IPV4 Exhaustion

- Short term solutions
- CIDR
- NAT
- VLSM
- Longterm solutions
- IPV6

NAT

IPv4 Private Address Space

- Private IP addresses are used within organization and home networks.

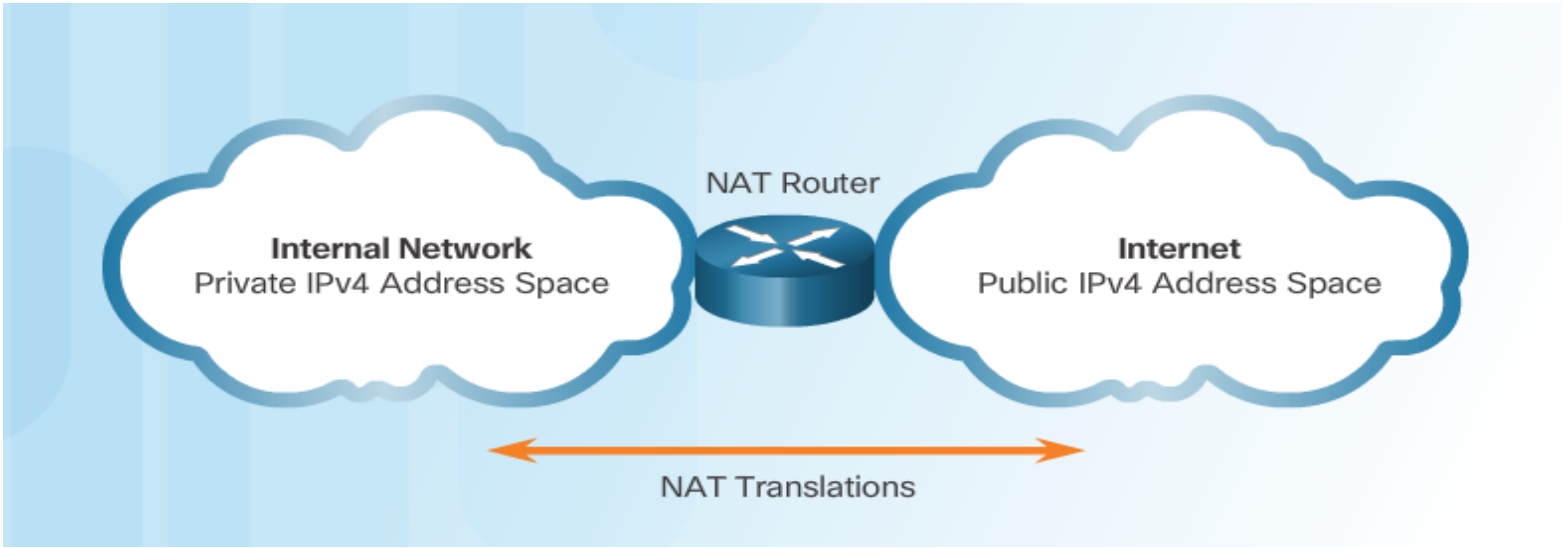
Did you ever notice how all your labs were based on these addresses?

Private Internet Addresses are Defined in RFC 1918

Class	RFC 1918 Internal Address Range	CIDR Prefix
A	10.0.0.0 - 10.255.255.255	10.0.0.0/8
B	172.16.0.0 - 172.31.255.255	172.16.0.0/12
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16

These are the IP addresses you will see assigned to company devices.

- Private IP addresses cannot be routed over the Internet.
- NAT is used to translate private IP addresses to public addresses that can be routed over the Internet.
- One public IPv4 address can be used for thousands of devices that have private IP addresses.



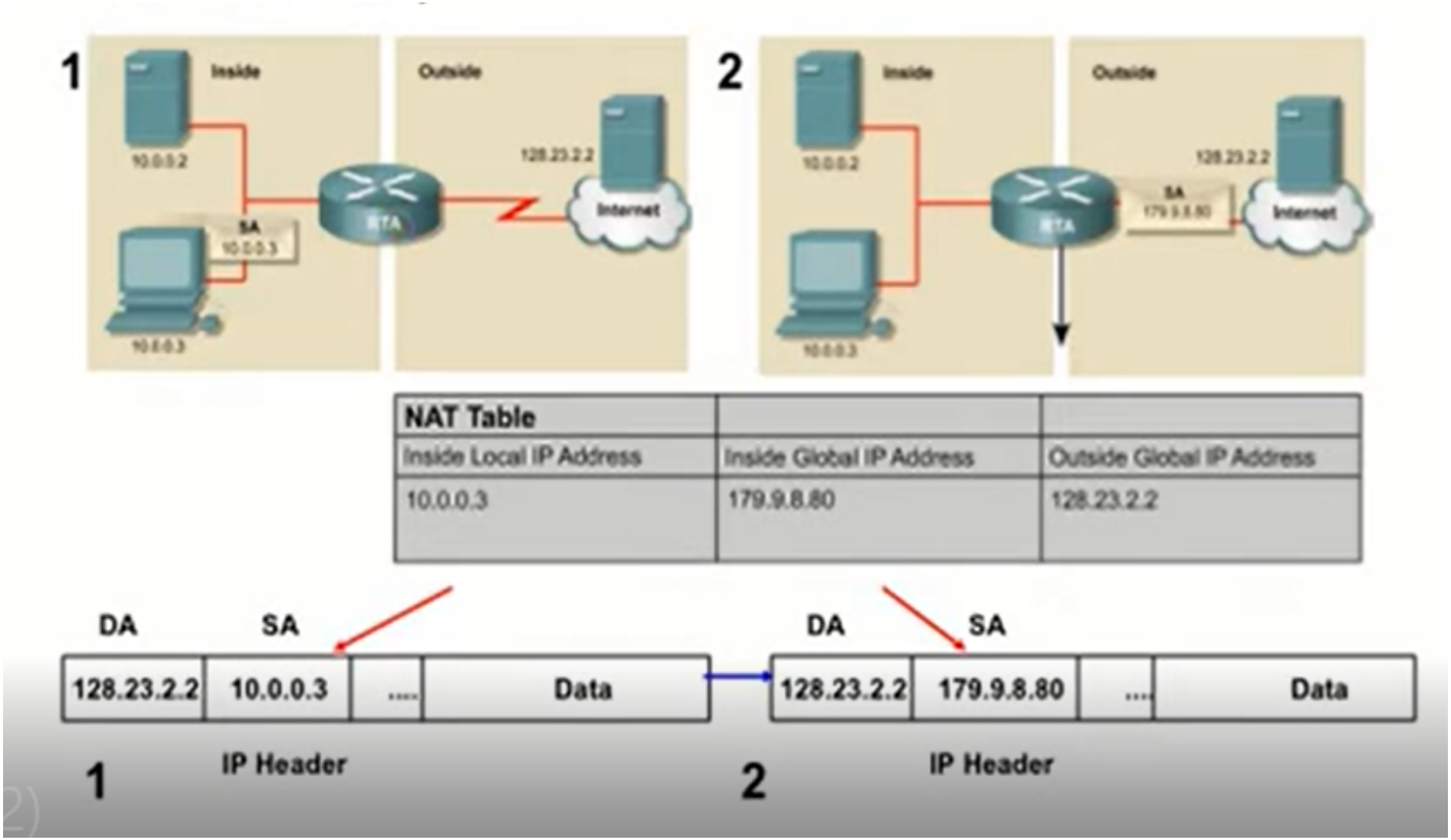
What is NAT?

- Private IP addresses cannot be routed over the Internet.
- NAT is used to translate private IP addresses used inside a company to public addresses that can be routed over the Internet.
- NAT hides internal IPv4 addresses from outside networks.
  - Companies use the same private IPv4 addresses so outside devices cannot tell one company's 10.x.x.x network from another company's 10.x.x.x network.
- A NAT-enabled router can be configured with a public IPv4 address.
- A NAT-enabled router can be configured with multiple public IPv4 addresses to be used in a pool or NAT pool for internal devices configured with private addresses

What is NAT?

- Use a Translation Table:
  (private source IP ↔ Global destination IP)
- NAT router may have:
  - One global IP address
  - Multiple global IP addresses

NAT

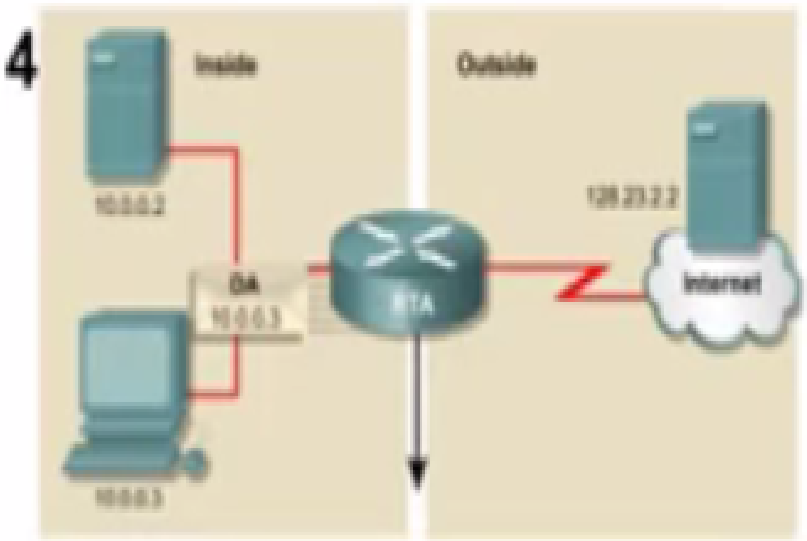


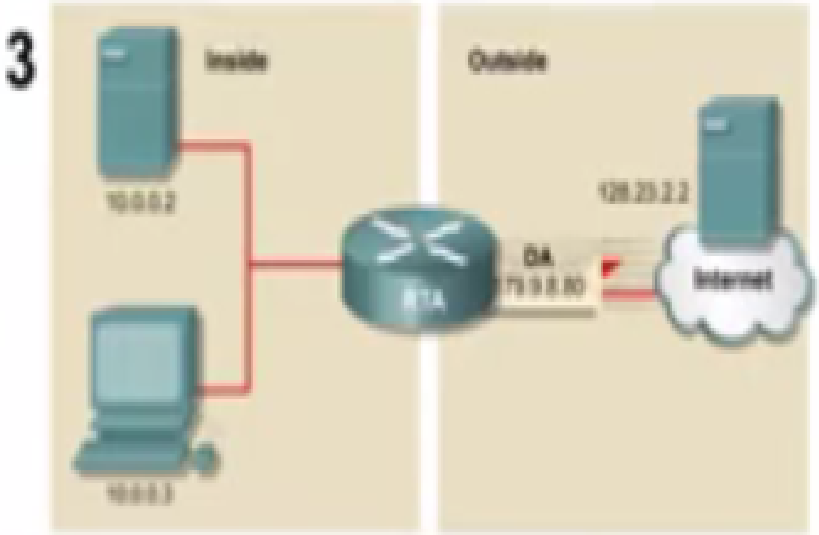
Case 1: NAT router uses one global IP address

restriction:

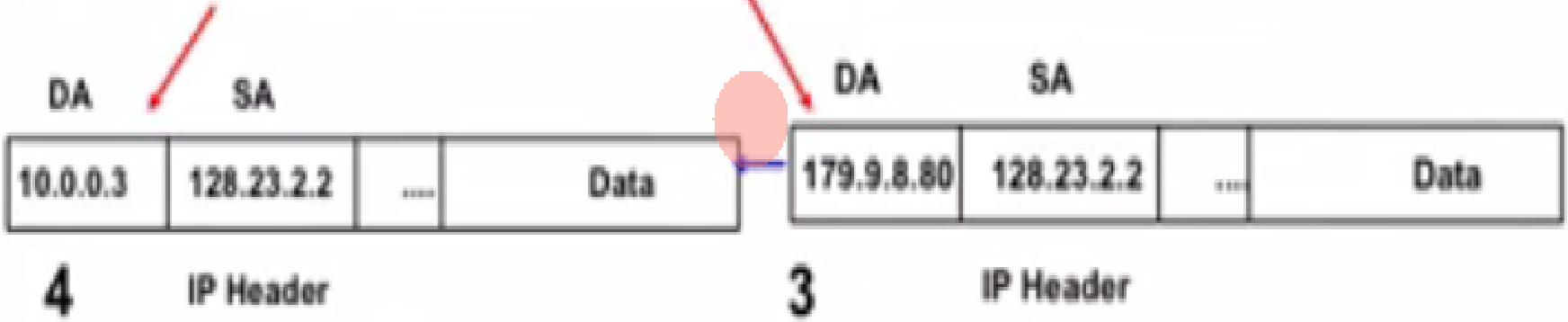
1)private network must start (initiate) the communication

2)Since the NAT router has only one global address, only one private network host can access the same external host





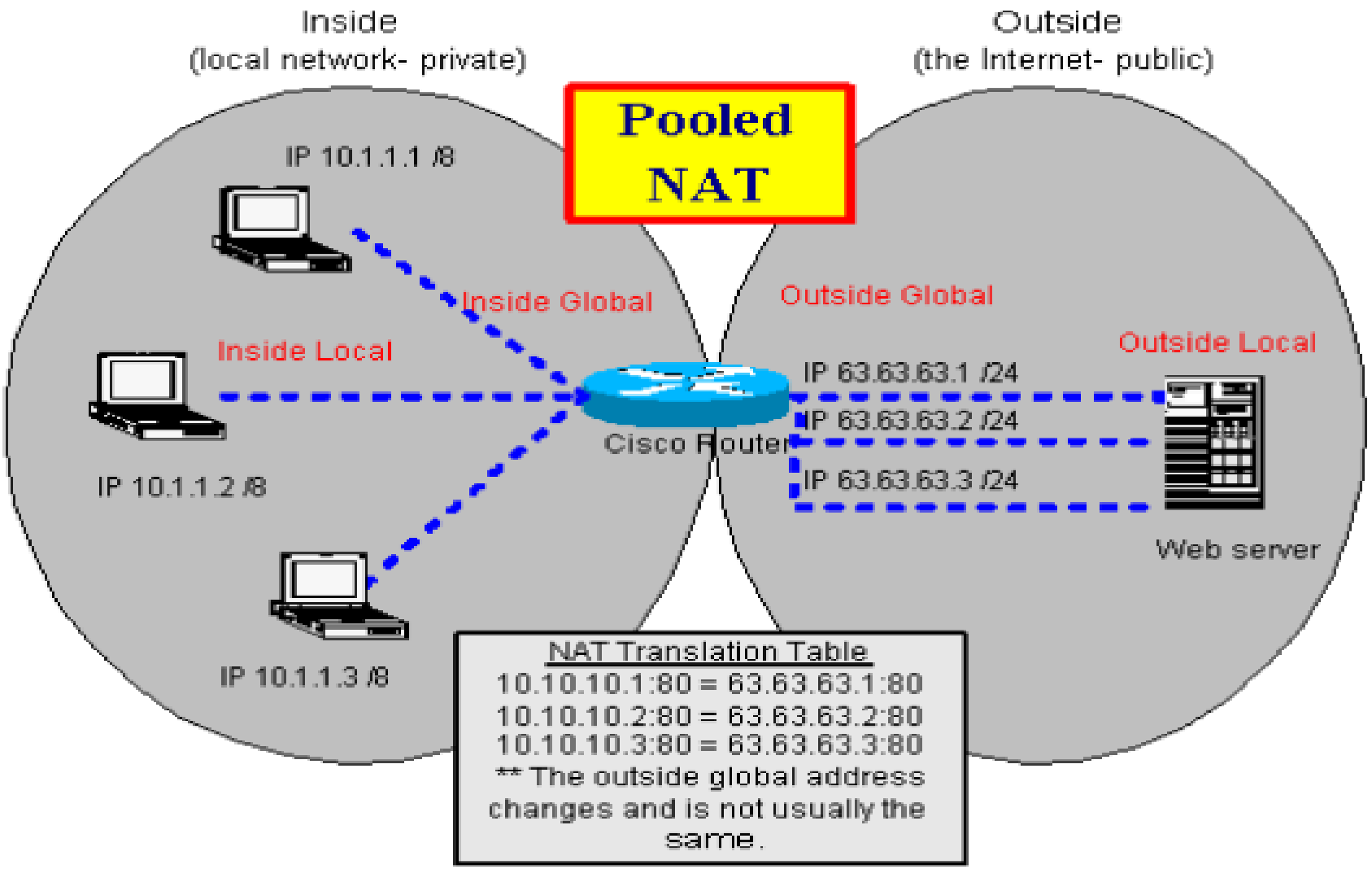
NAT Table		
Inside Local IP Address	Inside Global IP Address	Outside Global IP Address
10.0.0.2	179.9.8.80	128.23.2.2
10.0.0.3	179.9.8.80	128.23.2.2



2)Nat - pool of global addresses

- To remove the previous restriction, the NAT router uses a pool of global addresses
- For example instead of using one global address 200.24.5.8 , the NAT router can uses four addresses (200.24.5.8, 200.24.5.9, 200.24.5.10, 200.24.5.11).
- In this case Four private network hosts can communicate the same external host at the same time because each pair of addresses defines a connection.

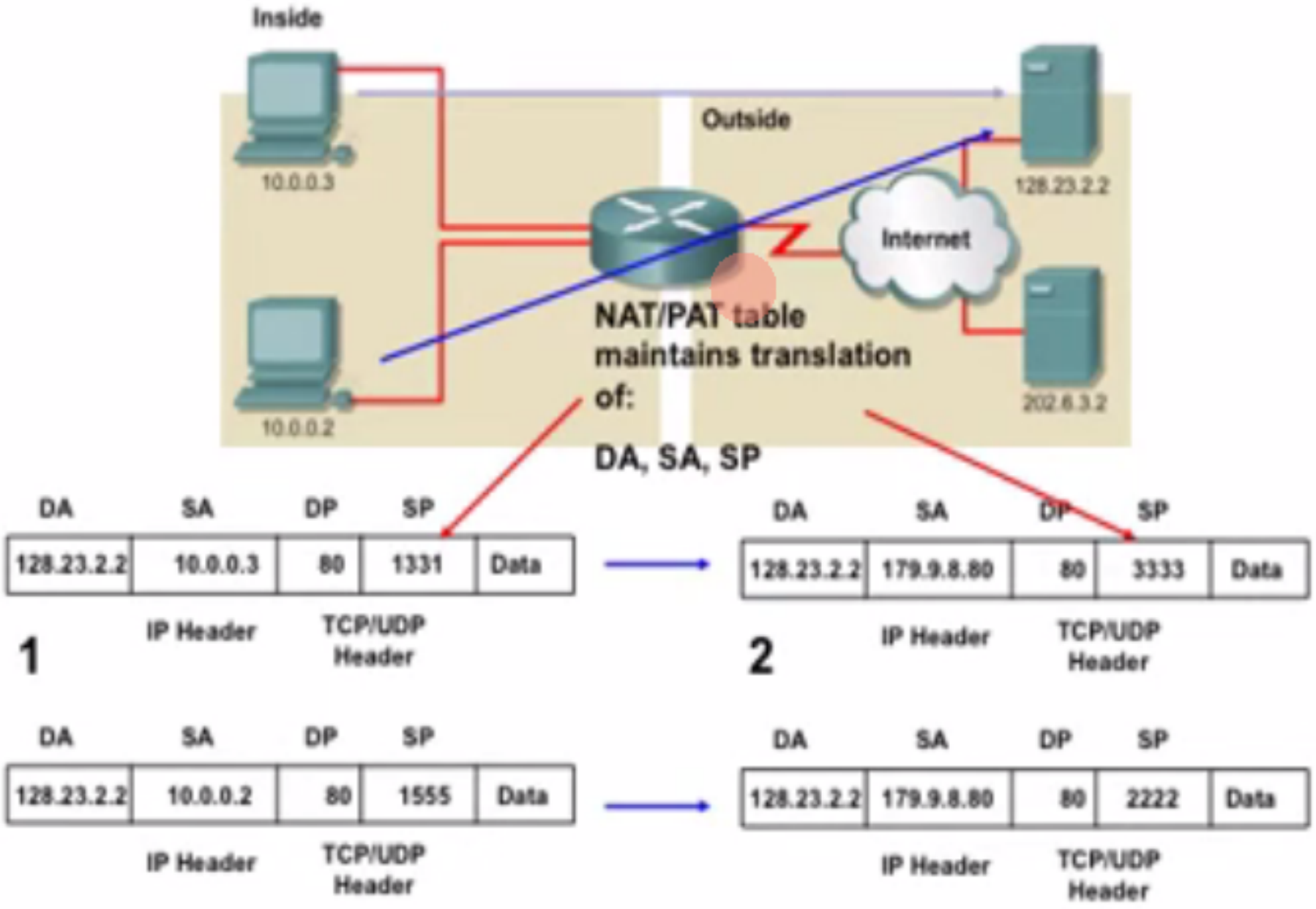
2)Nat - pool of global addresses



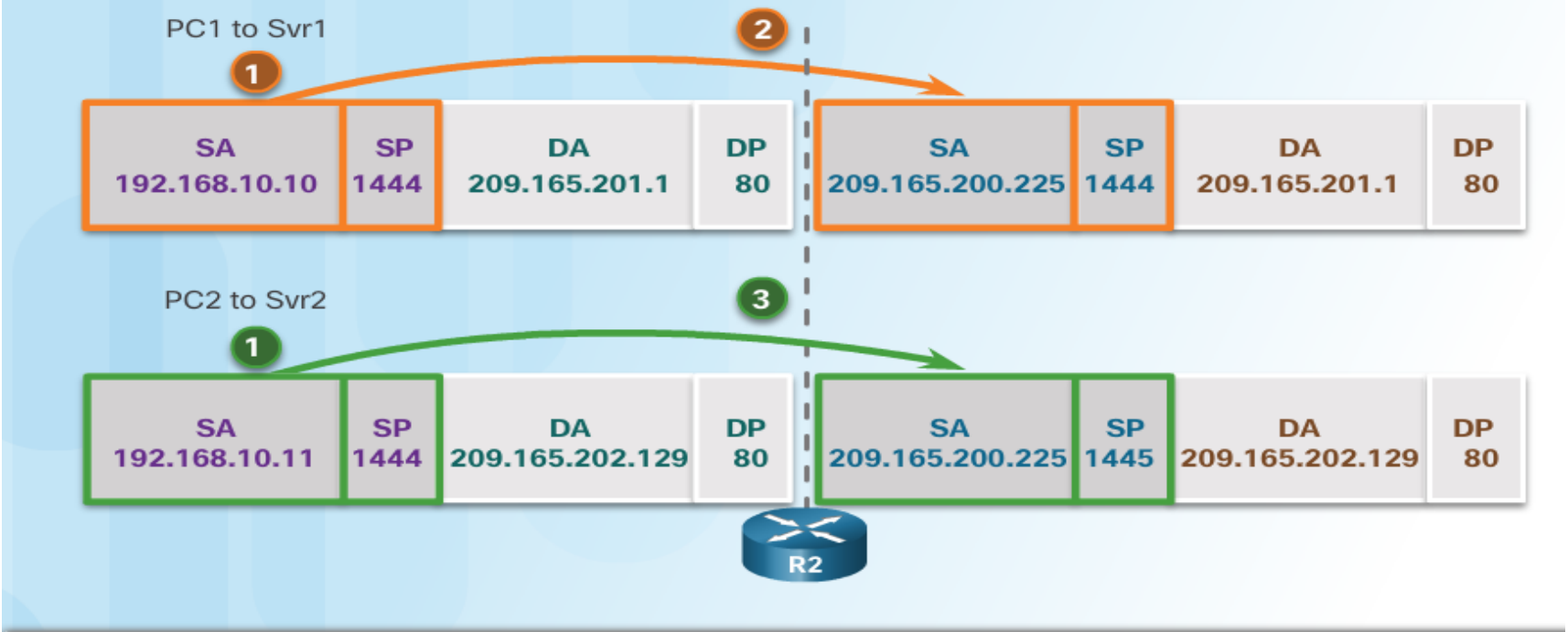
Case 2: NAT router uses multiple (say *K*) global IP address

- *K* local host to the same external destination at a time.
- Still:
  - No server programs inside the private network.
  - A private-network host may only access one server program in the same destination host.
  - No more than four connections can be made to the same destination
- Use of NAPT: Network Address Port Translation

PAT-Transport Layer Solution



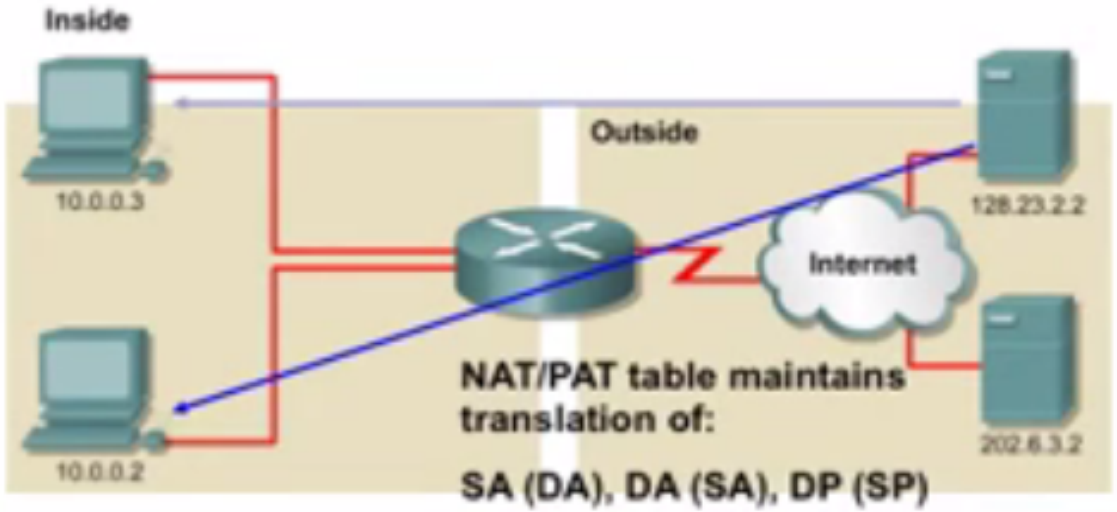
Port Address Translation



NAT Table

Inside Local Address	Inside Global Address	Outside Global Address	Outside Local Address
192.168.10.10:1444	209.165.200.225:1444	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1444	209.165.200.225:1445	209.165.202.129:80	209.165.202.129:80

PAT Example



DA	SA	DP	SP	
10.0.0.3	128.23.2.2	1331	80	Data

IP Header | TCP/UDP Header

4

DA	SA	DP	SP	
179.9.8.80	128.23.2.2	3333	80	Data

IP Header | TCP/UDP Header

3

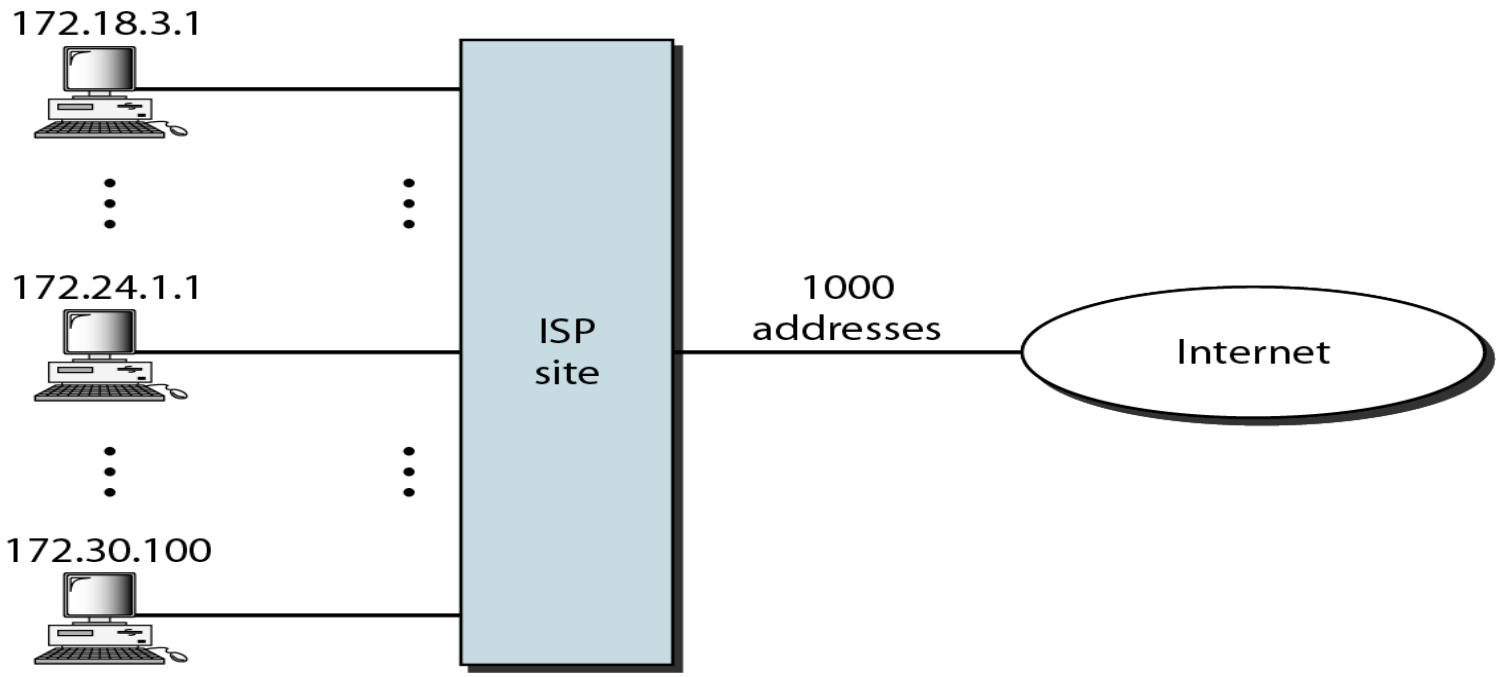
DA	SA	DP	SP	
10.0.0.2	128.23.2.2	1555	80	Data

IP Header | TCP/UDP Header

DA	SA	DP	SP	
179.9.8.80	128.23.2.2	2222	80	Data

IP Header | TCP/UDP Header

An ISP and NAT



Isp is granted 1000 global addresses but has 10,000 customers
Each of the customer assigned a private network address
ISP translates each of the 10,000 packets to one of the global addresses

IPv6 ADDRESSES

Despite all short-term solutions, address depletion is still a long-term problem for the Internet. This and other problems in the IP protocol itself have been the motivation for IPv6.

IPV4 -disadvantages

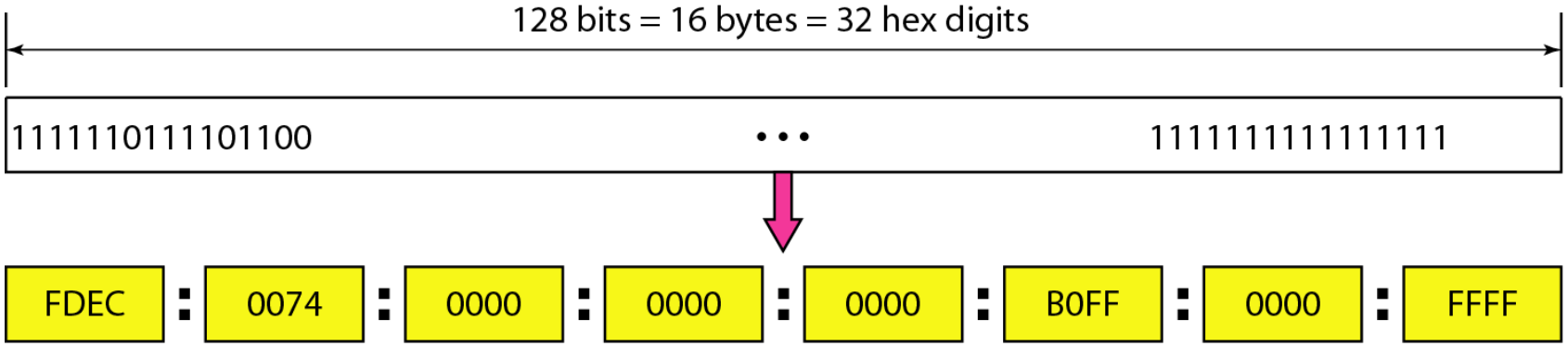
- IPv4 has 2 level of addresses structure (netid and hostid) categorized into the five classes A,B,C,D,E => inefficient use of address space / ip address scarce shortage and depletion although NAT.
- Inadequate QoS for nowadays application such as real-time audio and video transmission (due to delay & resource reservation) strategy
- No security mechanism (no encryption and authentication is provided by IPv4).

IPV6-advantages

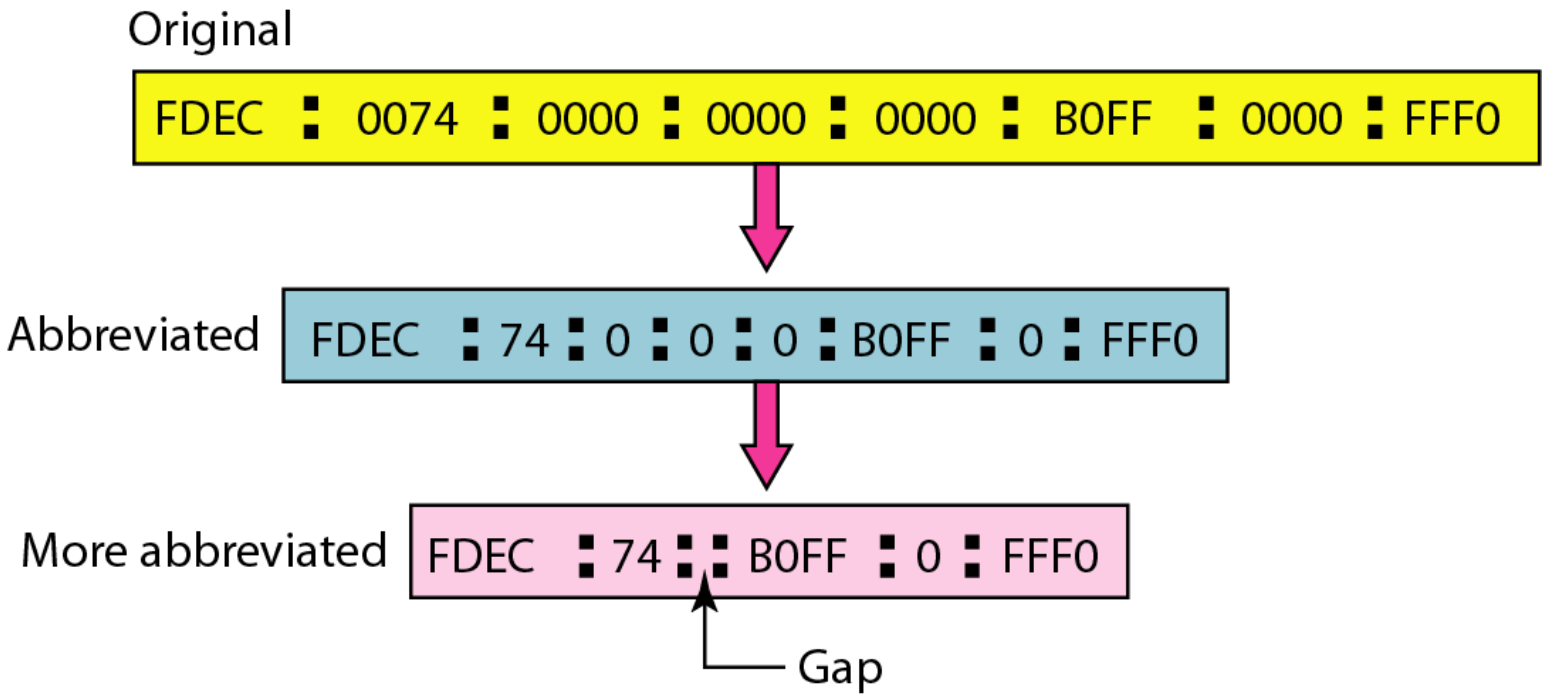
- Larger address space. IPv4 only 2^{32}. IPv6 2^{96} (7.92×10^{28}). Can stand more than 150 years
- Better header format
- New options: allow for additional functionalities for future use
- Allowance for extension: allow the extension of the protocol if required by new technologies or applications.
- Support for resource allocation.- to support traffic such as real-time audio and video very very efficiently compared to IPv4.
- Support for more security. The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet.

IPv6 address in binary and hexadecimal colon notation

An IPv6 address is 128 bits long



Abbreviated IPv6 addresses



Expand the address 0:15::1:12:1213 to its original.

Solution

We first need to align the left side of the double colon to the left of the original pattern and the right side of the double colon to the right of the original pattern to find how many 0s we need to replace the double colon.

```
xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
  0:   15:                  :    1:   12:1213
```

This means that the original address is.

```
0000:0015:0000:0000:0000:0001:0012:1213
```

Type prefixes for IPv6 addresses

Type Prefix	*Type*	*Fraction*
0000 0000	Reserved	1/256
0000 0001	Unassigned	1/256
0000 001	ISO network addresses	1/128
0000 010	IPX (Novell) network addresses	1/128
0000 011	Unassigned	1/128
0000 1	Unassigned	1/32
0001	Reserved	1/16
001	Reserved	1/8
010	**Provider-based unicast addresses**	**1/8**

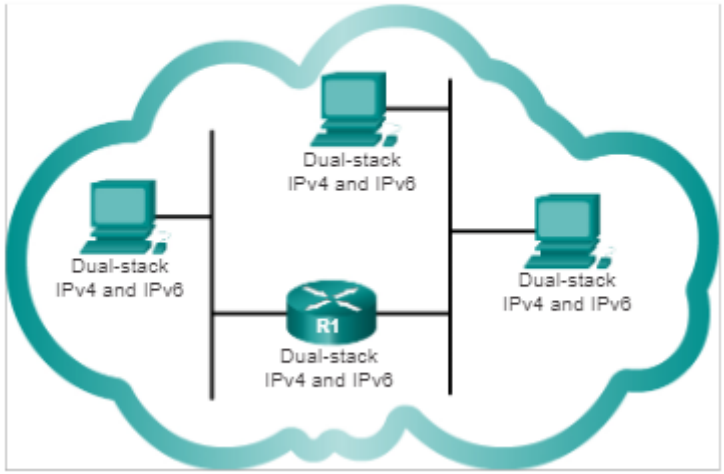
Type prefixes for IPv6 addresses (continued)

Type Prefix	*Type*	*Fraction*
011	Unassigned	1/8
100	Geographic-based unicast addresses	1/8
101	Unassigned	1/8
110	Unassigned	1/8
1110	Unassigned	1/16
1111 0	Unassigned	1/32
1111 10	Unassigned	1/64
1111 110	Unassigned	1/128
1111 1110 0	Unassigned	1/512
1111 1110 10	Link local addresses	1/1024
1111 1110 11	Site local addresses	1/1024
1111 1111	Multicast addresses	1/256

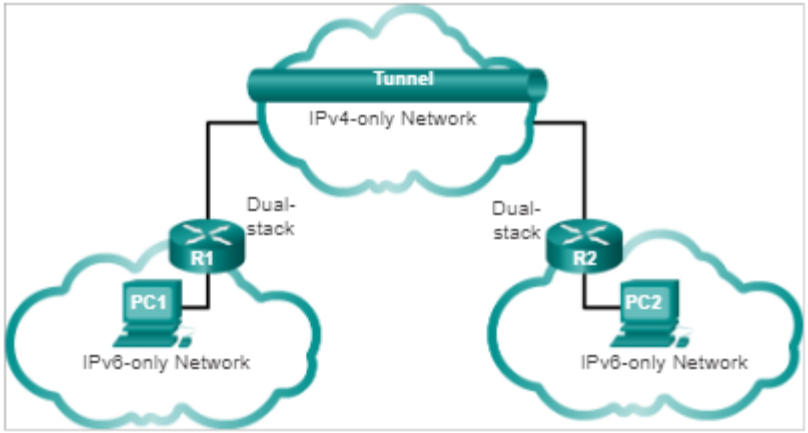
Migration to IPV6

- For the foreseeable future, both IPv4 and IPv6 will coexist. The transition is expected to take years. The IETF has created various protocols and tools to help network administrators migrate their networks to IPv6. The migration techniques can be divided into three categories:
- **Dual Stack** – As shown in Figure 1, dual stack allows IPv4 and IPv6 to coexist on the same network. Dual stack devices run both IPv4 and IPv6 protocol stacks simultaneously.
- **Tunneling** – As shown in Figure 2, tunneling is a method of transporting an IPv6 packet over an IPv4 network. The IPv6 packet is encapsulated inside an IPv4 packet, similar to other types of data.
- **Translation** – As shown in Figure 3, Network Address Translation 64 (NAT64) allows IPv6-enabled devices to communicate with IPv4-enabled devices using a translation technique similar to NAT for IPv4. An IPv6 packet is translated to an IPv4 packet, and vice versa.

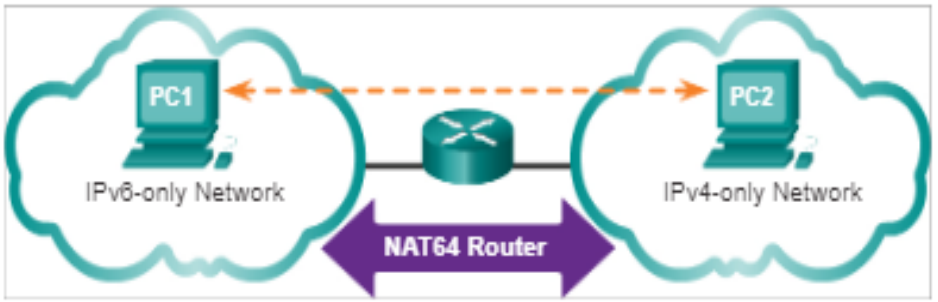
Dual-Stack



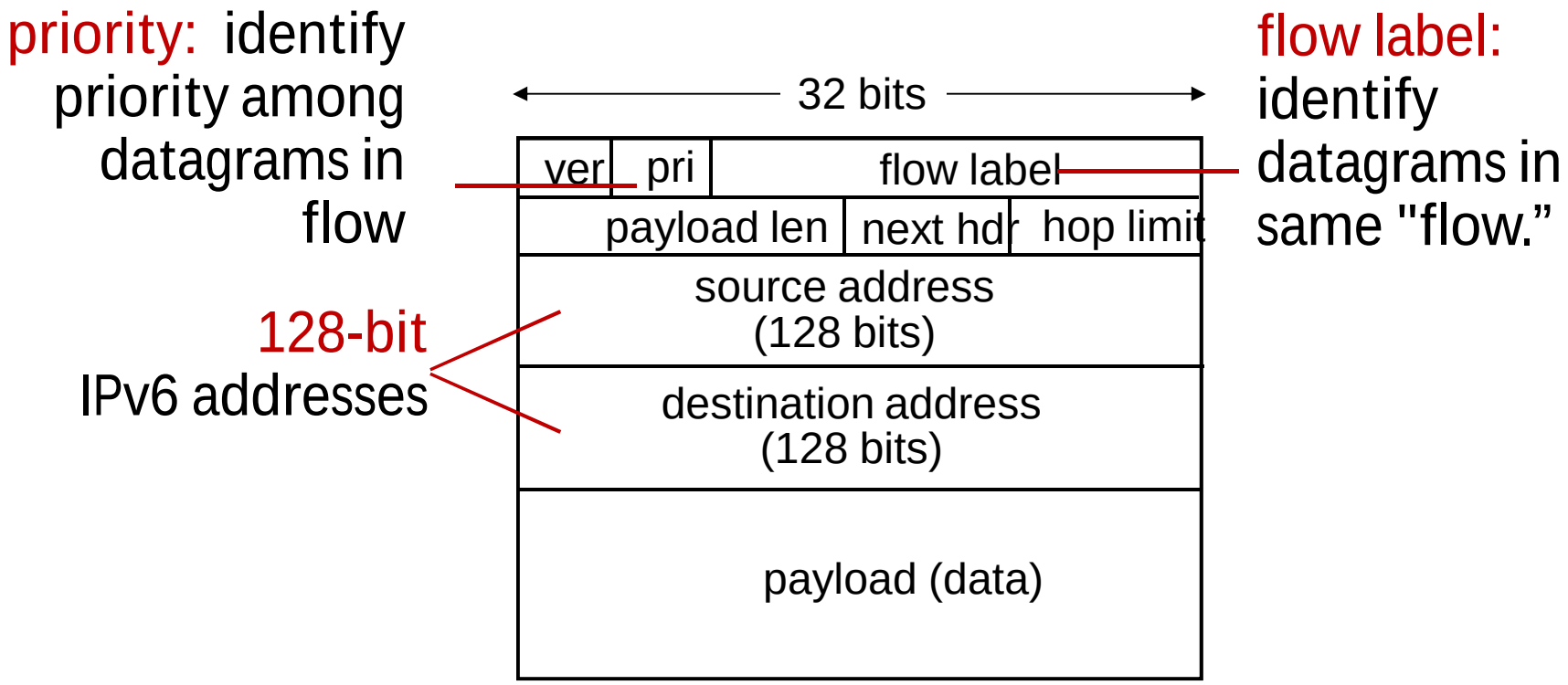
Tunnelling



Translation



IPv6 datagram format

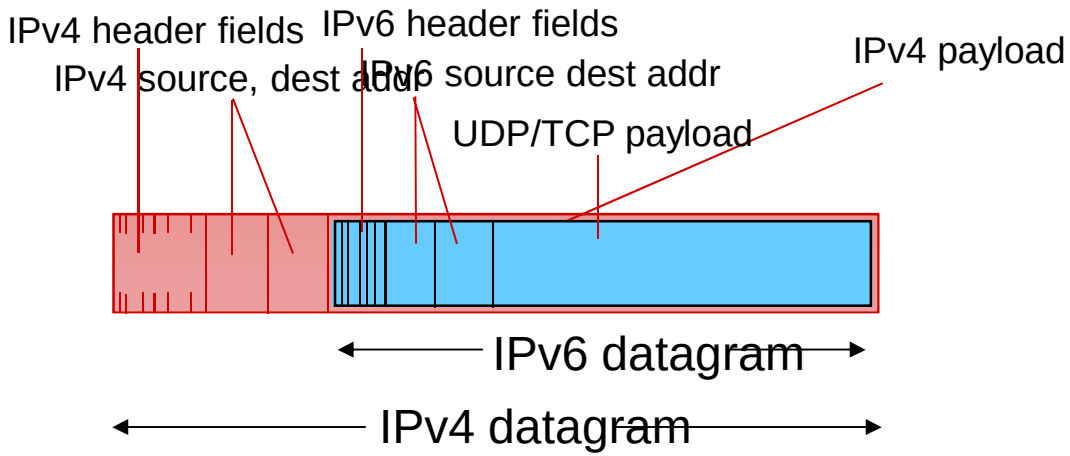


What's missing (compared with IPv4):

- no checksum (to speed processing at routers)
- no fragmentation/reassembly
- no options (available as upper-layer, next-header protocol at router)

Transition from IPv4 to IPv6

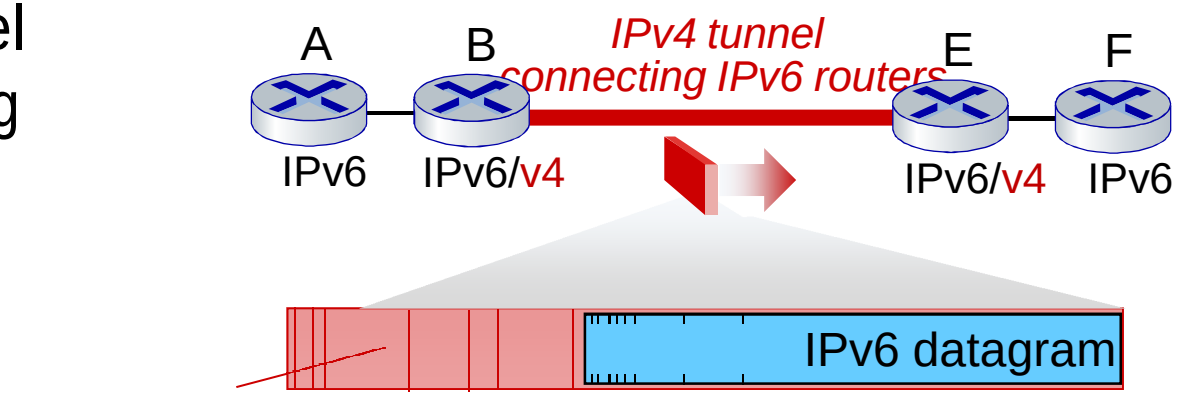
- not all routers can be upgraded simultaneously
  - no “flag days”
  - how will network operate with mixed IPv4 and IPv6 routers?
- tunneling: IPv6 datagram carried as *payload* in IPv4 datagram among IPv4 routers (“packet within a packet”)
  - tunneling used extensively in other contexts (4G/5G)



Tunneling and encapsulation

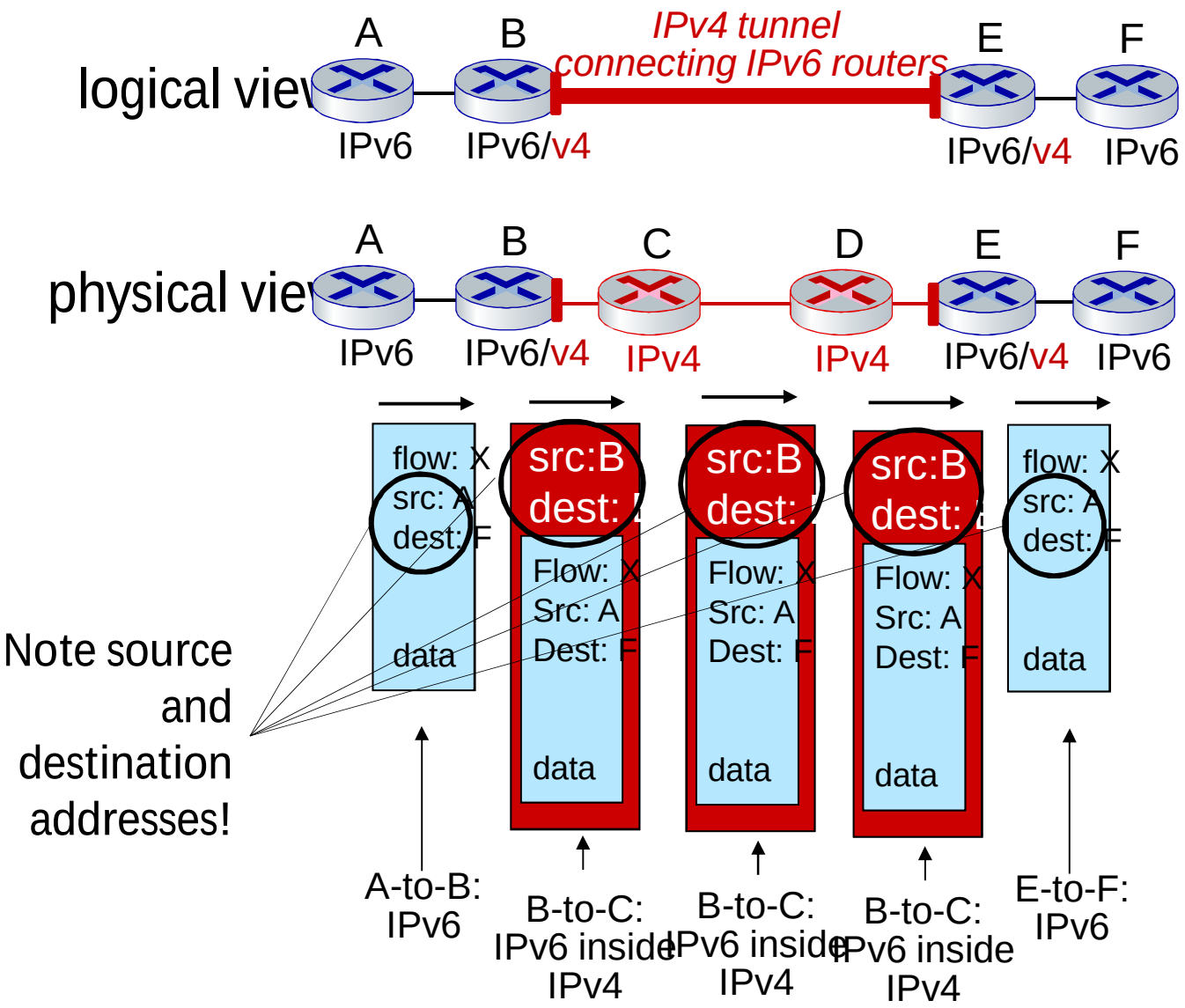
[redacted]

IPv4 tunnel connecting two IPv6 routers



tunneling: IPv6 datagram as payload in a IPv4 datagram

Tunneling

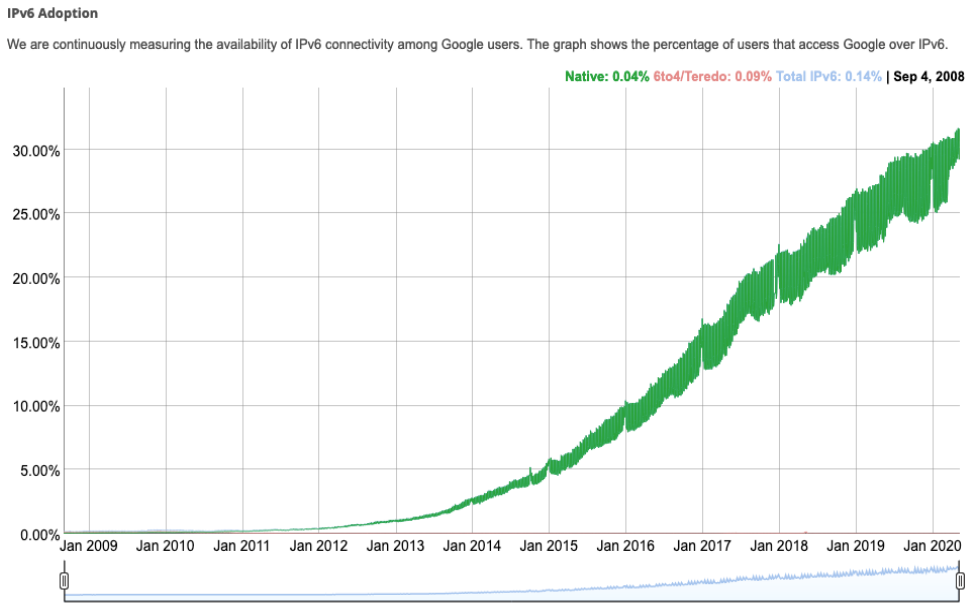

logical view:
A
B
IPv4 tunnel
connecting IPv6 routers
E
F
IPv6
IPv6/v4
IPv6/v4
IPv6
physical view:
A
B
C
D
E
F
IPv6
IPv6/v4
IPv4
IPv4
IPv6/v4
IPv6
Note source
and
destination
addresses!
flow: X
src: A
dest: F
data
src:B
dest:
Flow: X
Src: A
Dest: F
data
src:B
dest:
Flow: X
Src: A
Dest: F
data
src:B
dest:
Flow: X
Src: A
Dest: F
data
flow: X
src: A
dest: F
data
A-to-B:
IPv6
B-to-C:
IPv6 inside
IPv4
B-to-C:
IPv6 inside
IPv4
B-to-C:
IPv6 inside
IPv4
E-to-F:
IPv6

IPv6: adoption

- Google[1]: ~ 30% of clients access services via IPv6
- NIST: 1/3 of all US government domains are IPv6 capable
- Long (long!) time for deployment, use
  - 25 years and counting!
  - think of application-level changes in last 25 years: WWW, social media, streaming media, gaming, telepresence, ...
  - *Why?*

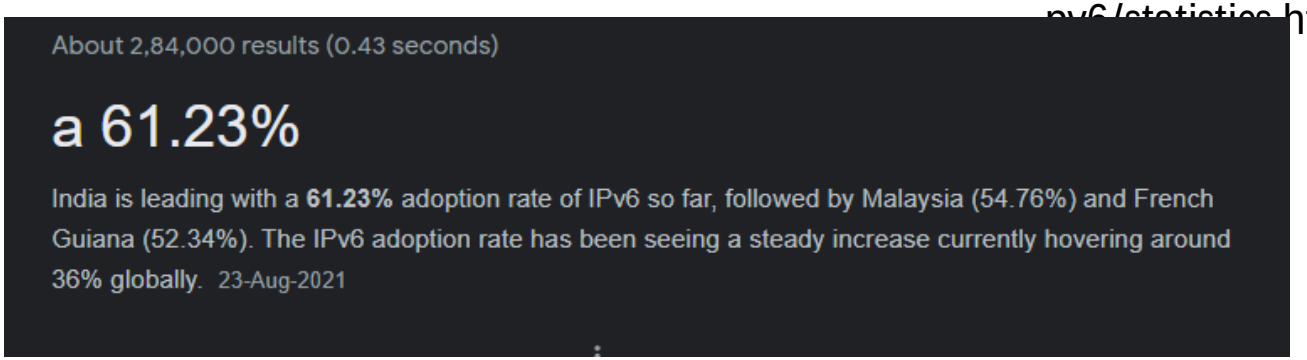
[1] https://www.google.com/intl/en/ipv6/statistics.html

IPV6 adoption



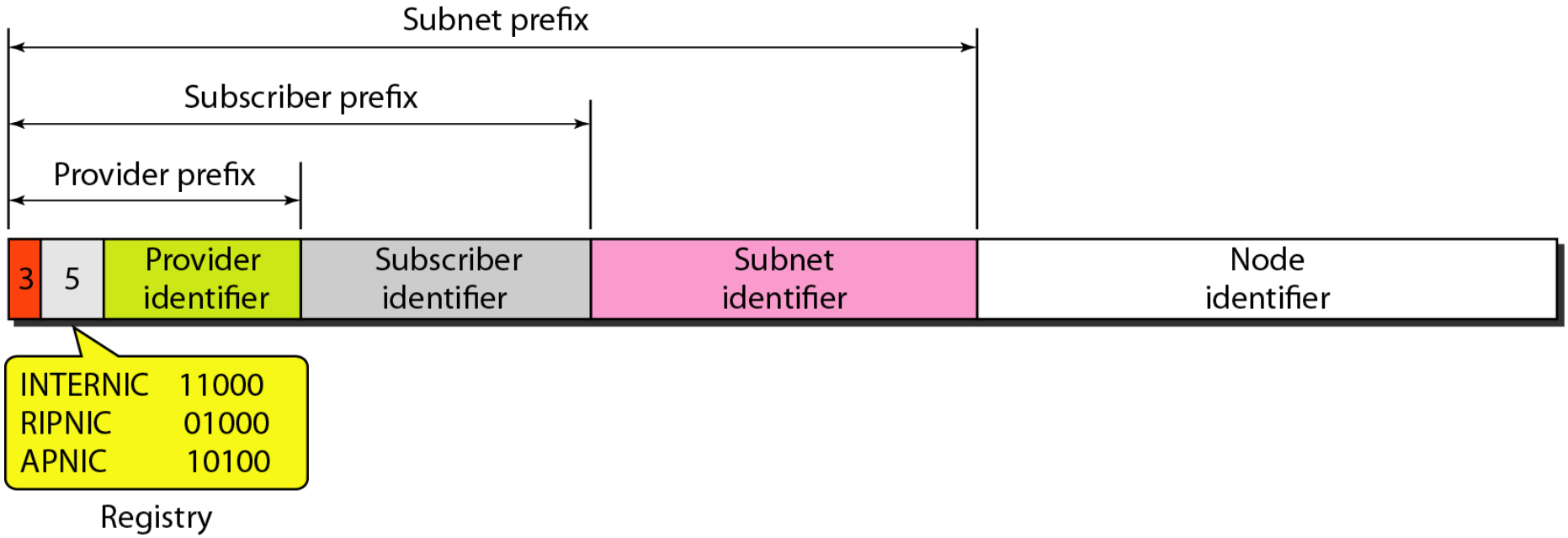
1

https://www.google.com/intl/en/ipv6/statistics.ht



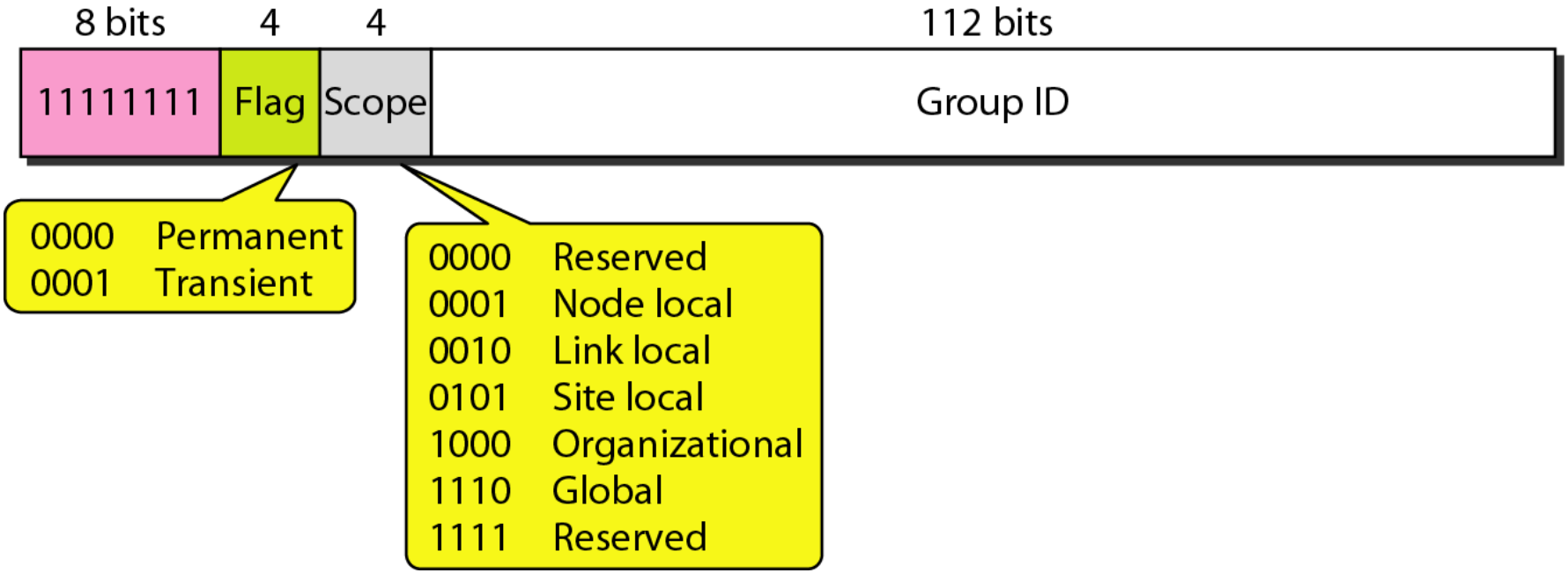
Prefixes for provider-based unicast address

Unicast: This type is the address of a single interface. A packet forwarded to a unicast address is delivered only to the interface identified by that address.



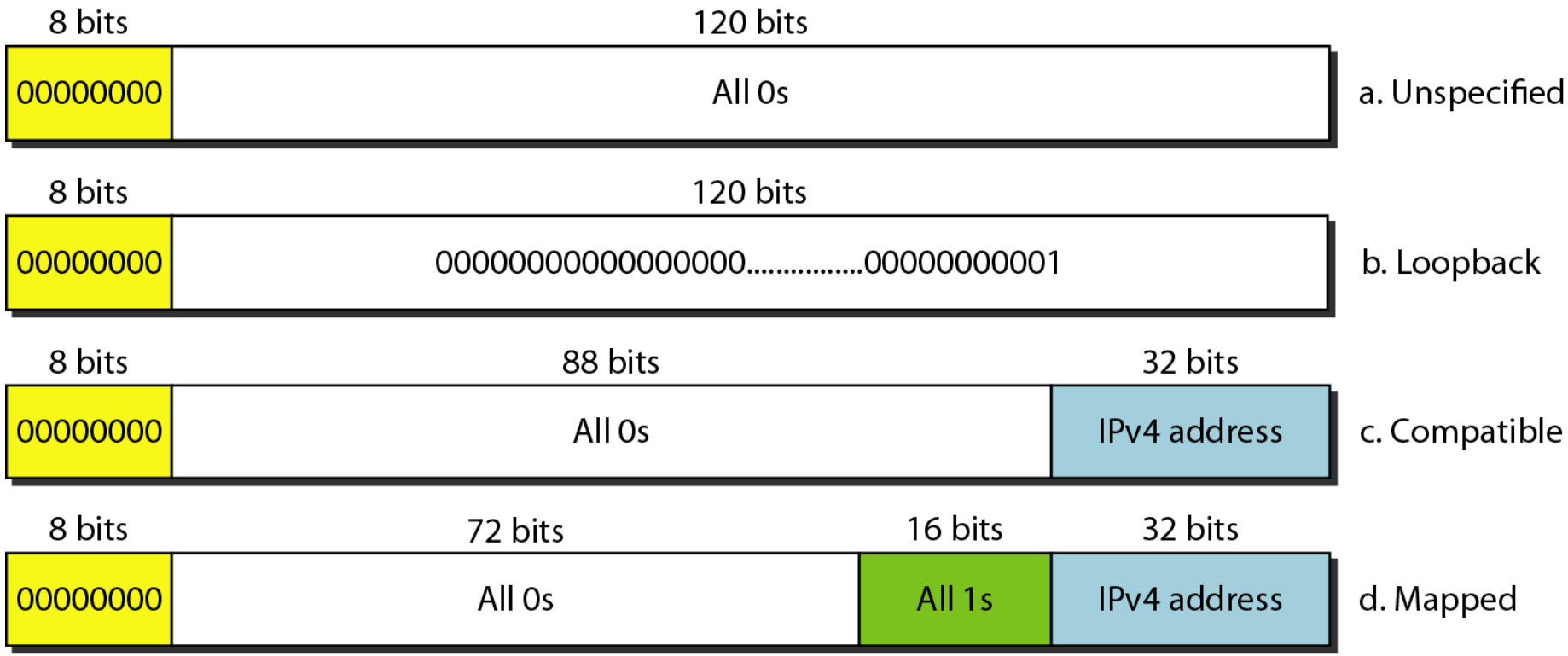
Multicast address in IPv6

Multicast: This type is the address of a set of interfaces that typically belong to different nodes. A packet forwarded to a multicast address is delivered to all interfaces belonging to the set.



Anycast: This type is the address of a set of interfaces typically belonging to different nodes. A packet forwarded to an anycast address is delivered to only one interface of the set (the nearest to the source node, according to the routing metric).

Reserved addresses in IPv6



- **1)The Unspecified Address**
  - It must never be assigned to any interface because it indicates the absence of an IPv6 address.

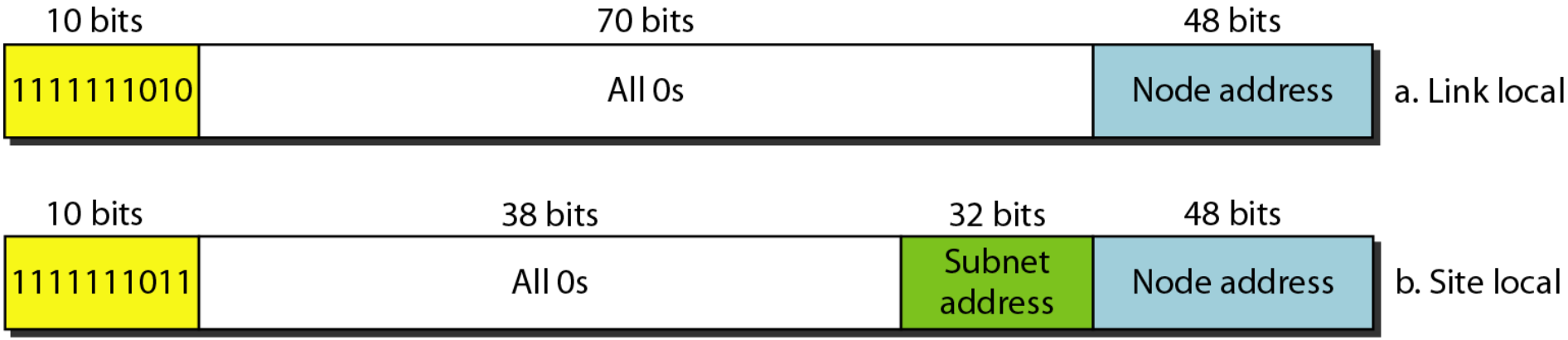
  2)The Loopback Address
    - used by a node to send an IPv6 packet to itself

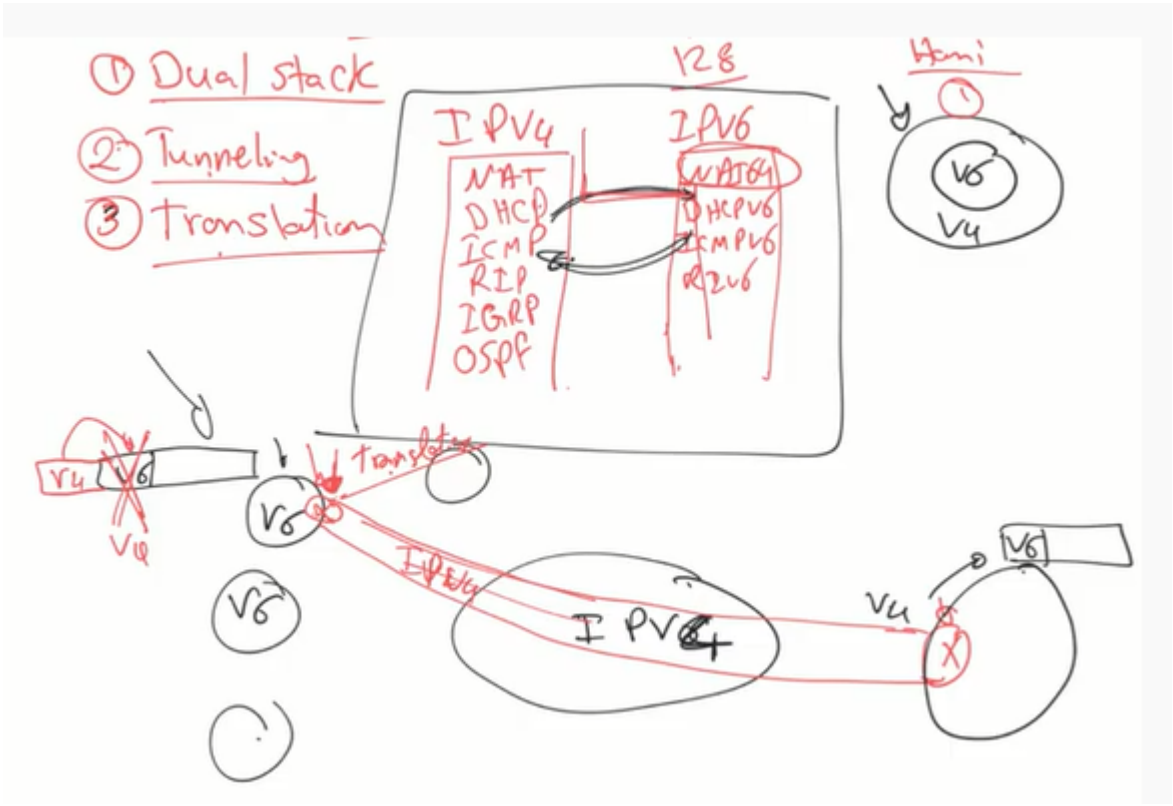
  3)Compatible Address
    - Source IPV6 destination IPV6 but in between IPV4

    - 4)**MAPPED**

      Source IPV6 destination IPV4

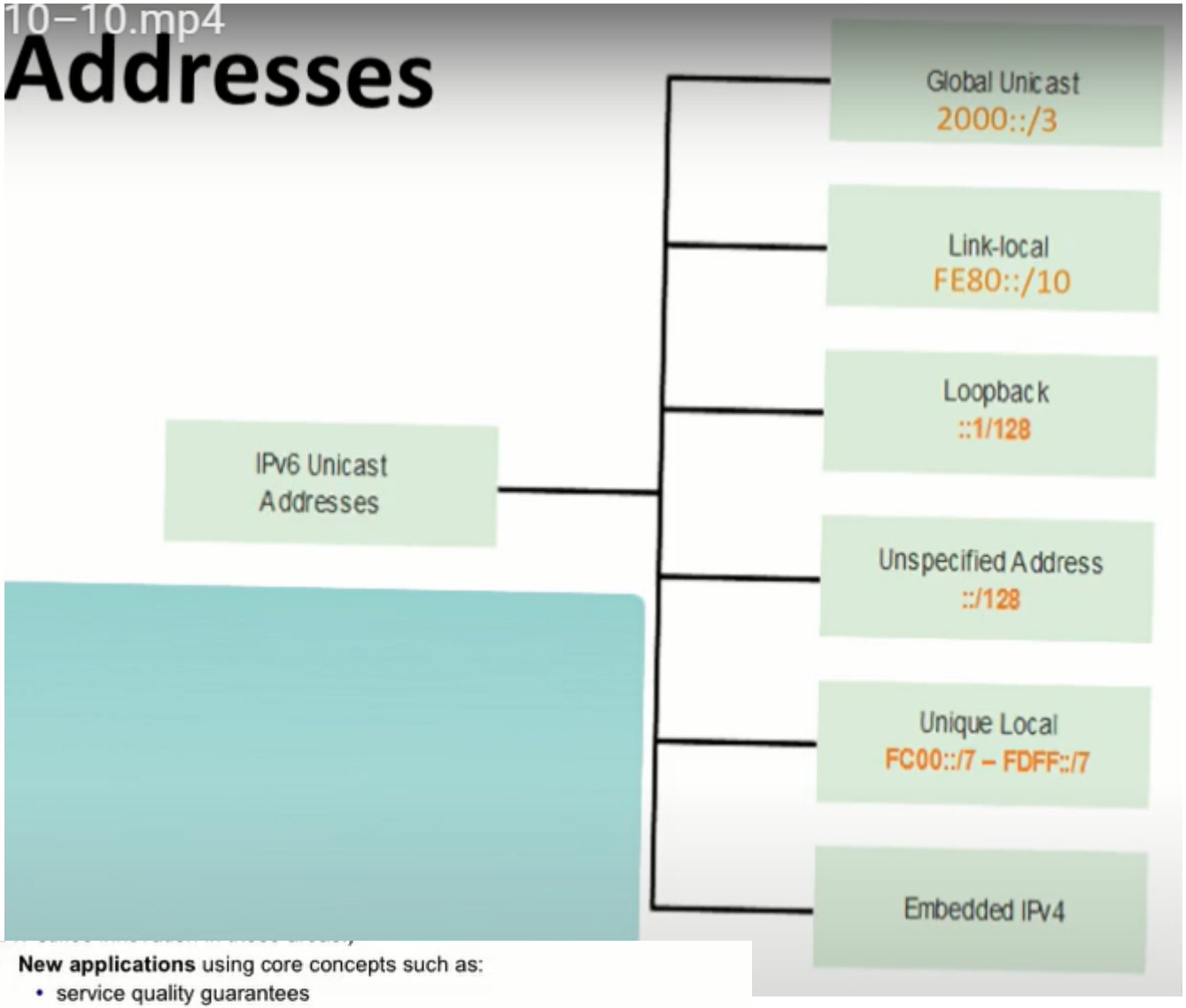
Local addresses in IPv6




① Dual stack
② Tunneling
③ Translation
R2
IPV4
NAT
DHCP
ICMP
RIP
IGRP
OSPF
IPV6
NAT64
DHCPV6
ICMPV6
RIP6
Host
V6
V4
V4
V6
V6
V6
V6
V4
X

10–10.mp4

Addresses



- **New applications** using core concepts such as:
  - service quality guarantees
  - end-to-end security
  - peer-to-peer networking (work as client and server, no private addresses)