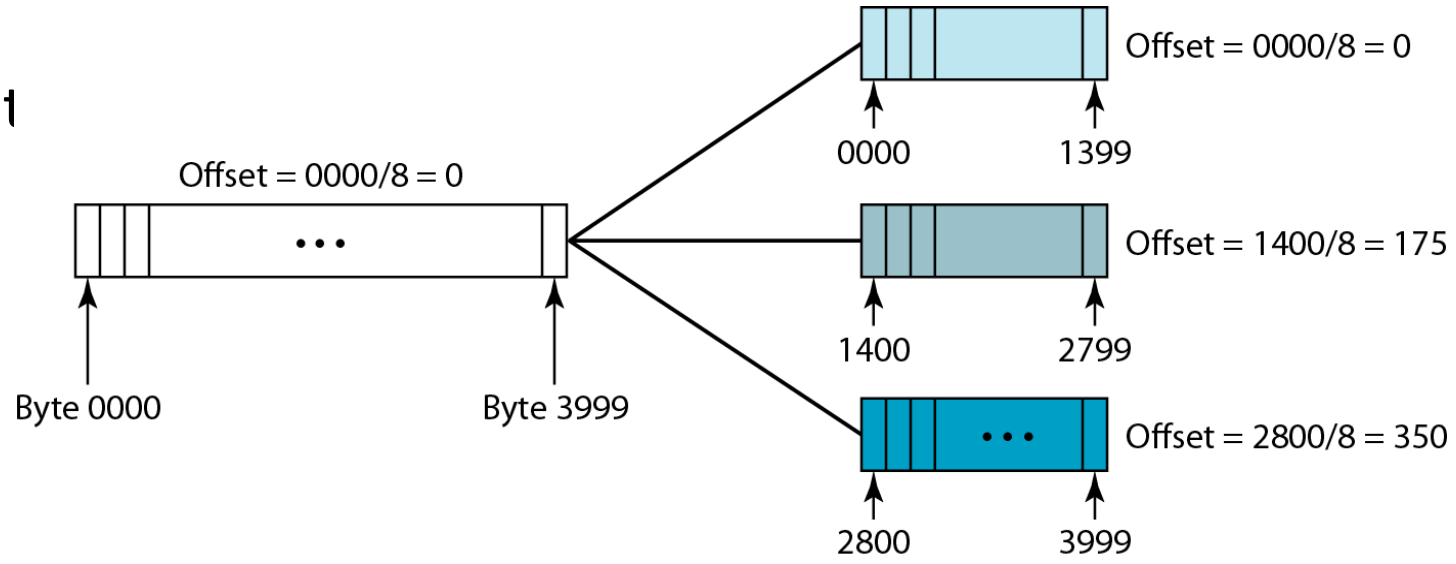


* Figure is courtesy of B. Forouzan

Header Fields

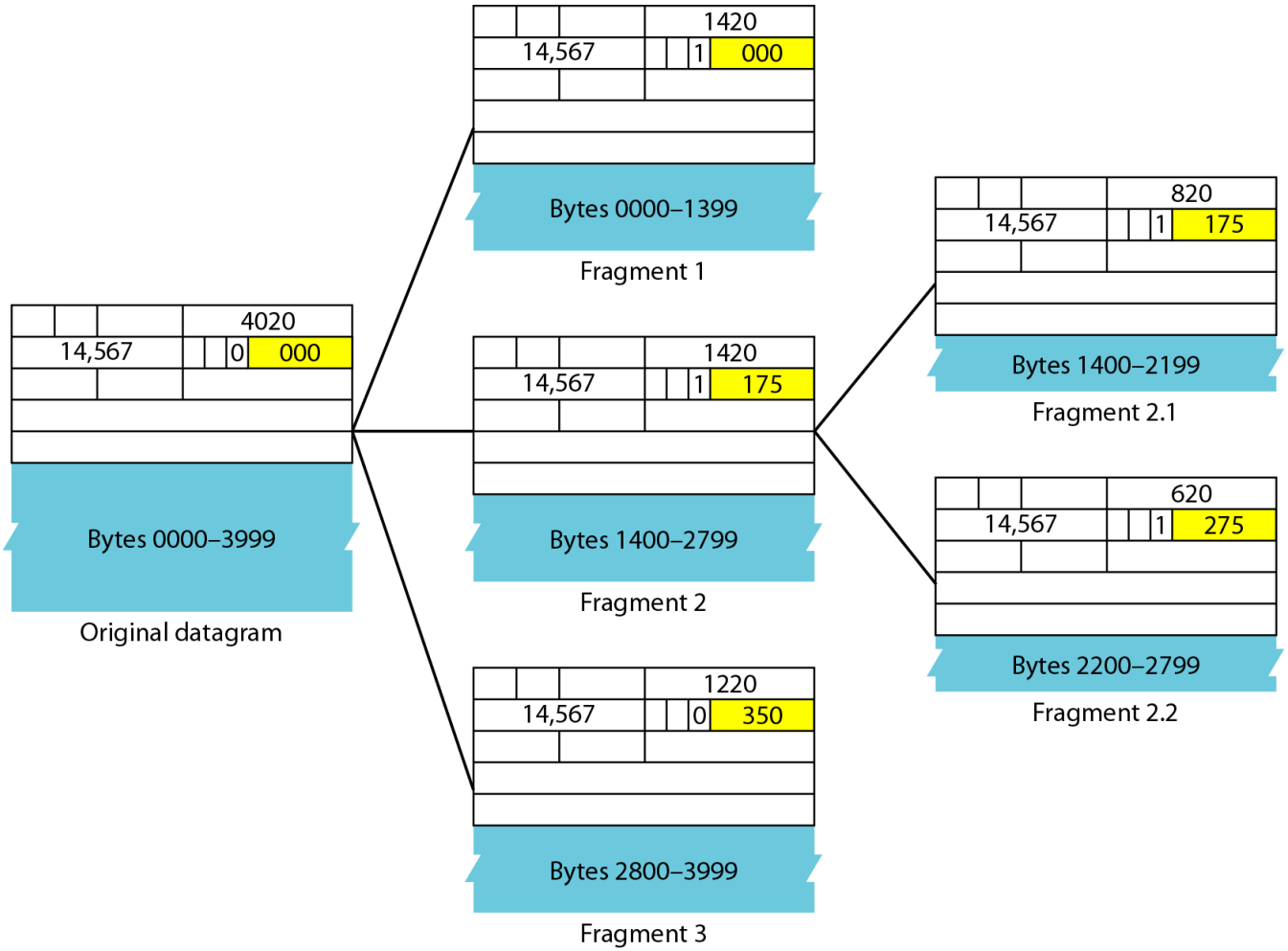
- "Do not fragment"-Request
- More Fragments

- Offset

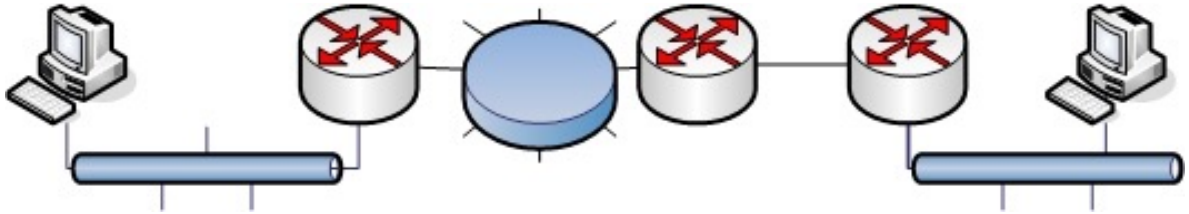


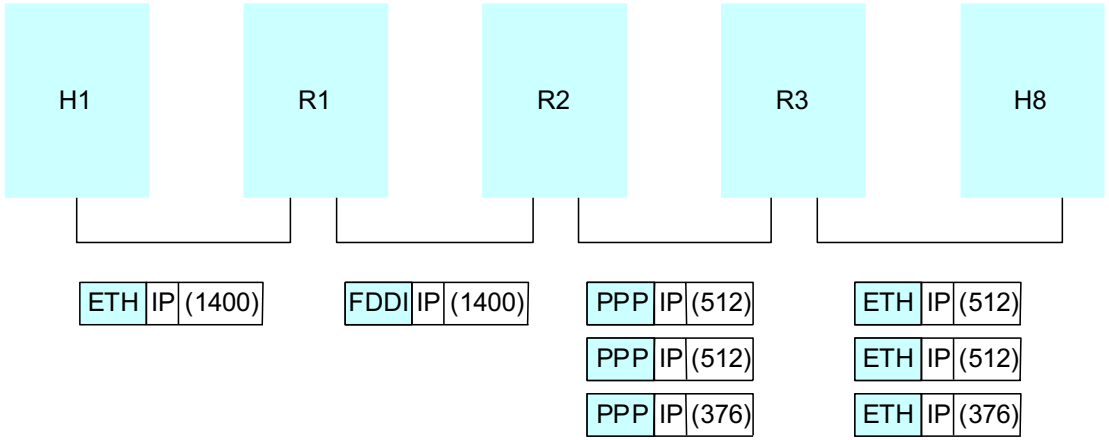
* Figure is courtesy of B. Forouzan

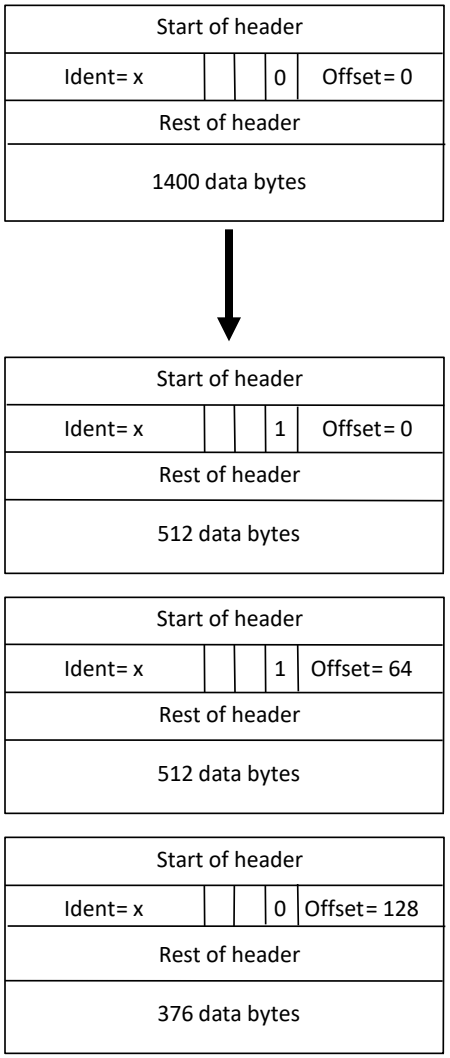
Fragmentation Example I



Fragmentation Example II



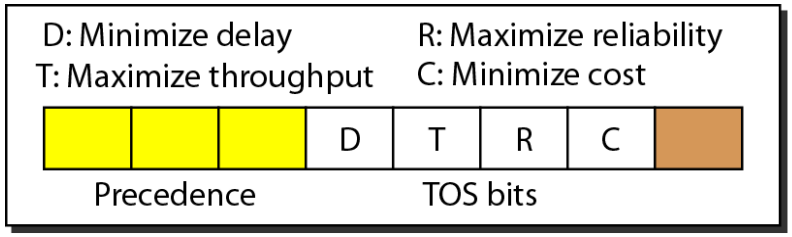




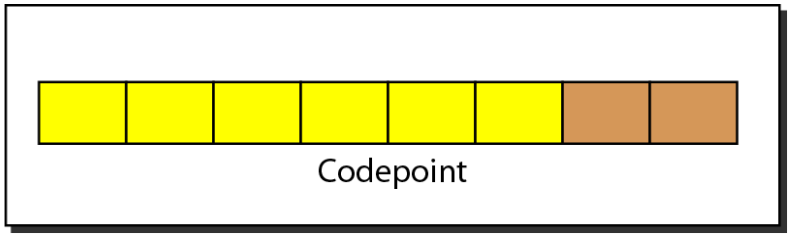
Fragment loss

- A fragment may be lost/dropped in transfer
- What happens to original datagram?
  - Destination drops entire original datagram
- How does destination identify lost fragment?
  - Sets timer with each fragment
  - If timer expires before all fragments arrive, fragment assumed lost
  - Packet dropped
- Source is assumed to retransmit

Service types



Service type



Differentiated services

TOS Bits	*Description*
0000	Normal (default)
0001	Minimize cost
0010	Maximize reliability
0100	Maximize throughput
1000	Minimize delay

* Figure is courtesy of B. Forouzan

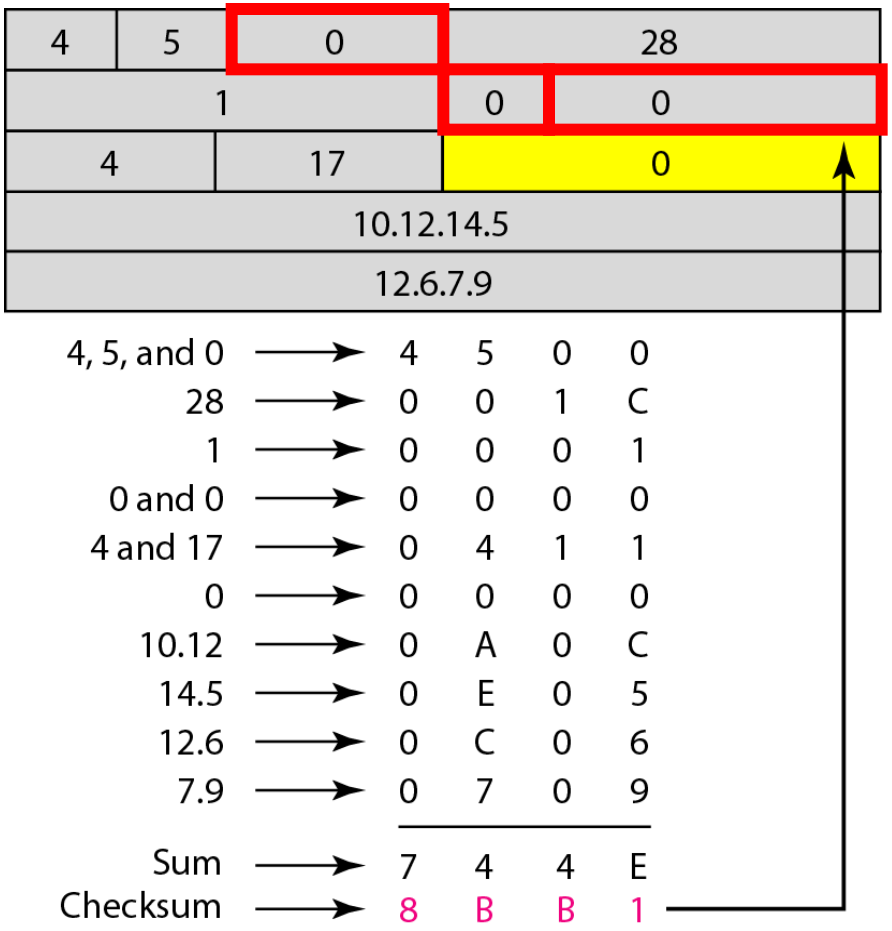
Protocols & TOS Bits

Protocol	*TOS Bits*	*Description*
ICMP	0000	Normal
BOOTP	0000	Normal
NNTP	0001	Minimize cost
IGP	0010	Maximize reliability
SNMP	0010	Maximize reliability
TELNET	1000	Minimize delay
FTP (data)	0100	Maximize throughput
FTP (control)	1000	Minimize delay
TFTP	1000	Minimize delay
SMTP (command)	1000	Minimize delay
SMTP (data)	0100	Maximize throughput
DNS (UDP query)	1000	Minimize delay
DNS (TCP query)	0000	Normal
DNS (zone)	0100	Maximize throughput

* Figure is courtesy of B. Forouzan

Checksum in IPv4 Header

- Calculation omits:
  - Service field
  - Fragment fields and offset
  - Checksum field

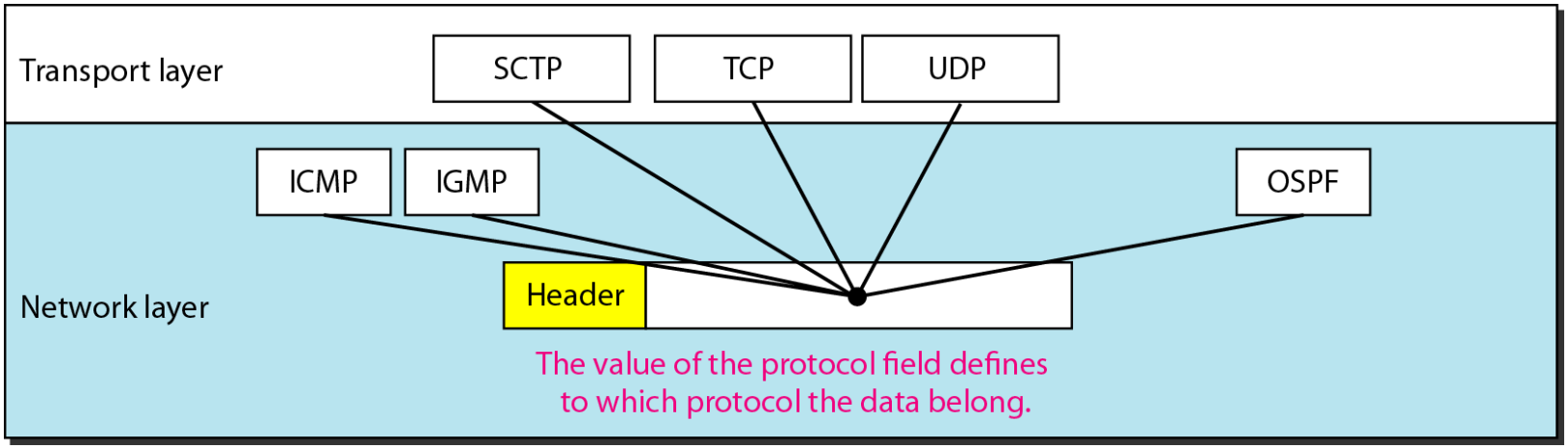


* Figure is courtesy of B. Forouzan

Protocol Field

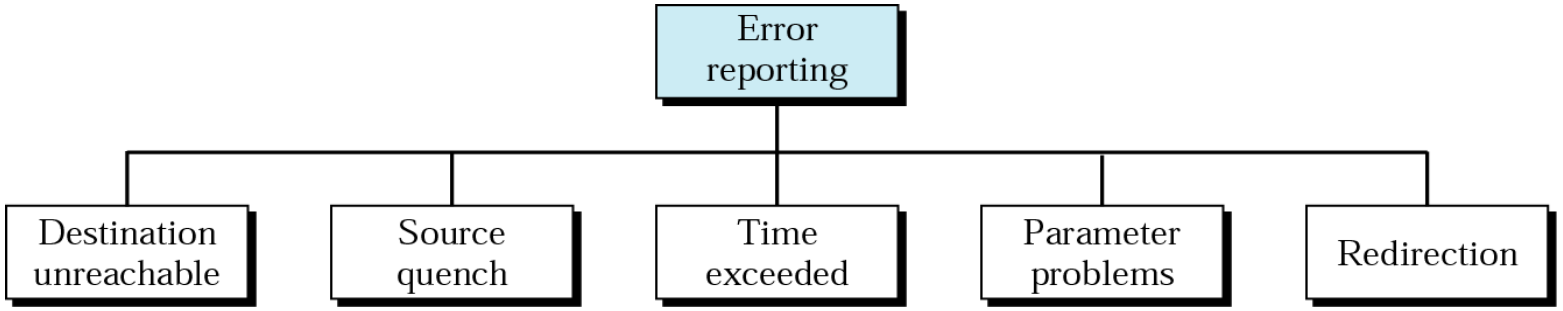
- Specifies next protocol in stack

Value	*Protocol*
1	ICMP
2	IGMP
6	TCP
17	UDP
89	OSPF



* Figure is courtesy of B. Forouzan

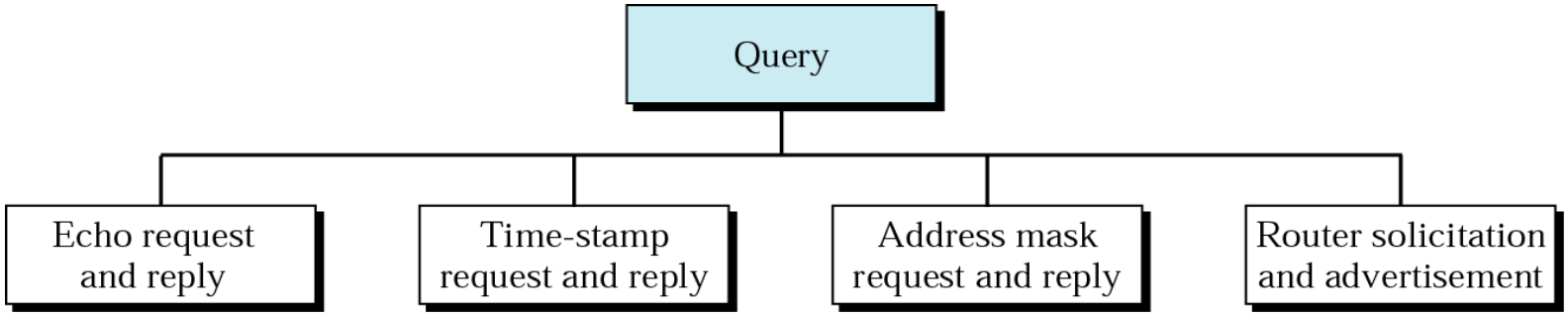
Internet Control Message Protocol



- Time exceeded
  - Send when datagram discarded due TTL value of 0
- Parameter problems
  - Send when datagram discarded due to parameter ambiguity
- Redirection
  - Send from router to update routing table of source

* Figure is courtesy of B. Forouzan

ICMP Queries



Ping

uses the ICMP protocol's mandatory ECHO_REQUEST datagram to elicit an ICMP ECHO_RESPONSE from a host or gateway. ECHO_REQUEST datagrams have an IP and ICMP header, followed by a struct timeval and then an arbitrary number of bytes used to fill out the packet.

```
$ ping www.tcd.ie
PING dux6.tcd.ie (134.226.1.61): 56 data bytes
64 bytes from 134.226.1.61: icmp_seq=0 ttl=64 time=0.781 ms
64 bytes from 134.226.1.61: icmp_seq=1 ttl=64 time=0.466 ms
64 bytes from 134.226.1.61: icmp_seq=2 ttl=64 time=0.490 ms
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.457/0.548/0.781/0.135 ms
```

Summary: Internet Protocol

- IP Service Model
  - Connection-less, no order guaranteed
- IP Header
  - 20 bytes + options
- Fragmentation
  - Datagrams split into fragments to fit MTUs
  - Only re-assembled at destination
- Internet Control Message Protocol (ICMP)
  - Error Reporting e.g. source quench
  - Querying e.g. Ping

Re Late Submissions/School Handbook

6.4 Penalties for Late Submission

Penalties for late submission of coursework may be specified for each module but in the absence of any such specification the following penalties may be applied:

- In the case of fourth and fifth year final year project reports, dissertations and internship reports, late submissions are penalised by 5% per 'day', and a mark of 0% is awarded if the submission is more than 2 weeks after the deadline.
- In fourth and fifth year, late submissions of coursework other than final year project reports, dissertations and internship reports are penalised by 10% per 'day' and a mark of 0% is awarded if the submission is more than 2 weeks after the deadline for submission.
- In all other years, late submissions are penalised by 20% per 'day' and a mark of 0% is awarded if the submission is more than 1 week after the deadline for submission.

20

- In the case of electronic submission, a 'day' is taken to be a 24 hour period (or any part thereof). In the case where physical submission is required, a 'day' is taken to be a working day (Monday to Friday) or any part thereof. For the purposes of this regulation, a working day ends at the latest time that work can be submitted to the School Office. In all cases a week is a calendar week.
- For coursework which must be submitted in both electronic and physical form, the larger of the two penalties will be applied.

Re Late Submissions/School Handbook

Extraction of the more relevant points

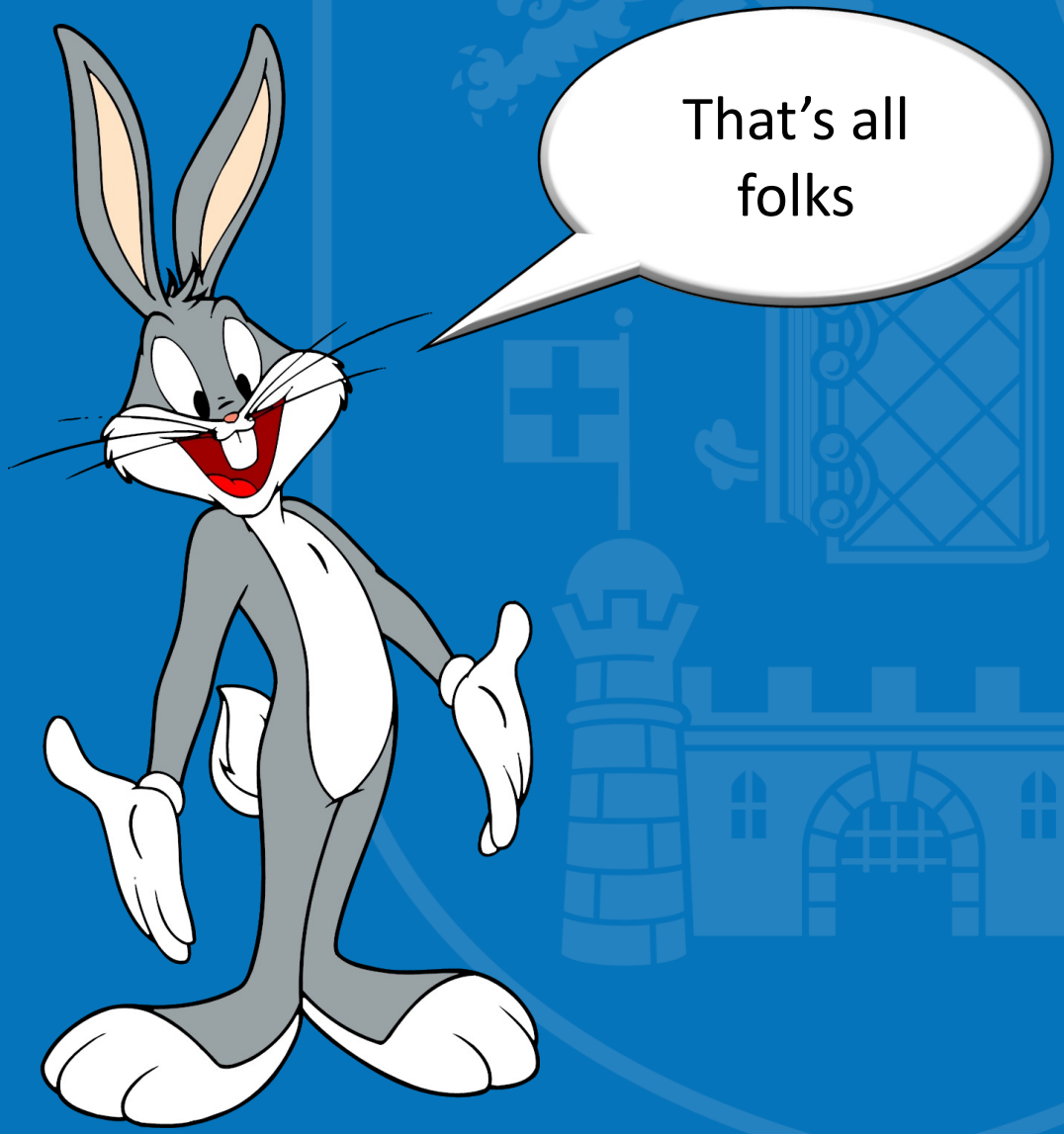
- In all other years, late submissions are penalised by 20% per ‘day’ and a mark of 0% is awarded if the submission is more than 1 week after the deadline for submission.

- In the case of electronic submission, a ‘day’ is taken to be a 24 hour period (or any part thereof). In the case where physical submission is required, a ‘day’ is taken to be a working day (Monday to Friday) or any part thereof. For the purposes of this regulation, a working day ends at the latest time that work can be submitted to the School Office. In all cases a week is a calendar week.

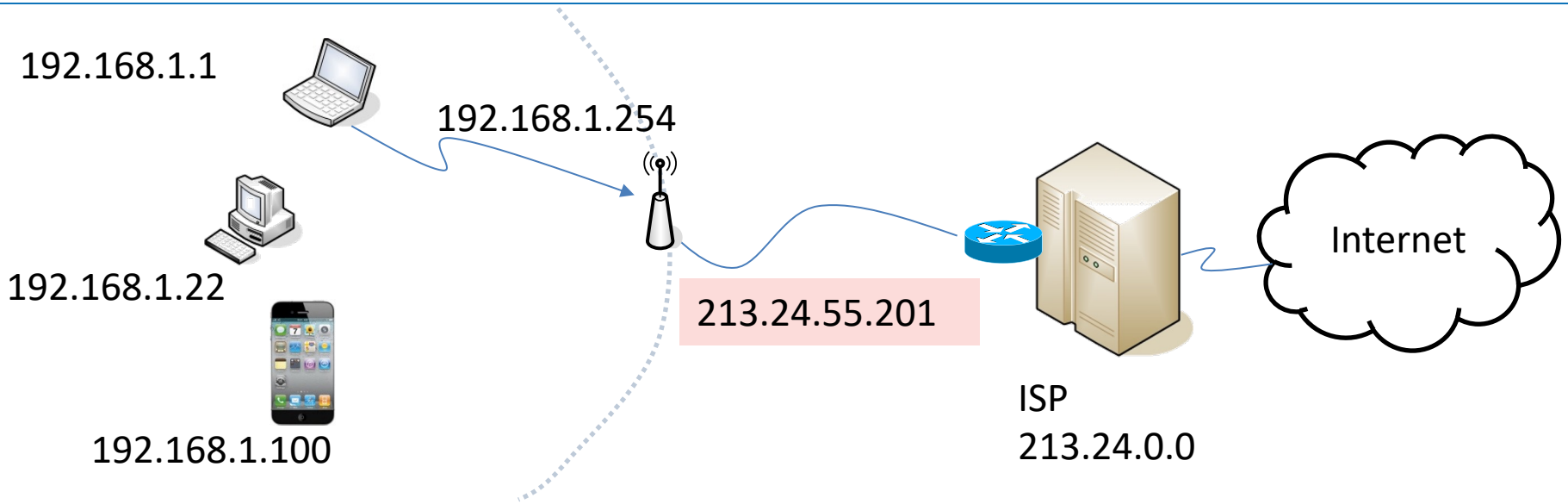
From the ICS handbook:

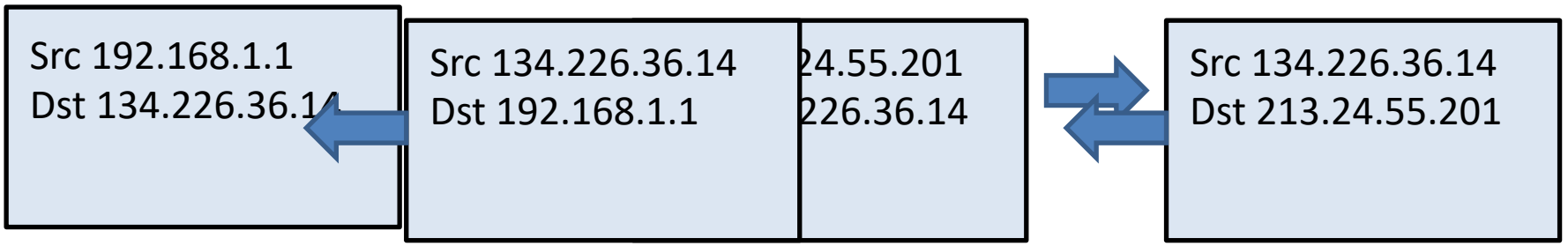
- Penalties for late submission of coursework are specified in the School Handbook. If there are extenuating circumstances warranting late submission students must request extensions through their tutors in advance of the deadline for submission. Extenuating circumstances include only serious circumstances such as certified medical conditions and bereavements.

Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin



NAT Example





NAT Table

Source	Destination
192.169.1.1:55612	134.226.36.14:80