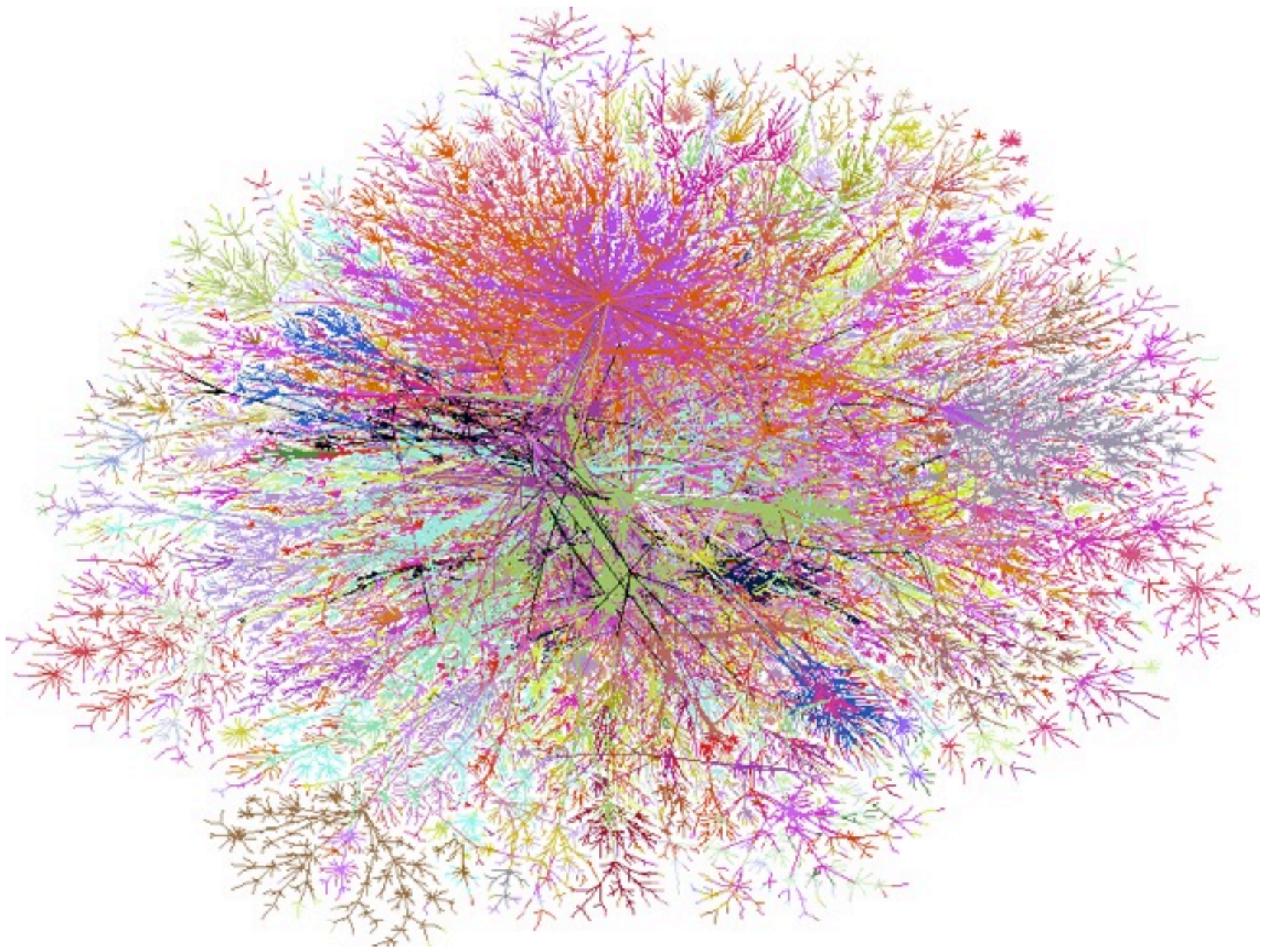
The Internet

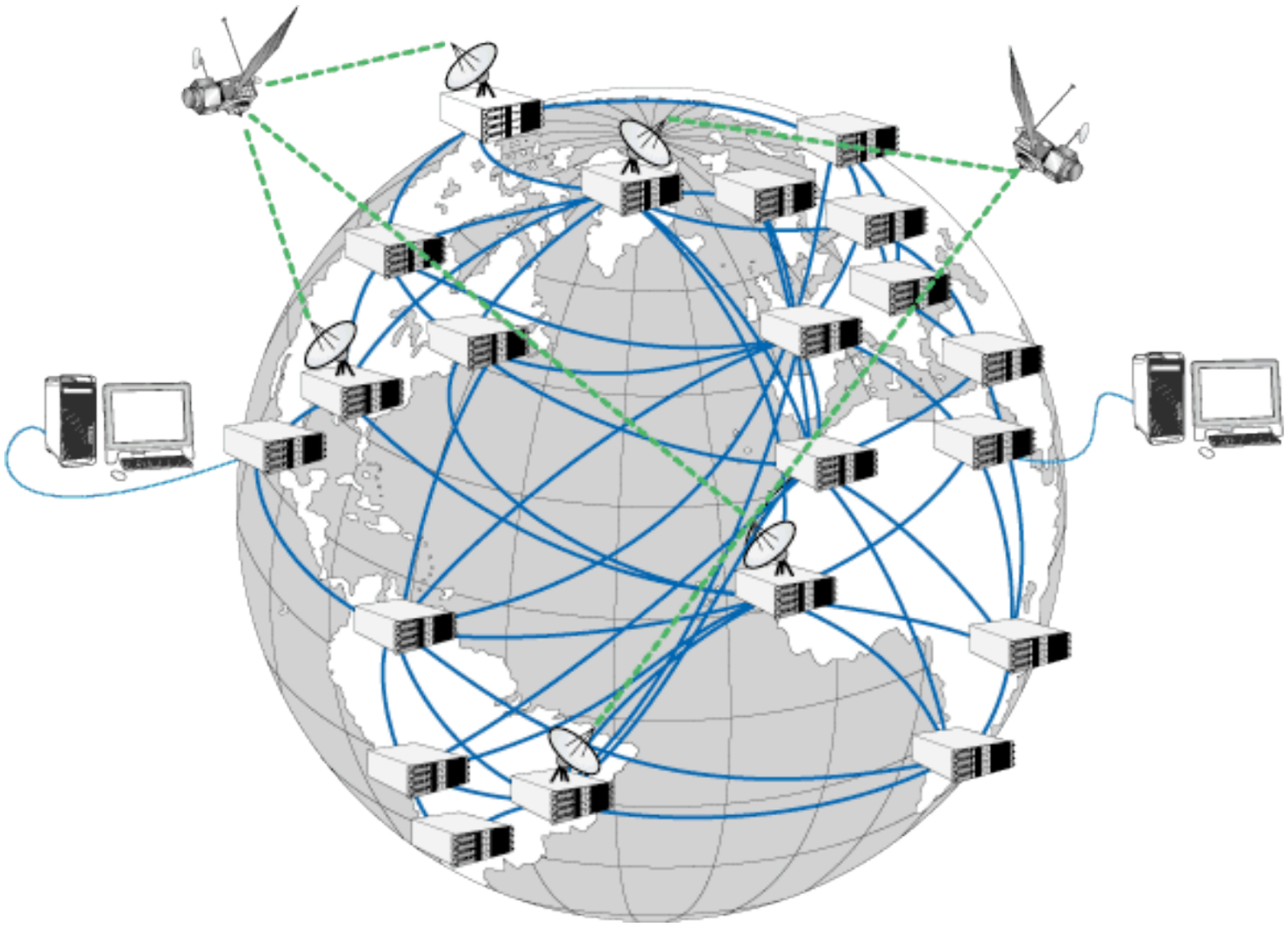
2011-10-10



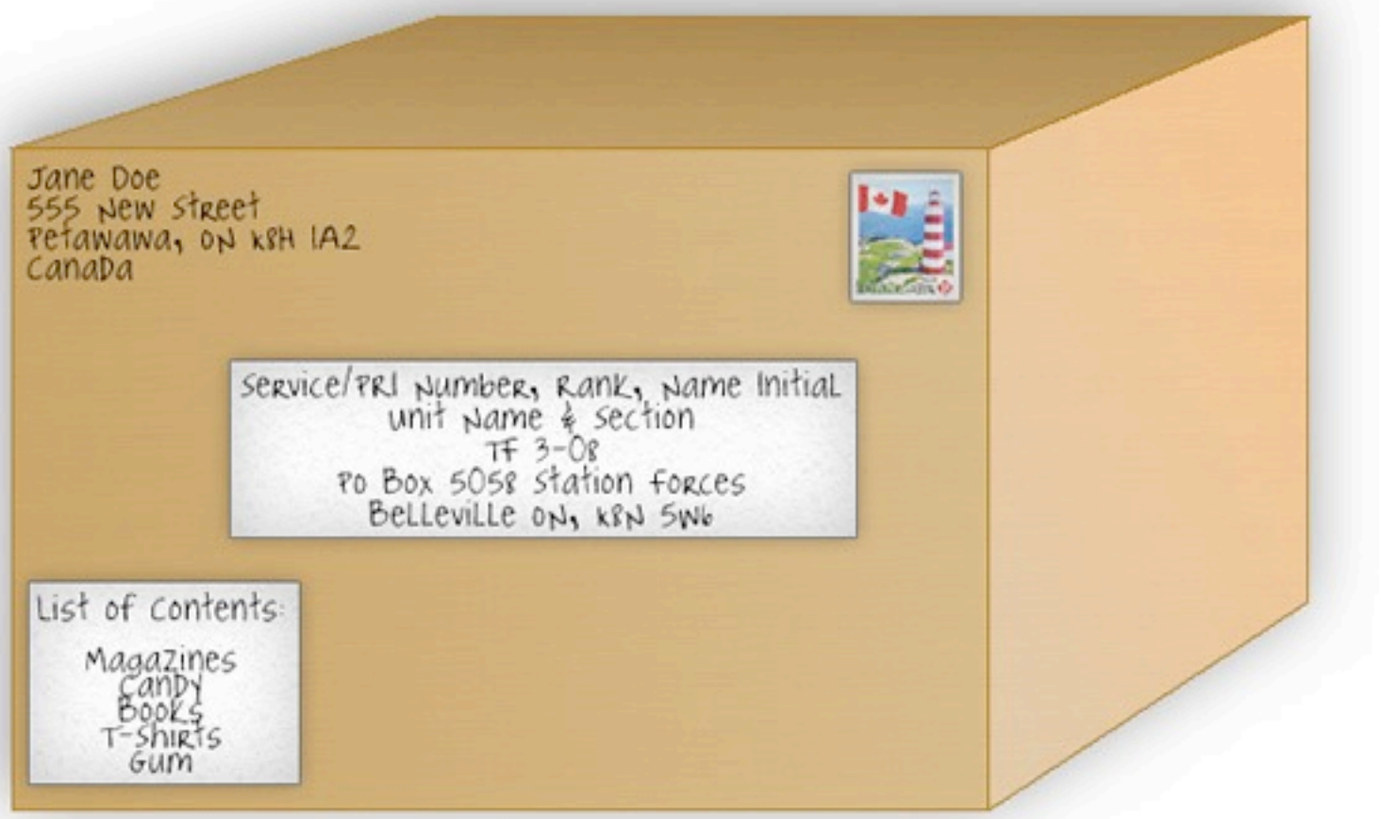
The internet has grown through cooperation and interconnection between countless local networks.

In principle the internet accepts information from any source and makes best efforts to deliver it to its destination.

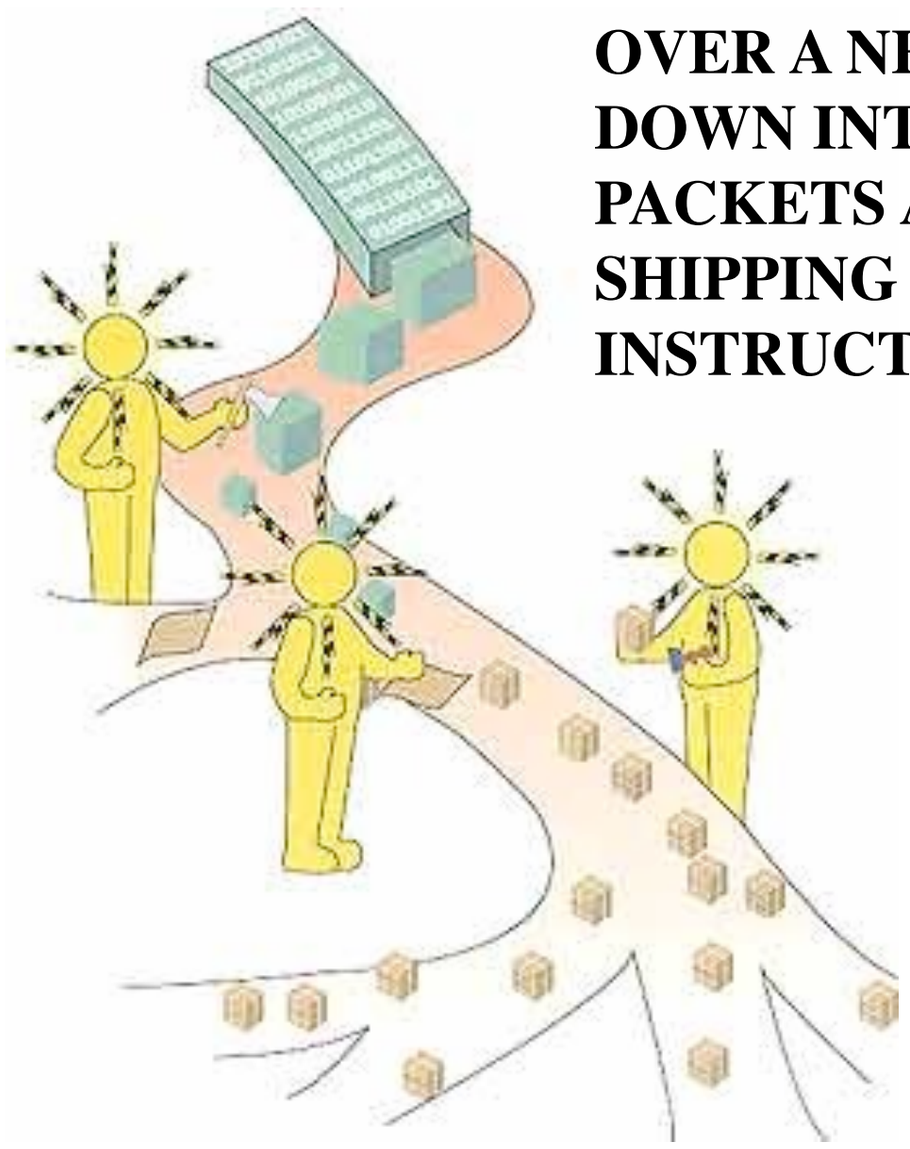
Connecting the world



packet network



packet switching



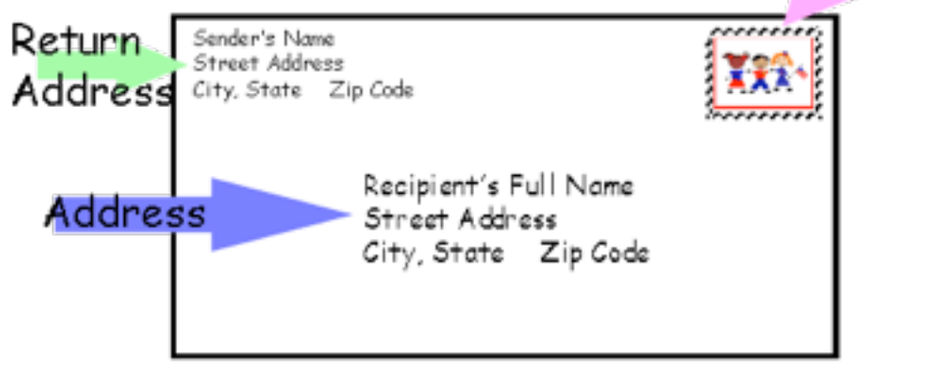
LIKE PACKAGES SENT THROUGH THE MAIL, COMMUNICATIONS SENT OVER A NETWORK ARE BROKEN DOWN INTO SMALL INFORMATION PACKETS AND WRAPPED WITH SHIPPING AND ASSEMBLY INSTRUCTIONS, CALLED PROTOCOLS

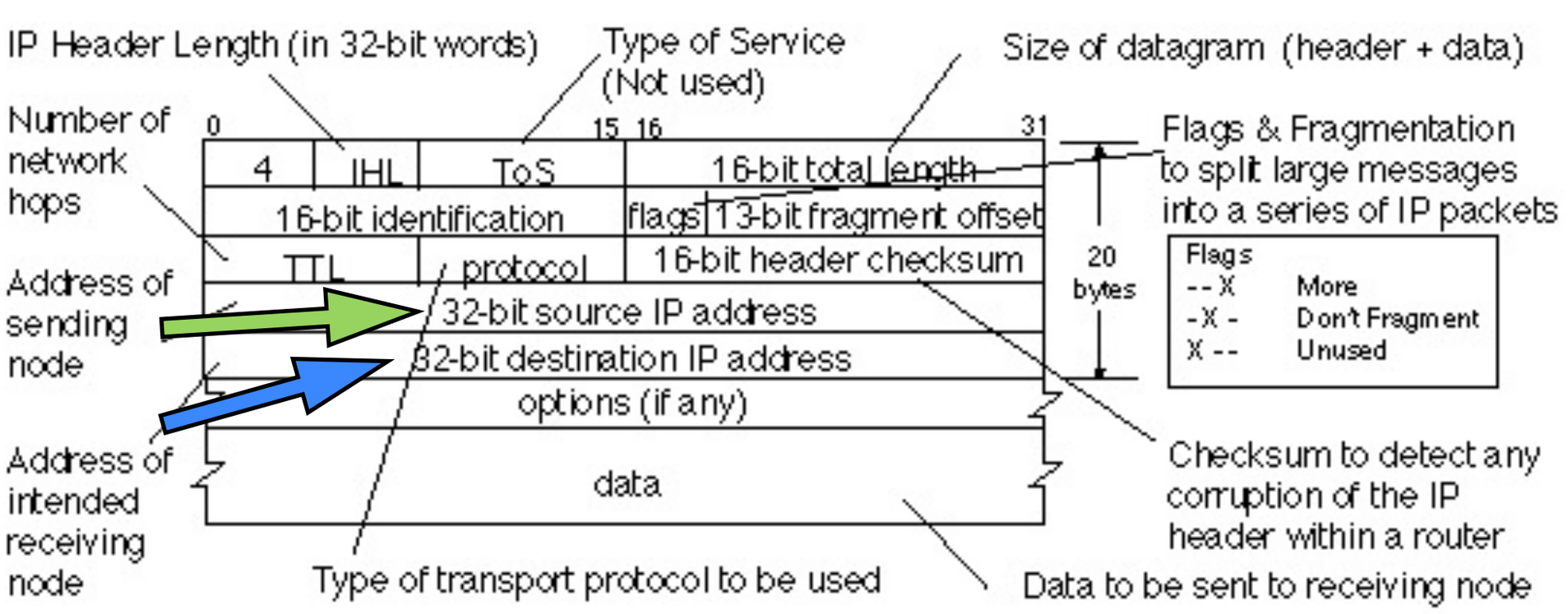
Unlike packages sent through the mail, if an information packet is damaged or lost it can be resent ...

Think about sending a book one page in each packet

Network Layer

- IP protocol operates at the network layer
  - best-effort service





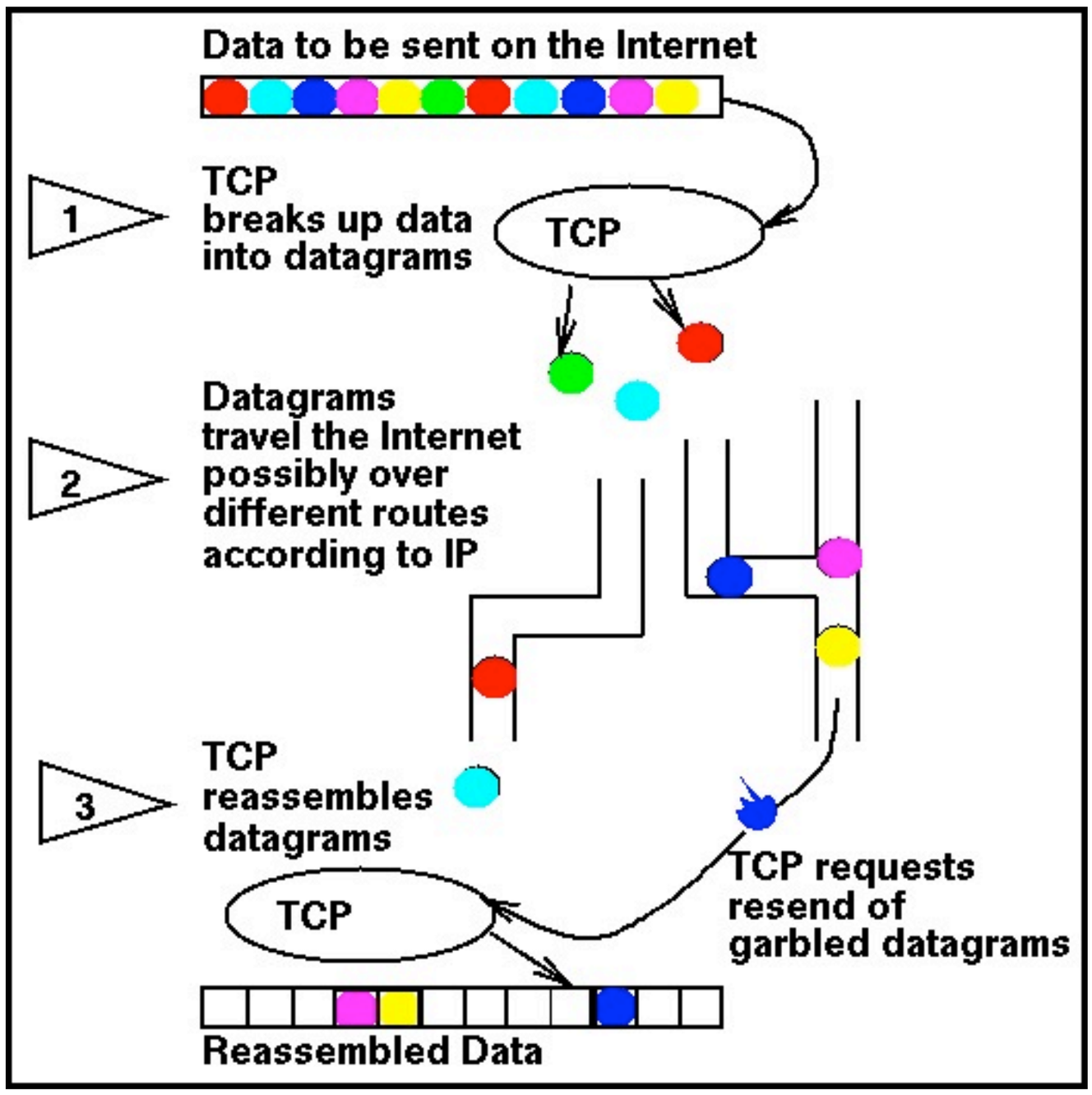
Diagrams thanks to Prof. Godred Fairhurst http://www.erg.abdn.ac.uk/~gorry/

Saturday, 3 December 2011

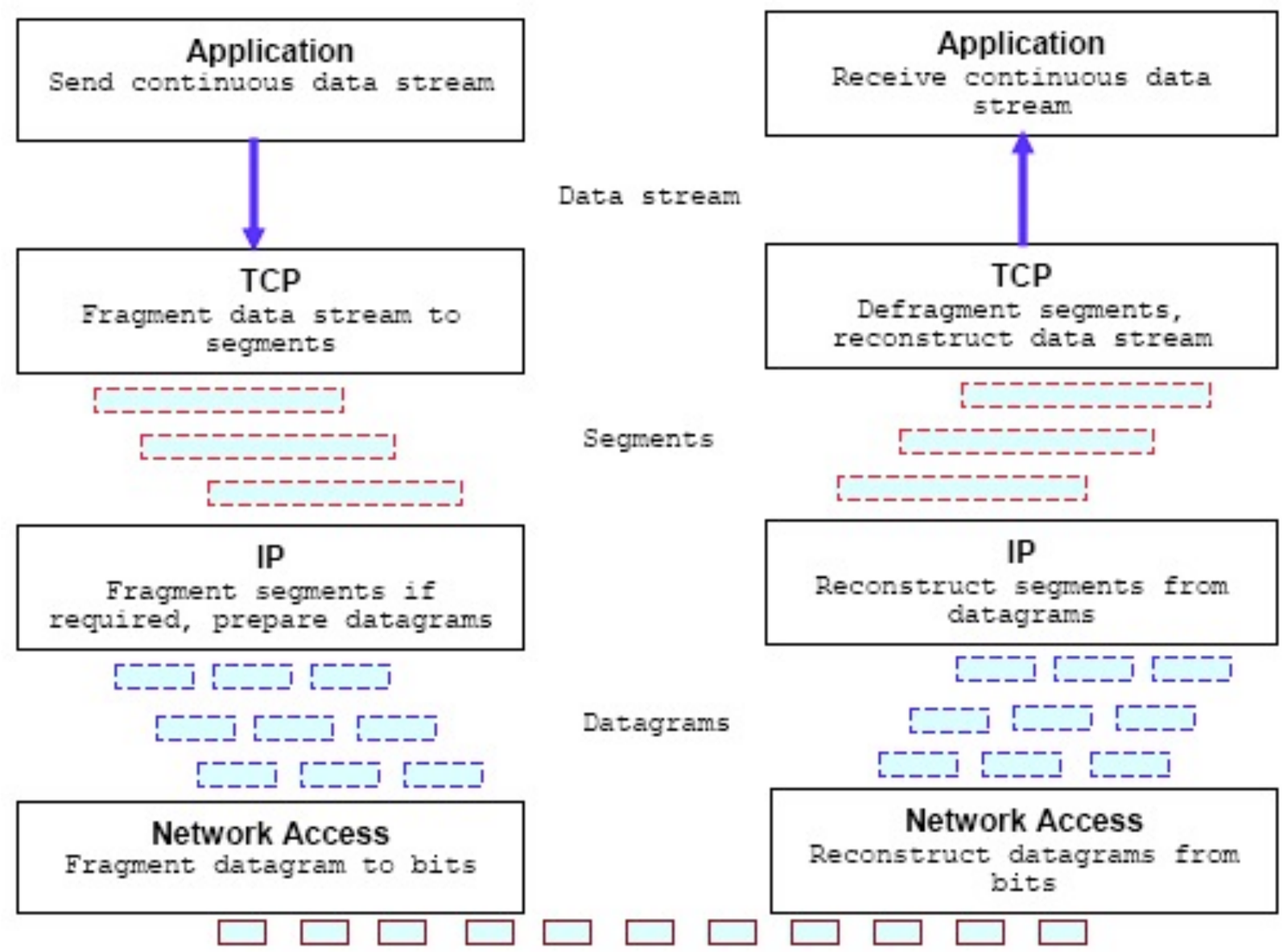
Source Address (the IP address of the original sender of the packet)
Destination Address (the IP address of the final destination of the packet)
Size of Datagram (in bytes, this is the combined length of the header and the data)
Header **Checksum** (A 1's complement checksum inserted by the sender and updated whenever the packet header is modified by a router - Used to detect processing errors introduced into the packet inside a router or bridge where the packet is not protected by a link layer cyclic redundancy check**.** Packets with an invalid checksum are discarded by all nodes in an IP network)
Identification (16-bit number which together with the source address uniquely identifies this packet - used during reassembly of fragmented datagrams)
Time To Live (Number of hops /links which the packet may be routed over, decremented by most routers - used to prevent accidental routing loops)

Protocol (Service Access Point (SAP) which indicates the type of transport packet being carried (e.g. 1 = ICMP; 2= IGMP; 6 = TCP; 17= UDP).
Version (always set to the value 4 in the current version of IP)
IP **Header Length** (number of 32 -bit words forming the header, usually five)
Type of Service (ToS), now known as Differentiated Services Code Point (DSCP) (usually set to 0, but may indicate particular Quality of Service needs from the network, the DSCP defines the way routers should queue packets while they are waiting to be forwarded).
Flags (a sequence of three flags (one of the 4 bits is unused) used to control whether routers are allowed to fragment a packet (i.e. the Don't Fragment, DF, flag), and to indicate the parts of a packet to the receiver)
Fragmentation Offset (a byte count from the start of the original sent packet, set by any router which performs IP router fragmentation)
Options (not normally used, but, when used, the IP header length will be greater than five 32-bit words to indicate the size of the options field)

Transmission Control Protocol Internet Protcol TCP/IP



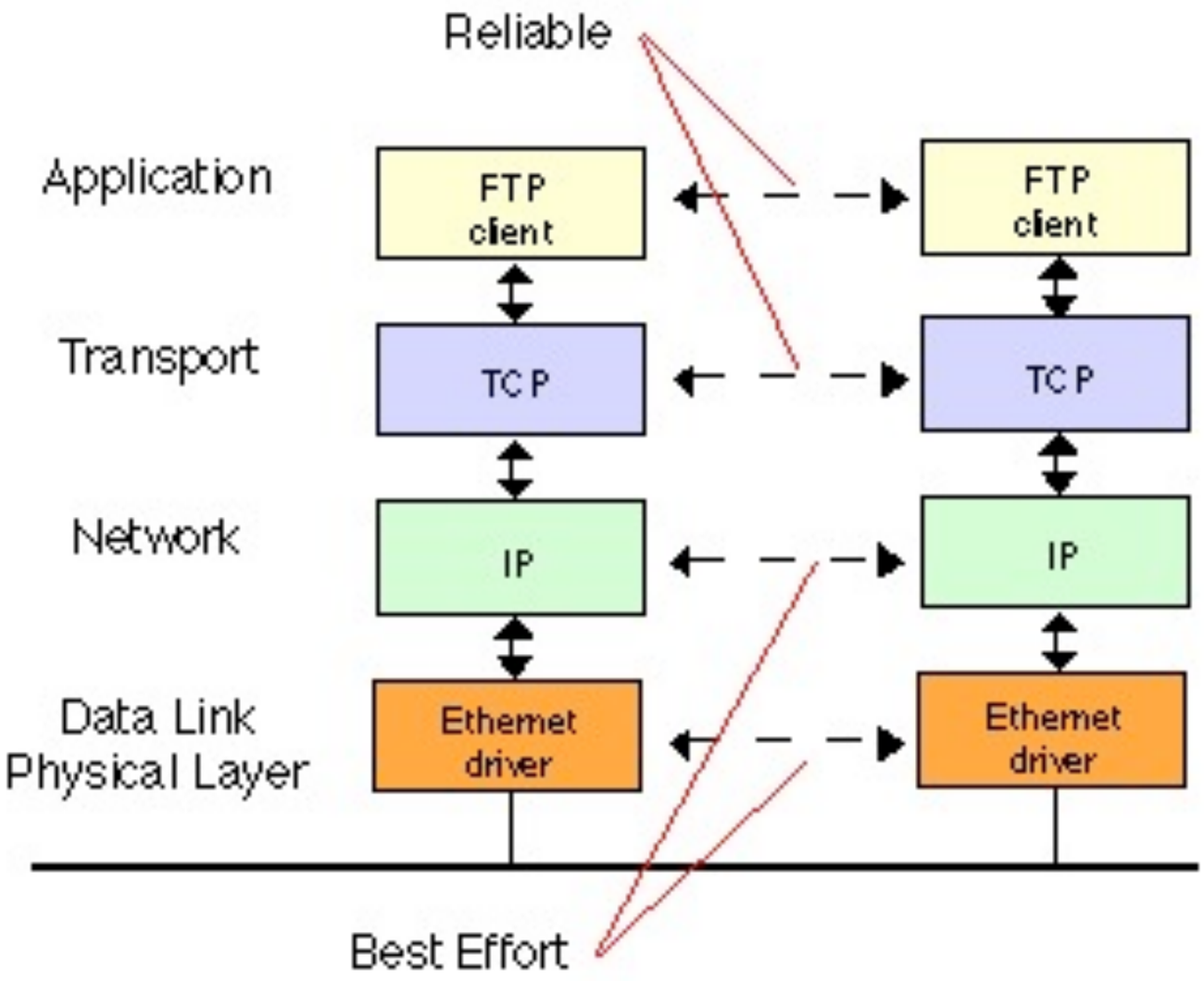
TCP/IP


Application
Send continuous data stream
TCP
Fragment data stream to segments
Segments
IP
Fragment segments if required, prepare datagrams
Datagrams
Network Access
Fragment datagram to bits
Data stream
Application
Receive continuous data stream
TCP
Defragment segments, reconstruct data stream
IP
Reconstruct segments from datagrams
Network Access
Reconstruct datagrams from bits

Transmission Contol Protocol
TCP

Uses:
copying data and texts

- reliable
- end-to-end transport

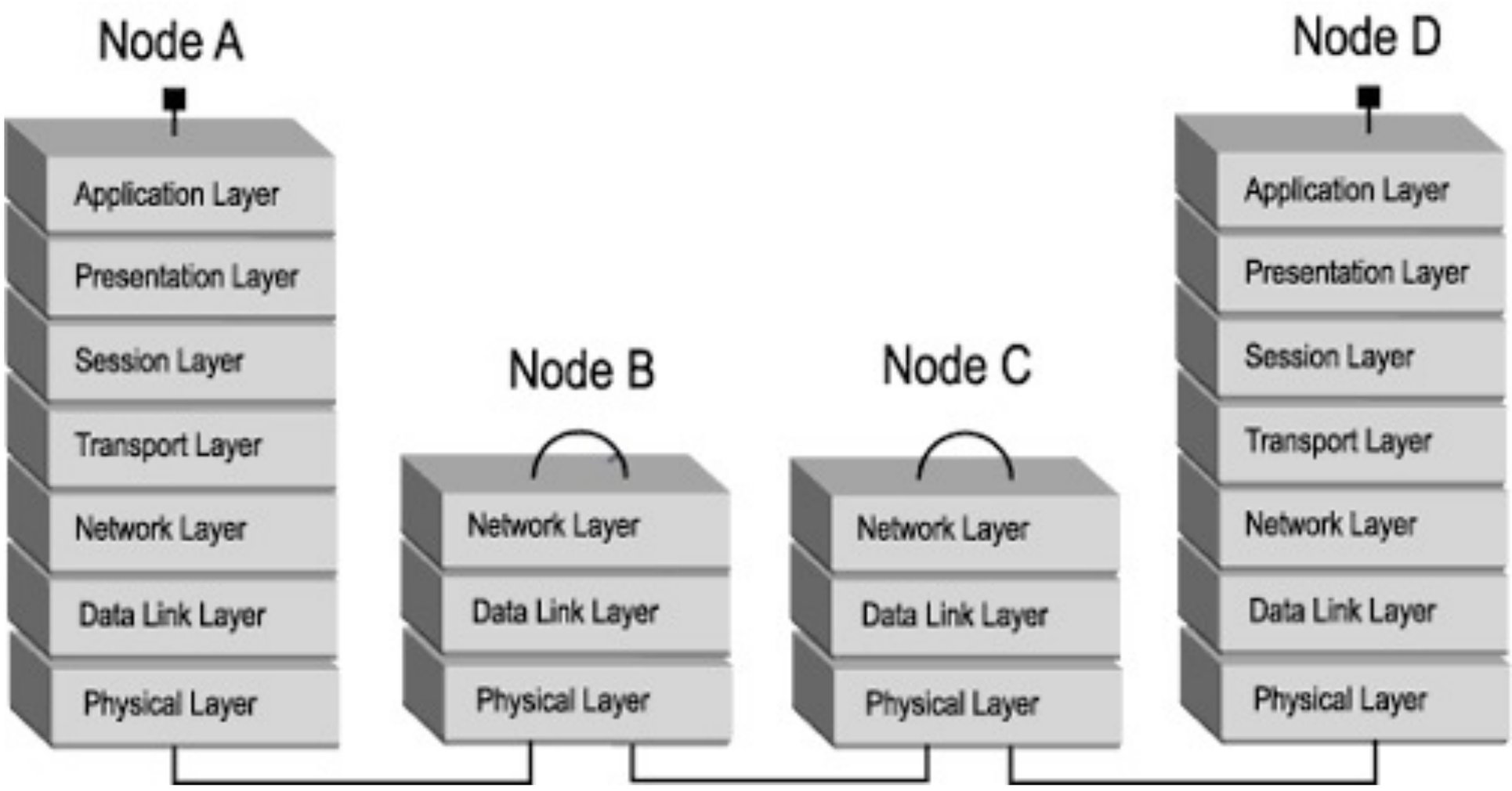


Saturday, 3 December 2011

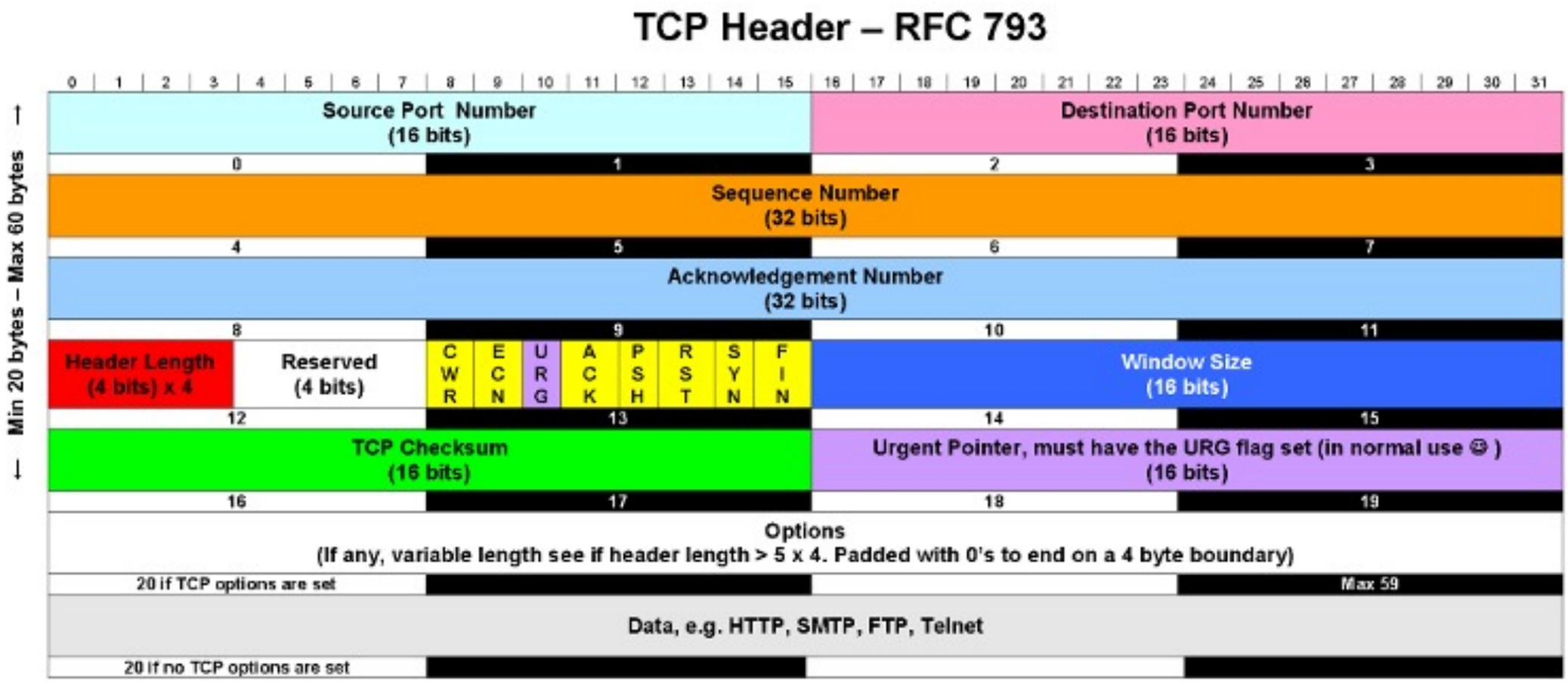
Transmission Control Protocol accepts data from a data stream, segments it into chunks, and adds a TCP header creating a TCP segment. The TCP segment is then encapsulated into an Internet Protocol (IP) datagram. A TCP segment is "the packet of information that TCP uses to exchange data with its peers."

For most networks approximately 90% of current traffic uses this transport service. It is used by such applications as telnet, World Wide Web (WWW), ftp, electronic mail. The transport header contains a Service Access Point which indicates the protocol which is being used (e.g. 23 = Telnet; 25 = Mail; 69 = TFTP; 80 = WWW (http)).

end-to-end


Node A
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer
Node B
Network Layer
Data Link Layer
Physical Layer
Node C
Network Layer
Data Link Layer
Physical Layer
Node D
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

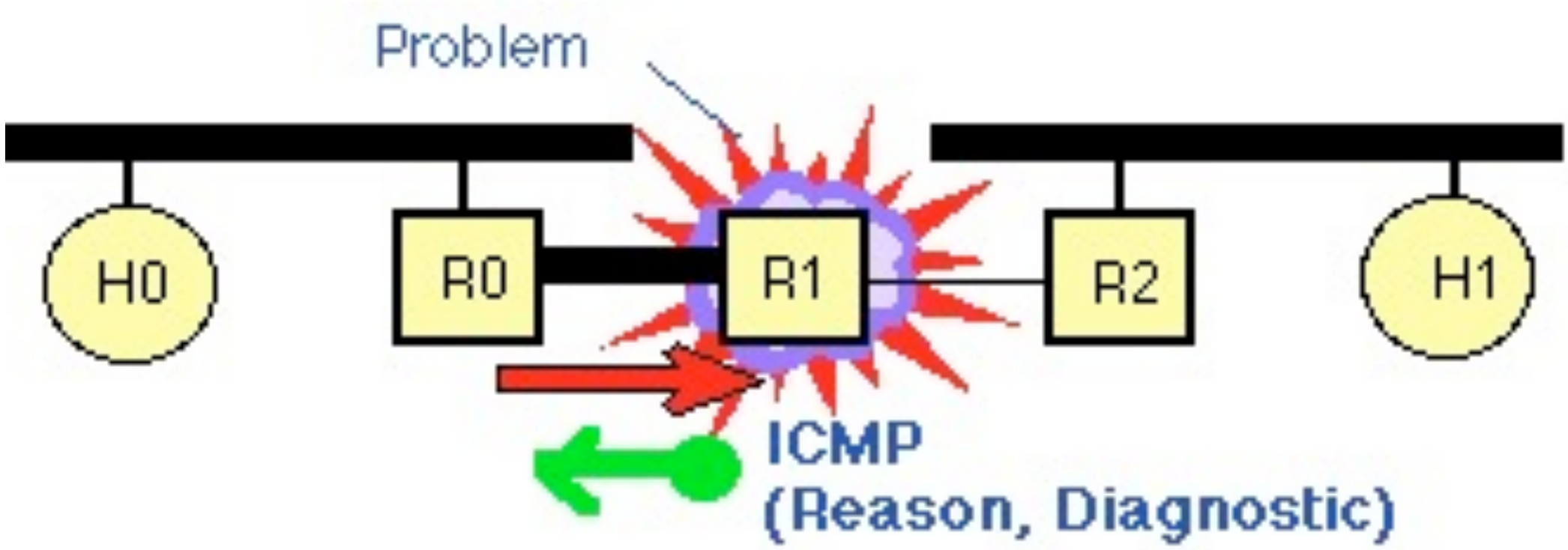
TCP header



Saturday, 3 December 2011

The sender keeps a record of each packet it sends, and waits for acknowledgment. The sender also keeps a timer from when the packet was sent, and retransmits a packet if the timer expires. The timer is needed in case a packet gets lost or corrupted.

Internet Control Message Protocol
ICMP



If something goes wrong a control message is sent using this special protocol

(We've been talking about point-to-point communication, but there is another Internet Group Management Protocol to support multicast.)

User Datagram Protocol
UDP

Uses:
real-time voice over IP

- minimal, unreliable, best-effort, message-passing transport
- no guarantees for message delivery

offset (bits)	0-15	16-31
0	Source Port Number	Destination Port Number
32	Length	Checksum
64	Data	

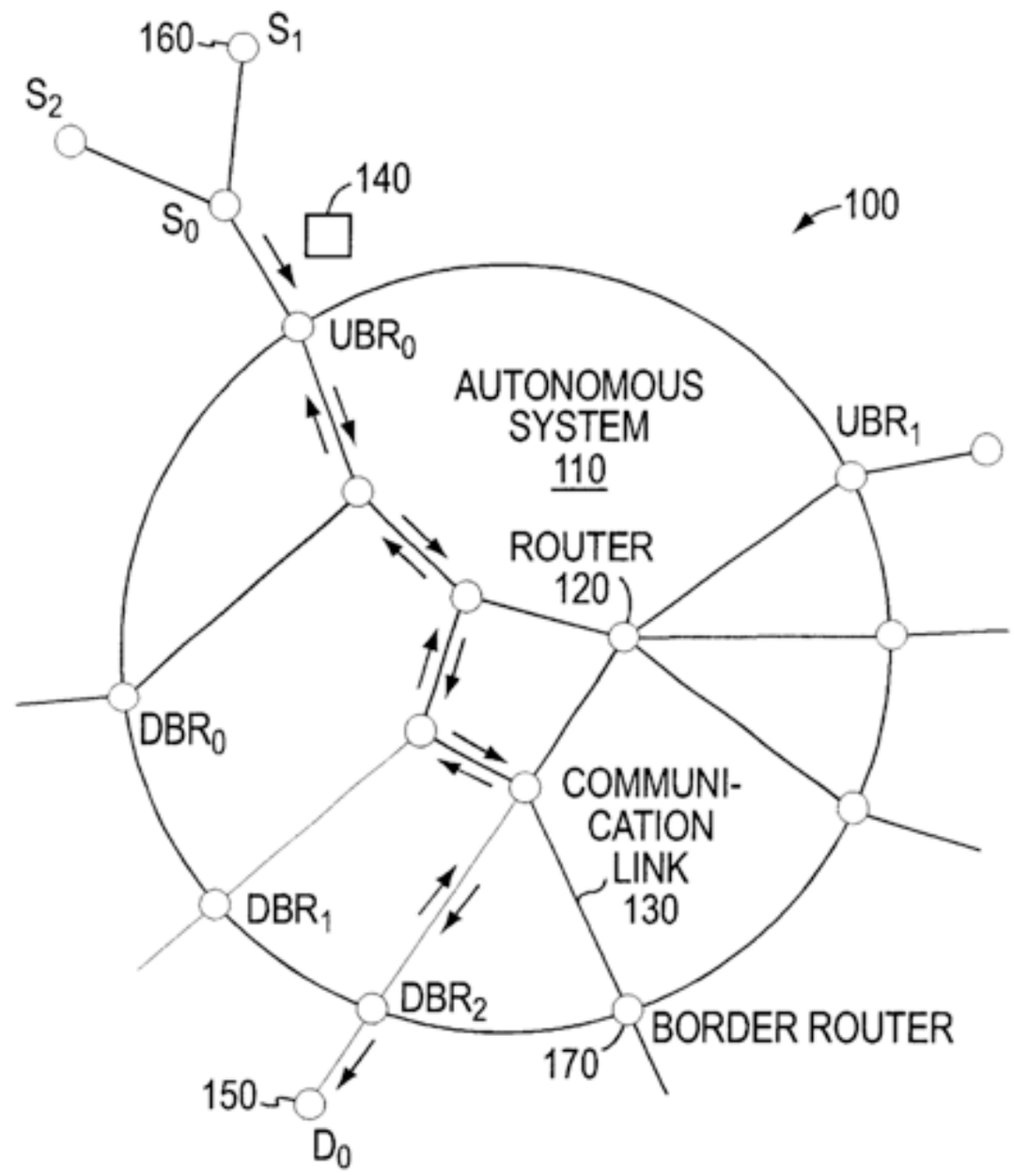
Saturday, 3 December 2011

TCP is complex so we look first at UDP

- **Source Port** (UDP packets from a client use this as a service access point (SAP) to indicate the session on the local client that originated the packet. UDP packets from a server carry the server SAP in this field)
- **Destination Port** (UDP packets from a client use this as a service access point (SAP) to indicate the service required from the remote server. UDP packets from a server carry the client SAP in this field)
- **UDP length** (The number of bytes comprising the combined UDP header information and payload data)
- **UDP Checksum** (A checksum to verify that the end to end data has not been corrupted by routers or bridges in the network or by the processing in an end system.

Transit

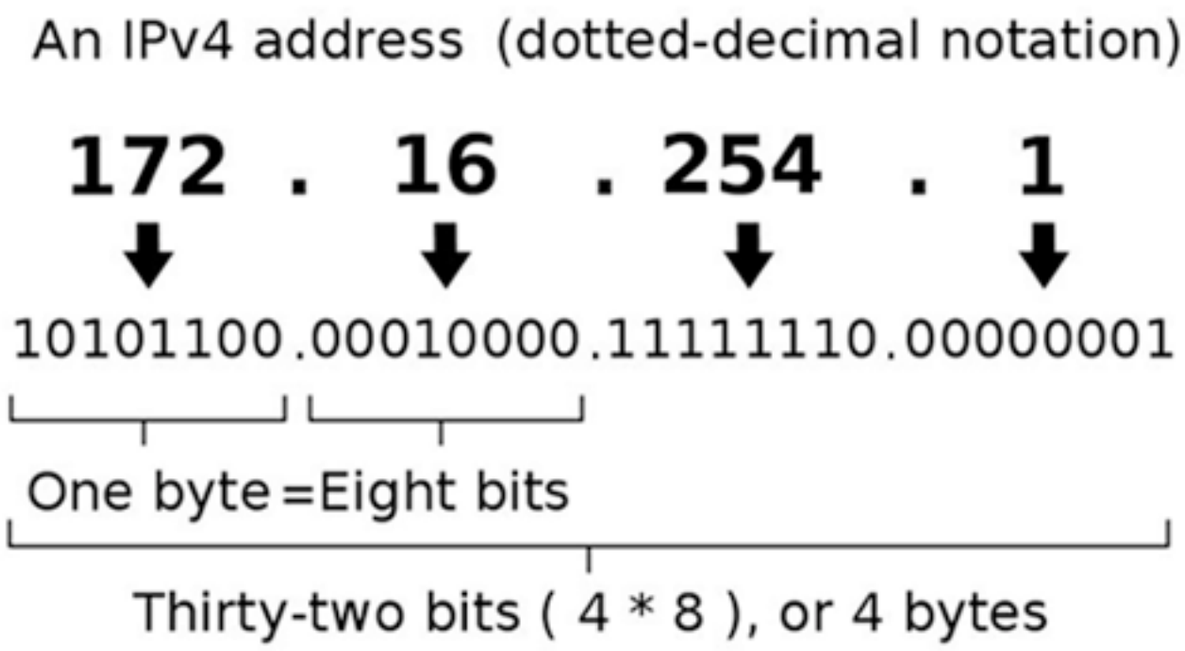
The transport layer (TCP or UDP) is unaware of the particular path taken by an IP packet.



How do the packets know where to go?

Each packet has an IP address

IPv4 address

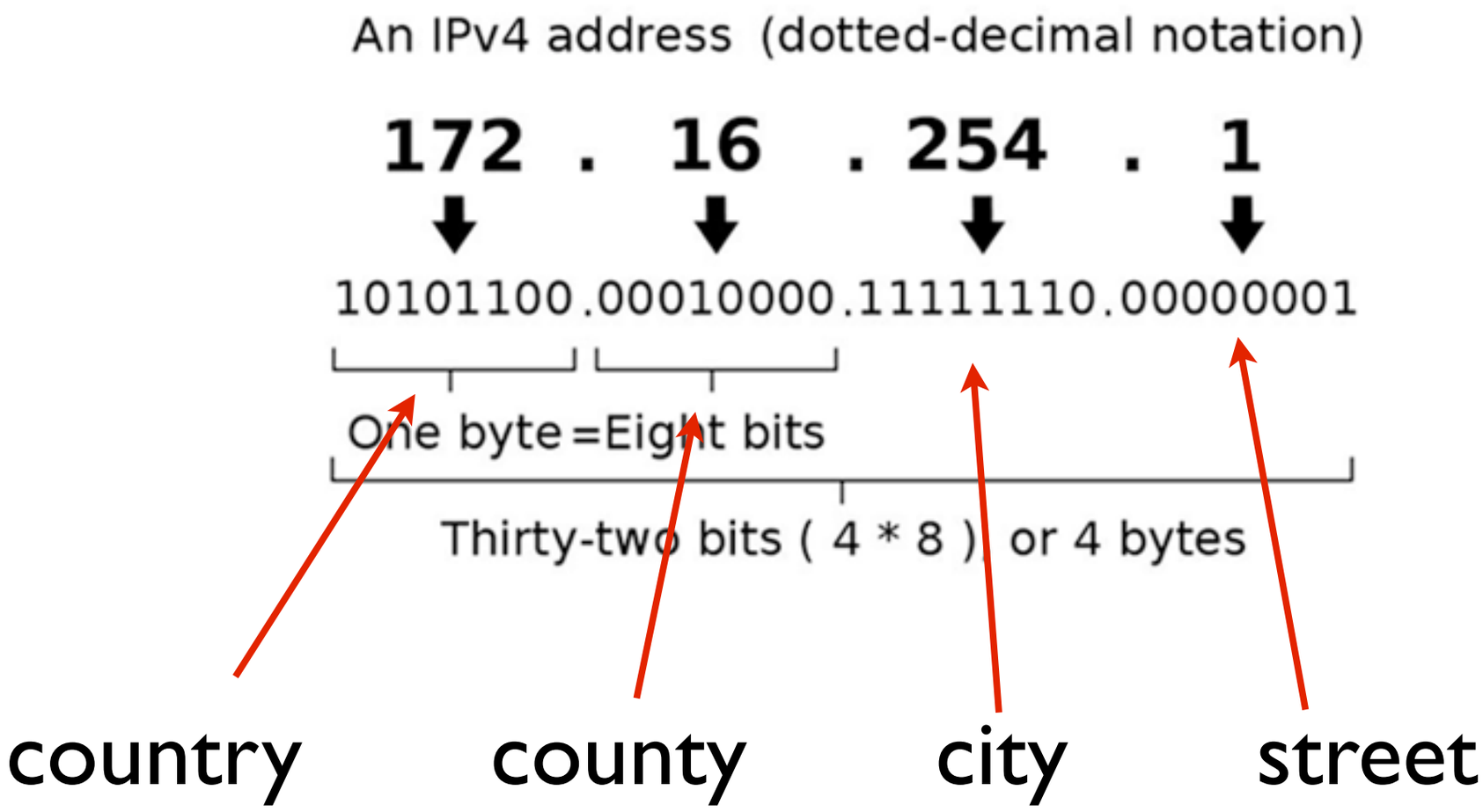


Saturday, 3 December 2011

This is a bit like a postal address

Passage through the network is like postal system

IPv4 address

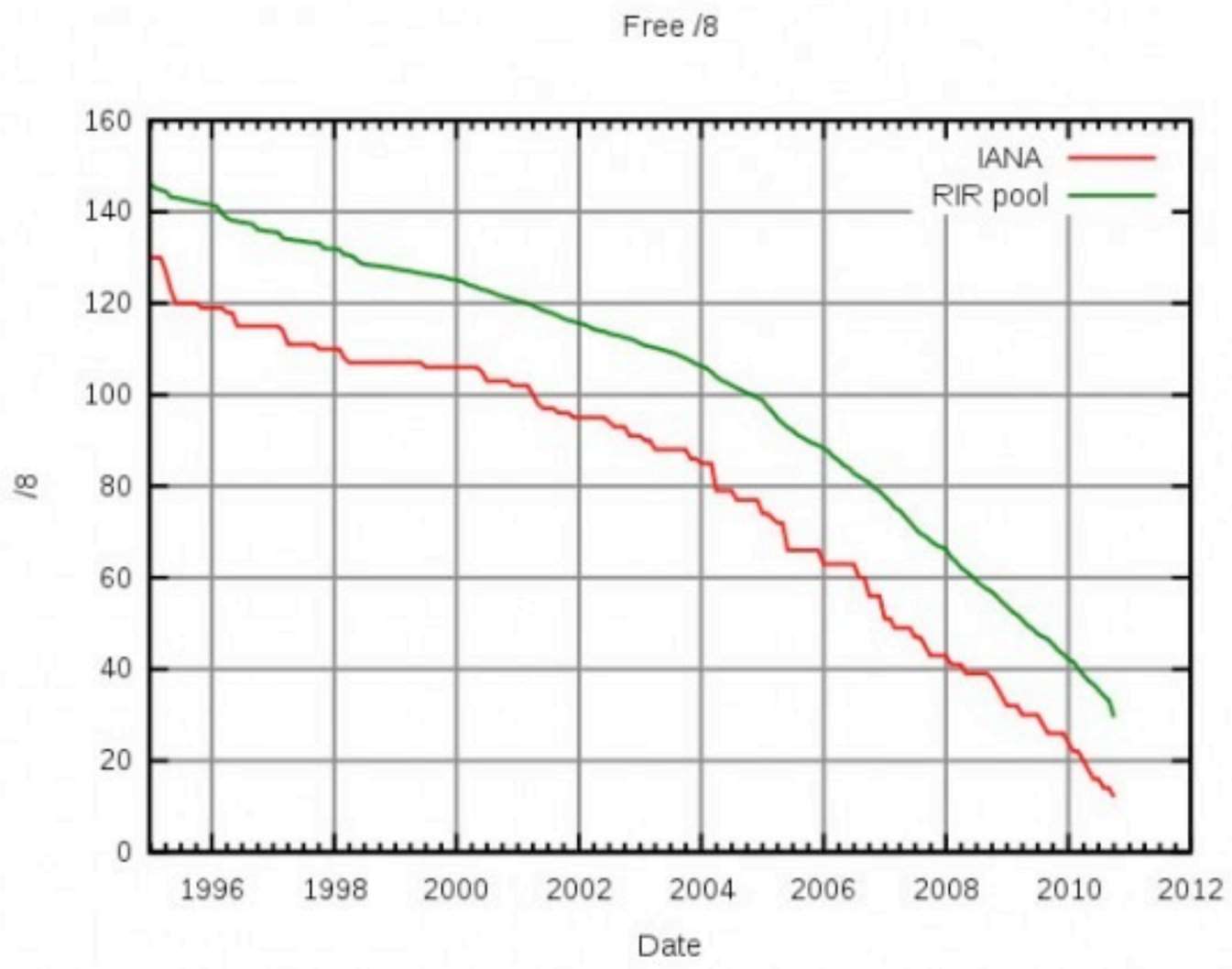


Saturday, 3 December 2011

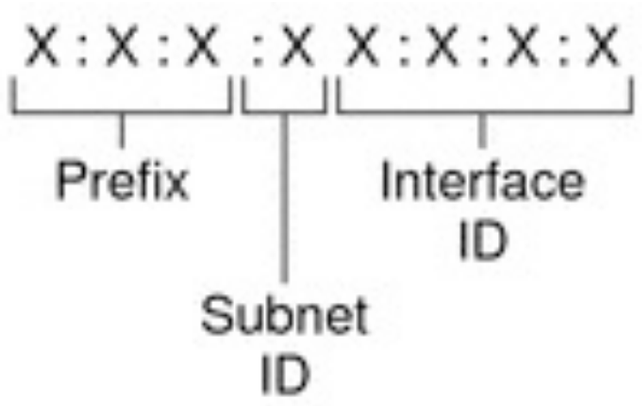
This is a bit like a postal address

Passage through the network is like postal system

Running out of addresses

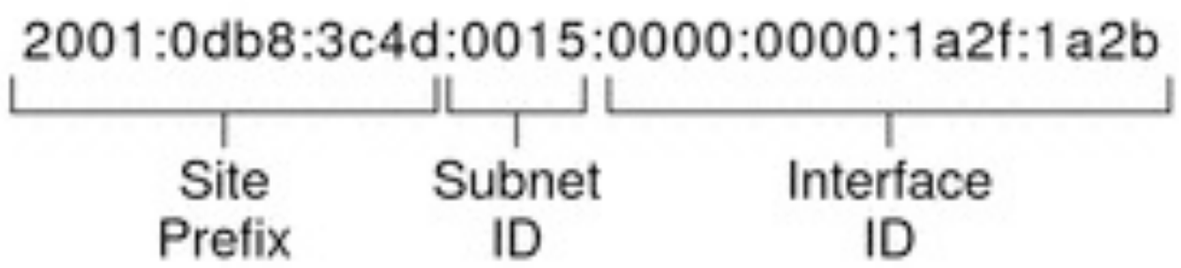


IPv6 address



128 bits

Example:



2^{48} sites : 2^{16} subnets : 2^{64} interface IDs

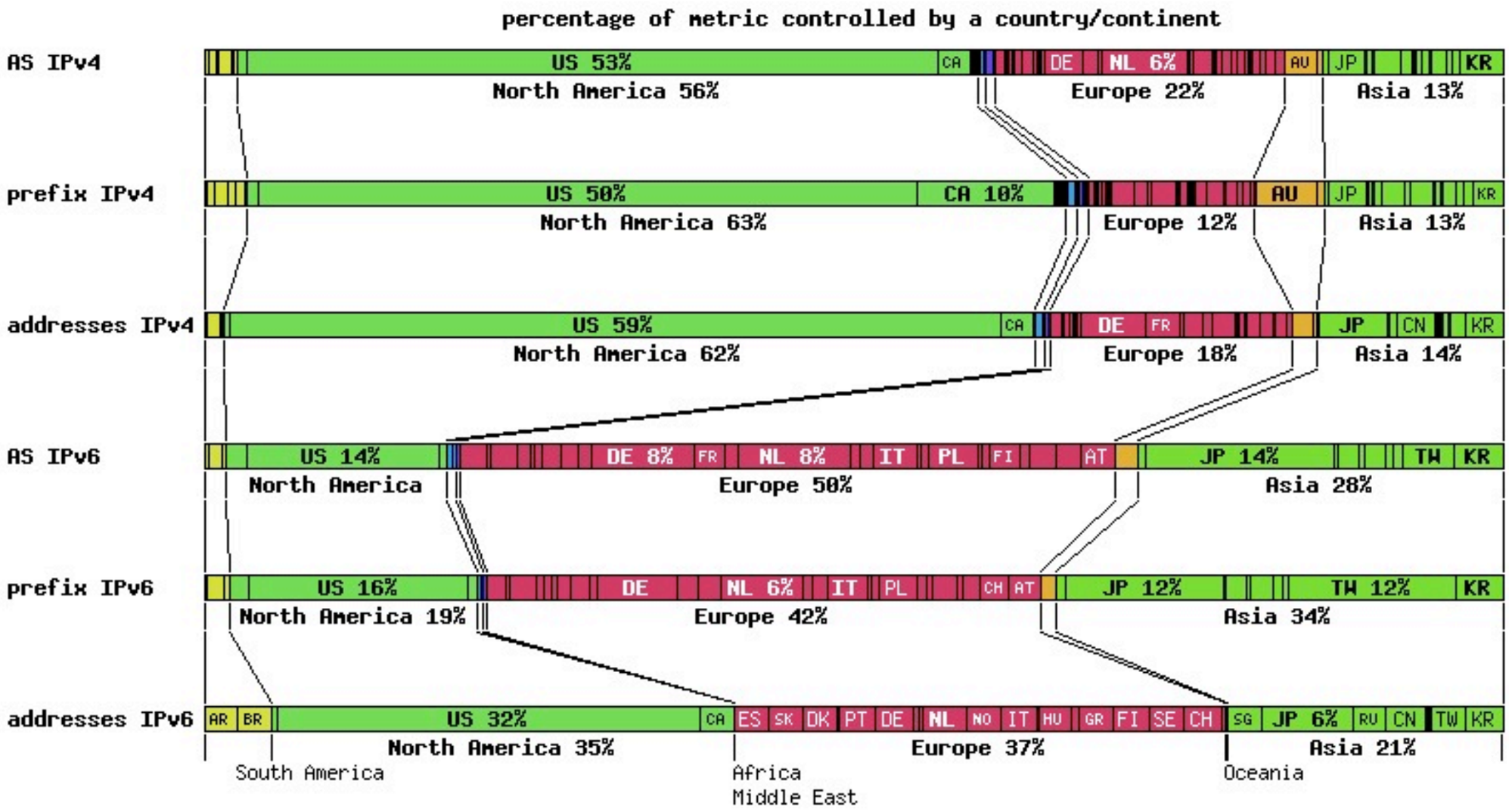
0 1 2 3 4 5 6 7 8 9 a b c d e f

IPv6

- simpler
  - no network-level checksum
  - no fragmentation
- larger network addresses,
  - increasing from 32 to 128 bits
  - 2001:0db8:0001:0035:0bad:beef:0000:cafe

use transport checksum to validate that a packet has been delivered to the intended recipient

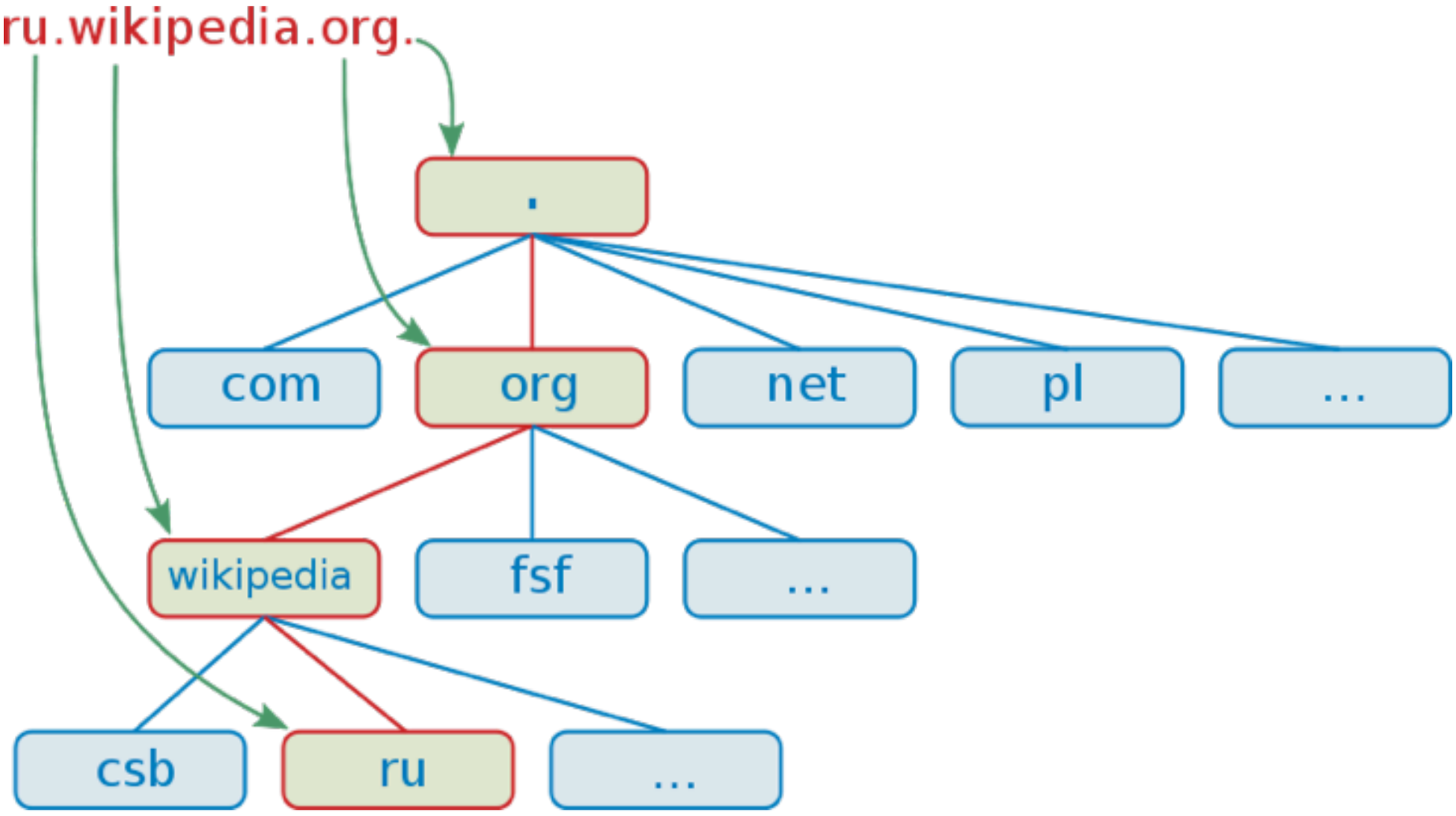
IP addresses



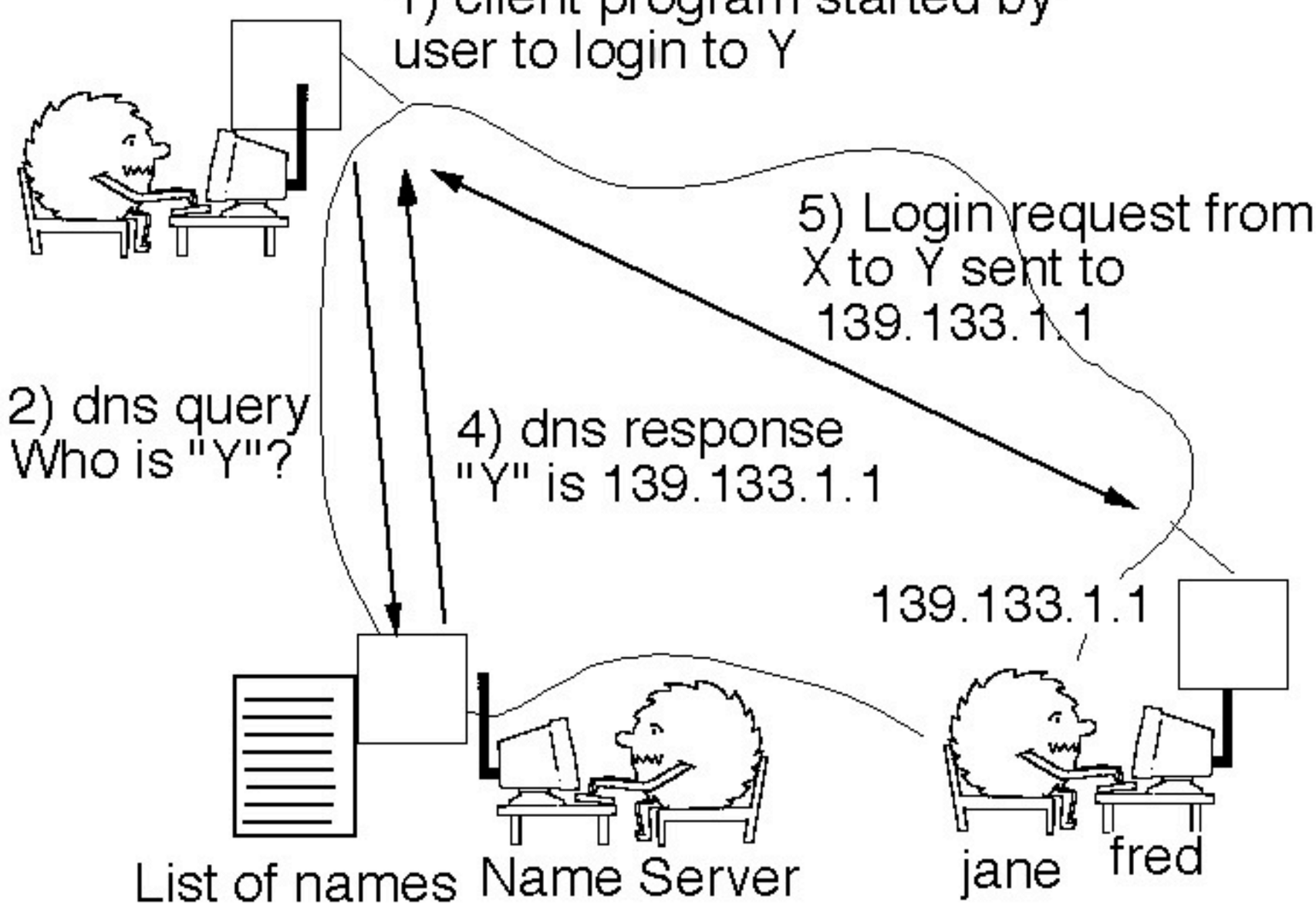
ASes
autonomous systems, the units of BGP routing policy (either single networks or groups of networks) representing a single administrative entity and controlled by a common network administrator. The Internet is a collection of ASes whose communication is negotiated via BGP peering sessions.
prefixes
slices of Internet address space that can be independently routed
IP addresses
the absolute number of addresses that are inside a country's set of prefixes

Cooperative Association for Internet Data Analysis
http://www.caida.org/research/policy/geopolitical/bgp2country/ipv6.xml

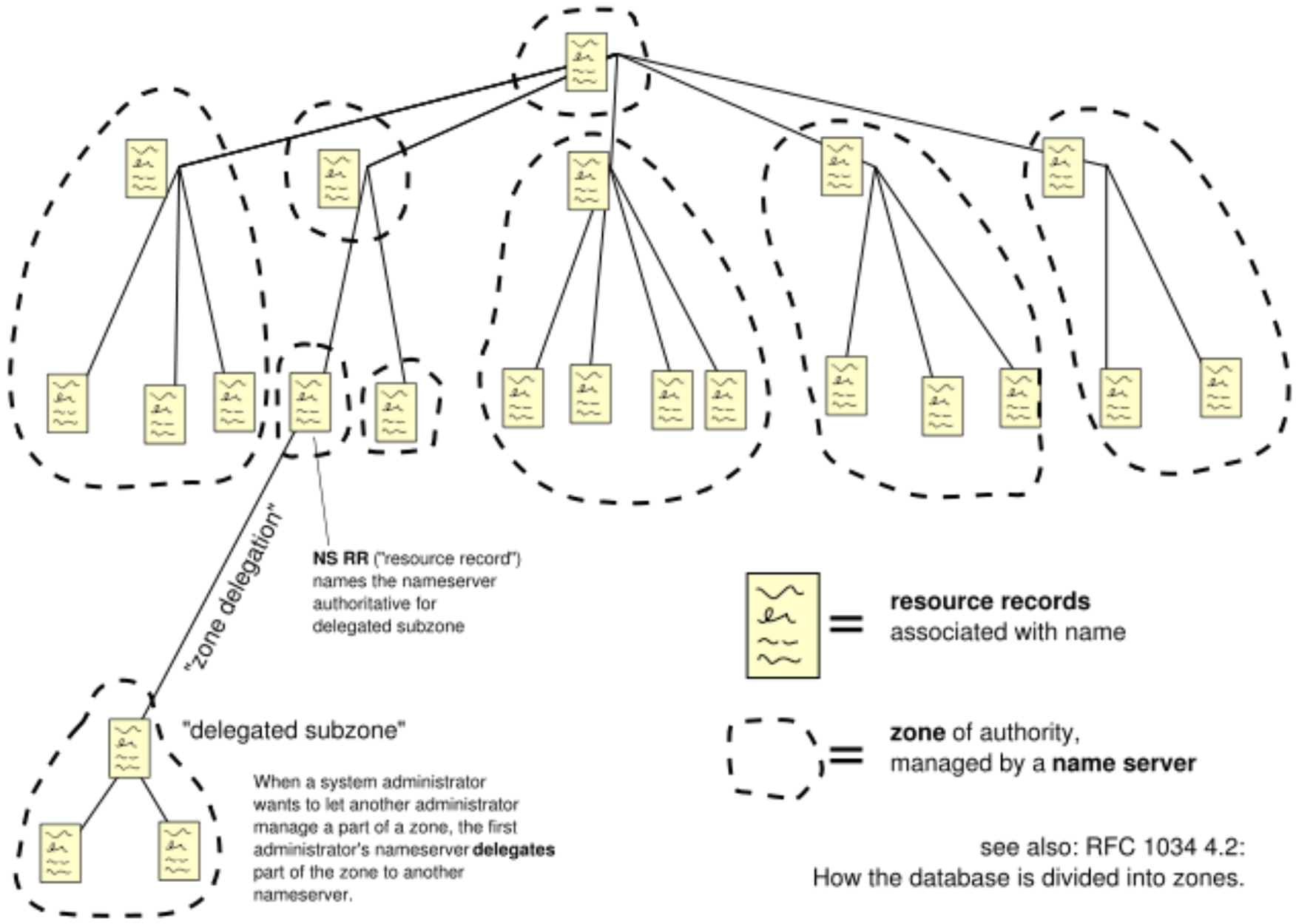
domain names



But we don’t (normally) use IP addresses

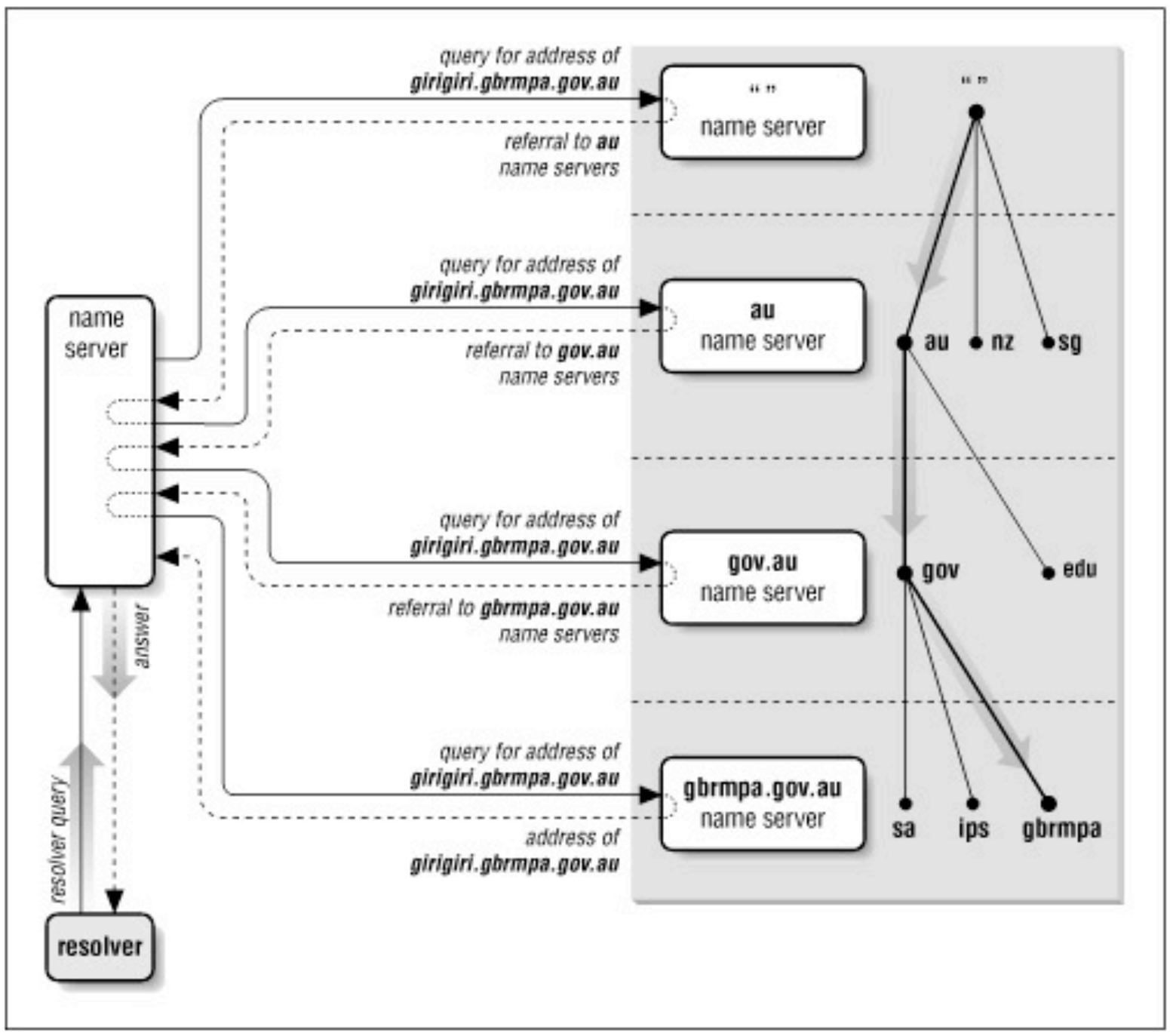

1) client program started by
user to login to Y
5) Login request from
X to Y sent to
139.133.1.1
2) dns query
Who is "Y"?
4) dns response
"Y" is 139.133.1.1
139.133.1.1
List of names
Name Server
jane
fred

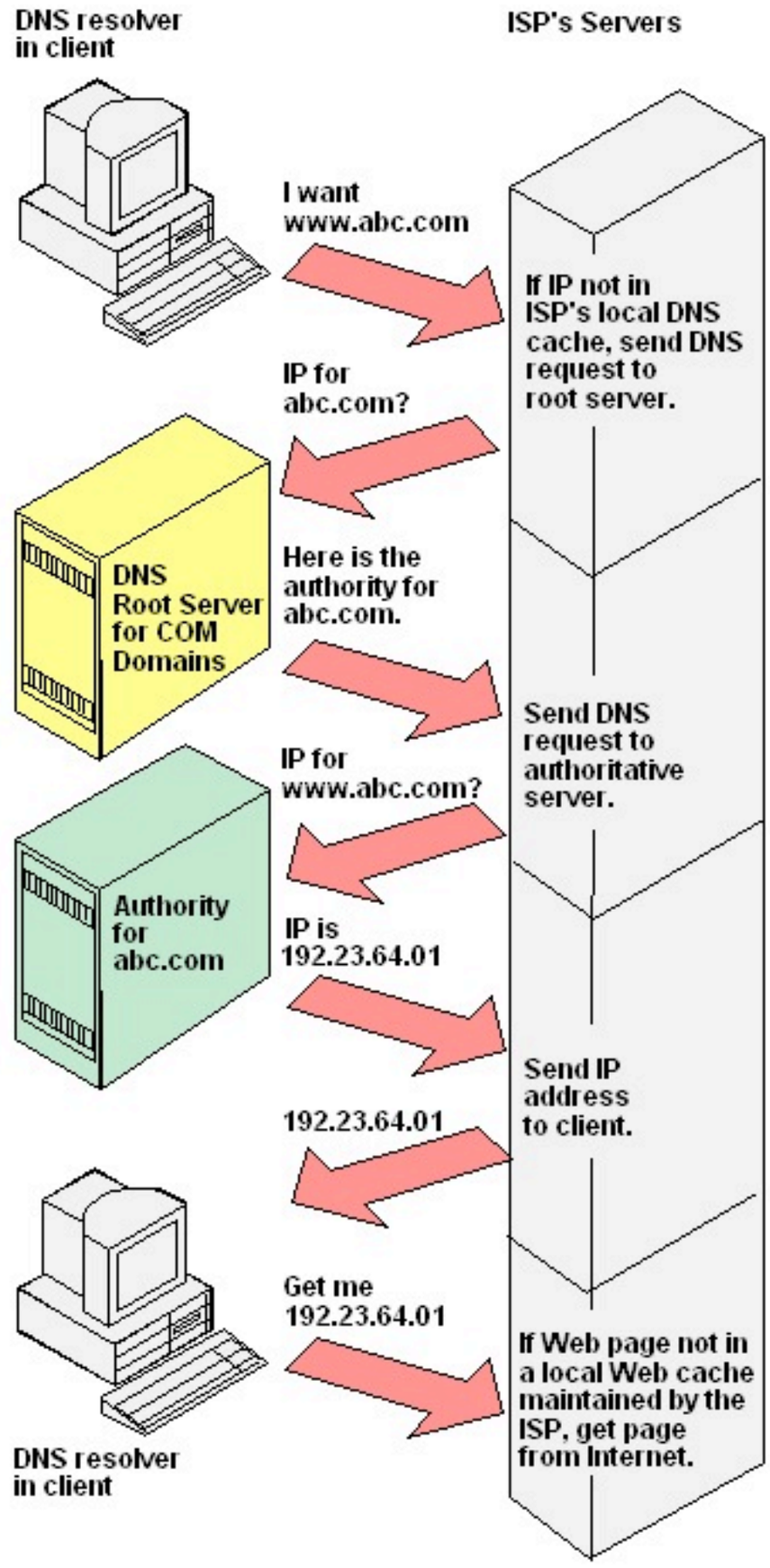
Domain Name Space



see also: RFC 1034 4.2:
How the database is divided into zones.

DNS lookup





DNS + ARP

- Network
  - Each node is identified by one or more globally unique IP addresses
  - DNS maps domain names to IP addresses
- Physical
  - Devices **Media Access Control address** (**MAC address**)
  - Address Resolution Protocol (arp) maps IP network addresses to the hardware addresses
    - **Media Access Control address** (**MAC address**)

Saturday, 3 December 2011

- Each node is identified by one or more globally unique IP addresses
- **Address Resolution Protocol (arp)** map IP network addresses to the hardware addresses

A global network