THE NETWORK LAYER NAT AND IPV6

COMP 30650: NETWORKS AND INTERNET SYSTEMS

Dr. Gavin McArdle
Email: gavin.mcardle@ucd.ie
Office: A1.09 Computer Science

NETWORK LAYER RECAP

- Network layer is responsible for joining networks together
  - Internetworking
- Use IP addresses
- Routers are the key technology in the Network Layer
  - Forwarding – sending a packet on its way
    - Longest common prefix
  - Routing – deciding best route to send packets
- DHCP
- Fragmentation
  - Classic Fragmentation/Maximum Transition Unit
- ICMP

TODAY'S PLAN

Public and Private IP Addresses

Network Address Translation Examples

IPv6

- Why?
- Challenges

PUBLIC VERSUS PRIVATE IP ADDRESSES - NAT

What is NAT (Network Address Translation)? How does it work?

- NAT is widely used at the edges of the network, e.g., homes

NAT (NETWORK ADDRESS TRANSLATION) BOX

NAT box connects an internal network to an external network

- Many internal hosts are connected using few external addresses
- Middlebox that “translates addresses”

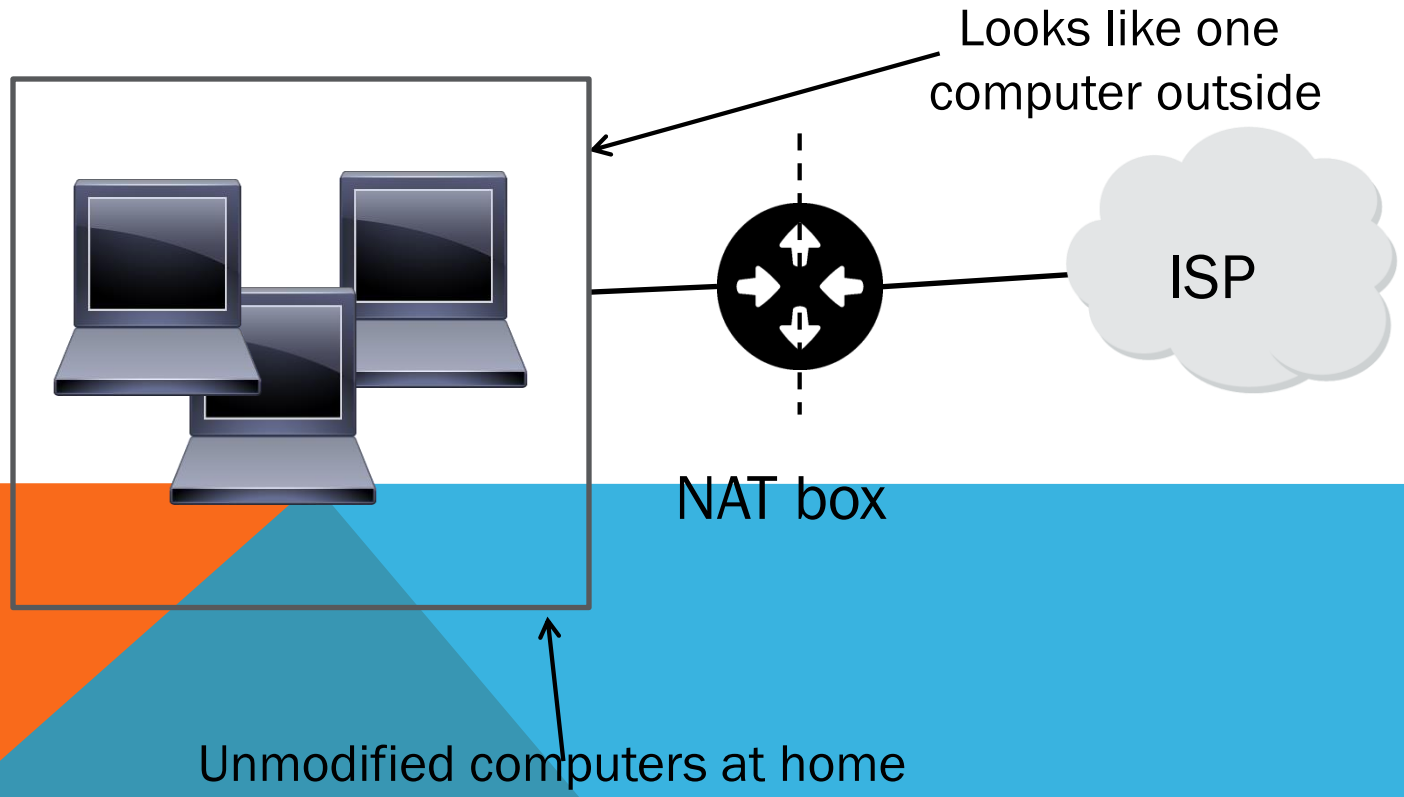
Motivated by IP address scarcity

- Controversial at first, now accepted

NAT

Common scenario:

- Home computers use “private” IP addresses
- NAT (in AP/firewall) connects home to ISP using a single external IP address



HOW NAT WORKS

Keeps an internal/external table

- Typically uses IP address + TCP port
- This is address and port translation
- Need ports to make mapping 1-1 since there are fewer external IPs

What host thinks	What ISP thinks
Internal IP:port	**External IP : port**
192.168.1.12 : 5523	44.25.80.3 : 1500
192.168.1.13 : 1234	44.25.80.3 : 1501
192.168.2.20 : 1234	44.25.80.3 : 1502

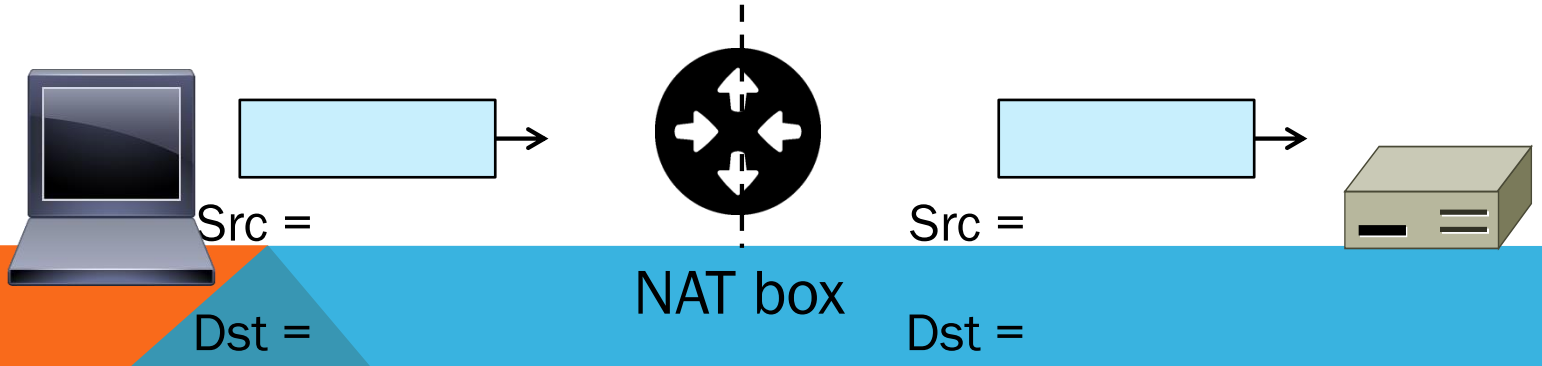
HOW NAT WORKS

Internal → External:

- Look up and rewrite Source IP/port

	Internal IP:port	External IP : port
Internal source	192.168.1.12 : 5523	44.25.80.3 : 1500

External destination IP=X, port=Y

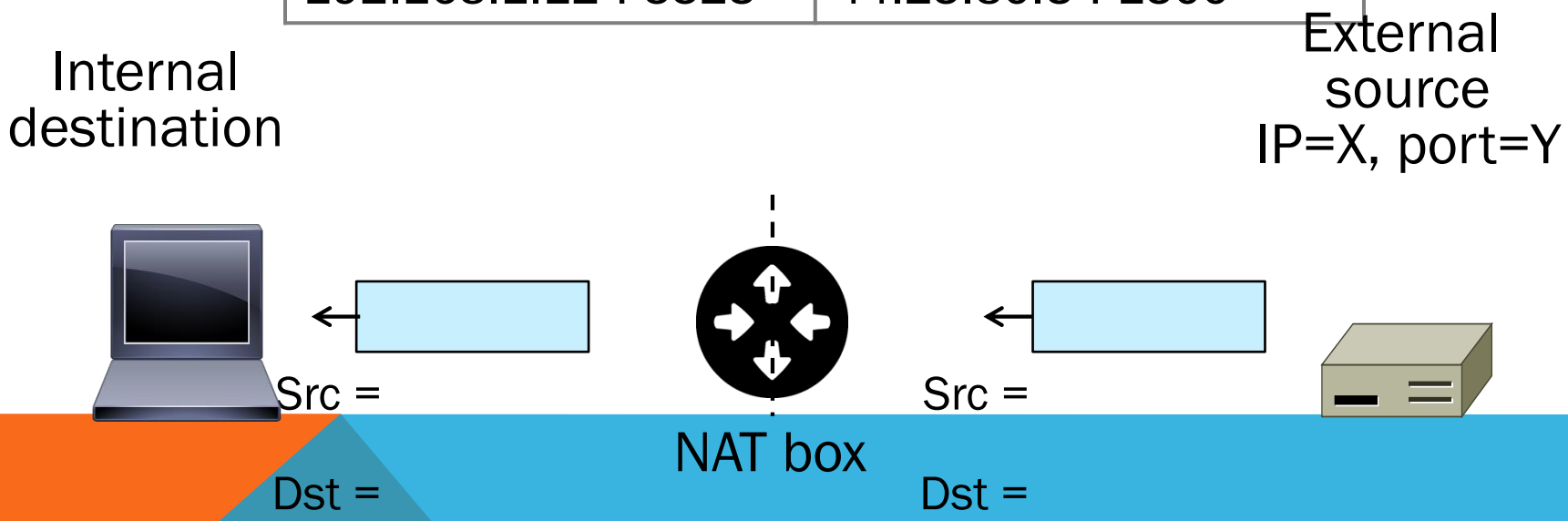


HOW NAT WORKS

External → Internal

- Look up and rewrite Destination IP/port

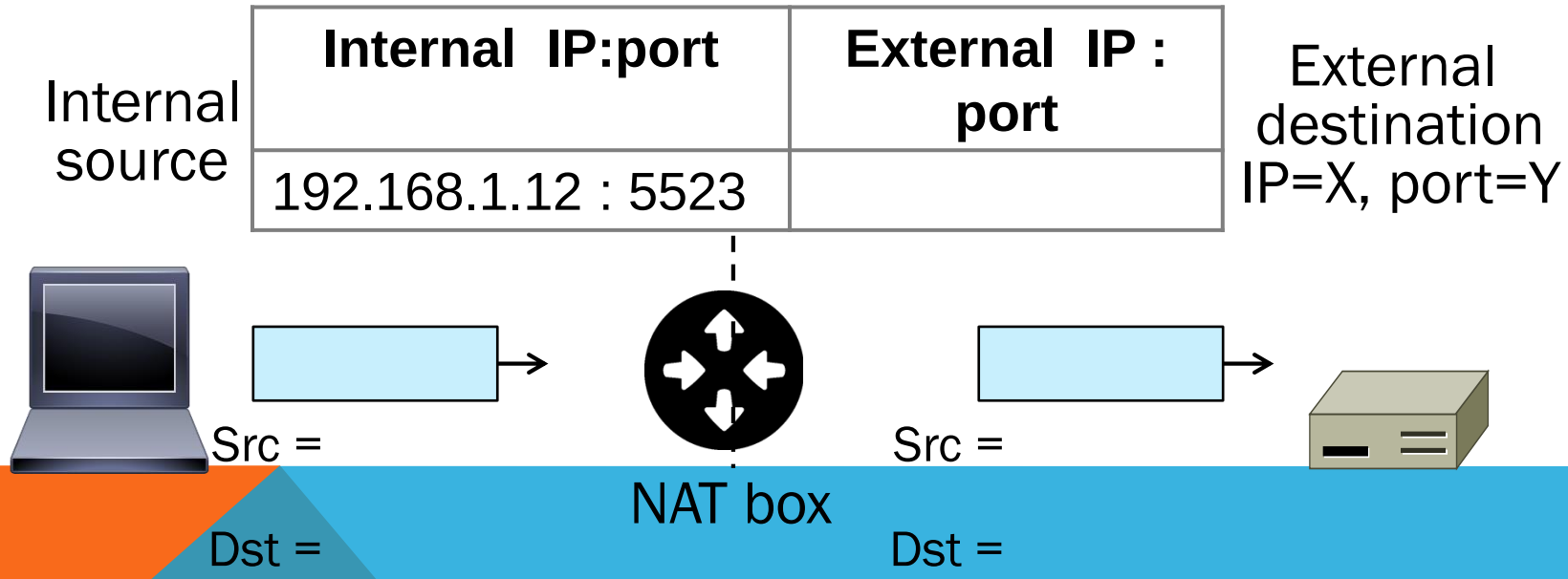
Internal IP:port	External IP : port
192.168.1.12 : 5523	44.25.80.3 : 1500



HOW NAT WORKS

Need to enter translations in the table for it to work

- Create external name when host makes a TCP connection



NAT DOWNSIDES

Connectivity has been broken!

- Can only send incoming packets after an outgoing connection is set up
- Difficult to run servers or peer-to-peer apps at home

Breaks apps that unwisely expose their IP addresses (FTP)

NAT UPSIDES

Relieves much IP address pressure

- Many home hosts behind NATs

Easy to deploy

- Rapidly, and by you alone

Useful functionality

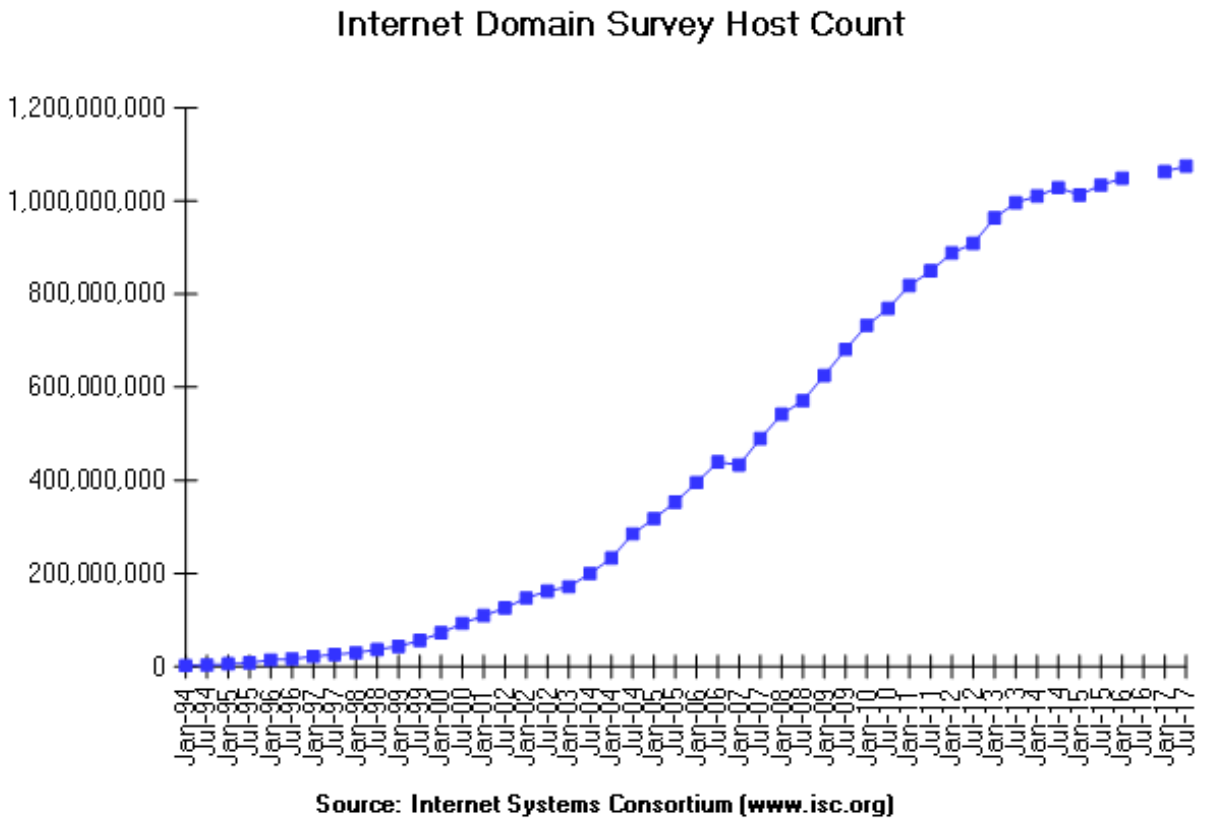
- Firewall, helps with privacy

INTERNET GROWTH

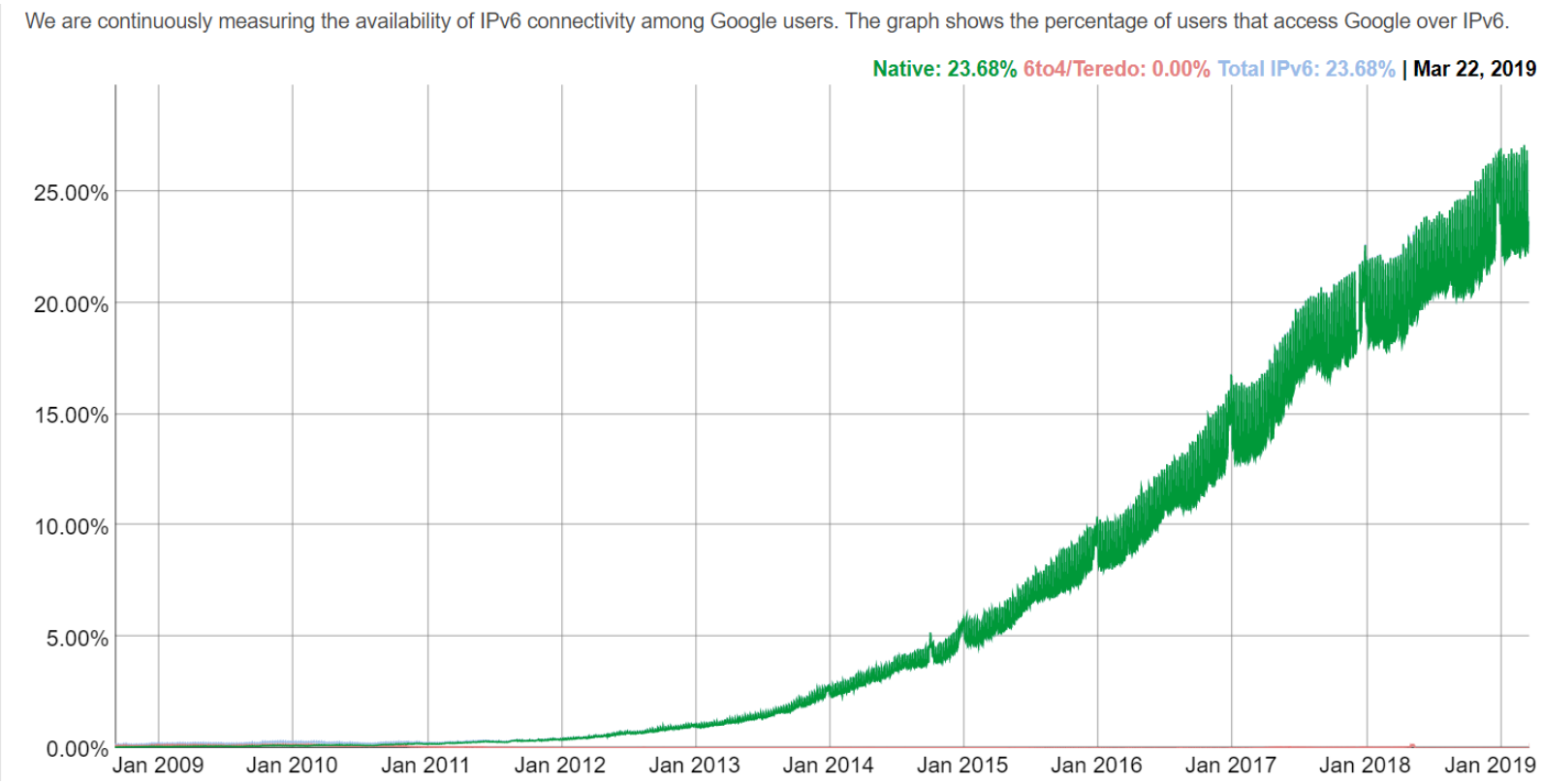
At least a billion Internet hosts and growing …

And we use 32-bit addresses!

2^{32} = 4294967296



IPV6 DEPLOYMENT



Time for growth!

Source: Google IPv6 Statistics,
https://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption&tab=ipv6-adoption

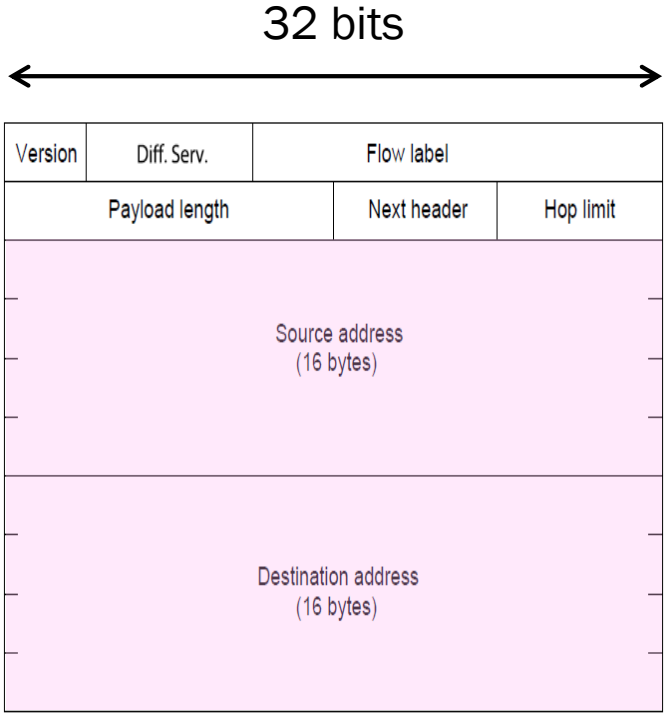
IPV6

Features large addresses

- 128 bits, most of header

New notation

- 8 groups of 4 hex digits (16 bits)
- Omit leading zeros, groups of zeros



Ex: 2001:0db8:0000:0000:0000:ff00:0042:8329

→

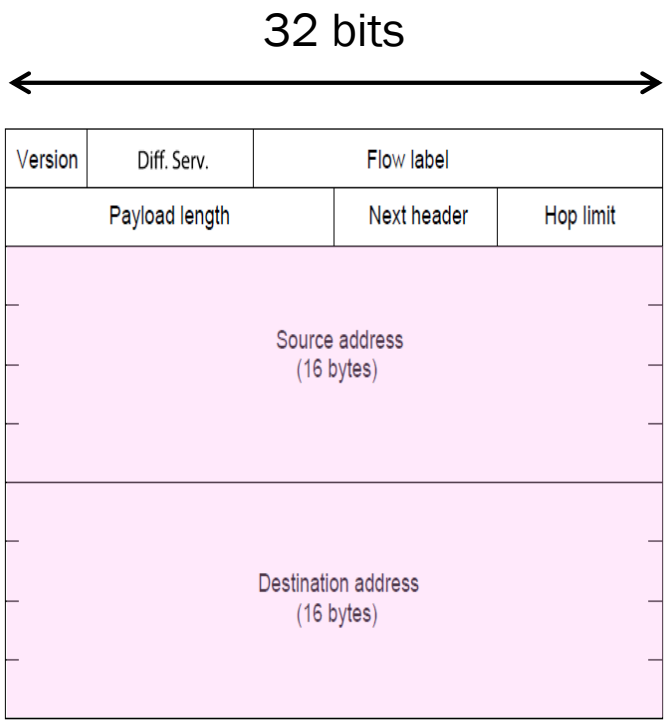
IPV6

Features large addresses

- 128 bits, most of header

New notation

- 8 groups of 4 hex digits (16 bits)
- Omit leading zeros, groups of zeros



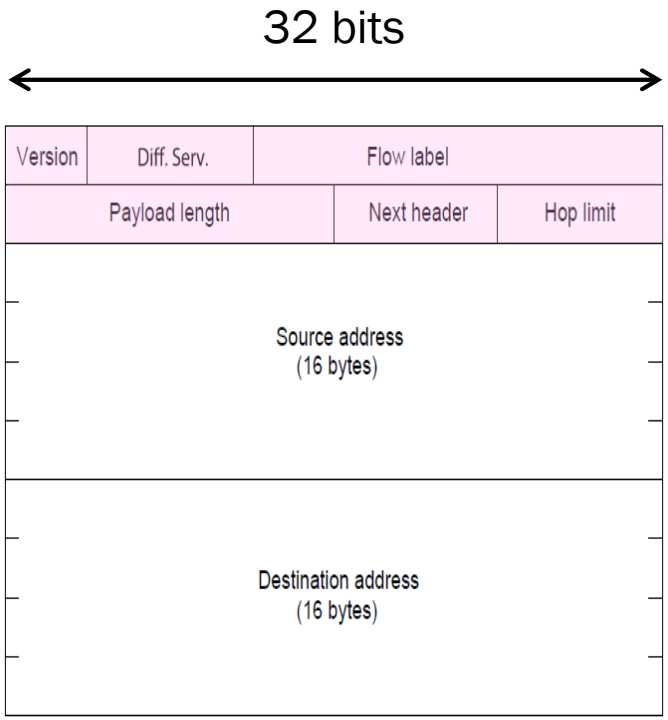
Ex: 2001:0db8:0000:0000:0000:ff00:0042:8329

→ 2001:db8::ff00:42:8329

IPV6 (2)

Lots of other, smaller changes

- Streamlined header processing
- Flow label to group packets
- Better fit with “advanced” features (mobility, multicasting, security)



IPV6 TRANSITION

The Big Problem:

- How to deploy IPv6?
- Fundamentally incompatible with IPv4

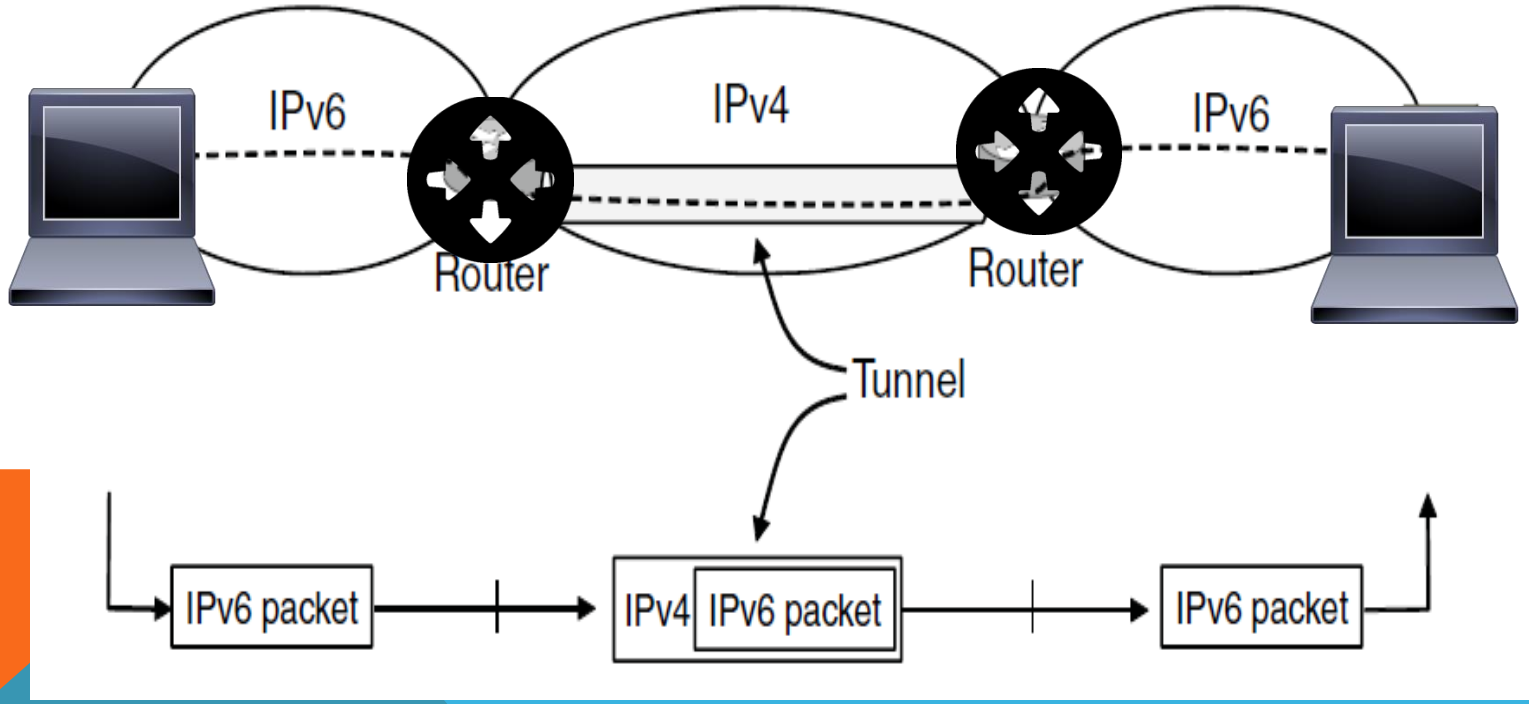
Dozens of approaches proposed

- Dual stack (speak IPv4 and IPv6)
- Translators (convert packets)
- Tunnels (carry IPv6 over IPv4)

TUNNELING

Native IPv6 islands connected via IPv4

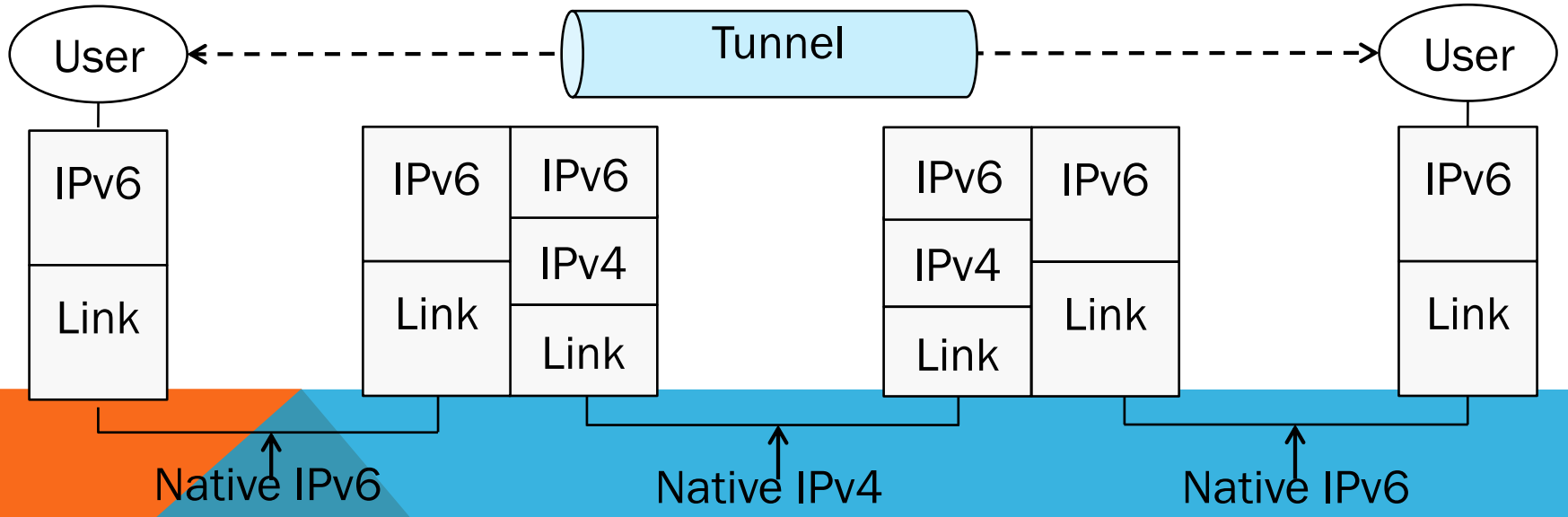
- Tunnel carries IPv6 packets across IPv4 network



TUNNELING

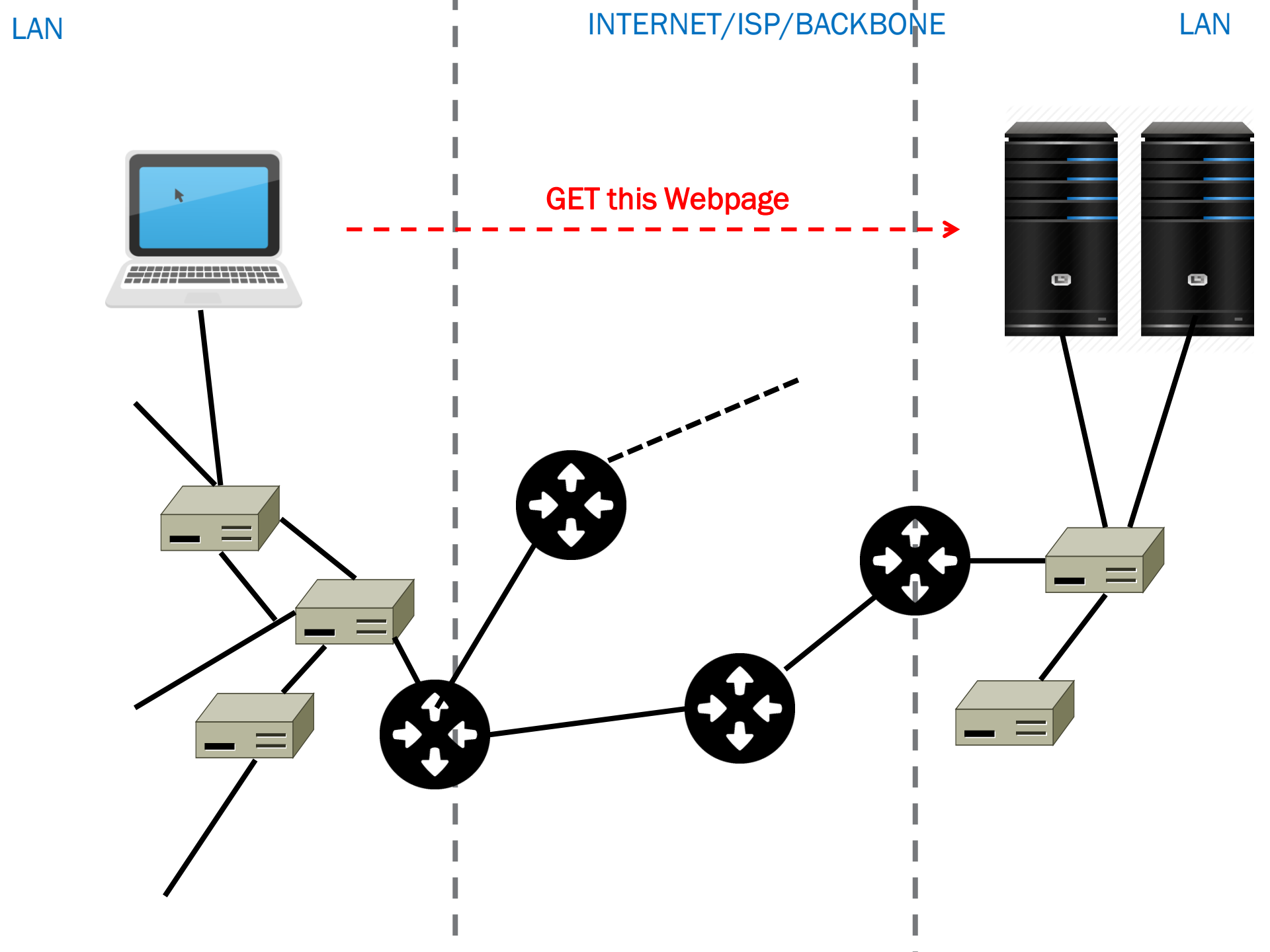
Tunnel acts as a single link across IPv4 network

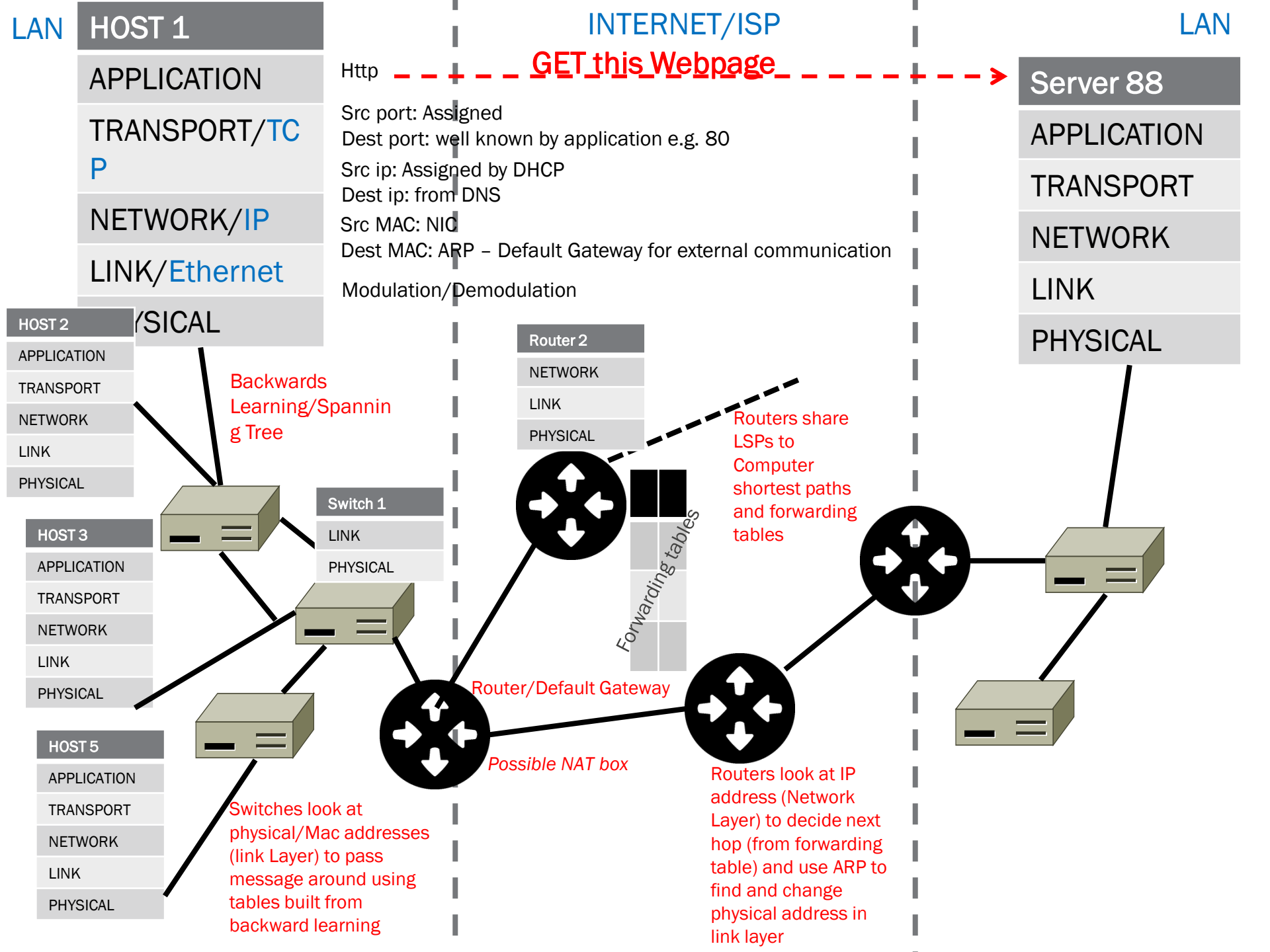
- Difficulty is to set up tunnel endpoints and routing



THE BIGGER PICTURE

Do we know how the Internet works yet?


LAN
INTERNET/ISP/BACKBONE
LAN
GET this Webpage


LAN
HOST 1
APPLICATION
TRANSPORT/TCP
NETWORK/IP
LINK/Ethernet
/SICAL
INTERNET/ISP
LAN
Http
GET this Webpage
Server 88
APPLICATION
TRANSPORT
NETWORK
LINK
PHYSICAL
Src port: Assigned
Dest port: well known by application e.g. 80
Src ip: Assigned by DHCP
Dest ip: from DNS
Src MAC: NIC
Dest MAC: ARP – Default Gateway for external communication
Modulation/Demodulation
HOST 2
APPLICATION
TRANSPORT
NETWORK
LINK
PHYSICAL
Backwards Learning/Spanning Tree
Router 2
NETWORK
LINK
PHYSICAL
Routers share LSPs to Computer shortest paths and forwarding tables
Switch 1
LINK
PHYSICAL
HOST 3
APPLICATION
TRANSPORT
NETWORK
LINK
PHYSICAL
Forwarding tables
Router/Default Gateway
HOST 5
APPLICATION
TRANSPORT
NETWORK
LINK
PHYSICAL
Possible NAT box
Switches look at physical/Mac addresses (link Layer) to pass message around using tables built from backward learning
Routers look at IP address (Network Layer) to decide next hop (from forwarding table) and use ARP to find and change physical address in link layer