Mainframe Networking 101
Share Session 15422

Laura Knapp
WW Business Consultant
Laurak@aesclever.com
ipv6hawaii@outlook.com

Agenda

- Requirements for Communication
- What are Networking Architectures?
- Networking Architectures on System z
- z Hardware Platform Support of Network Architectures
- Networking Applications
- Security Implementations
- References

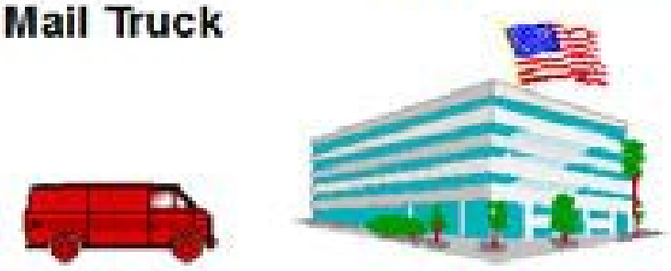
General Model for Sending Messages

- Format of a Destination address in the USA:
  - Name of Recipient
  - Street Address (Number + Name)
  - City, State
  - ZIP Code

Dead Letter Office

Post Office for ZIP Code

Mail Truck



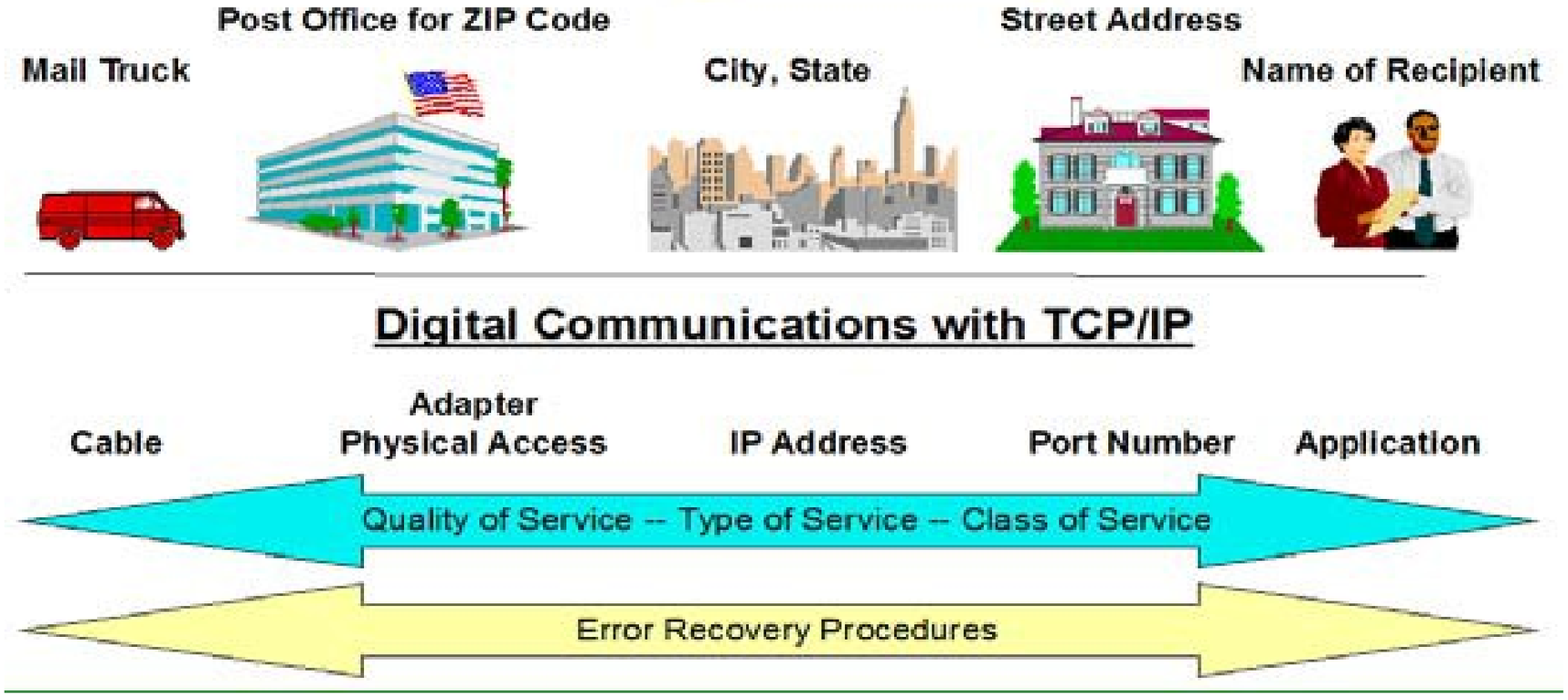
City, State

Street Address

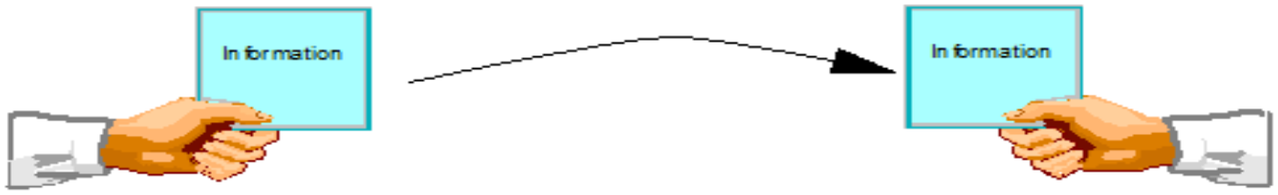
Name of Recipient

General Model for Sending Messages

- Identification of communication partners
- Rules for communicating
  - How to find the partner
  - Components of message path (Topology)
  - Type of delivery service
  - What to do in case of failed delivery



Requirements for Successful Communication



- *Connecting two entities in order to exchange information.*
  - ***How to identify and locate the opposite end?***
    Is there a name or address?
  - ***How to connect to the opposite end?***
    Can the message be sent directly or must it be transferred at intermediate stops along the way?
  - ***What are the rules to govern an orderly exchange of information?***
    What kind of service to provide to this piece of information?
    How to know that the data has been received?
    How much data should I send at once?
    How to end the communication?

- Communication Protocols
  - Naming and Addressing Conventions
  - Rules for organizing the network topology: nodes and links
  - Rules for connecting communication partners: communication setup and takedown
  - Rules for routing the information
  - Rules for managing performance on the connection

Basics Components of a Computing Platform

Laptop/Desktop/Tablet	Mainframe
CPU	CPU Specialty processors
Memory Cache Memory Disk/CD Rom Ethernet Port Serial, USB, etc Ports	Main Storage Cache Storage DASD OSA Adapter

Operating Systems
Middle Ware
Application Software
File Management
Access Methods
…..

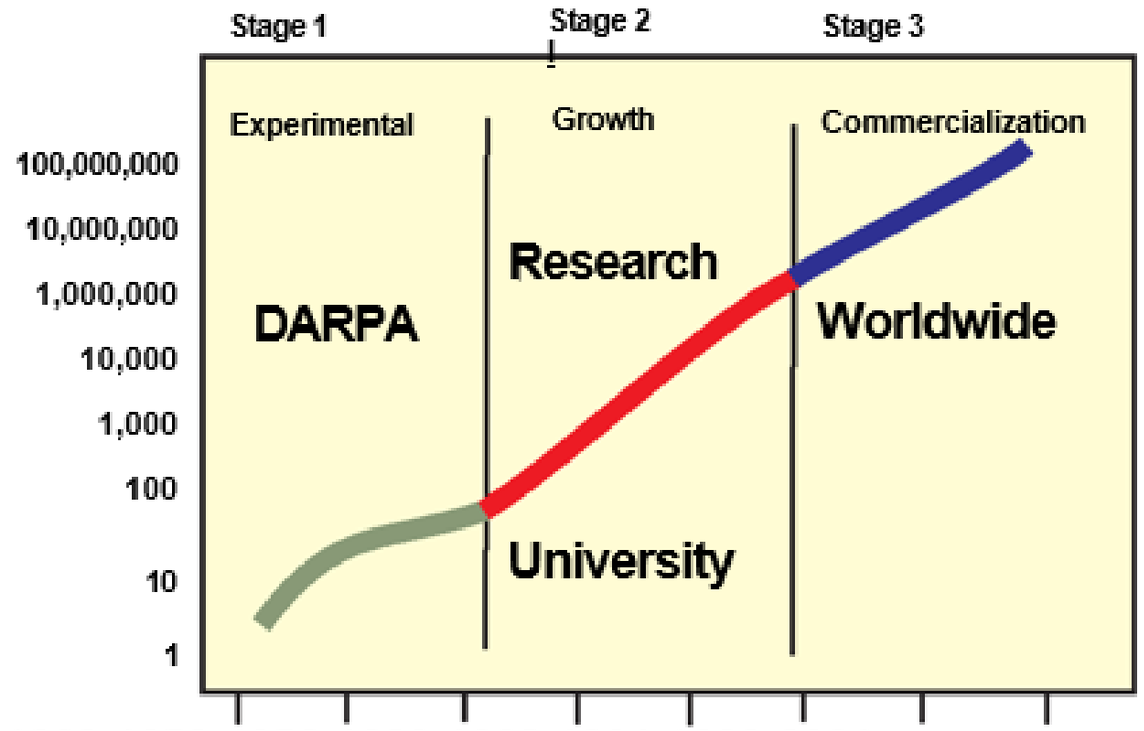
Agenda

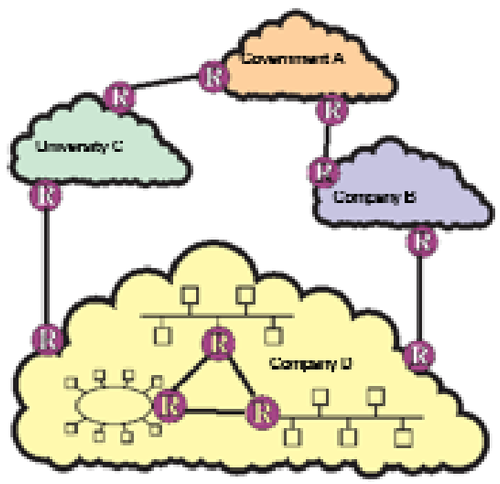
- Requirements for Communication
- What are Networking Architectures?
- Networking Architectures on System z
- z Hardware Platform Support of Network Architectures
- Networking Applications
- Security Implementations
- References

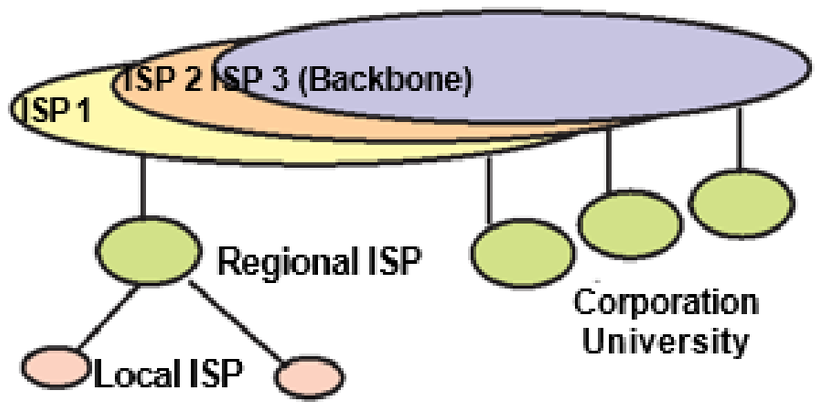
Foundations of Communications Across Networks

- **Guided by communication architectures**
  - **Pre 1995: SNA, BNA, DECnet, etc**
  - **Post 1995: TCP/IP (Transmission Control Protocol / Internet Protocol)**
- **Protocols (Controls or Rules) for Communication in General**
  - Roles of the **participants** (primary, sender, receiver, client, server, peers, etc.)
  - Rules for **starting and ending** communication
  - Rules for **identifying** hardware or software **participants**
    - (names, network IDs, addresses, etc.)
  - Rules for **locating** participants (finding a route or path between them)
  - Rules for managing the **performance** characteristics of the networking path
  - Rules for **recovering** interrupted communications
- **Controls or Rules for Communication over the Hardware Components:**
  - **Engineering and Signaling over the Data Links**
    - Channel Cables
    - Serial Cables
    - SDLC
    - Fiber Channel
    - Ethernet

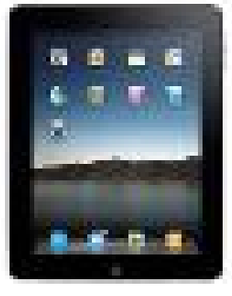
TCP/IP Networking





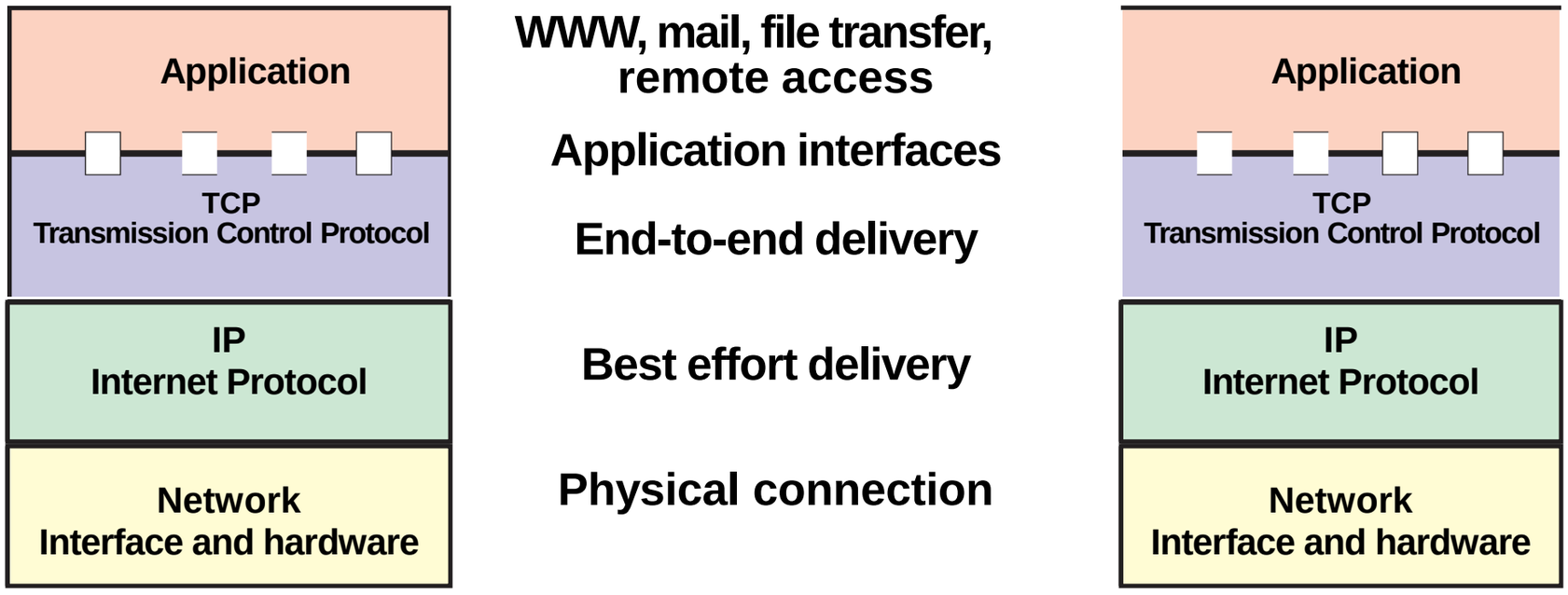


TCP/IP Layered Architecture

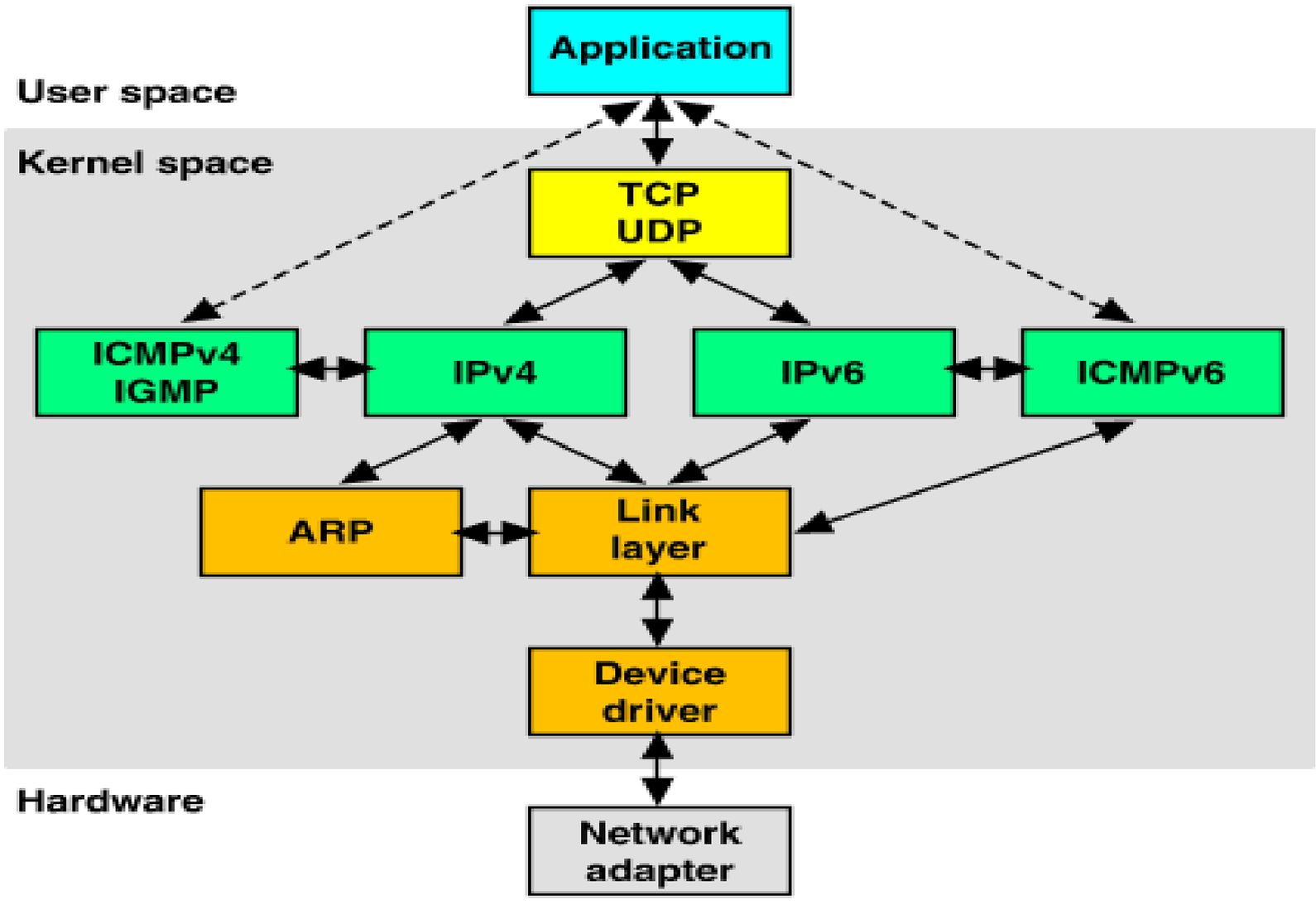


Browser

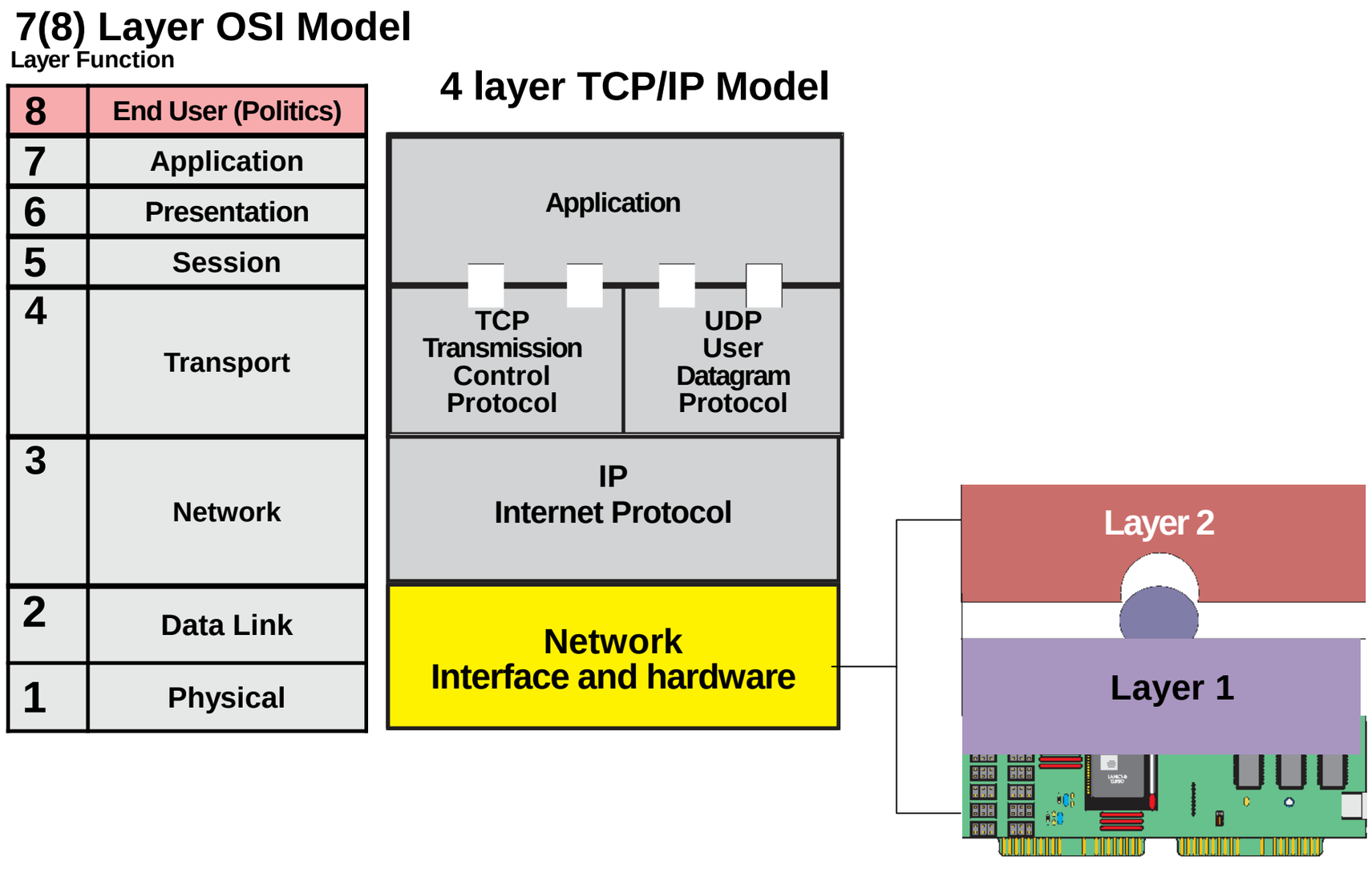
Server



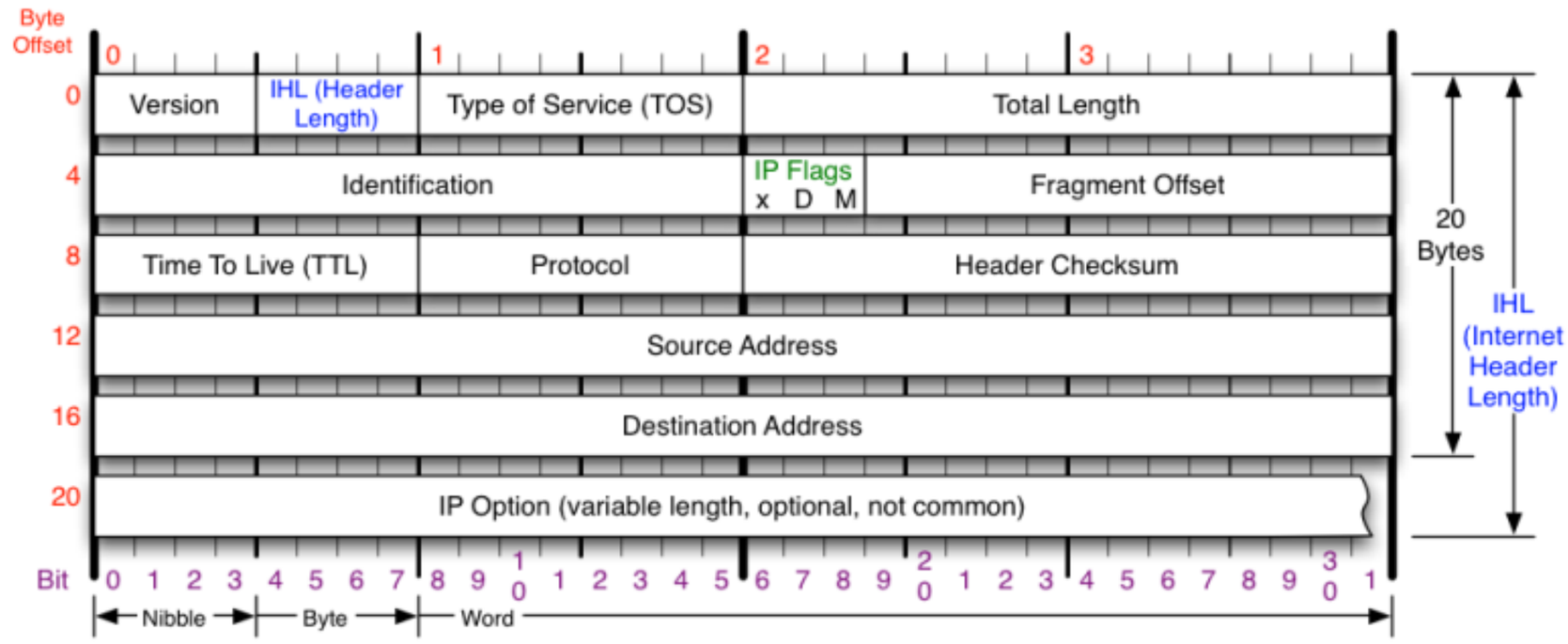
TCP/IP Stacks



TCP/IP Network Interface Layer



IP Protocol Header



Version

Version of IP Protocol. 4 and 6 are valid. This diagram represents version 4 structure only.

Header Length

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

Protocol

IP Protocol ID. Including (but not limited to):

1 ICMP	17 UDP	57 SKIP
2 IGMP	47 GRE	88 EIGRP
6 TCP	50 ESP	89 OSPF
9 IGRP	51 AH	115 L2TP

Total Length

Total length of IP datagram, or IP fragment if fragmented. Measured in Bytes.

Fragment Offset

Fragment offset from start of IP datagram. Measured in 8 byte (2 words, 64 bits) increments. If IP datagram is fragmented, fragment size (Total Length) must be a multiple of 8 bytes.

Header Checksum

Checksum of entire IP header

IP Flags

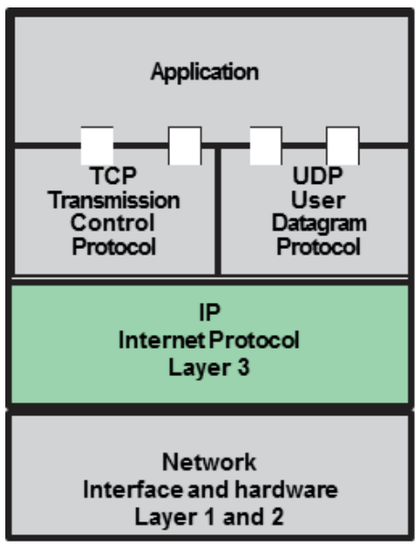
x D M

x 0x80 reserved (evil bit)
D 0x40 Do Not Fragment
M 0x20 More Fragments follow

RFC 791

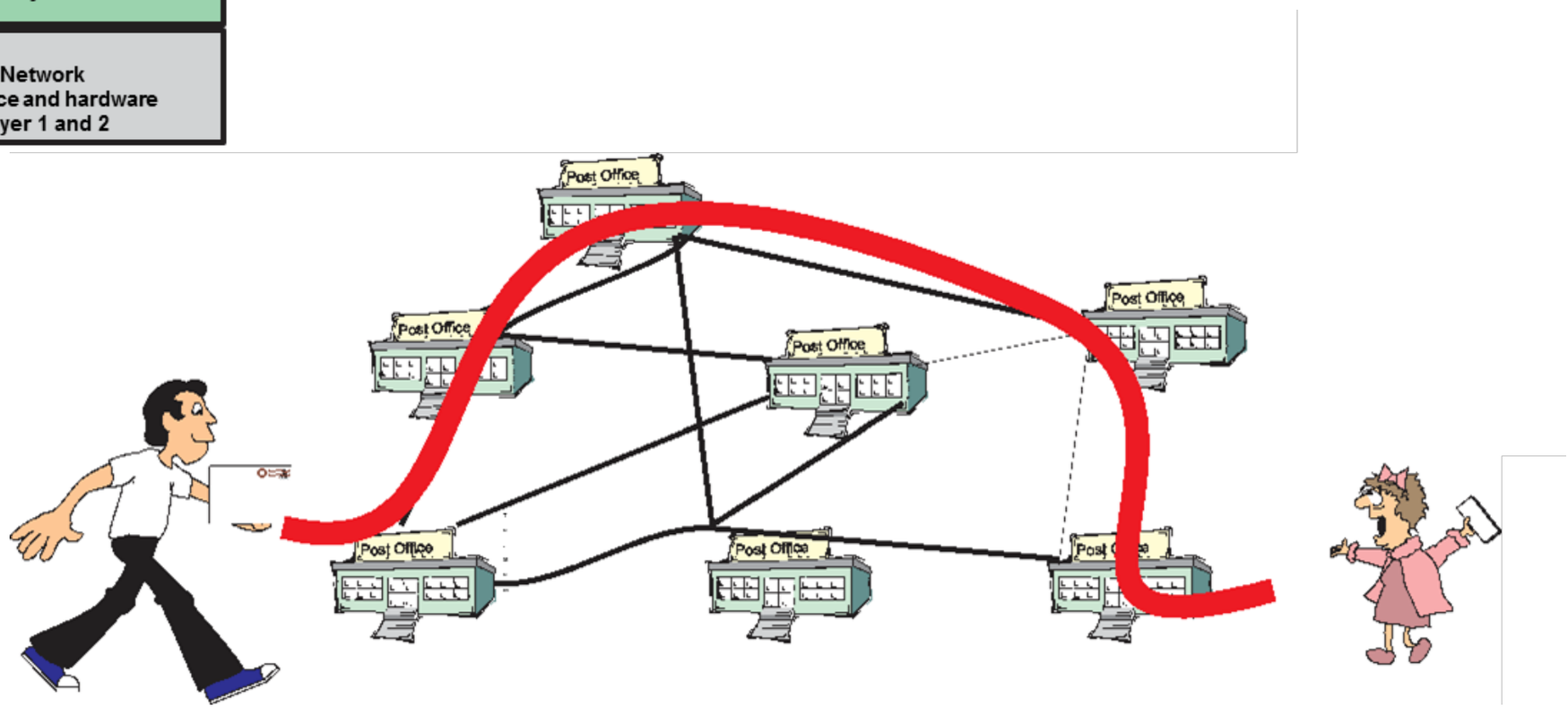
Please refer to RFC 791 for the complete Internet Protocol (IP) Specification.

IP Flows

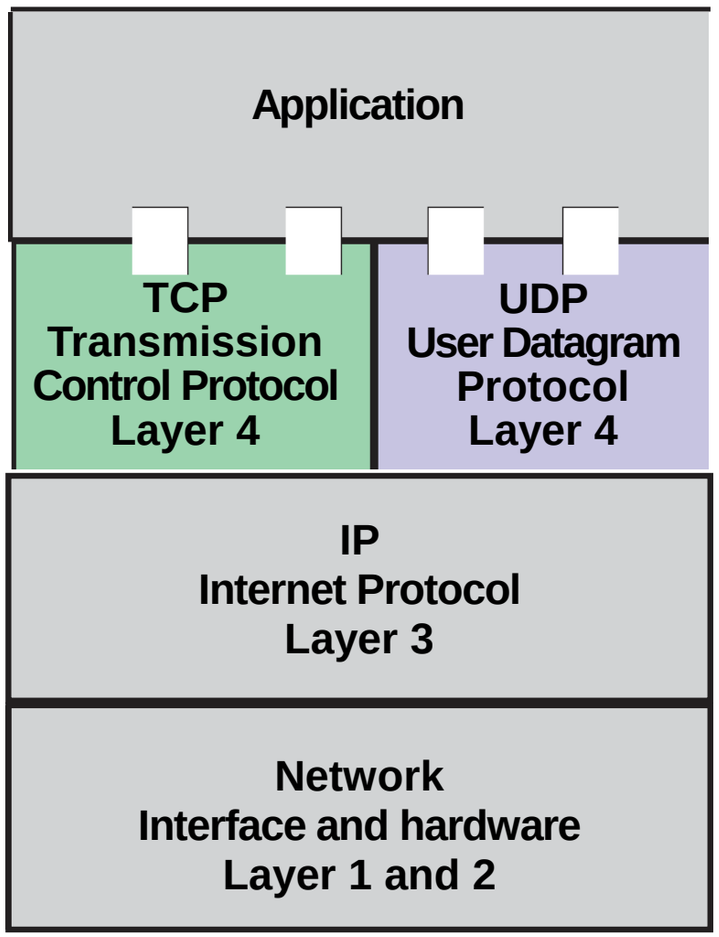


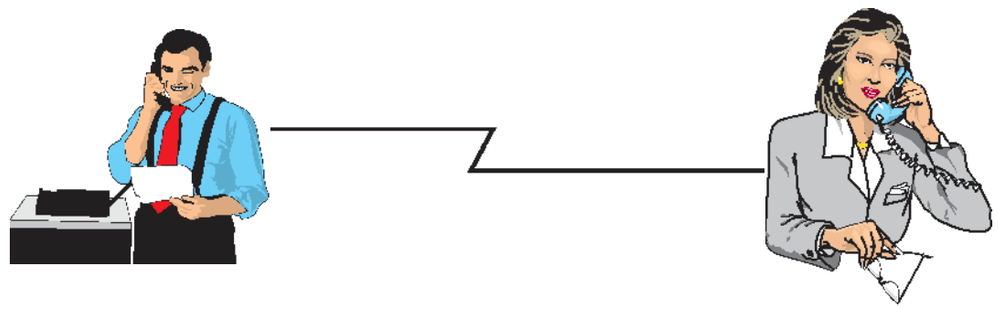
Dynamic path selection for every datagram

Handles datagram fragmentation & reassembly



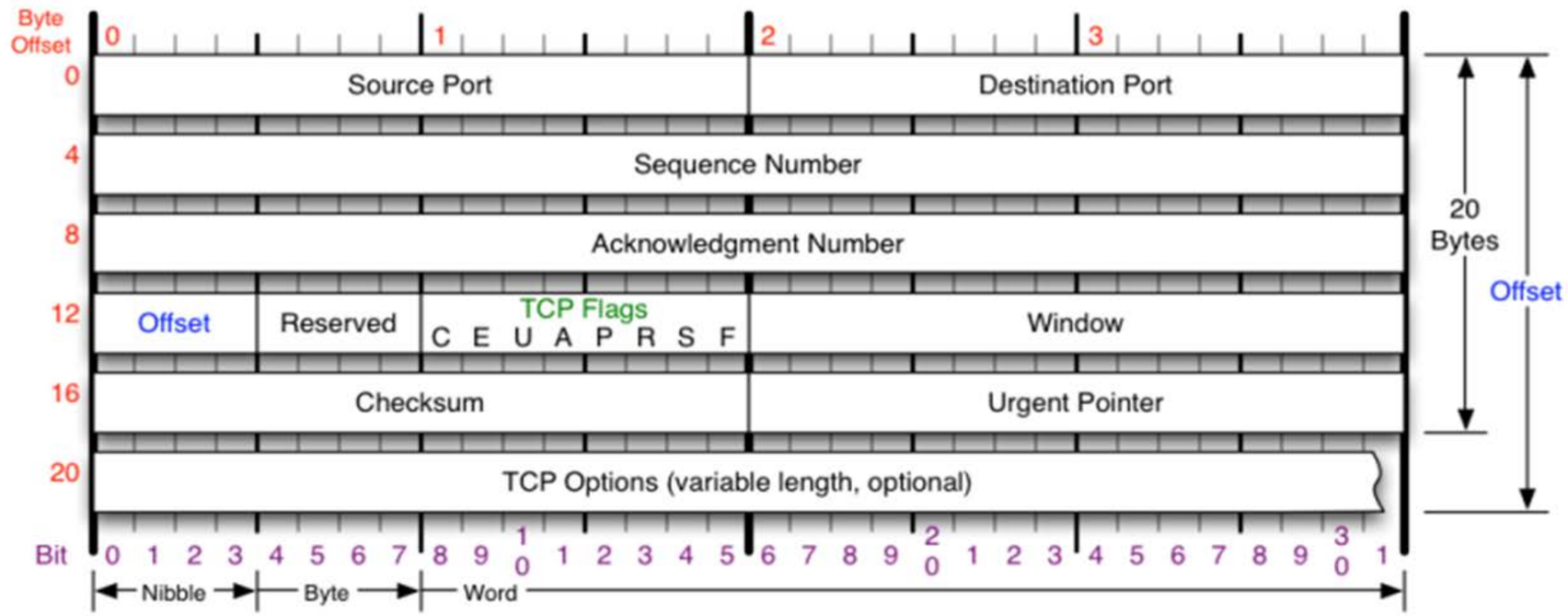
TCP Flows





- Connection established
- End-to-end acknowledgments
- Orderly delivery of datagrams to application
- Error and flow control
- Connection takedown

TCP Segment



TCP Flags

C E U A P R S F

Congestion Window
C 0x80 Reduced (CWR)
E 0x40 ECN Echo (ECE)
U 0x20 Urgent
A 0x10 Ack
P 0x08 Push
R 0x04 Reset
S 0x02 Syn
F 0x01 Fin

Congestion Notification

ECN (Explicit Congestion Notification). See RFC 3168 for full details, valid states below.

Packet State	DSB	ECN bits
Syn	0 0	1 1
Syn-Ack	0 0	0 1
Ack	0 1	0 0
No Congestion	0 1	0 0
No Congestion	1 0	0 0
Congestion	1 1	0 0
Receiver Response	1 1	0 1
Sender Response	1 1	1 1

TCP Options

0 End of Options List
1 No Operation (NOP, Pad)
2 Maximum segment size
3 Window Scale
4 Selective ACK ok
8 Timestamp

Checksum

Checksum of entire TCP segment and pseudo header (parts of IP header)

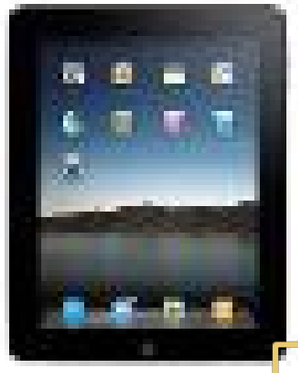
Offset

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

RFC 793

Please refer to RFC 793 for the complete Transmission Control Protocol (TCP) Specification.

TCP Connection Setup – Three Way Handshake



Client

Server

Socket

Connect
Let's Talk
SYN-SENT

SYN
Seq Num = 3557
ACK Num = 0

Socket
Bind
Listen
LISTEN

ACK/SYN
ACK Num = 3558
Seq Num = 91248

OK, Let's Talk
SYN-RCVD

Thanks!
ESTABLISHED

ACK
ACK Num = 91249

Accept
Conversation
Established
ESTABLISHED

TCP Connection Close

Client

Server

FIN

Ok!
FIN-WAIT2

OK!
CLOSE-WAIT

ACK

Wait

Hey, Application, We're Shutting down!
LAST-ACK

You're done!

FIN

OK!
TIME-WAIT

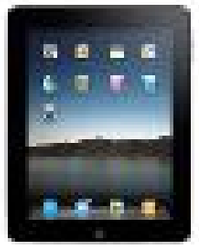
ACK

OK, Goodbye
CLOSED

Connection Closed

Connection Closed

TCP Acknolodgements

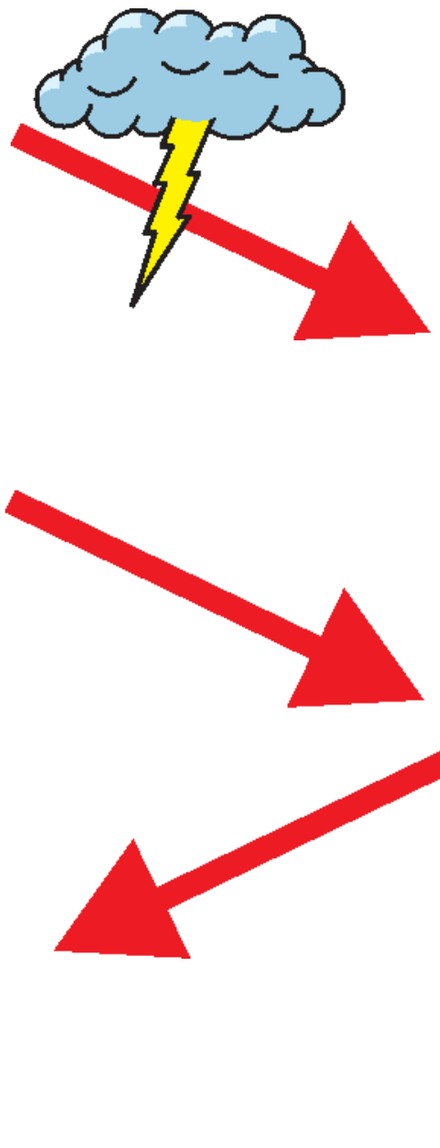


Host A

Sends datagram
Starts timer

Acknowledgment
was not received

Timer expires
and datagram retransmitted

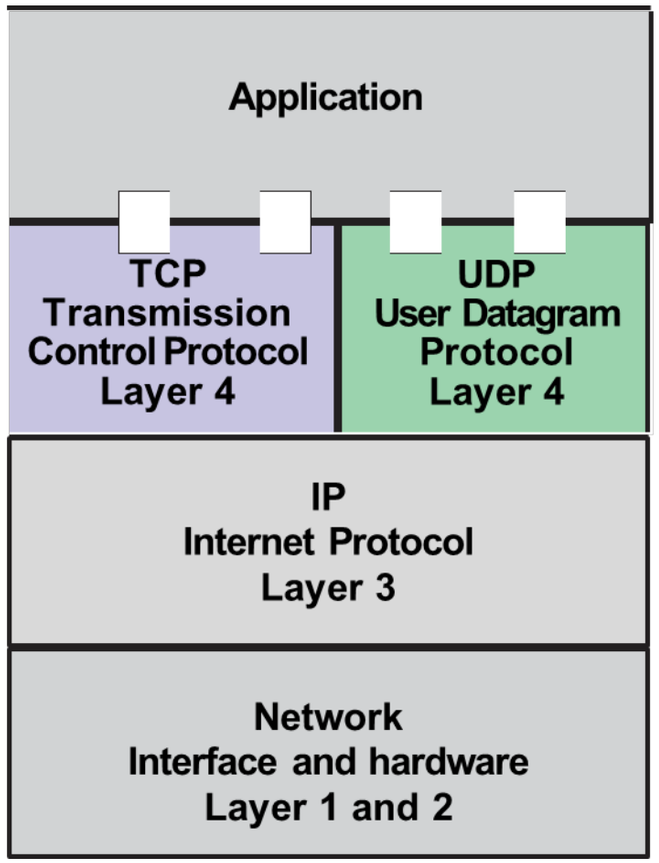


Host B receives datagram
and acknowledges receipt

Host A receives acknowledgment,
resets timer, and clears buffer

Host B

UDP – User Datagram Protocol

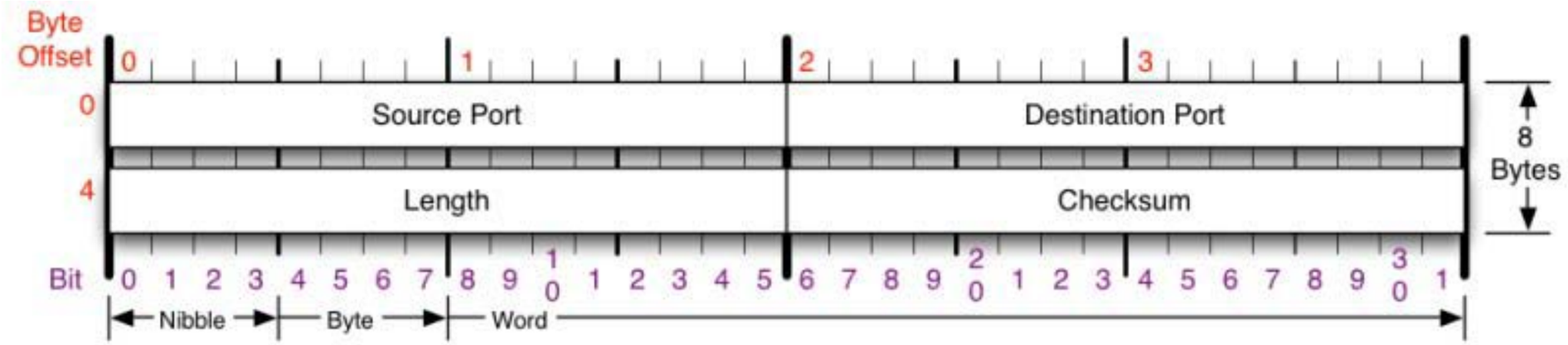


Program to program datagram transfer

Fast mechanism

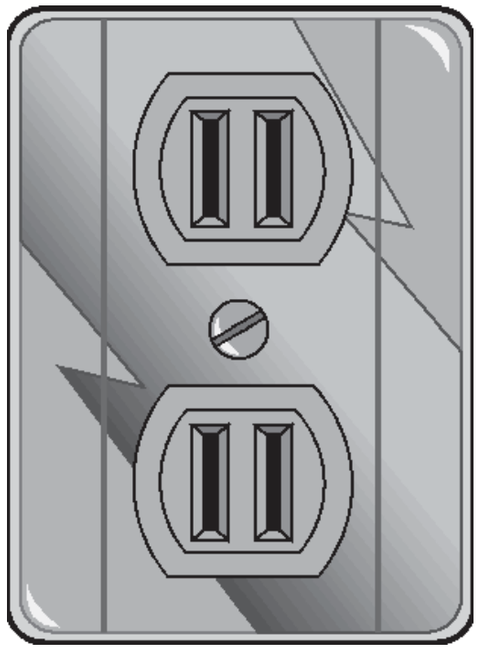
Used for management frames, streaming audio

UDP Header



Checksum	RFC 768
Checksum of entire UDP segment and pseudo header (parts of IP header)	Please refer to RFC 768 for the complete User Datagram Protocol (UDP) Specification.

TCP/IP Sockets/Ports



Sockets

Network I/O for UNIX
Library of C routines
Berkeley UNIX (BSD) API

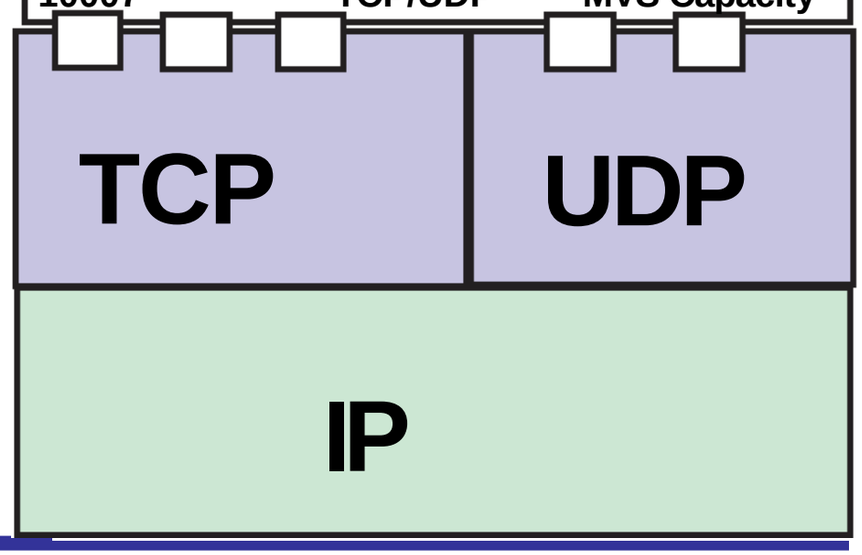
Also called Ports
Well known 0 – 1023
Registered 1024 – 49151
Dynamic 49152 - 65535
(also called Private)

Application address

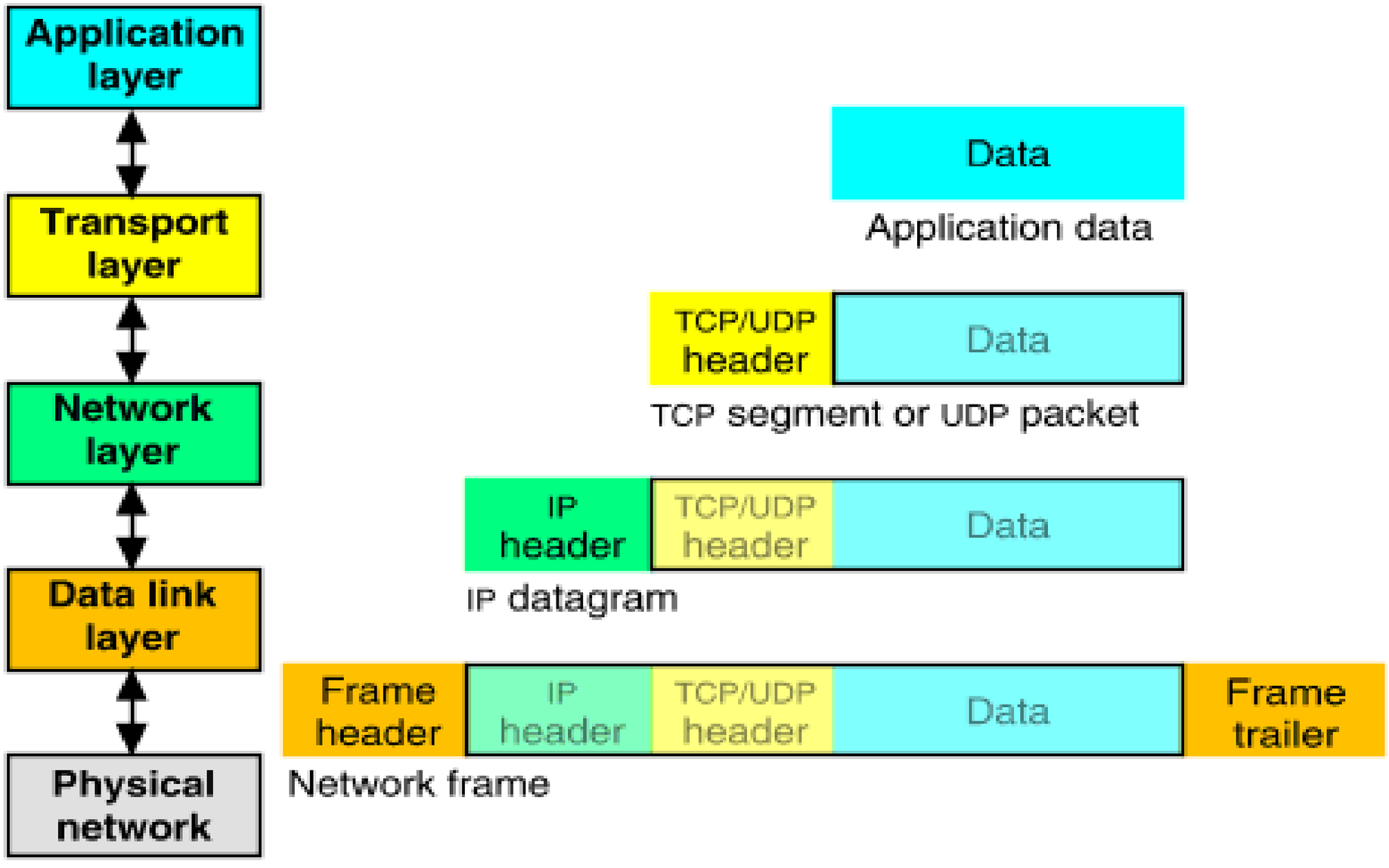
IP Address
Protocol (TCP or UDP)
Port Number

Application code

Port Number	Protocol	Application
20	TCP	FTP-data
21	TCP	FTP-control
23	TCP	Telnet
25	TCP	SMTP
53	TCP/UDP	DNS
70	TCP	Gopher
79	TCP	Finger
80	TCP	HTTP
110	TCP	POP3
161	UDP	SNMP
162	UDP	SNMP-trap
520	UDP	RIP
1435	TCP/UDP	IBM CICS
1525	TCP/UDP	Oracle
10007	TCP/UDP	MVS Capacity



Encapsulation of Application Data



Source: http://uw713doc.sco.com/en/NET_tcpip/tcpN.tcpip_stack.html

IP Addressing

IP address is 32 bits long

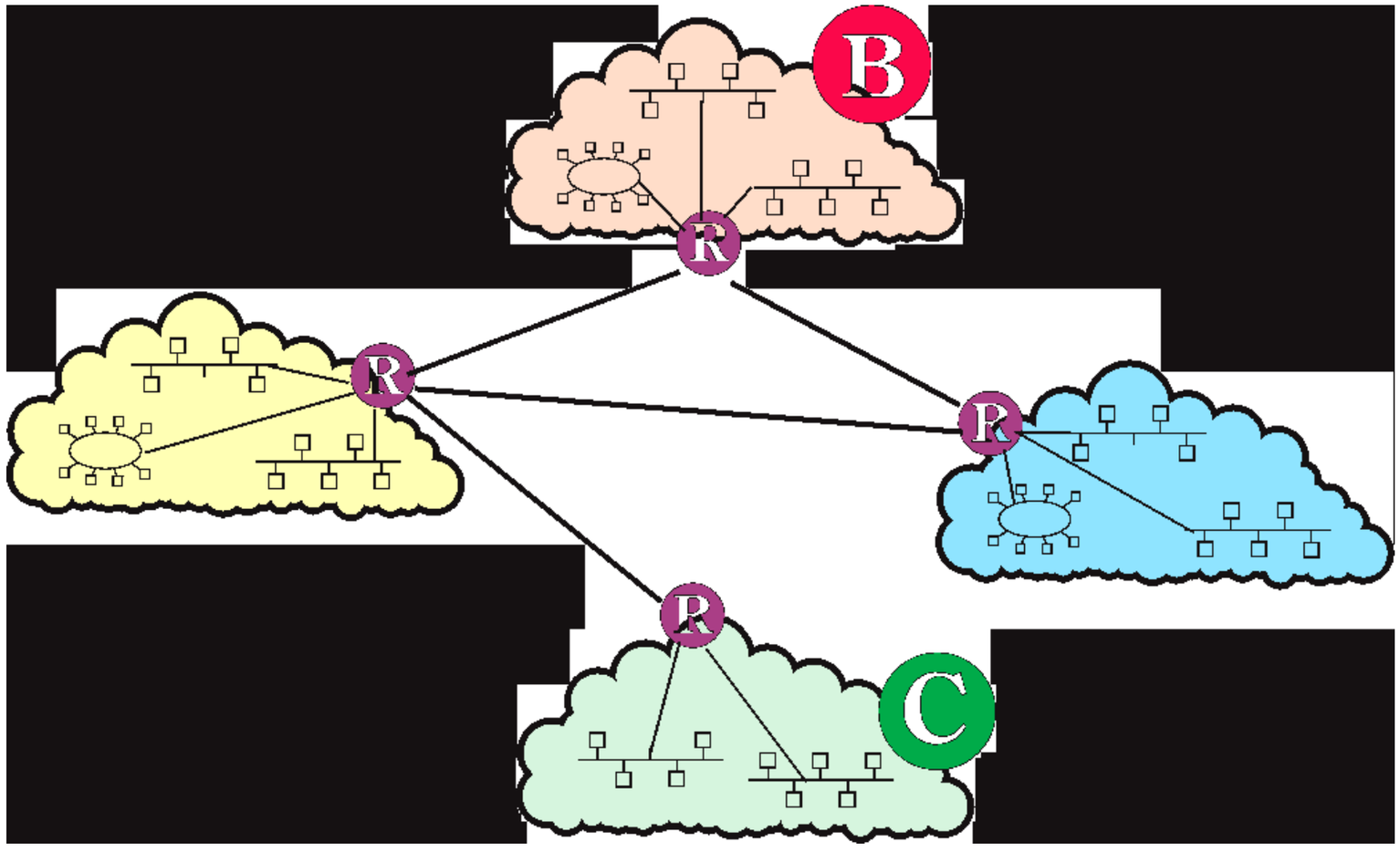
Expressed as 4 decimal numbers

Format: 24.25.20.137

Your Network = 192.168..0

Your Computer = 192.168.100.24

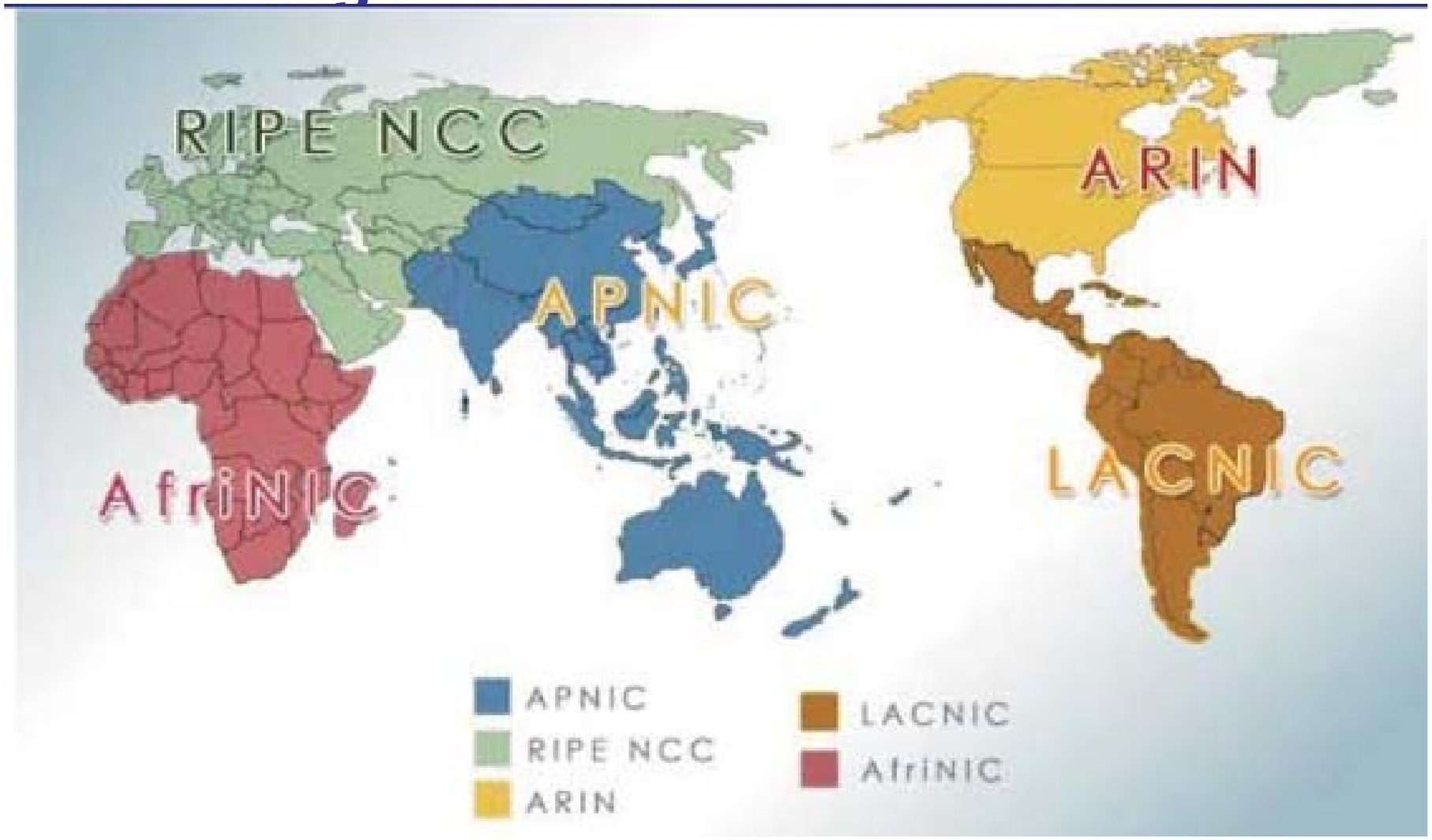
Your home router = 192.168.1.1/24.25.20.137



Network = 66.0.0.0

lauraknapp.com = 66.175.58.9

IP Address Assignment



Public network addresses originally assigned to using organizations

Today regional authority assigns to Internet Service Providers (ISPs)

Network Address Translation

Hides internal addresses and systems
From outsiders

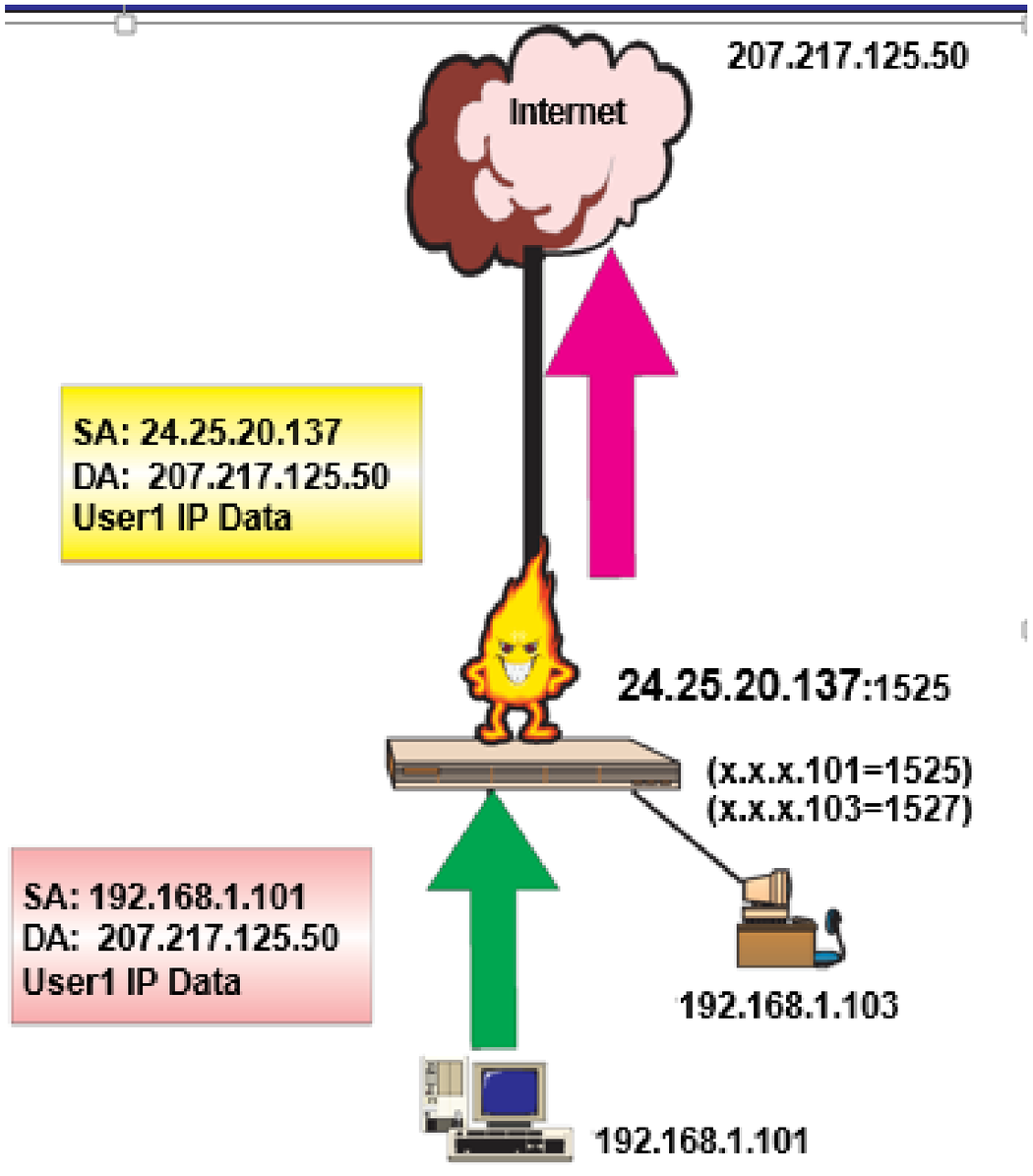
Use private IP address internally

Everything appears to be coming from the firewall

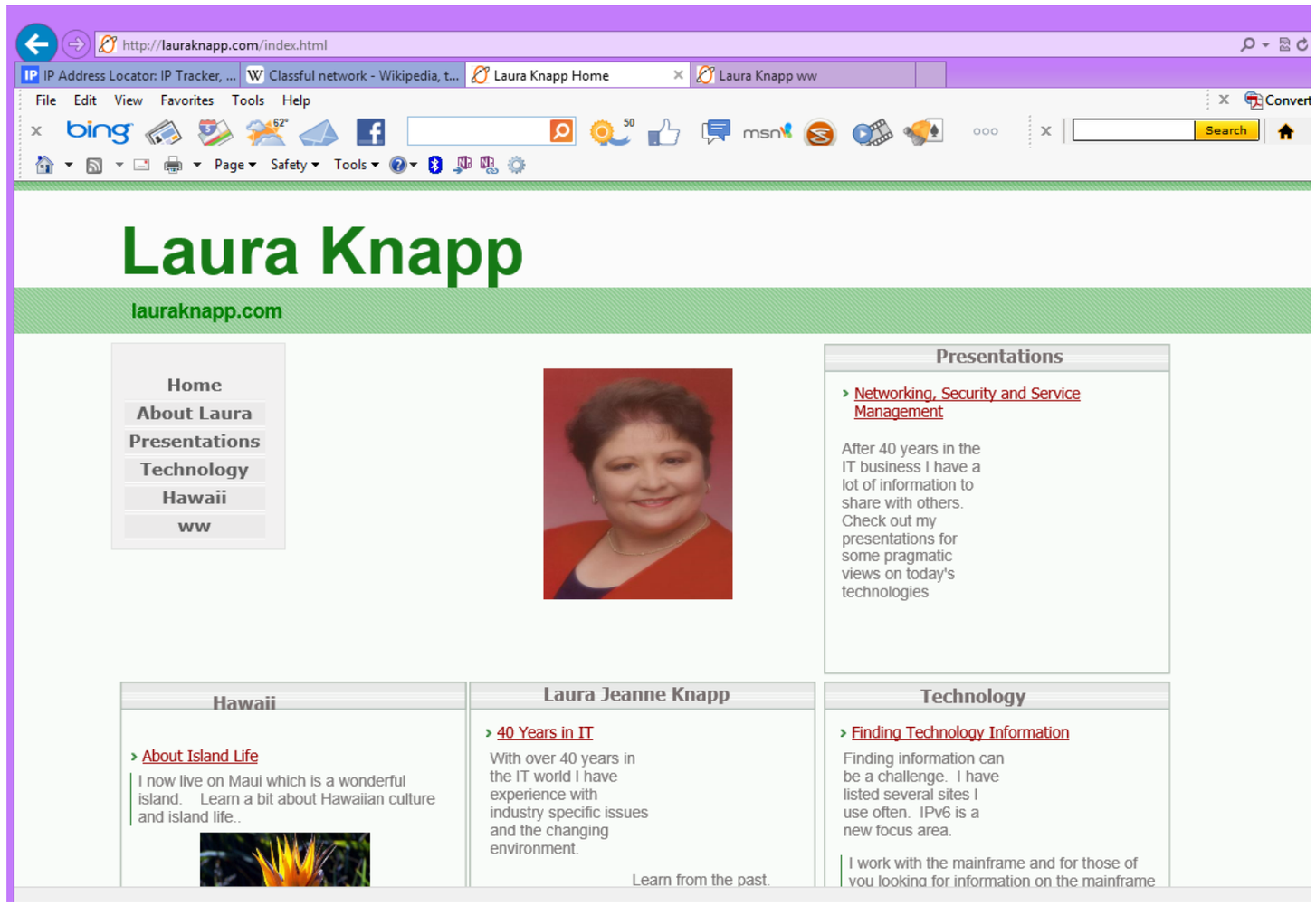
High performance

Transparent to clients

Configuration options on mapping internal to
External addresses implemented in firewall or router

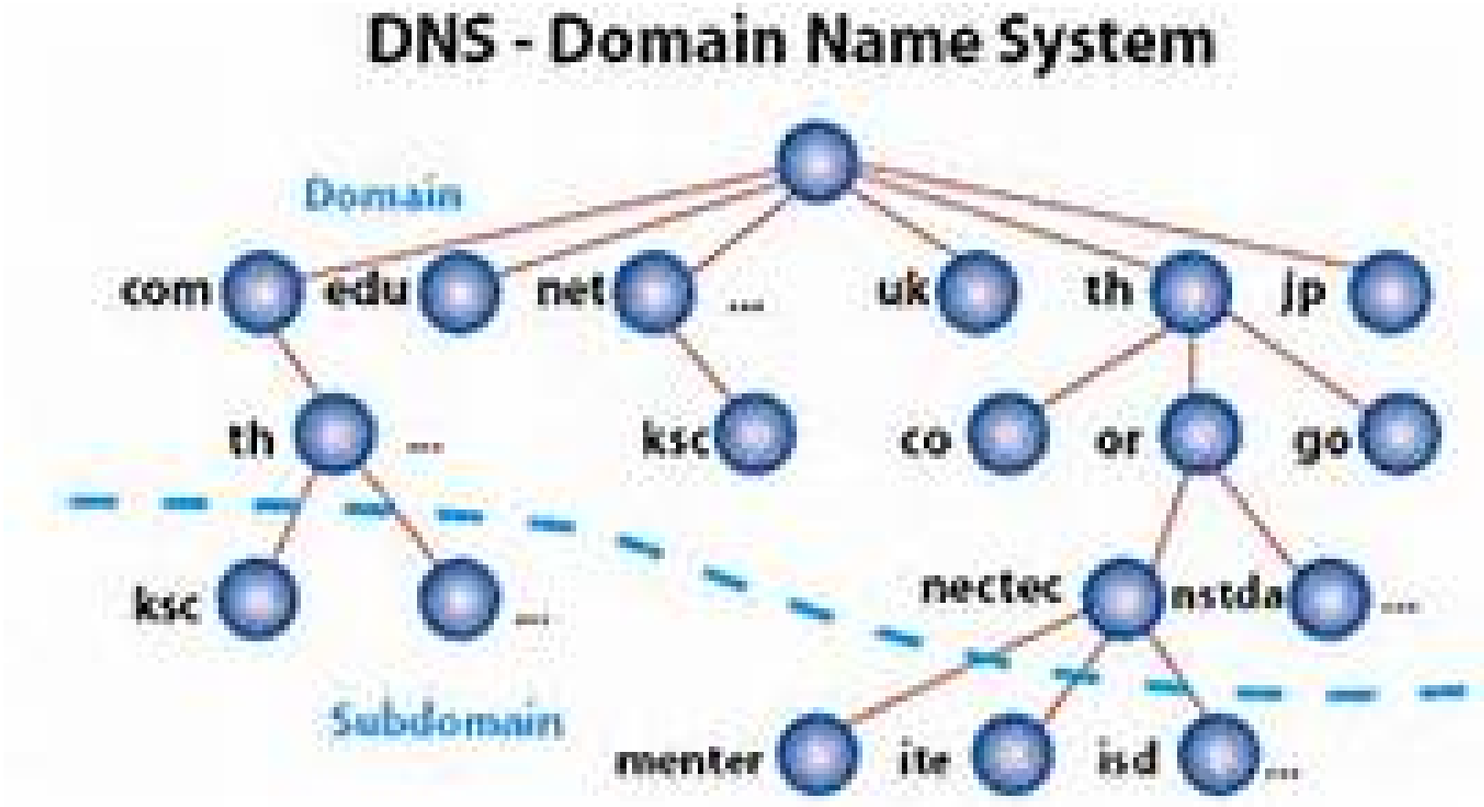


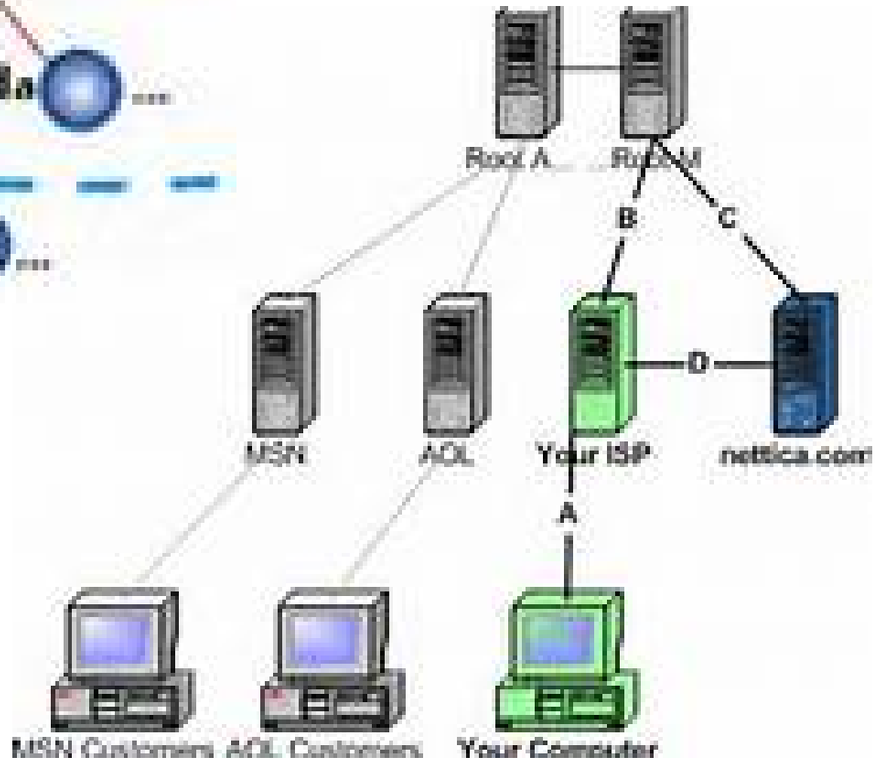
Name and Address Resolution



How does my URL get transformed into an IP address?

DNS – Domain Name Server

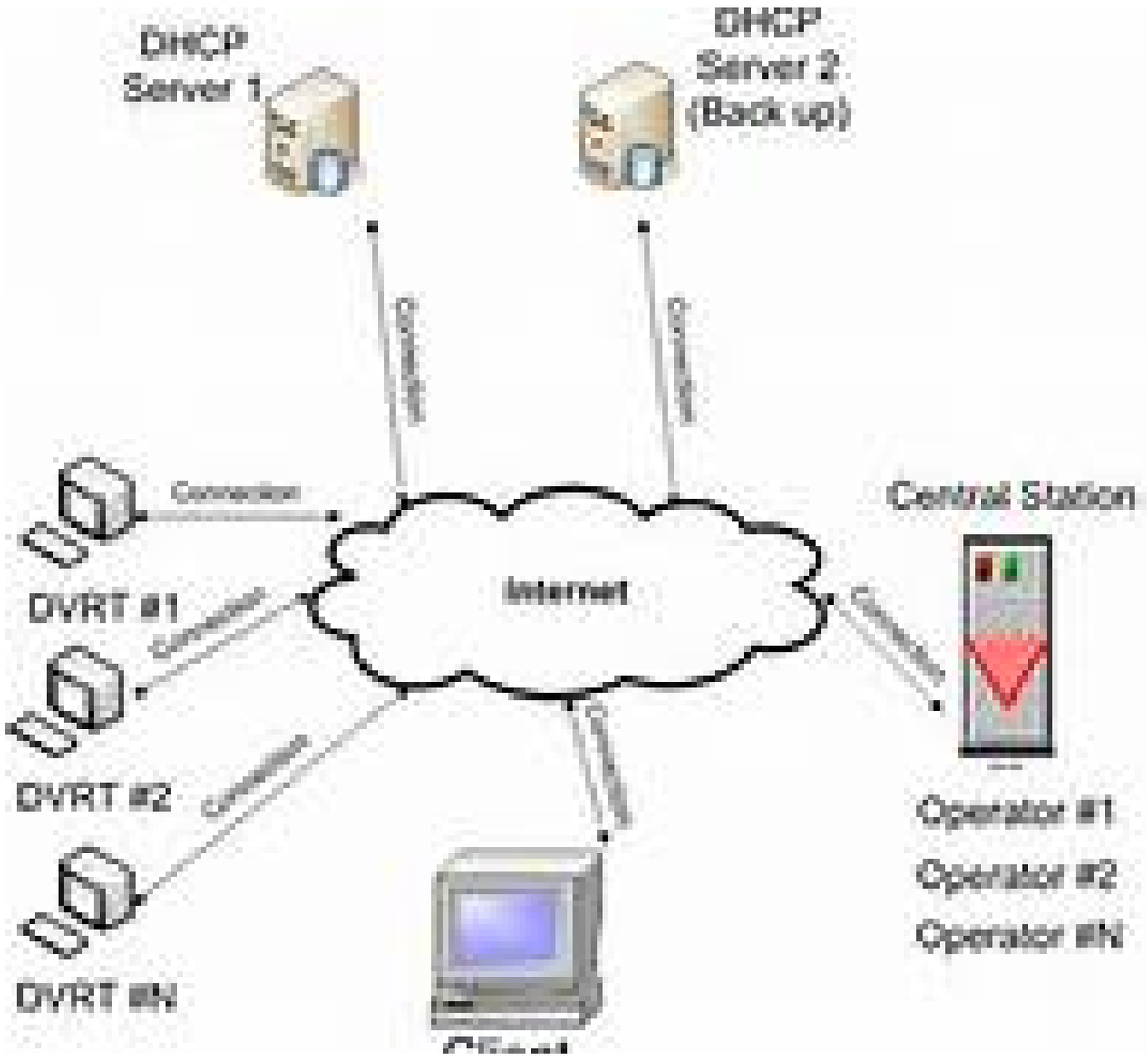




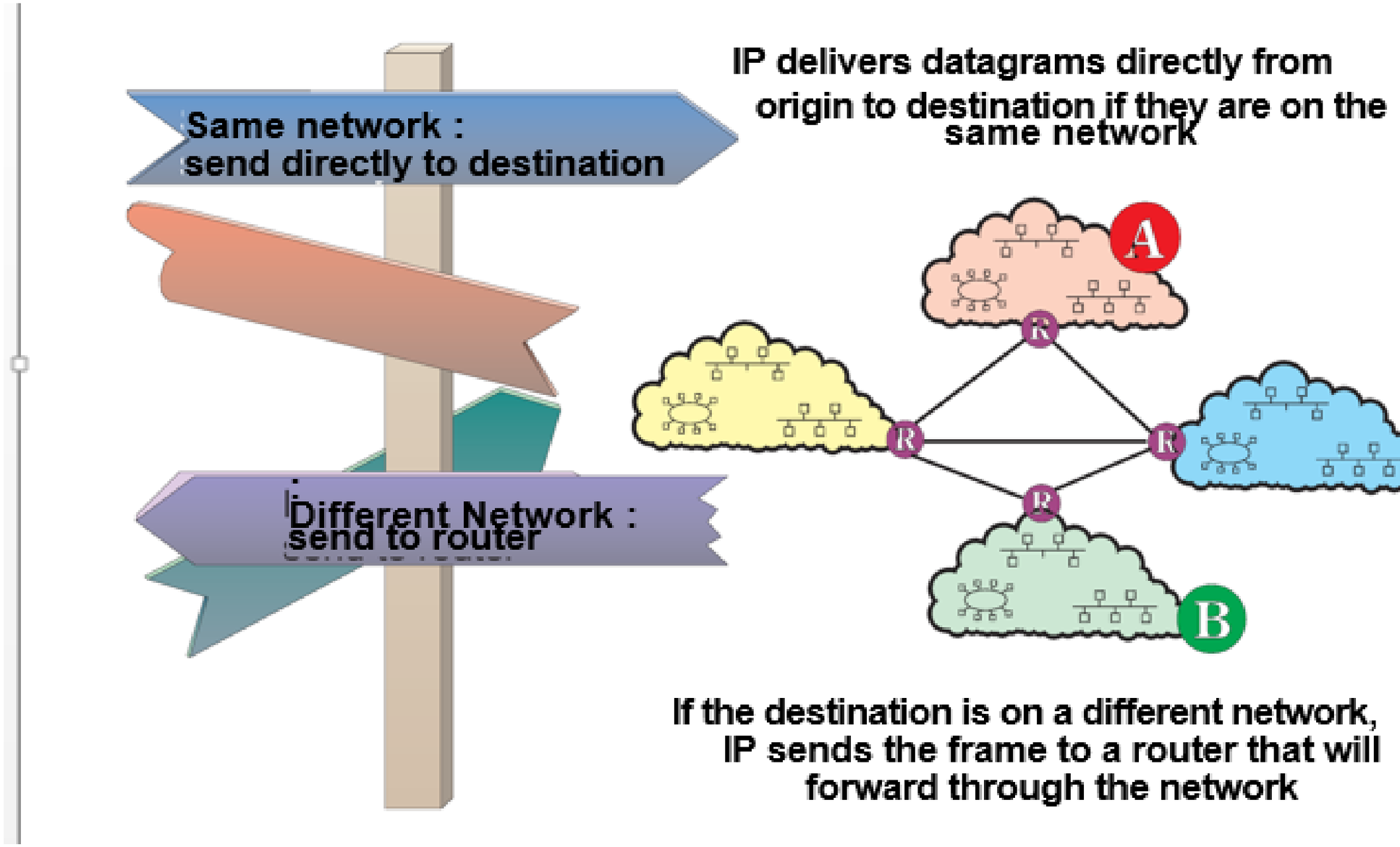
DNS Root Servers

http://www.root-servers.org/map/

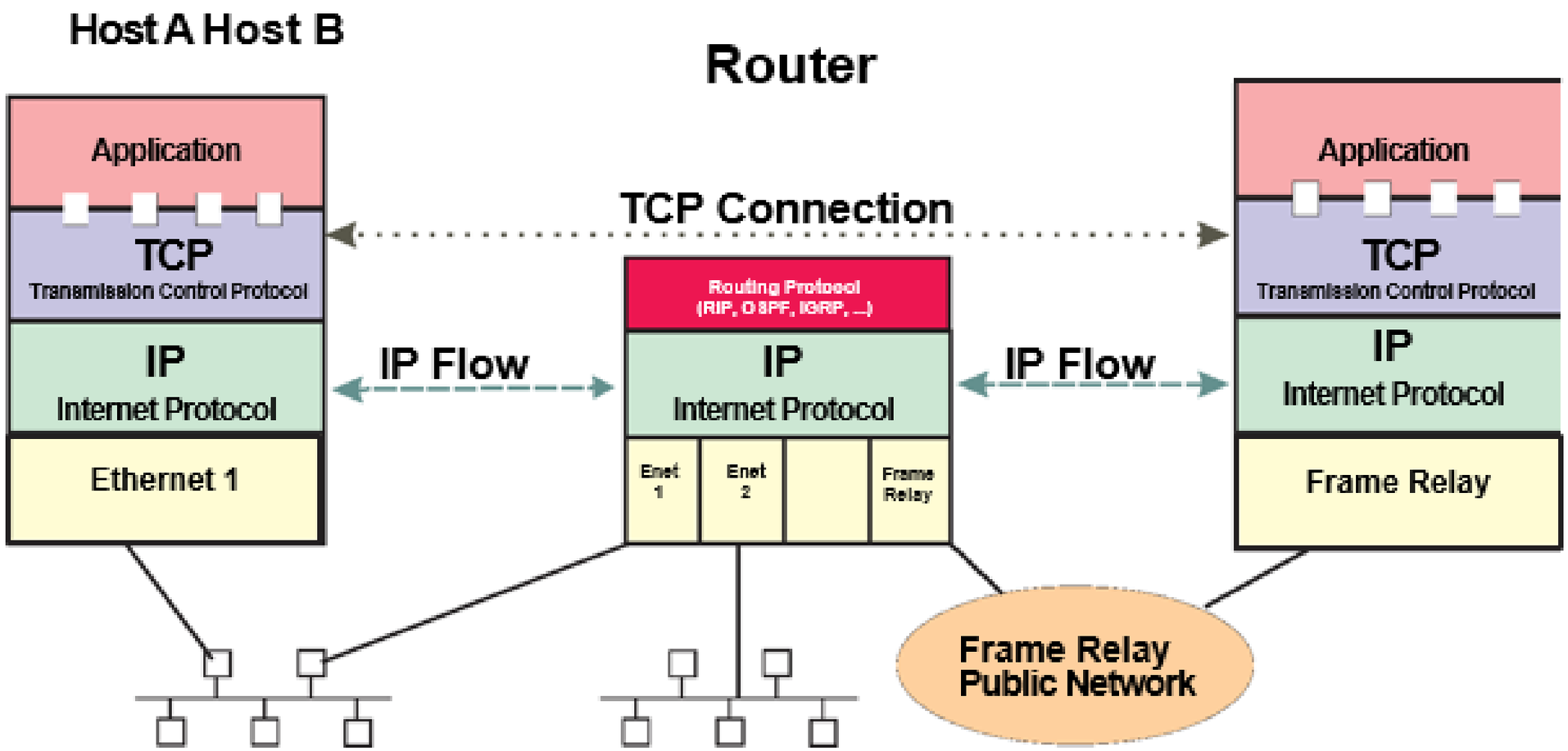
DHCP Servers



IP Routing



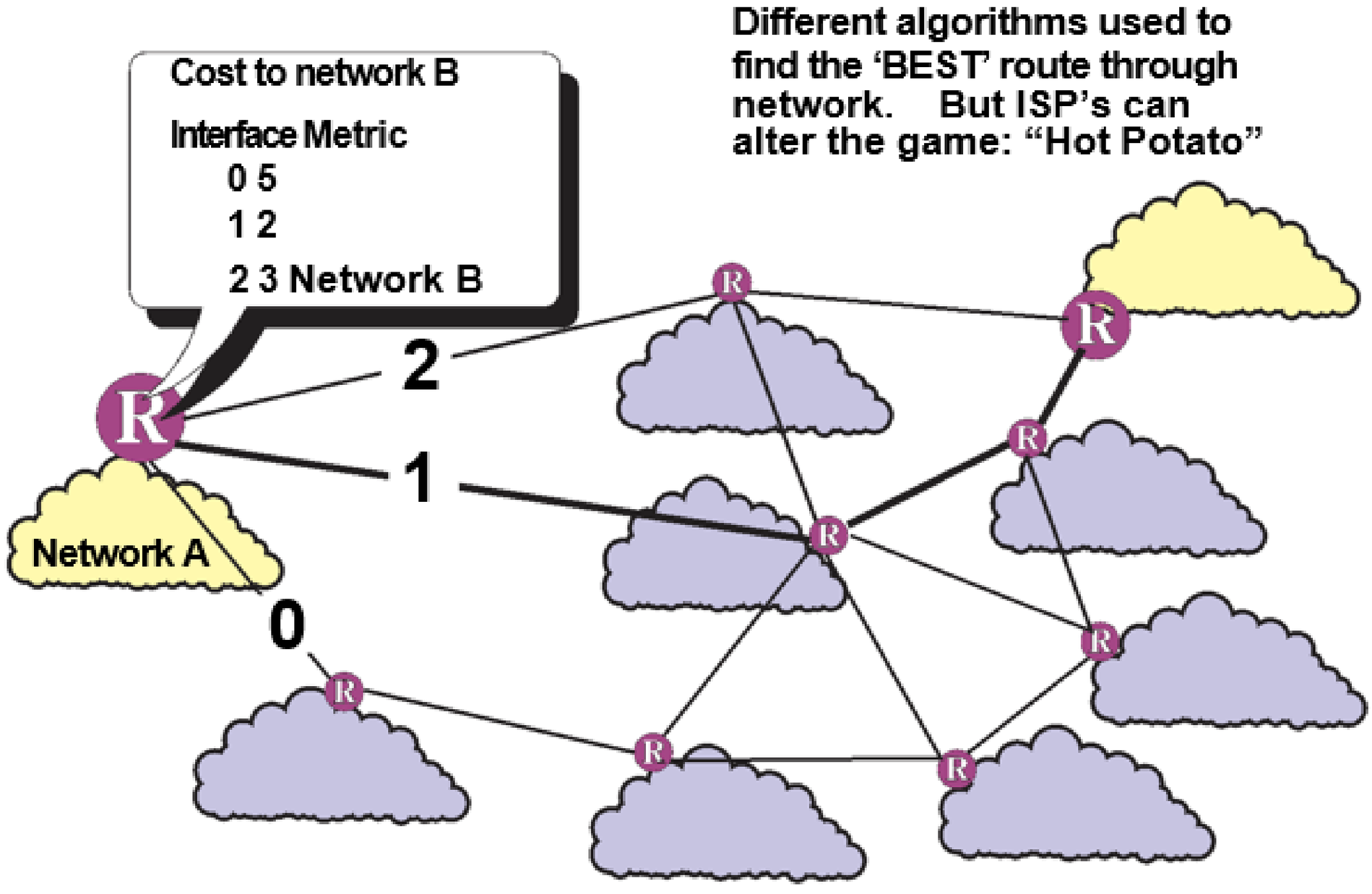
IP Routing Flows



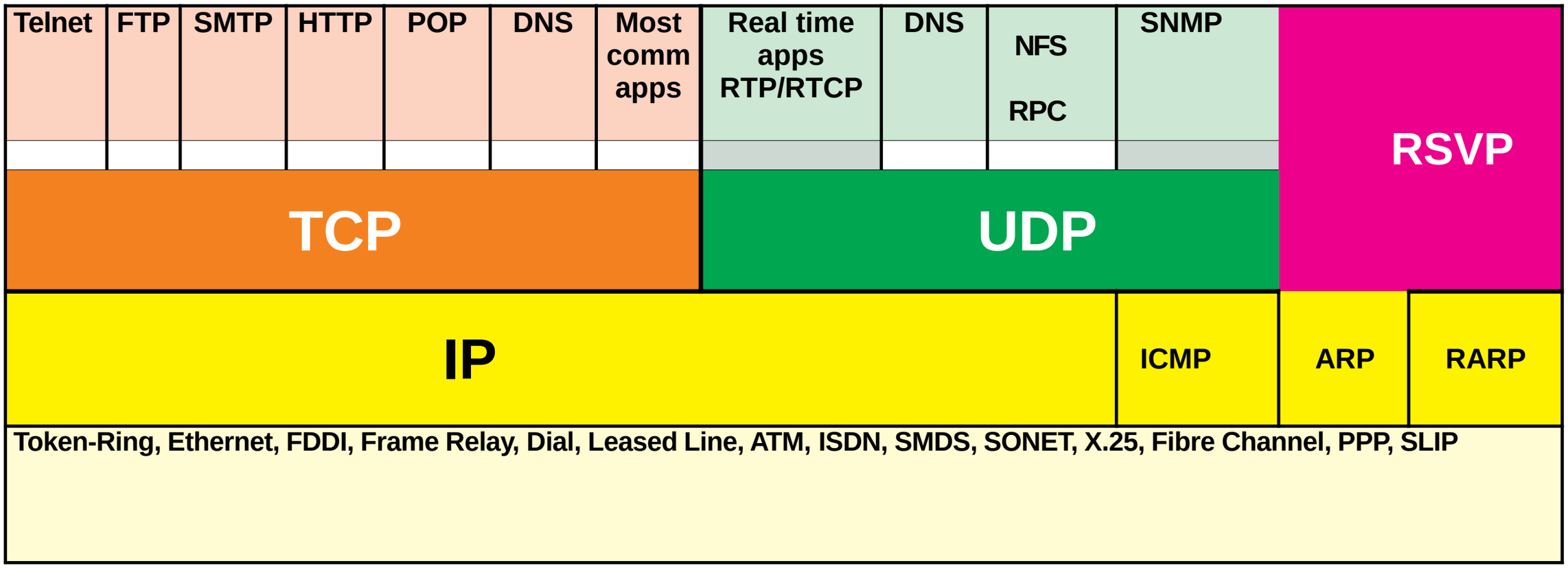
The routing function is performed by the IP protocol and routers

RIP - Routing Information Protocol
OSPF - Open Shortest Path First
IGRP - Interior Gateway Routing Protocol

IP Alternate Routes



IP Family



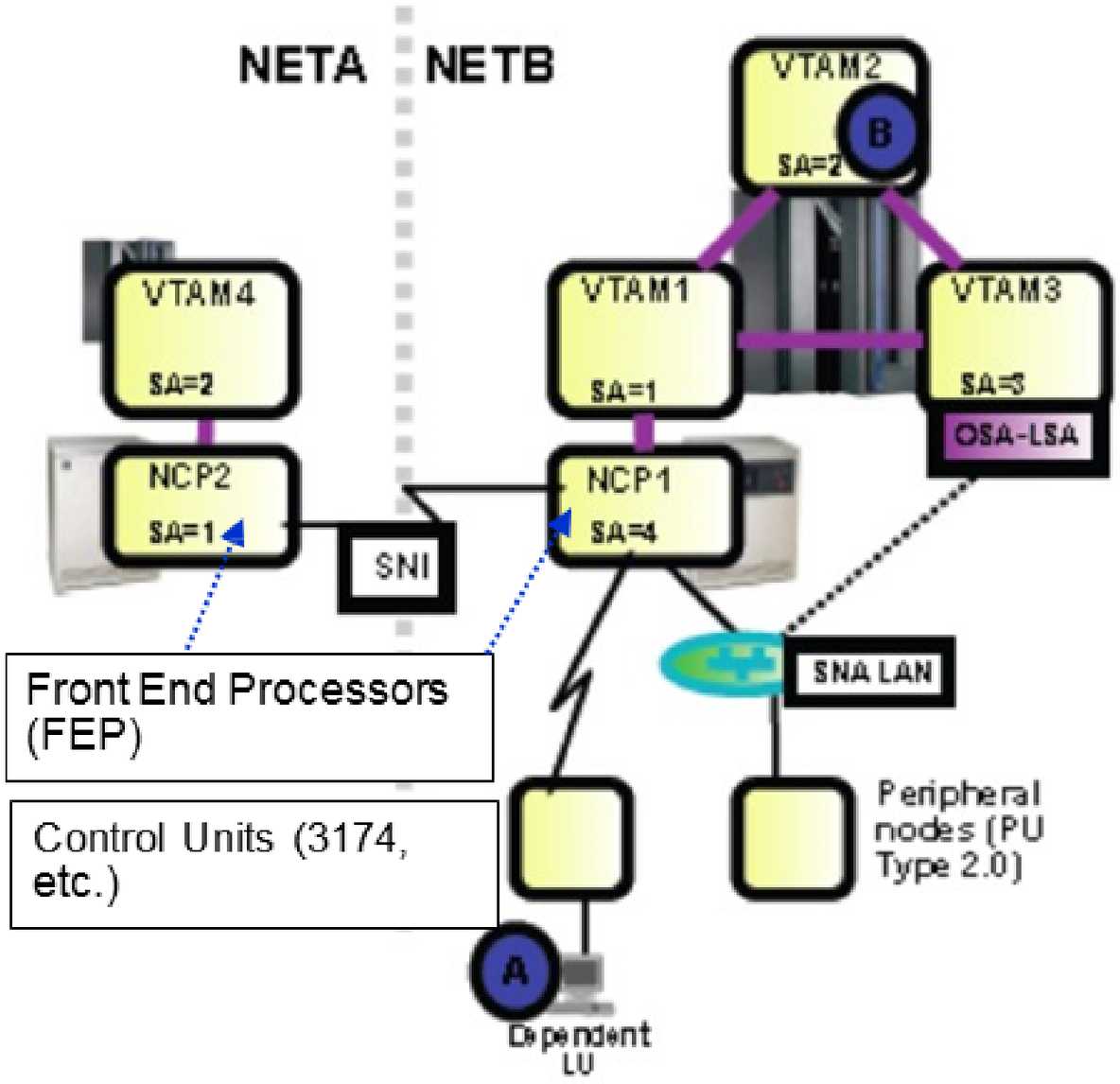
IP - Internet Protocol
ICMP - Internet Control Message Protocol ARP - Address Resolution Protocol
RARP - Reverse Address Resolution Protocol TCP - Transmission Control Protocol
UDP - User Datagram Protocol
POP - Post Office Protocol
DNS - Domain Name System

Telnet - Teletype Network
FTP - File Transfer Protocol
SMTP - Simple Mail Transfer Protocol
HTTP - Hypertext Transport Protocol
NFS - Network File System
RPC - Remote Procedure Call
SNMP - Simple Network Management Protocol

Agenda

- Requirements for Communication
- What are Networking Architectures?
- Networking Architectures on System z
- z Hardware Platform Support of Network Architectures
- Networking Applications
- Security Implementations
- References

SNA



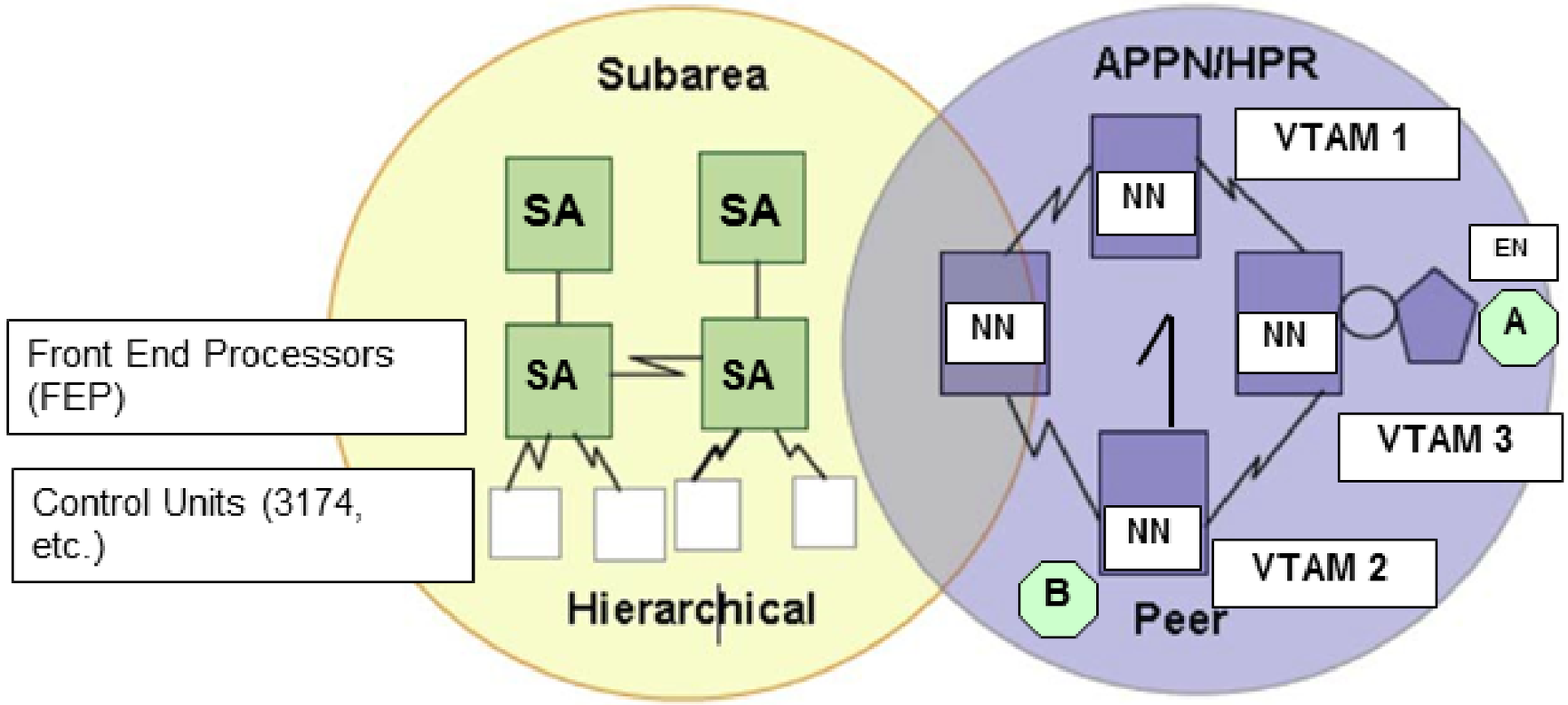
VTAM = Virtual Telecommunications Access Method

NCP = Network Control Program (runs in a physical Front-End Processor (FEP) called a 3745/6 or an emulated 3745/6 called Communication Controller on Linux (CCL) in System z)

Offloads processing from the VTAM in a partition to the FEP.

SNI=SNA Network Interconnect (to establish connections between partners in different NETIDs)

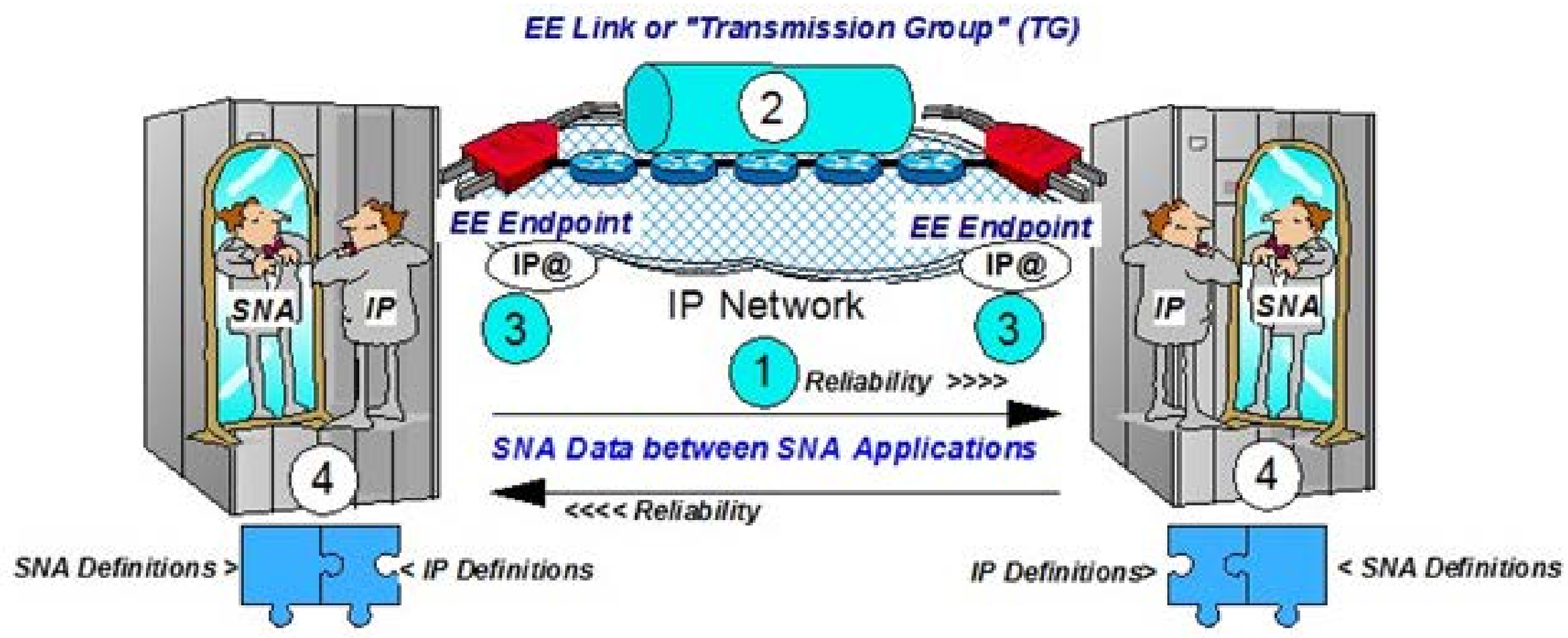
Evolution of SNA



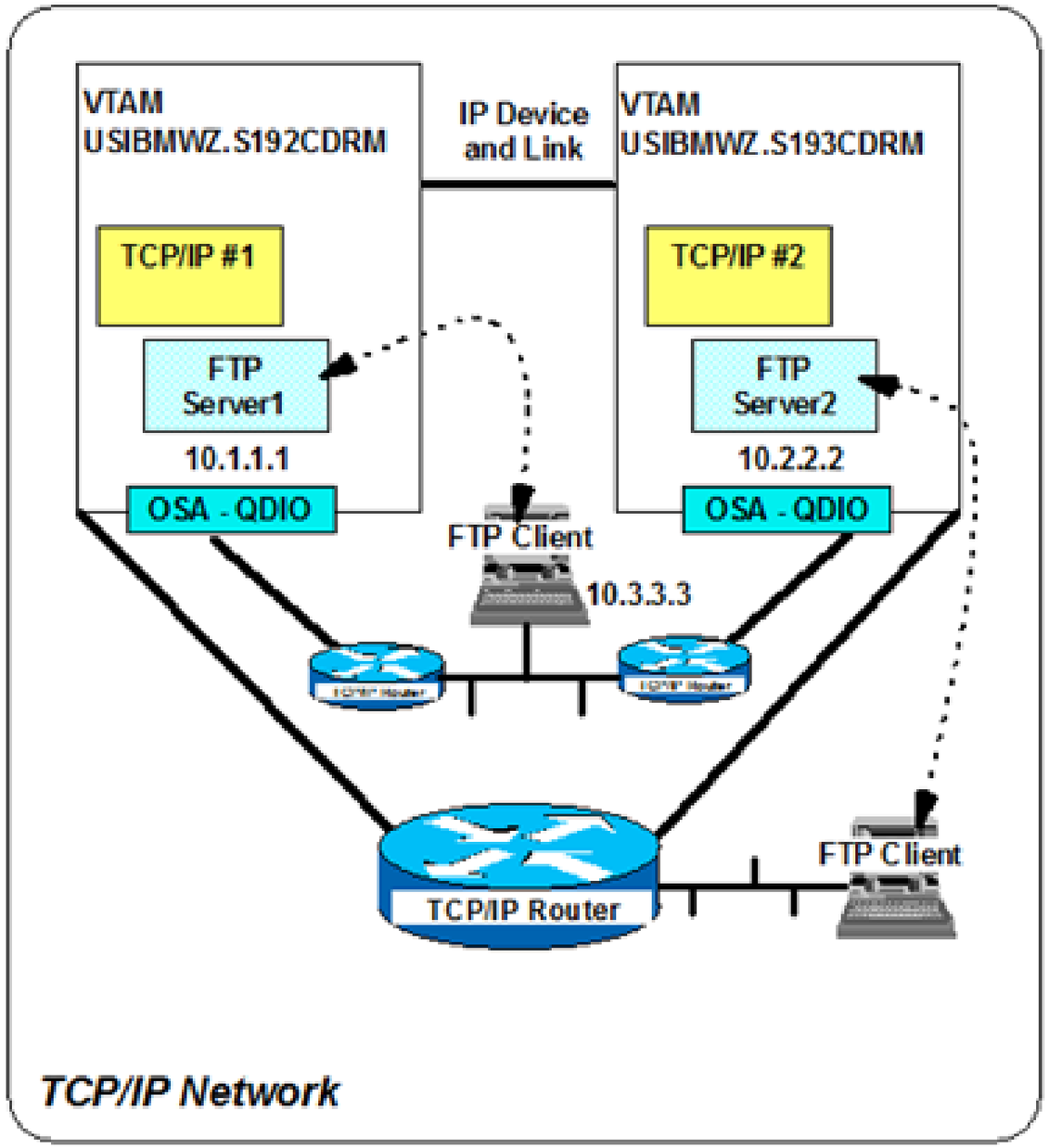
SNA originally consisted of subarea protocols

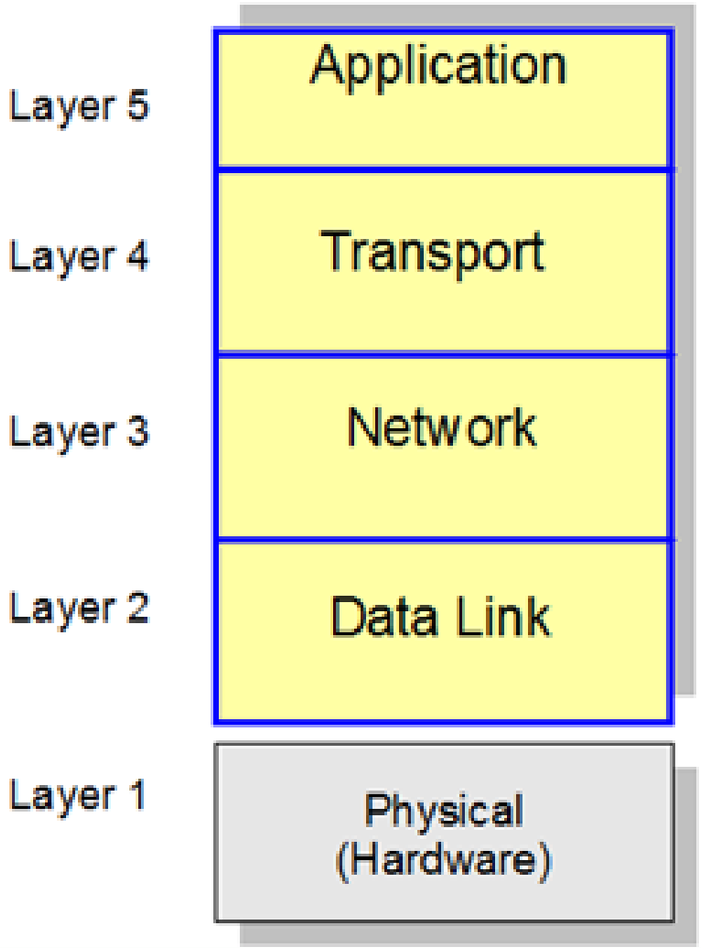
- Advanced Peer to Peer networking (APPN) introduced mid 1980s
- High Performance Routing (APN/HPR)introduced in 1990s
- Enterprise Extender (EE; HPR over UDP) introduced in 1999

Enterprise Extender – SNA over IP



TCP/IP on System z

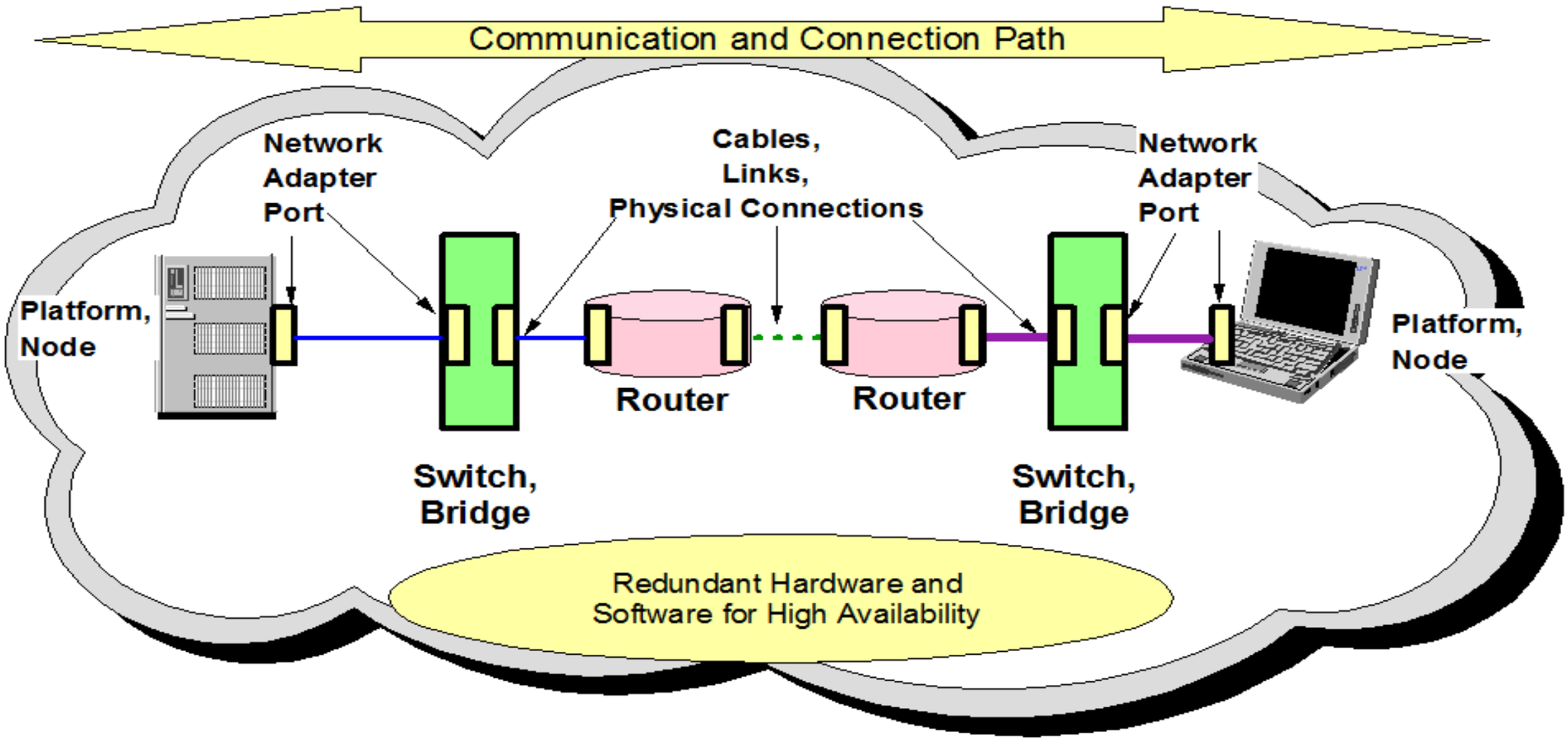




Agenda

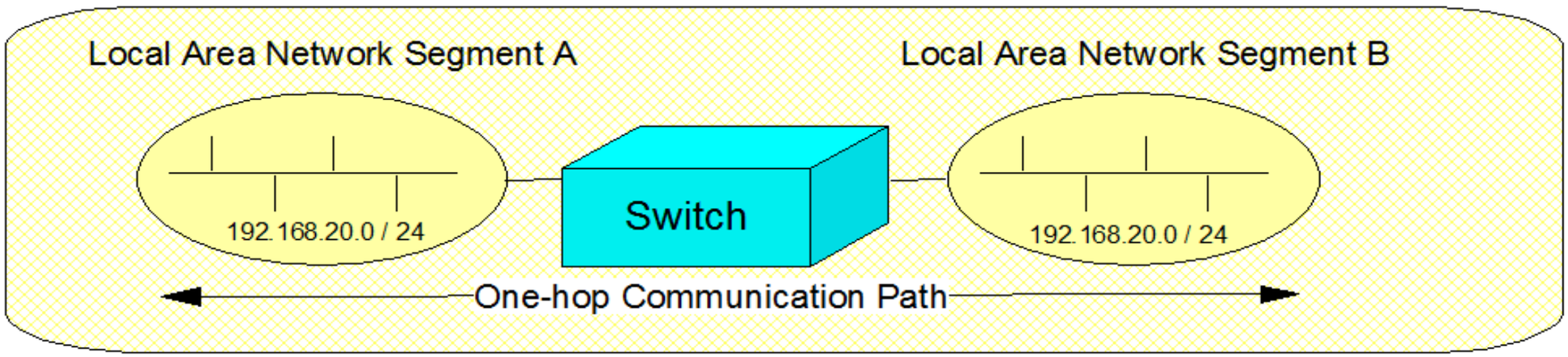
- Requirements for Communication
- What are Networking Architectures?
- Networking Architectures on System z
- z Hardware Platform Support of Network Architectures
- Networking Applications
- Security Implementations
- References

Overall Network Perspective

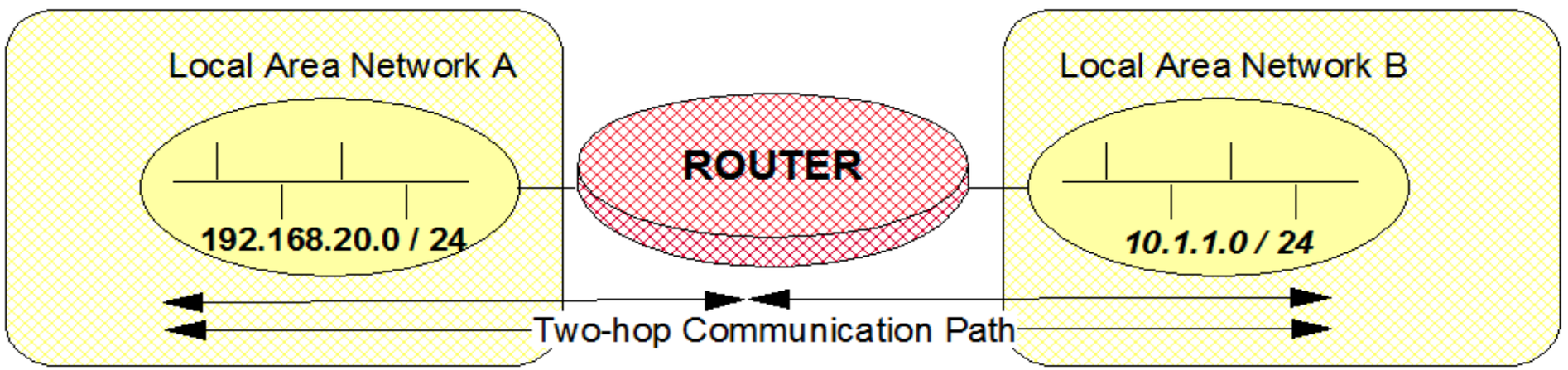


Switching vs. Routing

- **A Switch connects multiple LAN Segments into a single logical LAN.**
  - We have one LAN with network address of 192.168.20.0 / 24

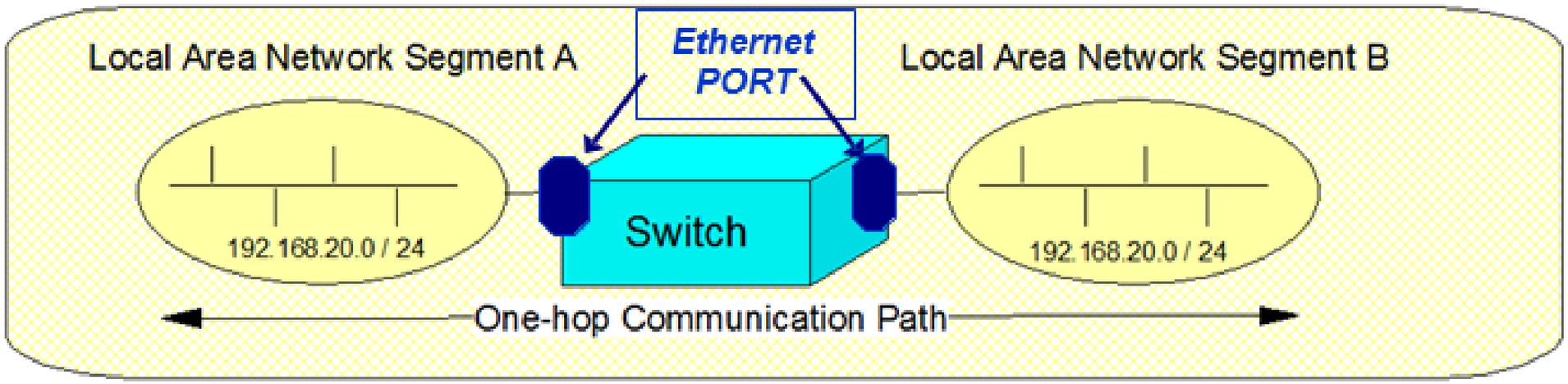


- **A Router connects multiple distinct LAN Segments to create a routing path.**
  - We have two LANs -- each with a separate network address. Nodes in LAN A can communicate over the router with Nodes in LAN B.

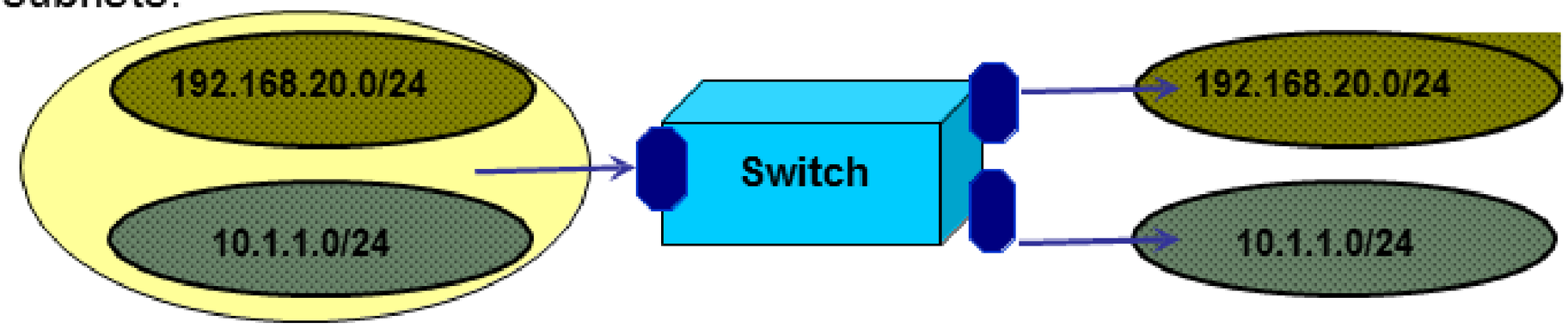


Virtual Local Area Networks

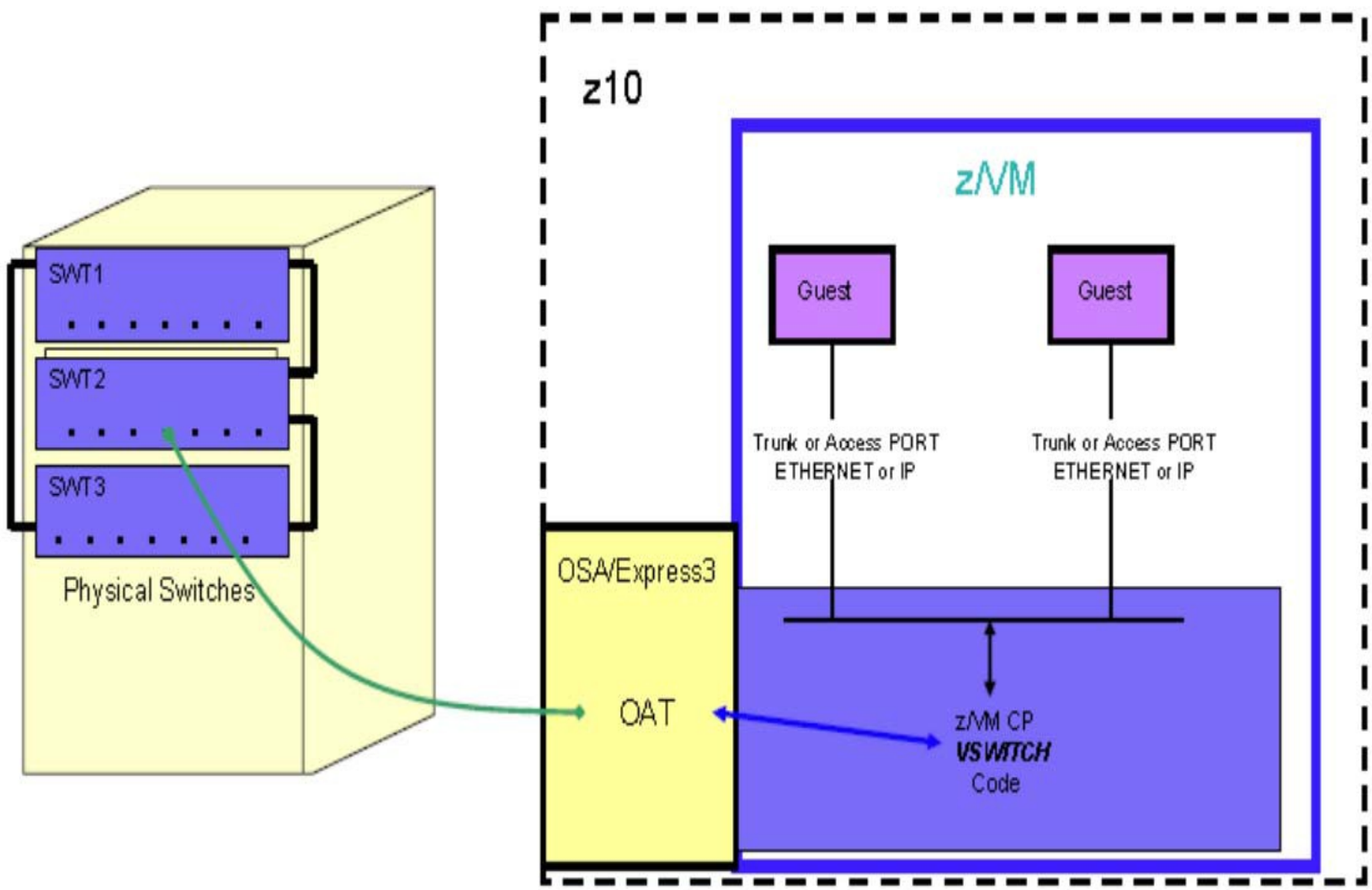
- **A Switch connects multiple LAN Segments into a single logical LAN.**
  - We have one LAN with network address of 192.168.20.0 / 24



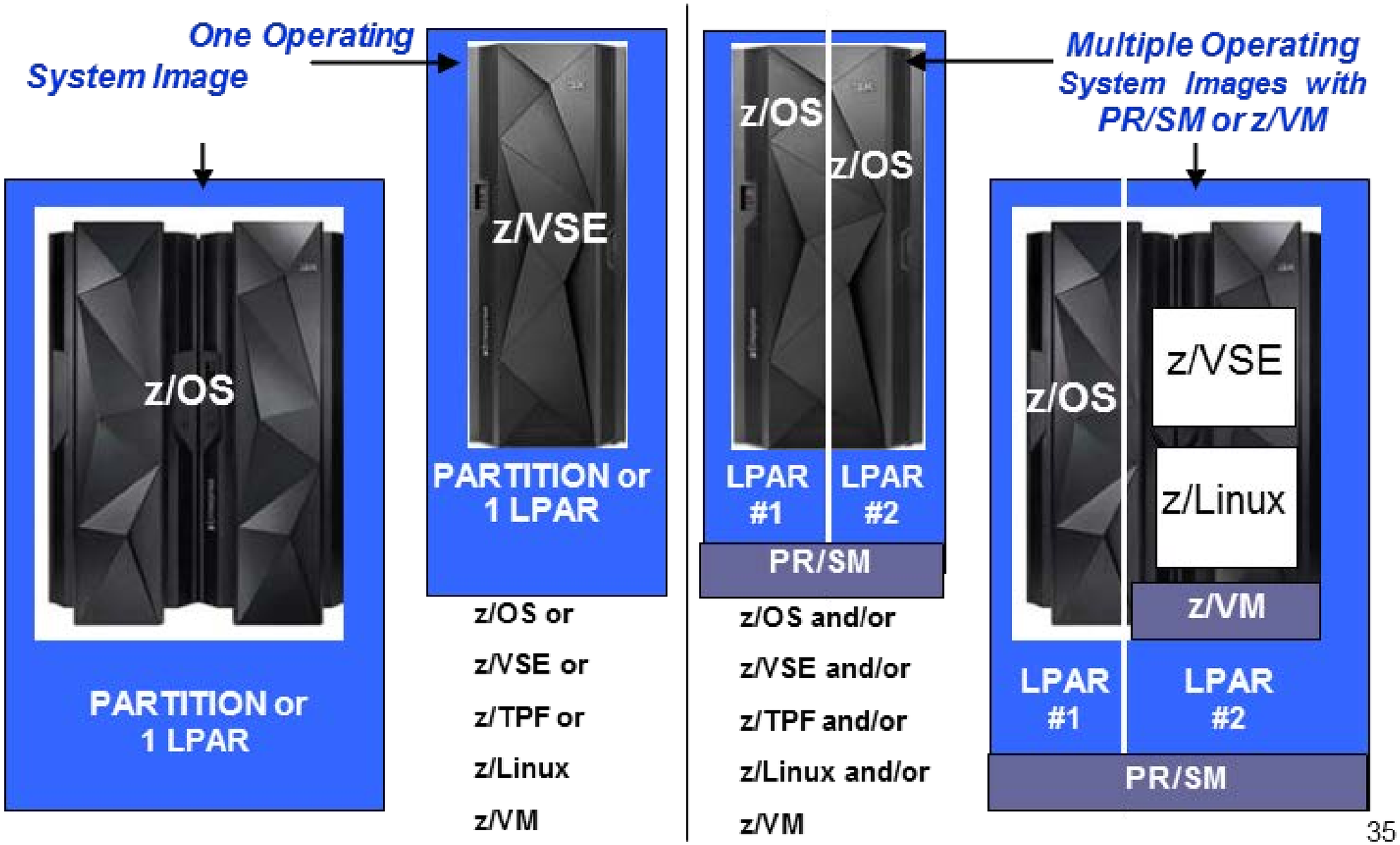
A single physical Ethernet Cable on the left can be subdivided into multiple VIRTUAL LAN cables to produce multiple VLAN connections to different subnets.



Virtual Switch (VSwitch)

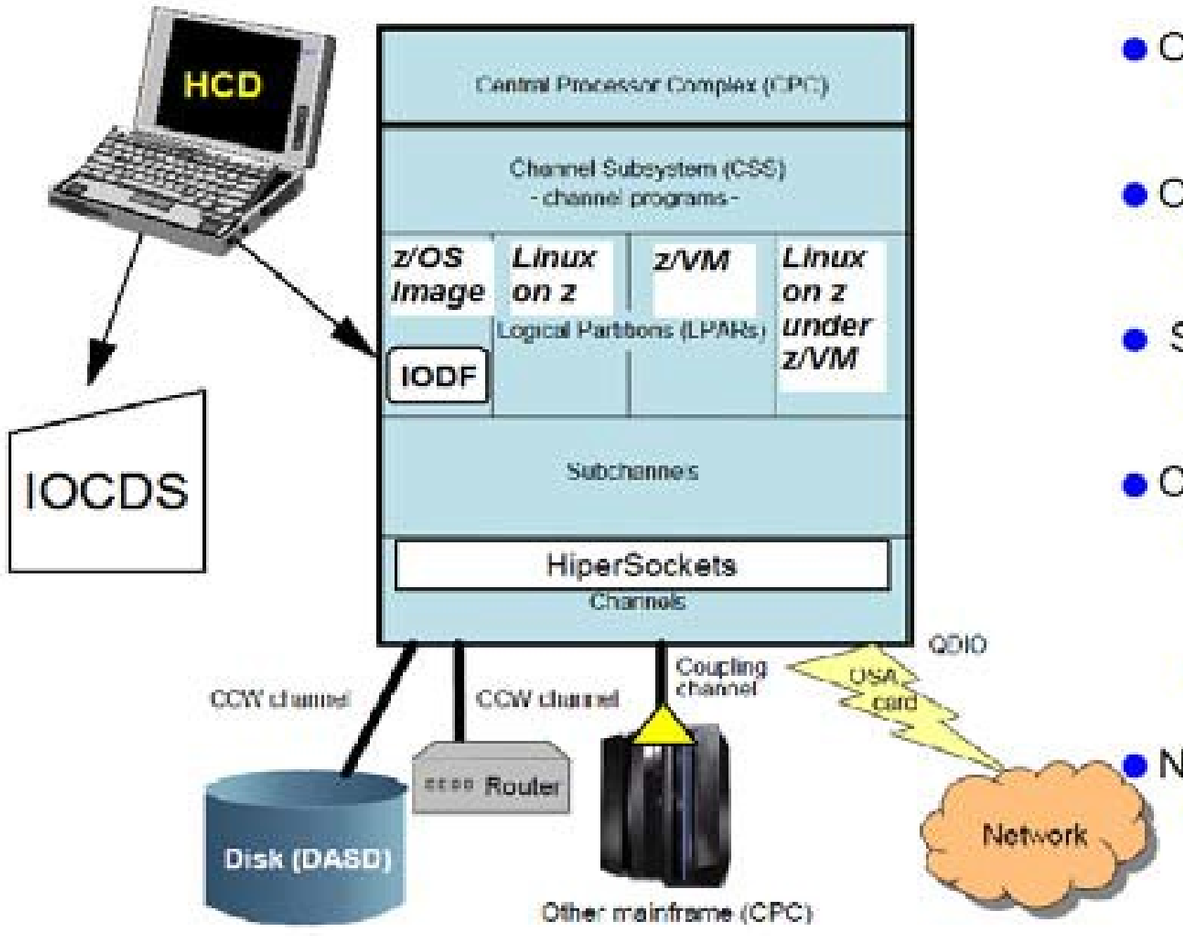


Complexity of System z Networking



35

Channel and Network Interface Structure



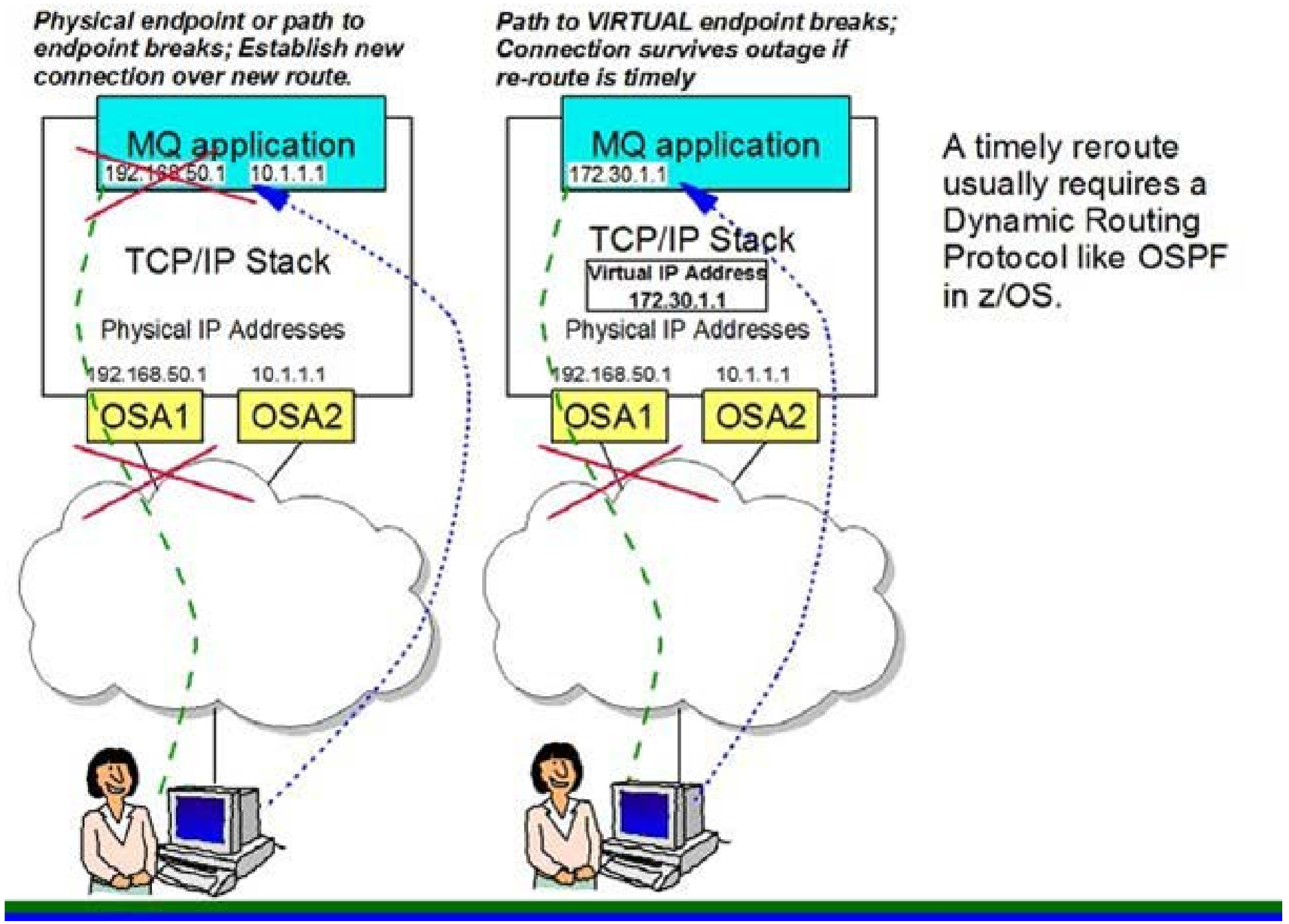
- Central Processor Complex (CPC):
  - passes input/output (I/O) Request to CSS
- Channel Subsystem (CSS):
  - moves data asynchronously to its input/outpt devices
- Subchannel:
  - the individual input/output devices in the CSS that are assigned to the LPARs
- Channel:
  - represented by a channel path ID or CHPID and represents the actual communication path.
  - CHPID is mapped to the PCHID in the HCD and the IOCDS.
- Network Interfaces:
  - identified to TCP/IP by the CHPID and the Subchannel address that are defined in the IOCDS.

The I/O configuration of the central processor complex is defined in a data set called the I/O Configuration Data Set, or IOCDS.

System z : Connectivity Adapters

•zVSE •zOS •z/VM	MPC CTC CDLC	CHANNEL CONNECTIONS PARALLEL or ESCON or FICON or VIRTUAL (z/VM)
•zVSE •zOS •z/VM •zLinux (for CCL)	XCF LCS LSA QDIO	LOCAL AREA NETWORK (LAN) CONNECTIONS ETHERNET, 802.3, TOKEN RING**
•zOS •z/VM •zLinux	iQDIO	HIPERSOCKETS INTERNAL CONNECTION
•zLinux •z/VM	VSwitch	LAN CONNECTION over VIRTUAL SWITCH ETHERNET, 802.3
•zOS	RoCE	Remote Direct Memory Access over Converged Ethernet LAN CONNECTIONS --- ETHERNET

Virtual IP Address

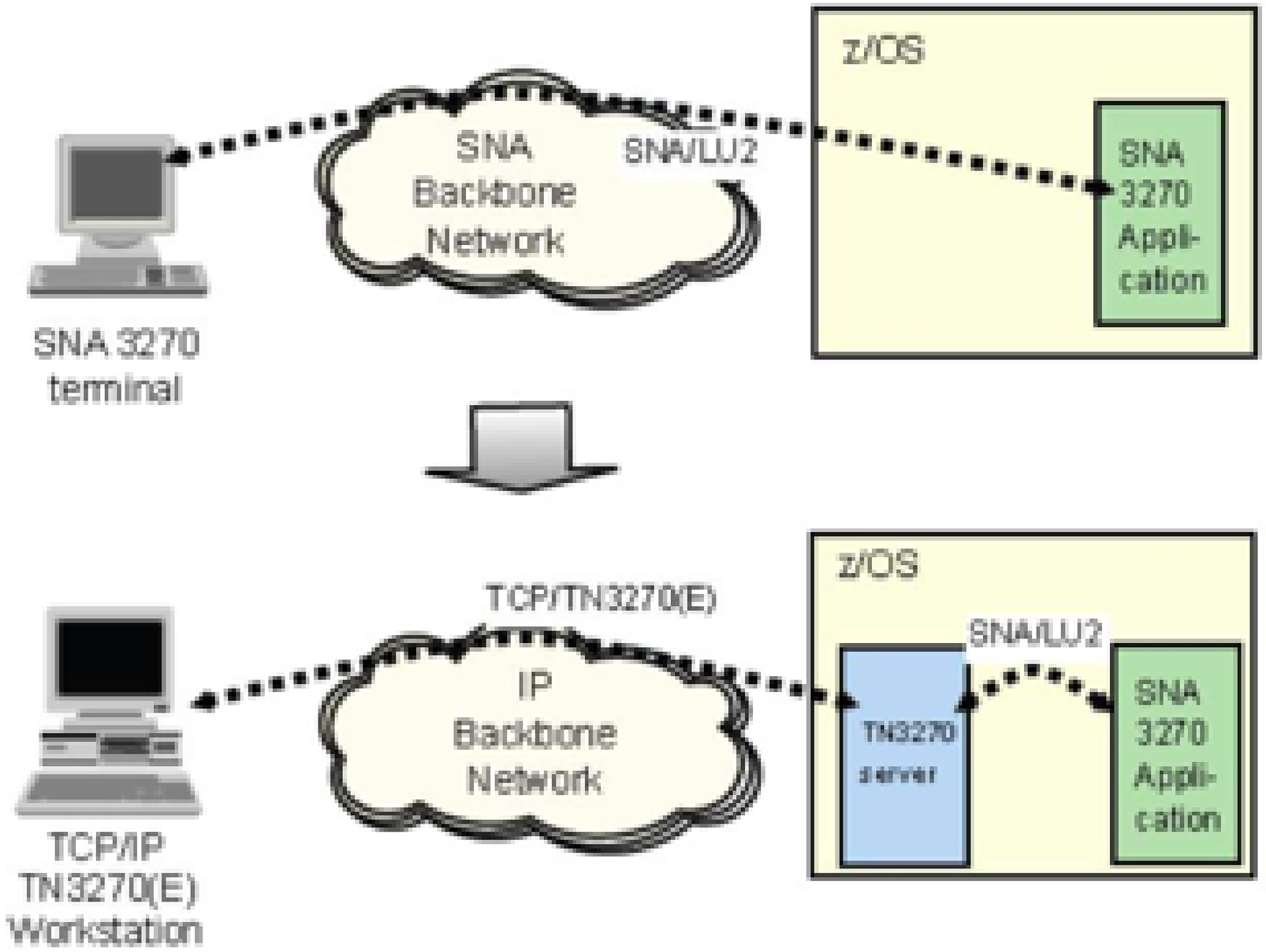


A timely reroute usually requires a Dynamic Routing Protocol like OSPF in z/OS.

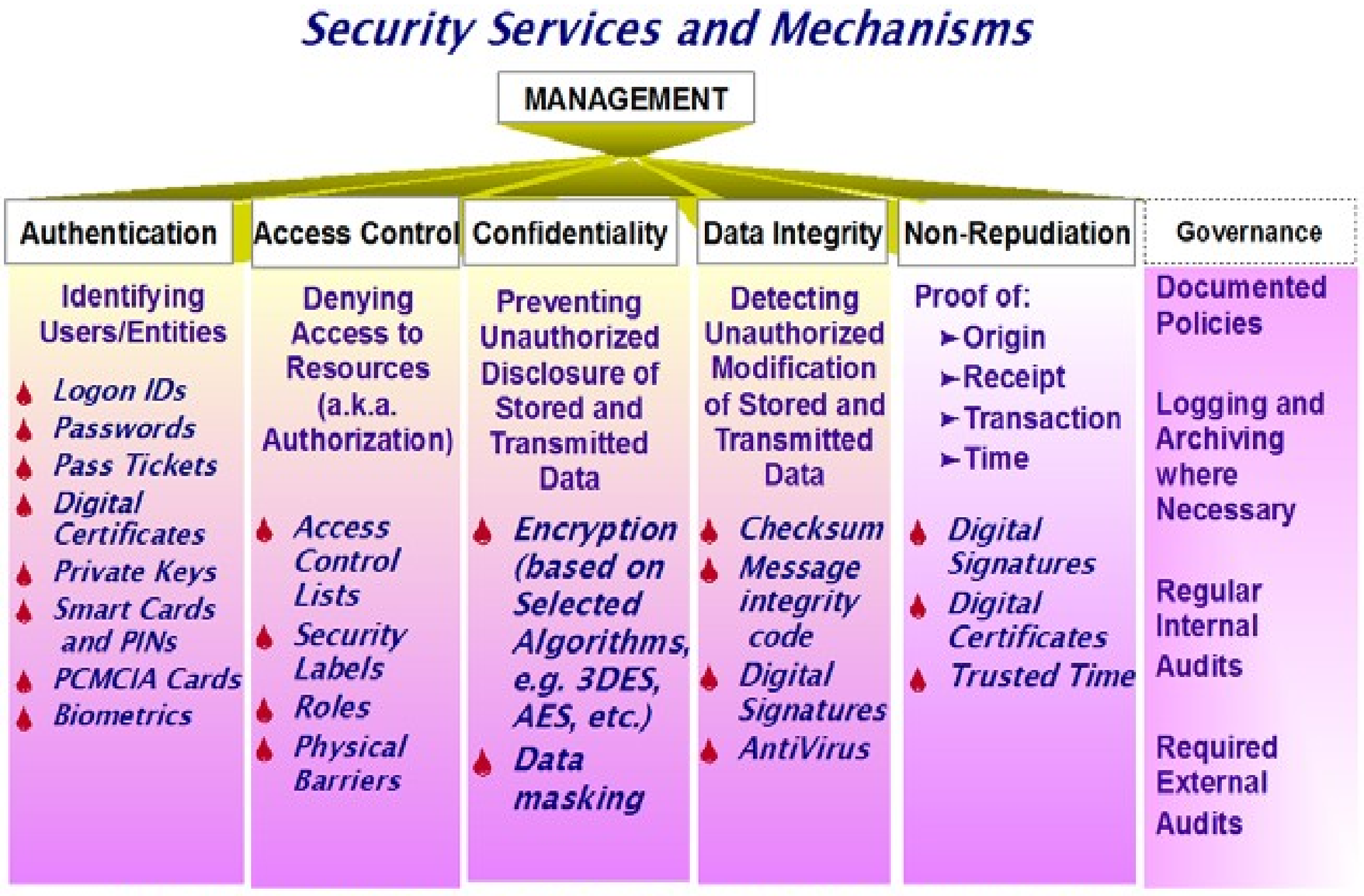
Agenda

- Requirements for Communication
- What are Networking Architectures?
- Networking Architectures on System z
- z Hardware Platform Support of Network Architectures
- Networking Applications
- Security Implementations
- References

TN 3270

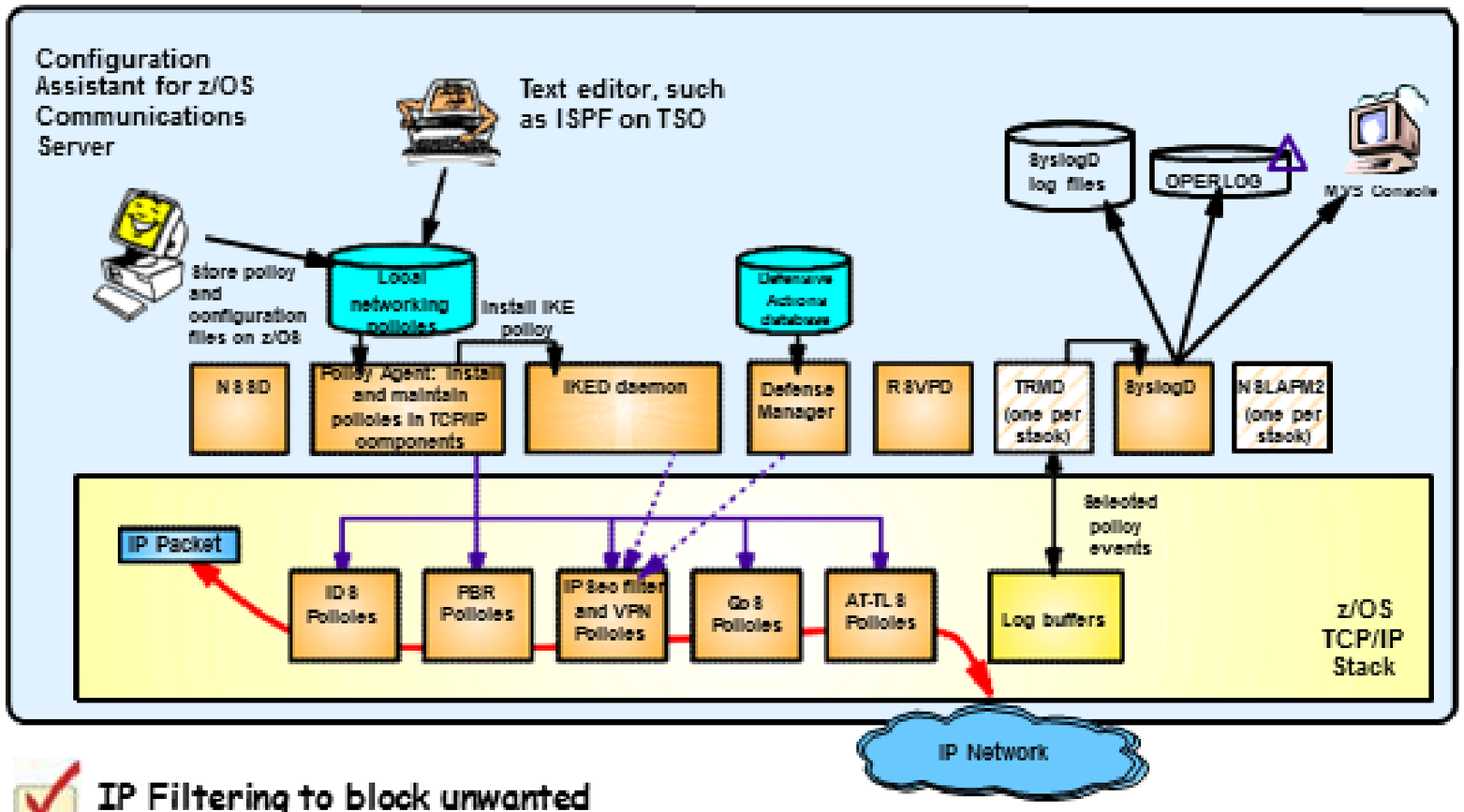


System z Security



International Standard ISO 7498-2, *"Security Architecture"*, provides a good starting point

z/OS CS Security Policies

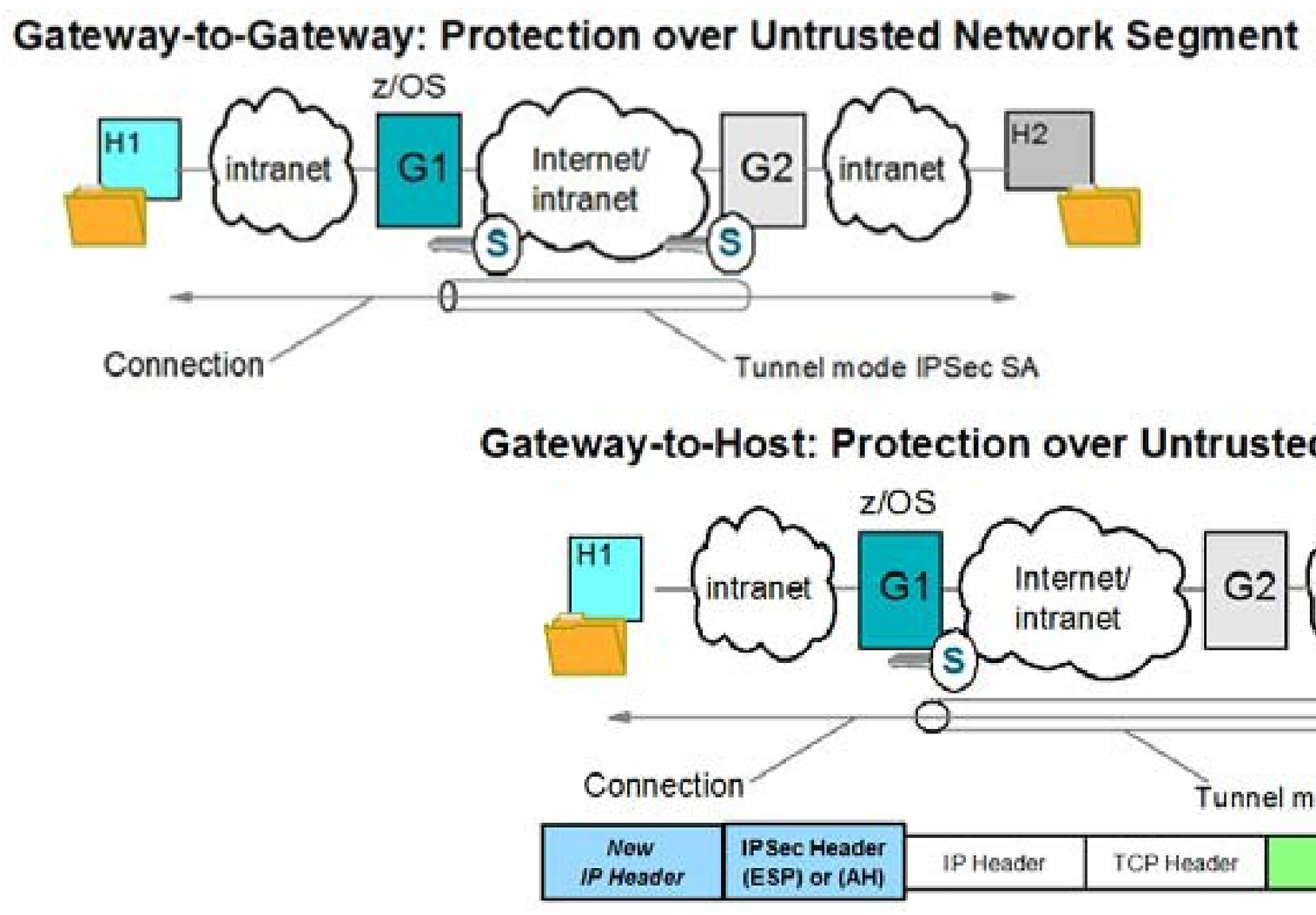


- IP Filtering to block unwanted traffic from entering or leaving your z/OS system
- Connection-level security for TCP applications without application changes
- Making sure high-priority applications also get high-priority processing by the network
- Application-specific selection of outbound interface and route (Policy-based routing PBR)
- Providing secure end-to-end IPSec VPN tunnels on z/OS
- Protection against "bad guys" trying to attack your z/OS system

CS Security Alphabet Soup

	Stands for:	Designed by:	Main Features:	CS Applications
SSL V2	Secure Sockets Layer	NetScape	Server Authentication	TN3270 Server
SSL V3	Secure Sockets Layer	NetScape	Client Authentication	TN3270 Server, FTP
TLS-enabled Telnet (SSL V3.1)	Transport Layer Security -Enabled Telnet	IETF Draft RFC	Single port for SSL Negotiation or non-SSL	TN3270 Server
TLS 1.0	Transport Layer Security	IETF RFC 2246	Standards-Based; Negotiable TLS or SSL port	FTP Server & Client, TN3270 Server, AT-TLS
TLS 1.1	Transport Layer Security	IETF RFC 4346	Standards-Based; New notes, error handling, notes …	Any applications with AT-TLS -- ***At V1R11 it is AT-TLS default***
AT-TLS	Application-Transparent TLS	IBM; complies with previous standards, incl. de facto	Foundation based on Standards; Application Transparency	Any application; some applications enjoy additional options

Virtual Private Network (VPN) with IPSec



REFERENCES

References

For More Information

- IBM z/OS Communications Server Product Manuals
  - Resource Link
- IBM Redbooks on http://www.redbooks.ibm.com/
  - z/OS Communications Server
  - OSA-Express
  - IBM System z Connectivity Handbook
- Web Document ***z/OS V1R11 Communications Server Scalability, performance, constraint relief, and accelerator***
  - http://publib.boulder.ibm.com/infocenter/ieduasst/stgv1r0/topic/com.ibm.iea.commserv_v1/commserv/1.11z/hardware/perf.pdf
- Web Documents on ATS TechDocs web site http://www.ibm.com/support/techdocs/atsmastr.nsf/Web/Techdocs
  - FLASH10744 QDIO OSA Definition Migration: Device/Link to Interface
  - WP101327 Performance and Capacity Planning Information for z/OS Communications Server
  - PRS1707 z/OS OMPROUTE Hints and Tips -- Focus on OSPF
  - PRS4927 Ordering OSA Adapters with Multiple Ports per CHPID? Don't Make these Mistakes!!
  - PRS3950 Avoiding the Pitfalls of an OSA-E3 or OSA-E4S Migration (z/OS Examples)
  - PRS3296 Understanding VLANs when Sharing OSA Ports on System z

URLs

- http://www-01.ibm.com/support/docview.wss?uid=swg27020466&aid=3
  - OSA Performance Improvements
- http://www-01.ibm.com/support/docview.wss?uid=swg27005524
  - **z/OS Communications Server Performance Index**
- http://www-947.ibm.com/support/entry/portal/
  - http://www- 947.ibm.com/support/entry/portal/overview//software/other_software/z~os_communications_server
    - **IBM Support Assistant**
- **http://publib.boulder.ibm.com/infocenter/ieduasst/stgv1r0/index.jsp**
  - **IBM Education Assistant**