# Peer 2 Peer


## Patrik Fältström

**<paf@cisco.com>**

**Corporate Consulting Engineer, Cisco Systems**

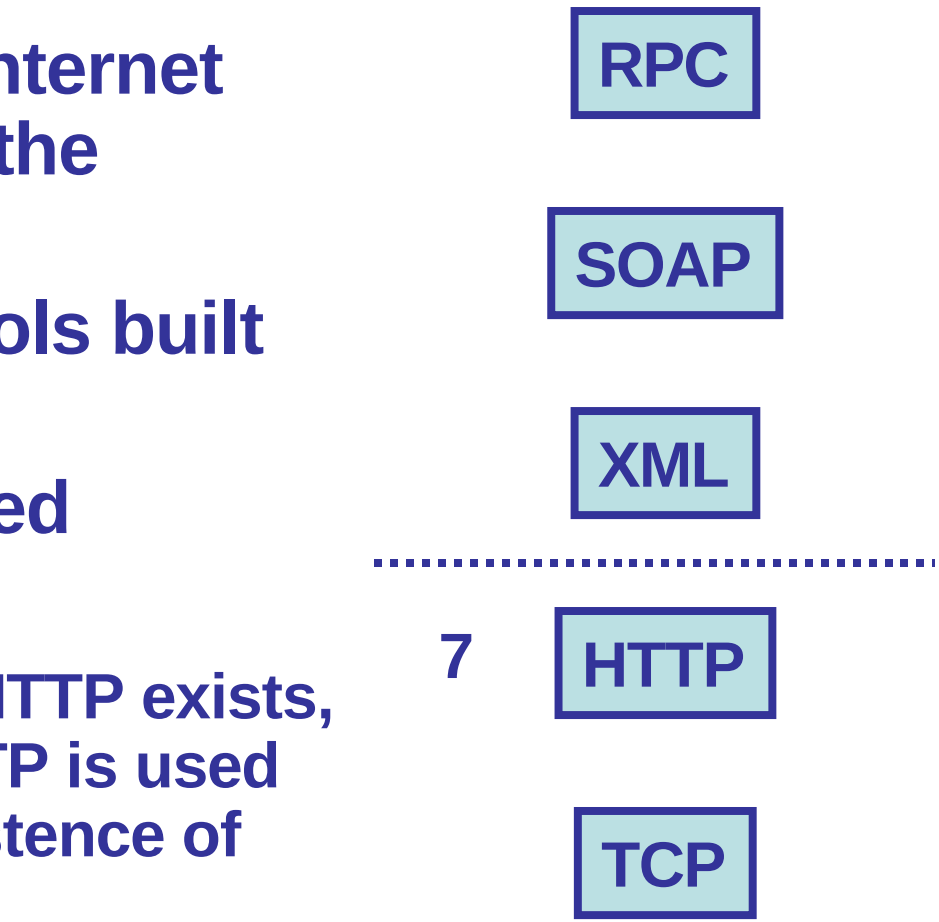
**Area Director, Applications Area, IETF**

# Peer 2 Peer?

- Any Internet Traffic is Peer 2 Peer
- Current design of Internet for home use claim homes are “consumers” which fetch information from “producers”
- That is fine in a “web” environment
- It is not proper Internet Architecture

# So, why so important?

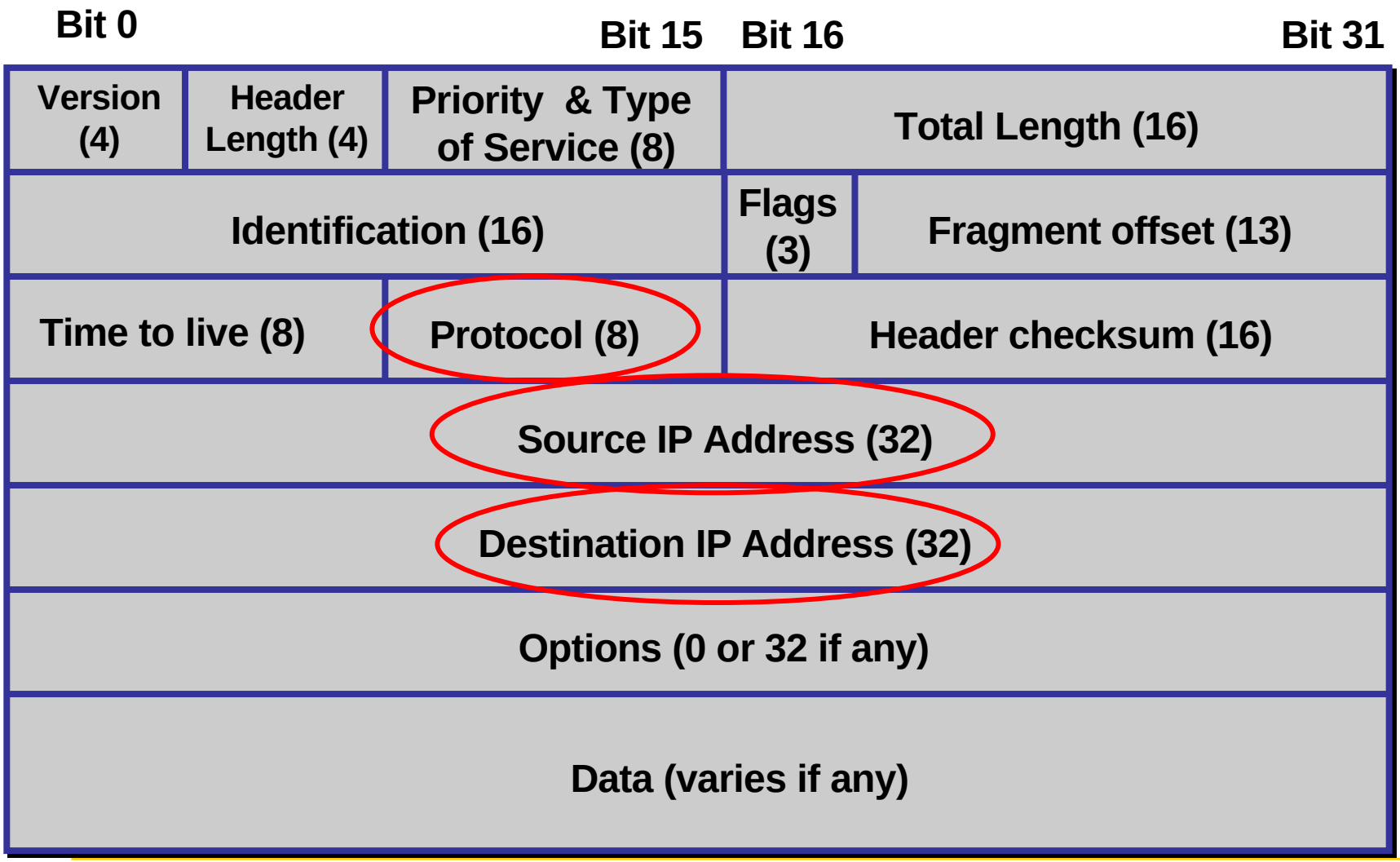
- Once upon a time Internet was built on top of the telephony network
- Now we see protocols built “on top of Internet”
- Routing is reinvented
- HTTP is a “link”
  - Better things than HTTP exists, like BEEP, but...HTTP is used just because of existence of firewalls



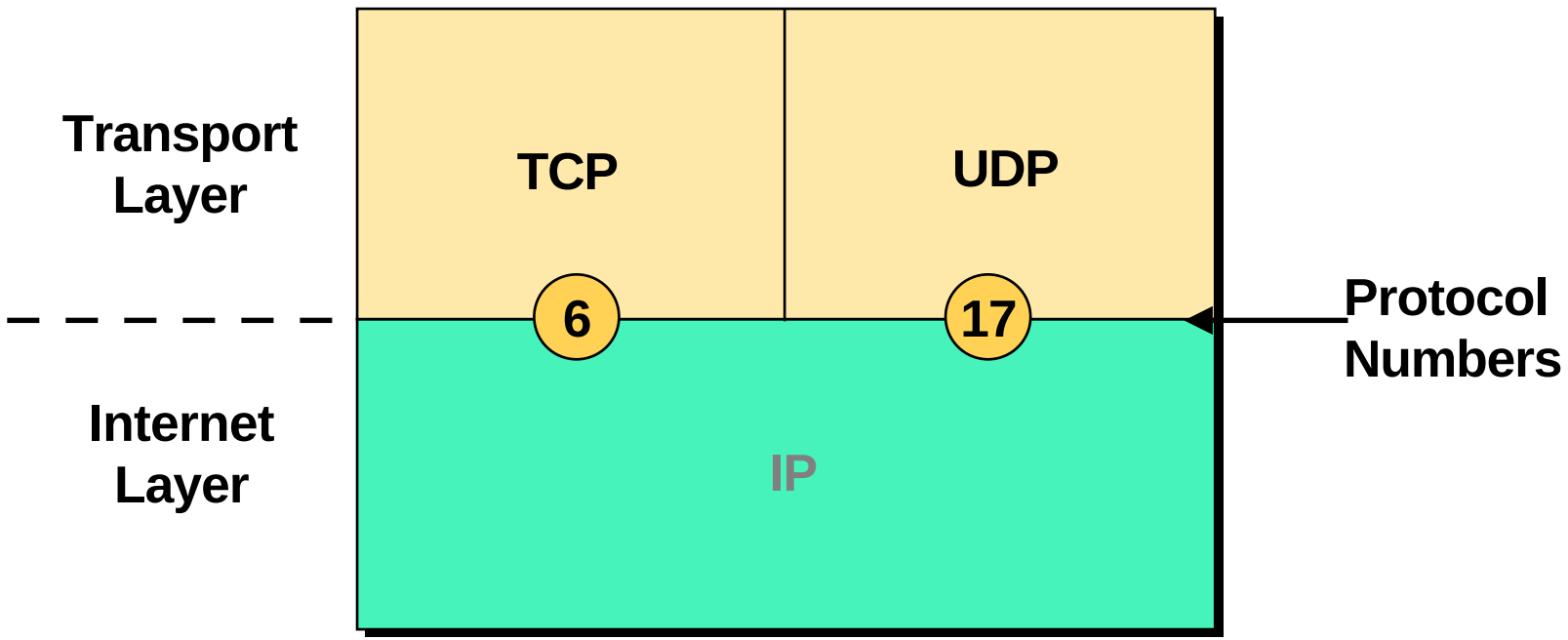
# Introduction to TCP/IP

- IP is a simple protocol (I claim)
  - Create a packet
  - Include your (sender) information
  - Add address of destination
  - Send on your local interface
  - Packet will reach destination
    - Or you will be told otherwise
- But, how does this work?

# IPv4 Datagram

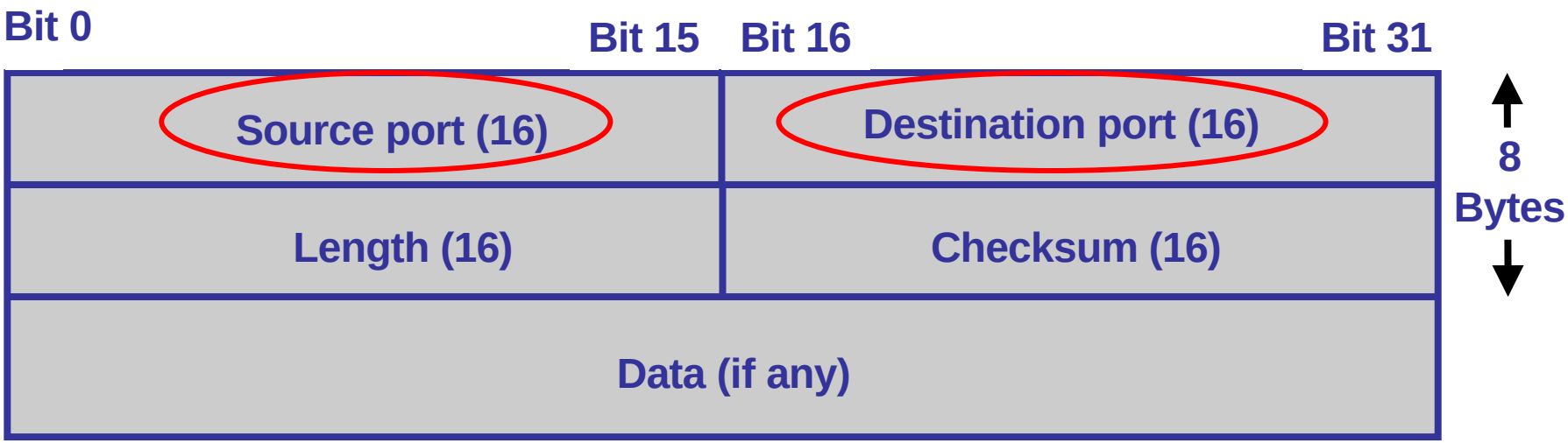


# Protocol field



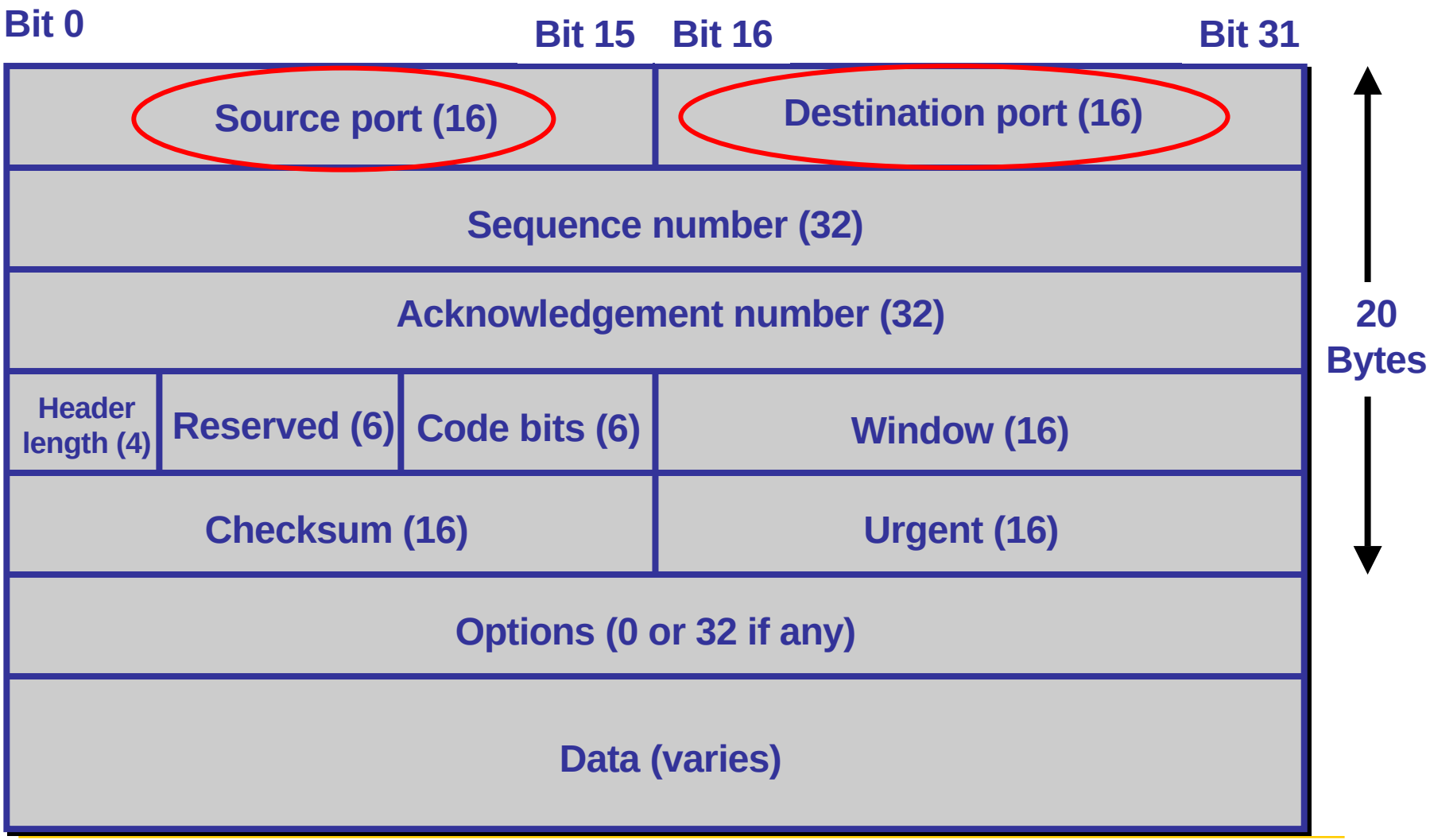

- Decide the protocol used

# UDP Segment Format

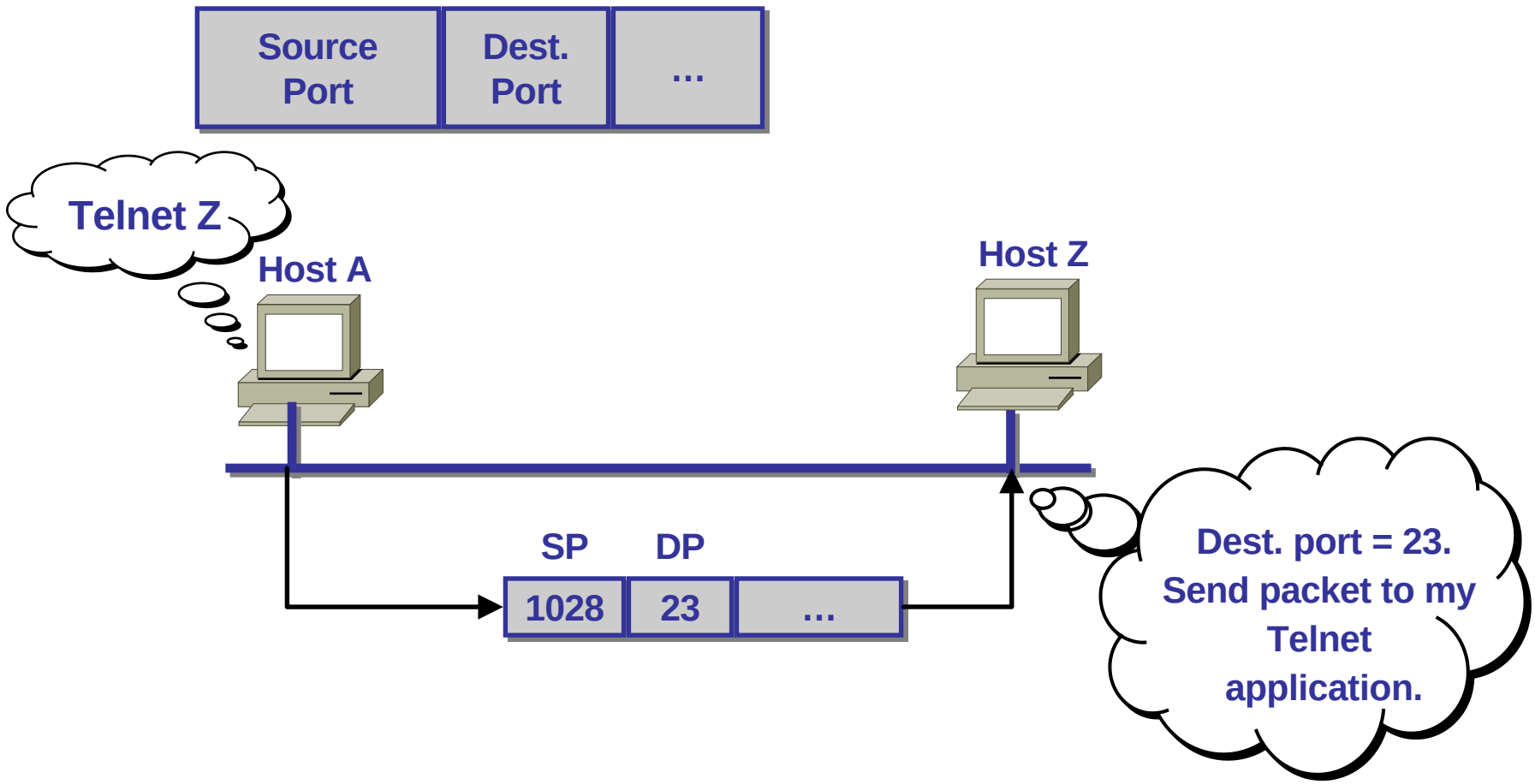



- No sequence or acknowledgment field

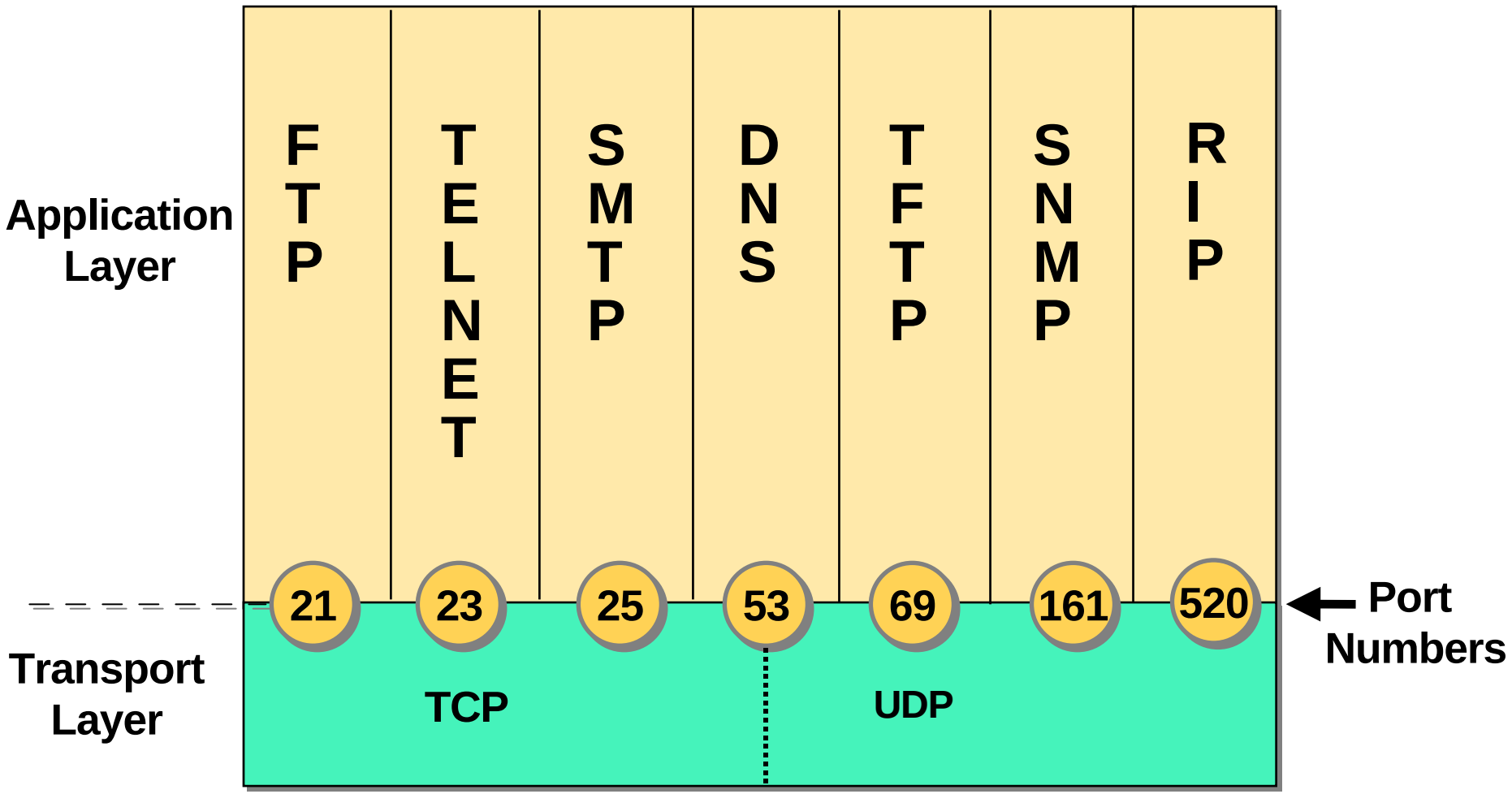
# TCP Segment Format



# Port Numbers

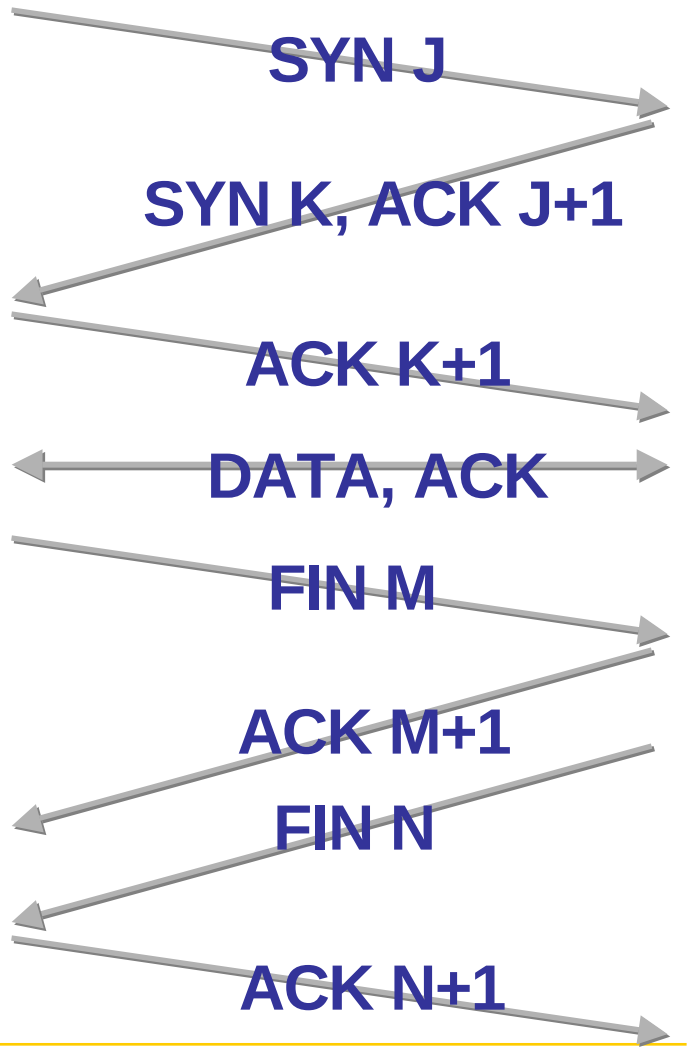


# Port numbers



# TCP

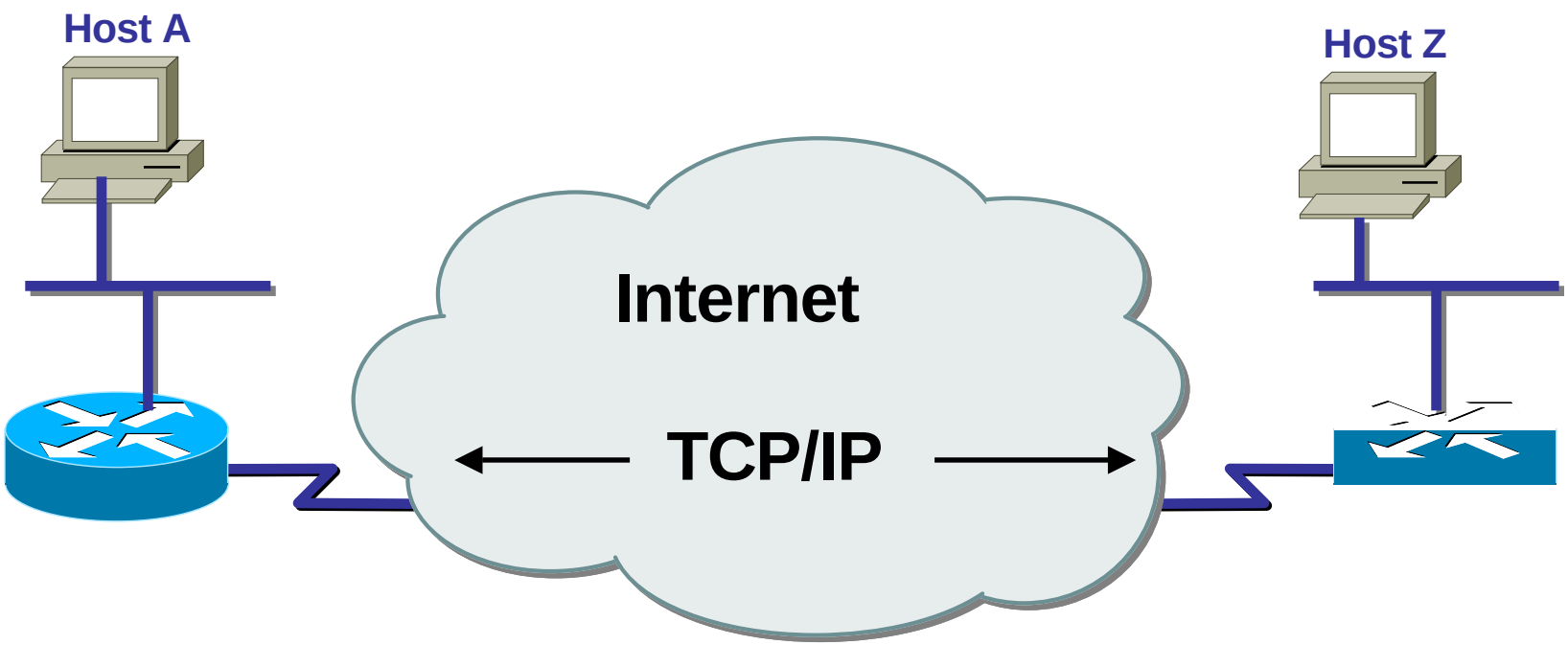
- Opening of a normal TCP session
- The famous...
  - "3-way handshake"



# A simple network

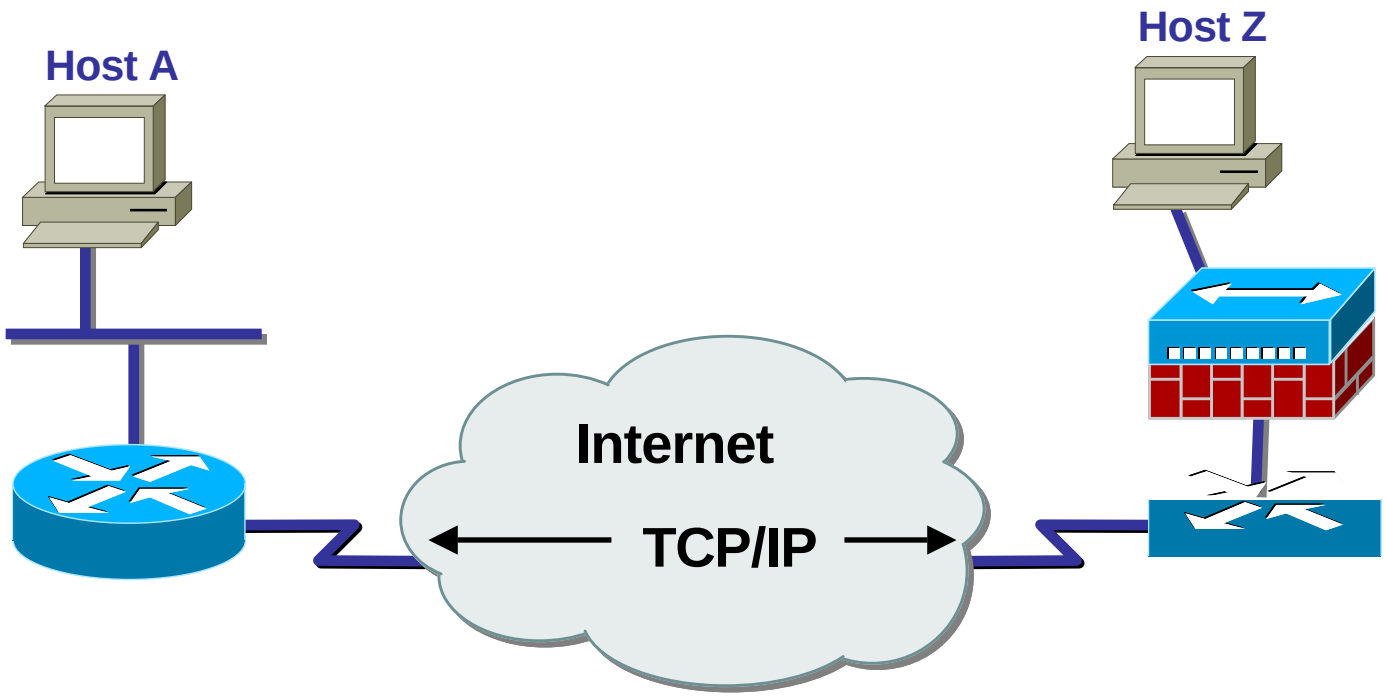

- Two hosts, connected to the same network

# More complicated?



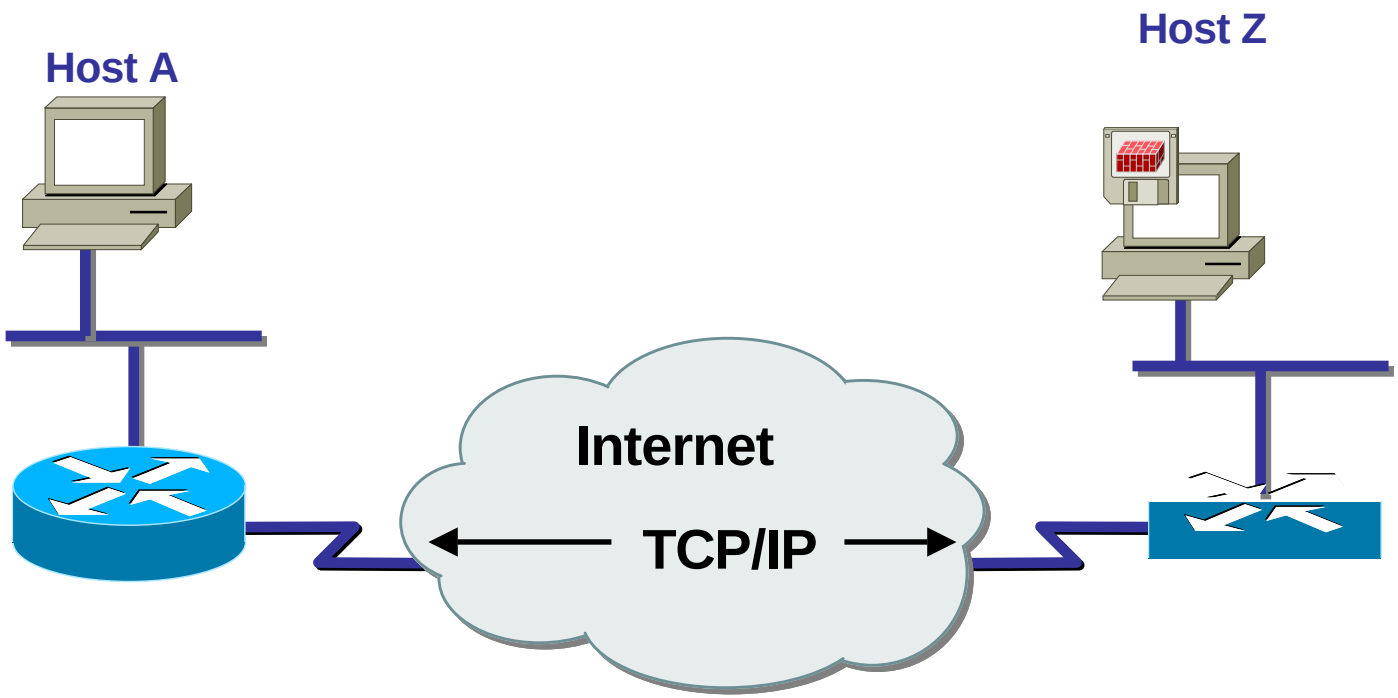

- Two hosts connected to the Internet

# With one firewall



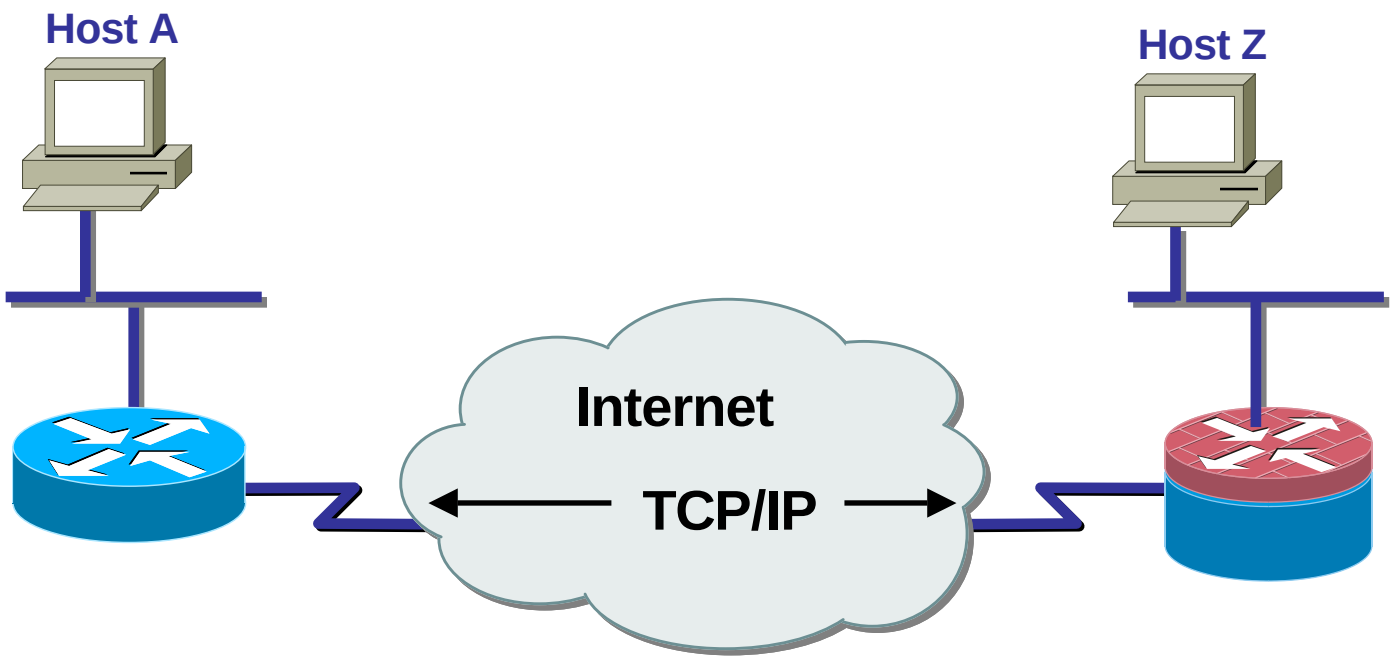

- As a feature in a local hub...

# With one firewall



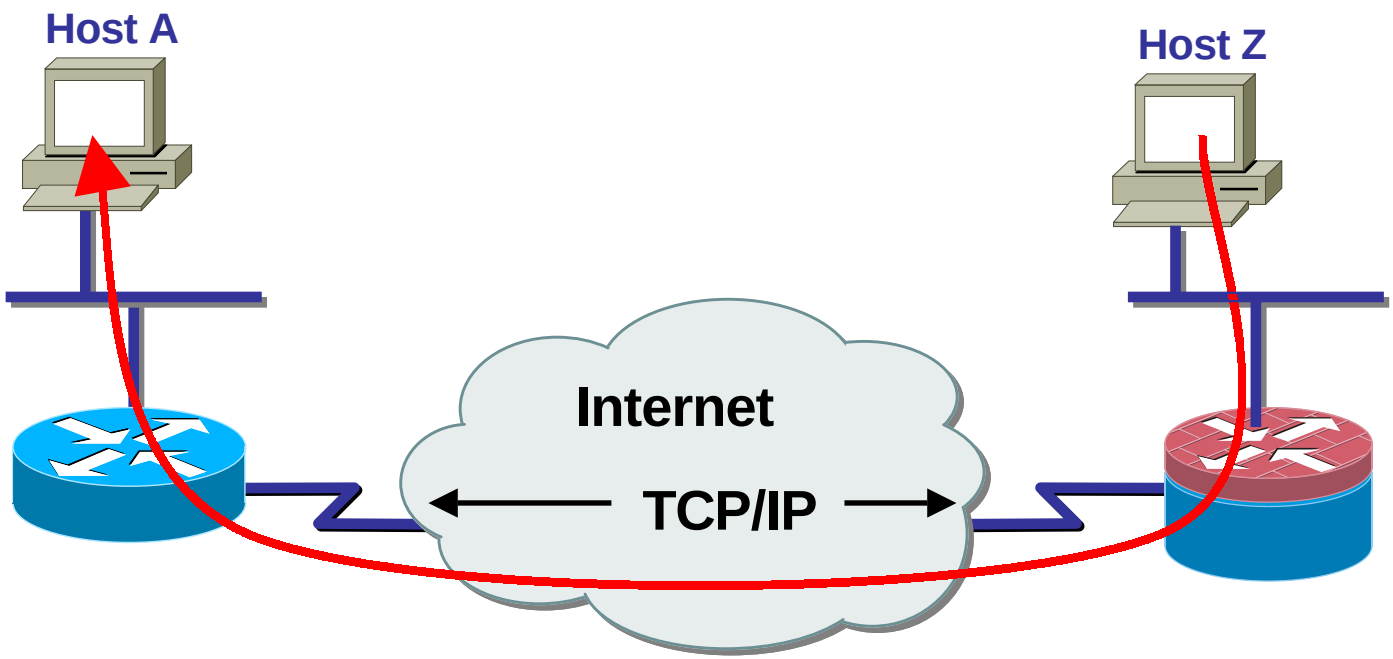

- As software in the local host...

# With one firewall



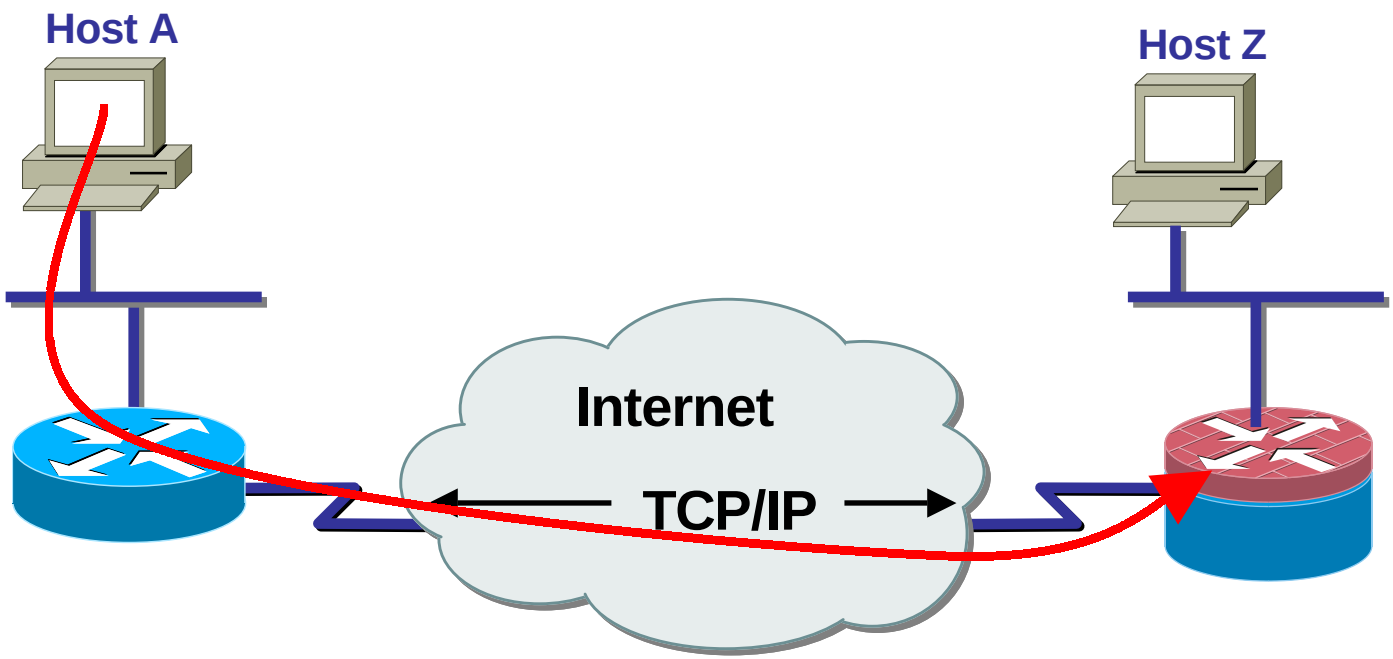

- As part of the physical attachment...

# With one firewall



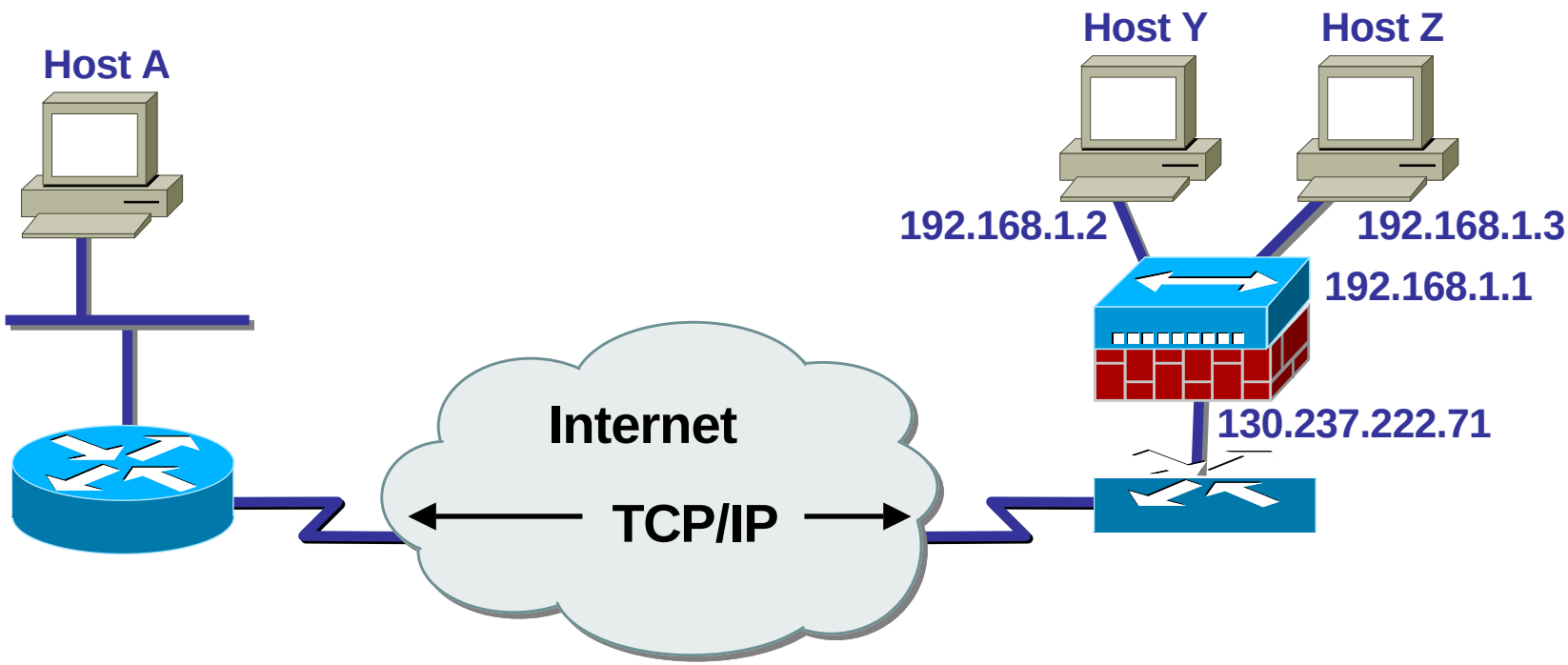

- The firewall only accepts connections initiated from the inside
- It remembers the first packet

# With one firewall




- If the first packet comes from the outside, it is blocked

# ISP give one IP address

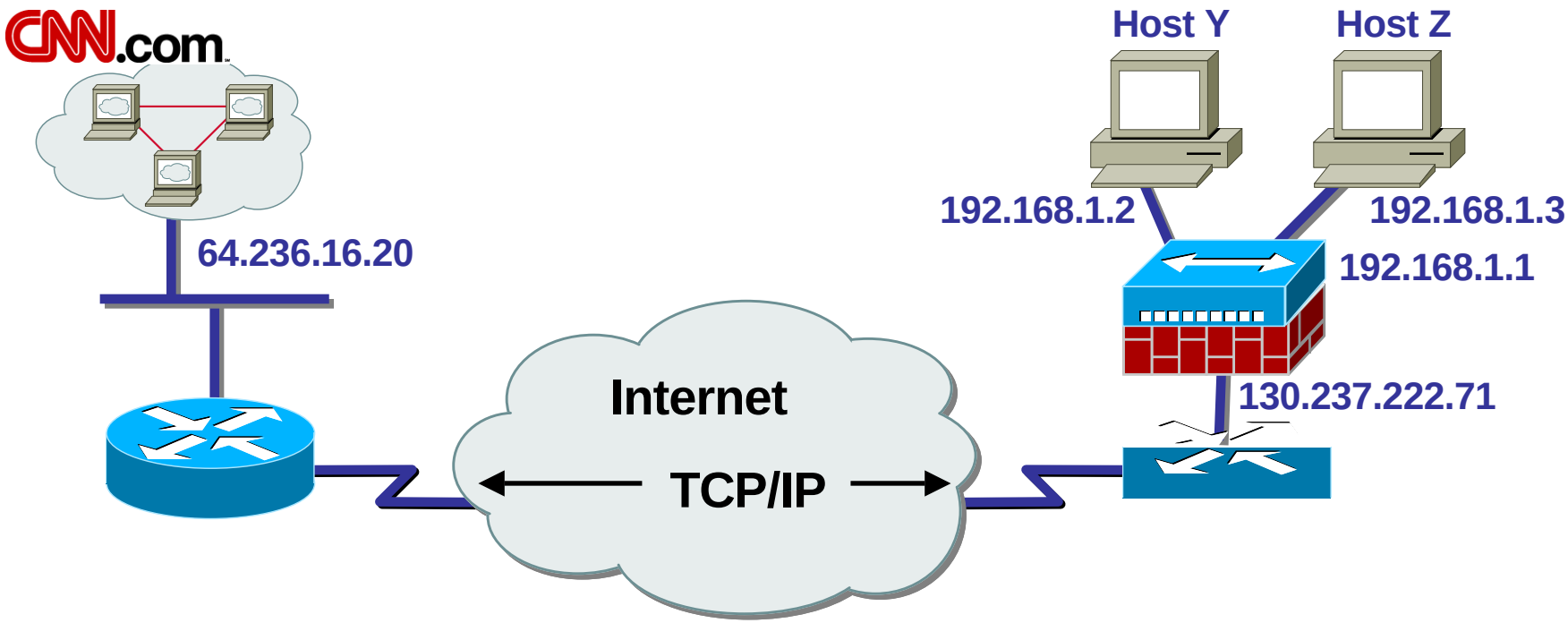



- The local NAT-box remember connections

# One Connection

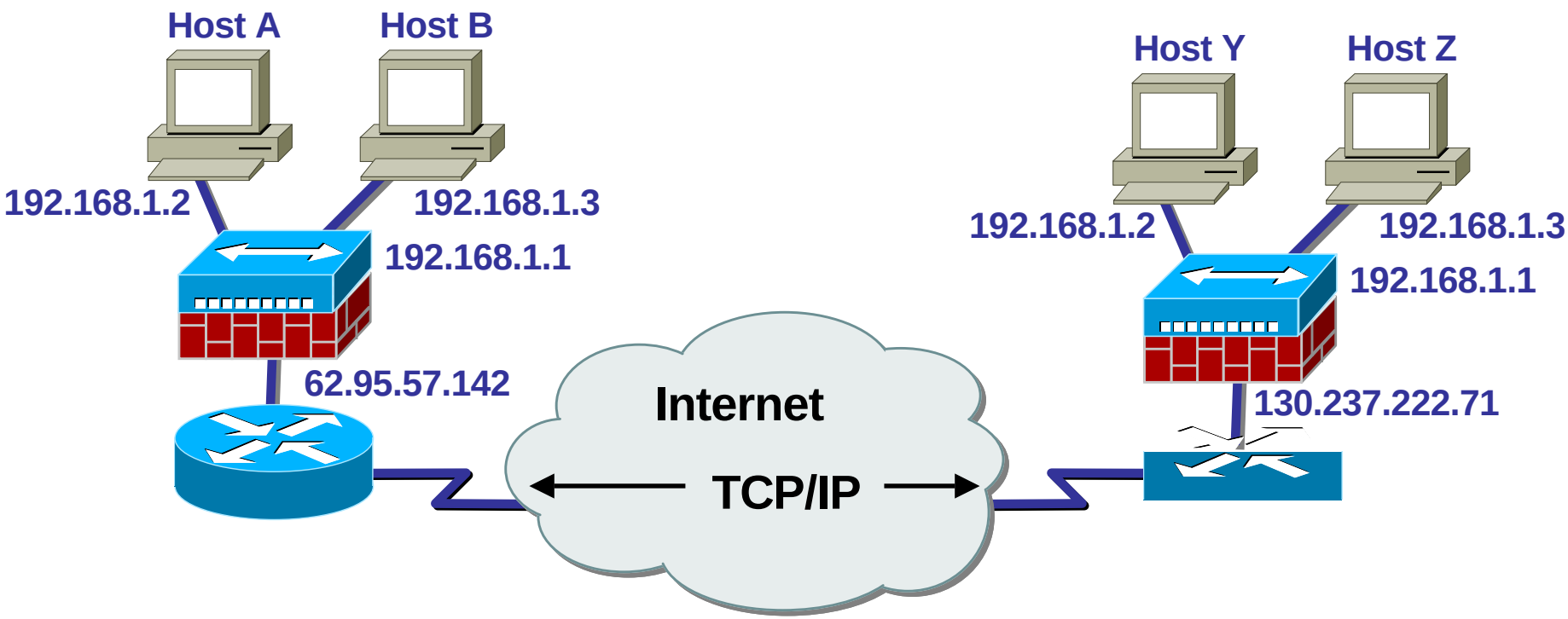
- Inside
  - Source:
    - 192.168.1.2:1027
  - Destination:
    - 64.236.16.20:80
  - Protocol:
    - TCP
- Outside
  - Source:
    - 130.237.222.71:3625
  - Destination:
    - 64.236.16.20:80
  - Protocol:
    - TCP

# This sort of works...




- When the client connects to servers

# But...




- Can host Y connect to host A?
- Only if firewall/NAT in front of A has specific (forwarding) configuration

# Configuration

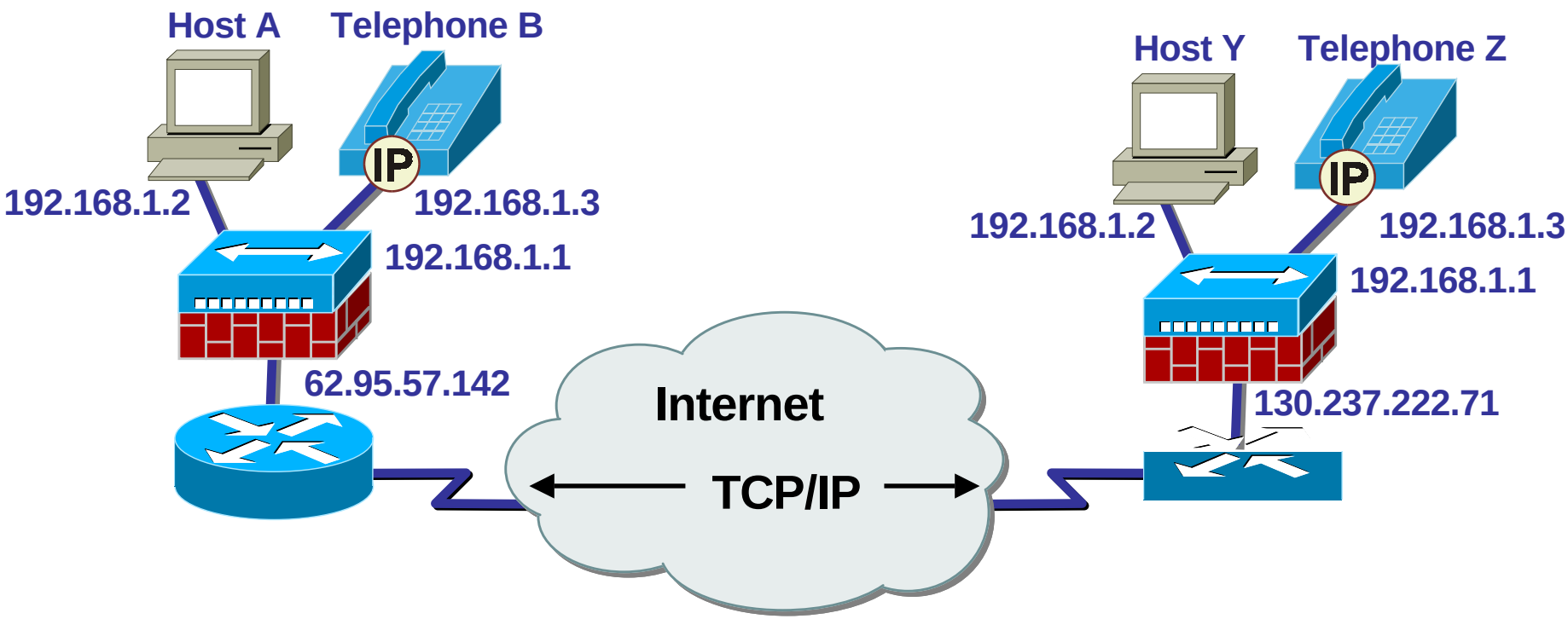
- “If connection arrives to 62.95.57.142 port 80, forward that to the inside, IP-address 192.168.1.1 port 80”

- This makes it possible to connect to A on port 80, but not B on port 80
- Y can not select A or B

# Protocols

- Both SIP and FTP protocol have one control and one data connection
- Control connection:
  - Negotiation of features
  - Commands
  - IP address and port number of Data connection
- Data connection
  - “The Meat”

# VoIP



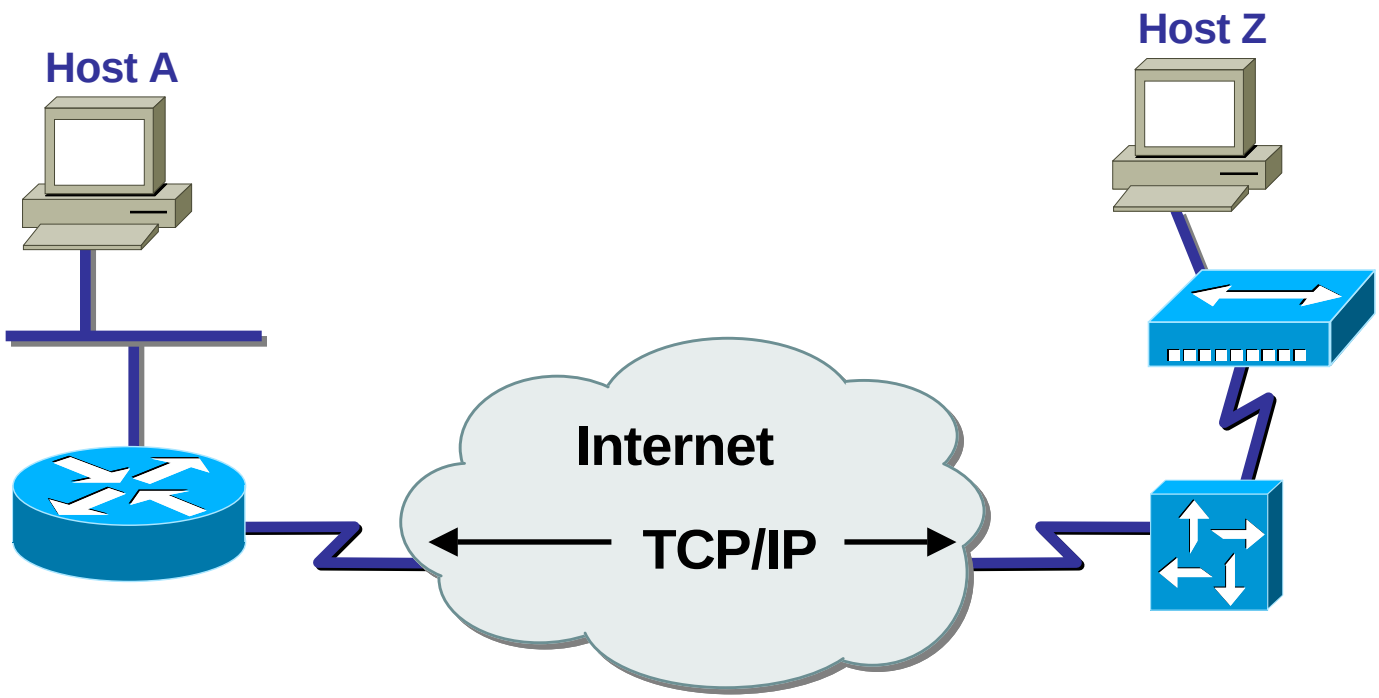

- What IP-address and port number is to be used for the actual voice call?

# Inbound signalling

- The problem with SIP and FTP is that the client doesn't know the IP-address and port number to use
- Those values are allocated in the NAT

- Current state of VoIP and "broadband" is like a cellphone where you only can make calls to some numbers (or friends which happen to have real connectivity)
- Who would buy such a phone?

# Always connected




- Not all “broadband” connections are always connected
  - PPPoE, DSL with authentication via a WEB application...

# A good design

- Internet Connection
  - Always connected
  - Routed IP-addresses
  - No filters
- People can sell other things, but, it should not be called a connection to the Internet
  - My guess is that many customers are happy with such products
- Today the market is confused
  - Create “smart” boxes...

# Remember

- Bad
  - Do “this” before you surf
  - Filter on ports
  - One address only
  - Private addresses
  - “Smart” boxes
  - NAT
- Good
  - + Always Connected
  - + No filter
  - + Public IP-addresses
  - + Transparent network
  - + Firewall is “extra”
  - + Layering
    - IP is one thing
    - Application another

# “In theory there is no difference between theory and practice, but in practice there is”

**Patrik Fältström**

**<paf@cisco.com>**