Week 10

STEVENS
INSTITUTE of TECHNOLOGY
THE INNOVATION UNIVERSITY®

An Introduction to Cyber Security – CS 573

Instructor: Dr. Edward G. Amoroso
eamoroso@tag-cyber.com

Week 10

Required Week Ten Readings

1. “TCP Wrapper: Network monitoring, Access Control, and Booby Traps,” Wietse Venema, *USENIX Security Symposium*, 1992. https://static.usenix.org/publications/library/proceedings/sec92/full_papers/venema.pdf

2. Finish reading “*From CIA to APT: An Introduction to Cyber Security,*” E. Amoroso & M. Amoroso

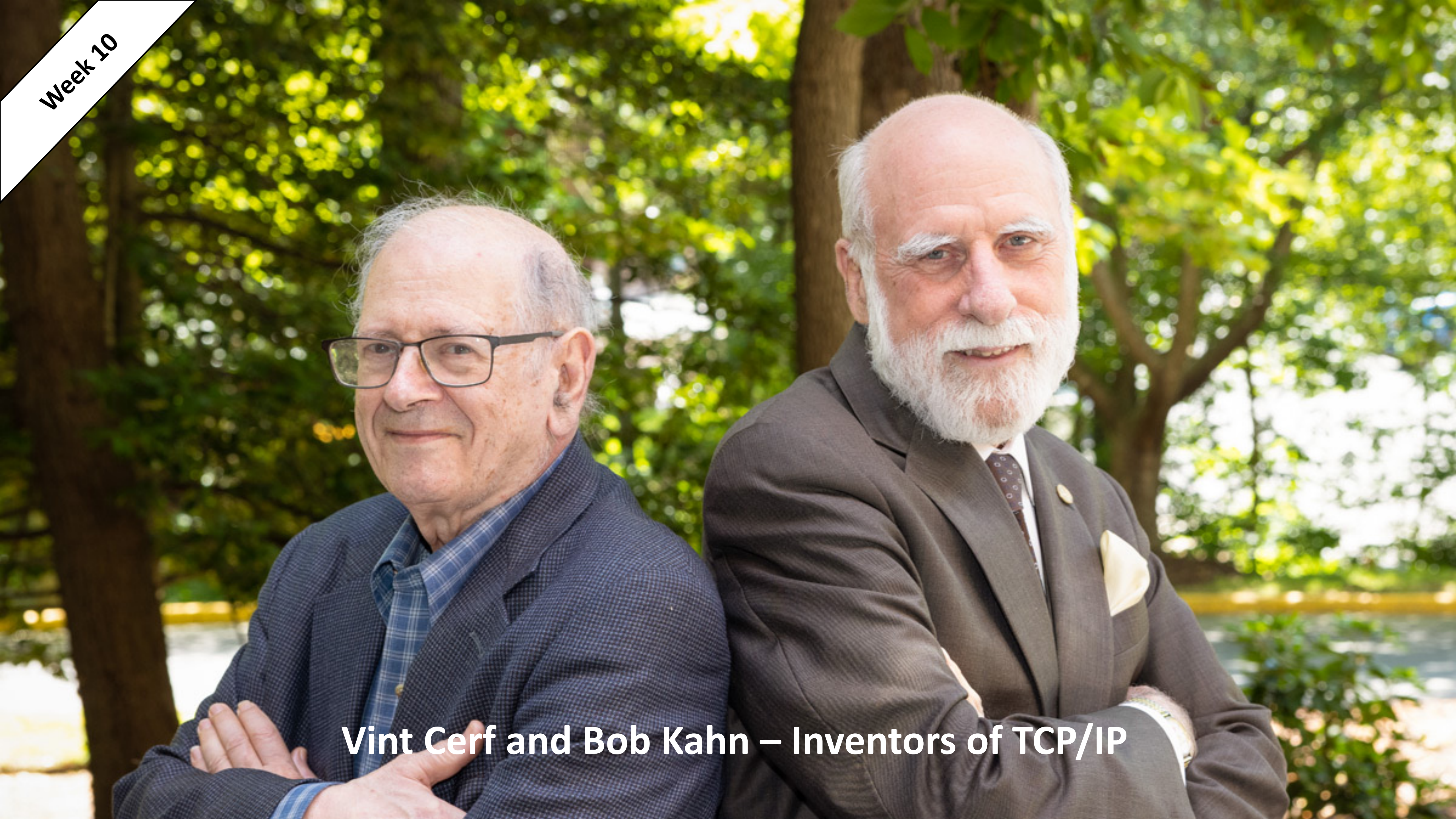
Twitter: @hashtag_cyber
LinkedIn: Edward Amoroso

Week 10

Week 10: Firewalls and Network Security

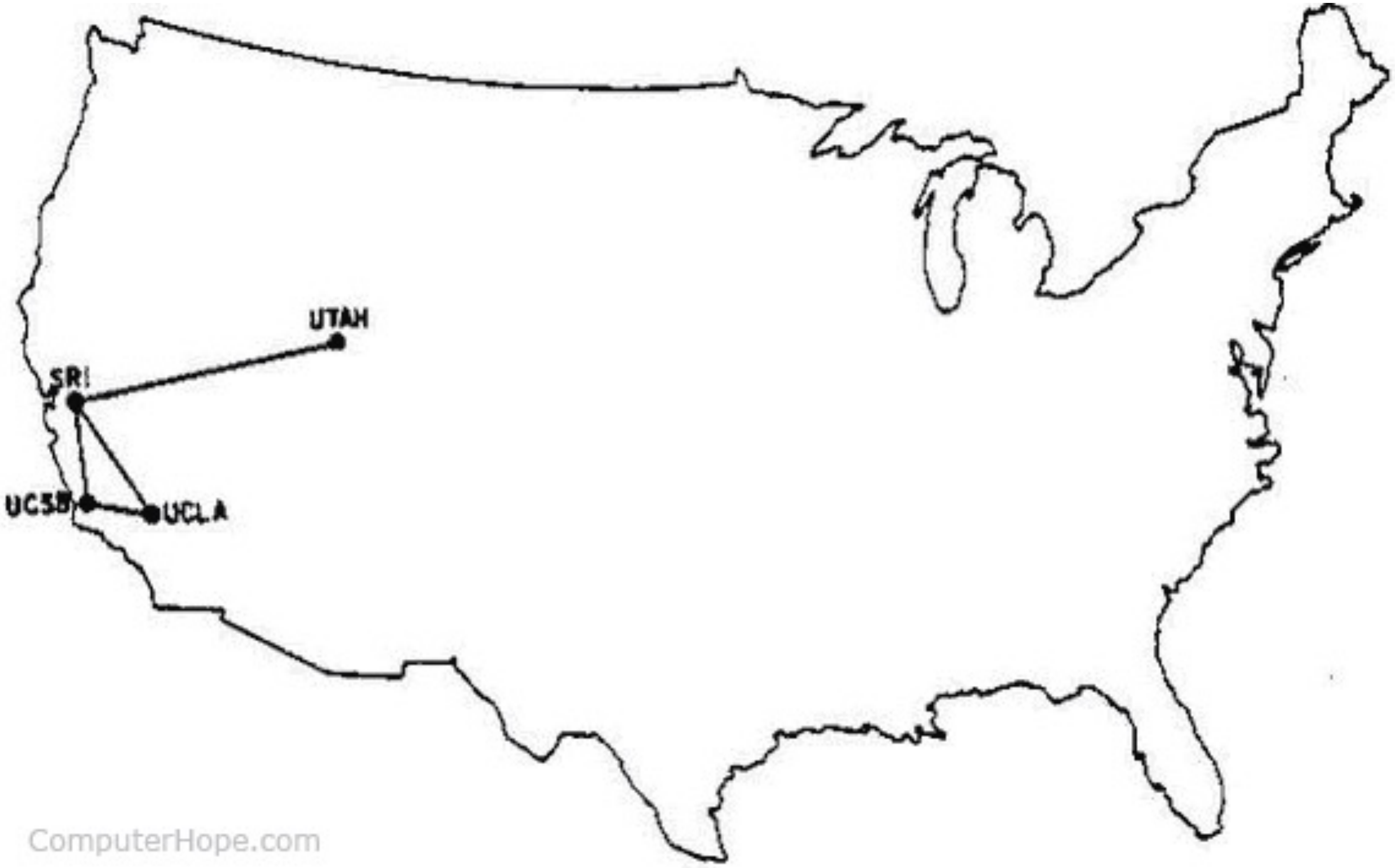
How Did the Internet Grow?

Week 10

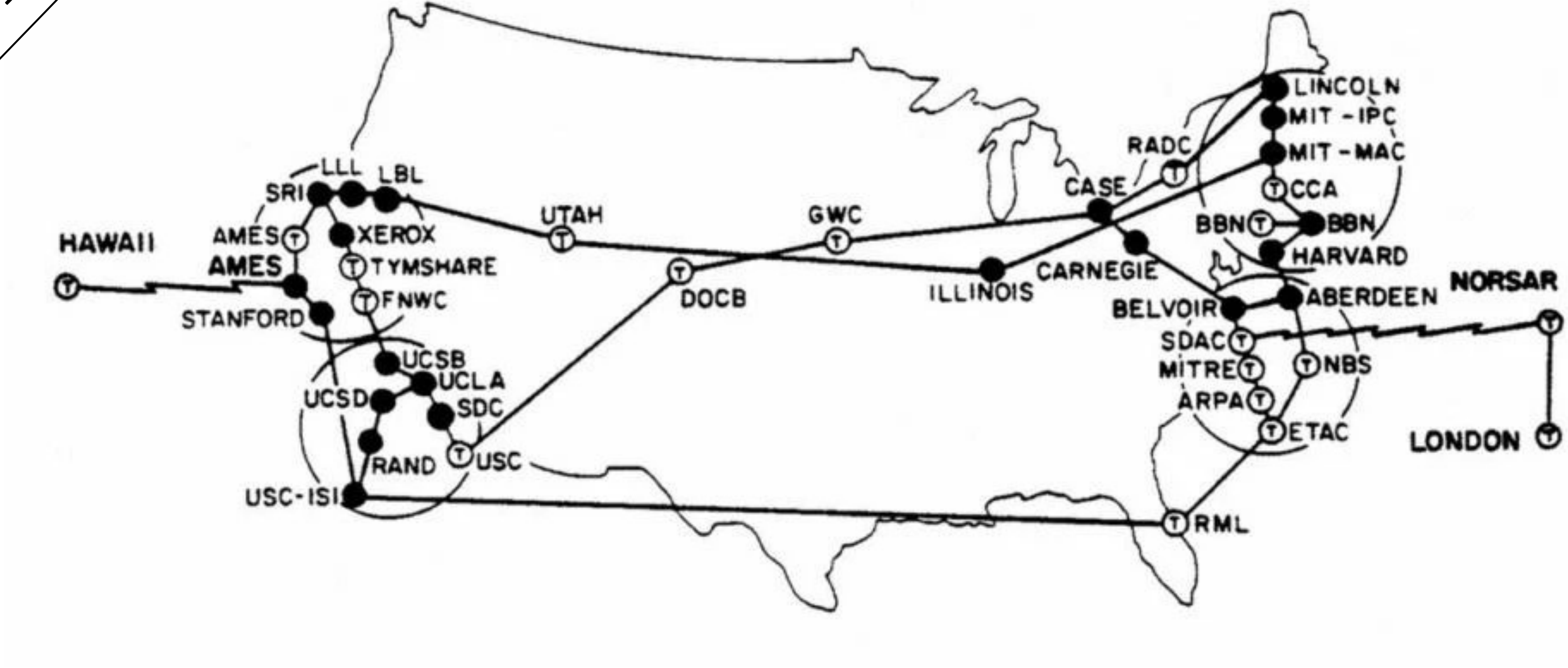


Vint Cerf and Bob Kahn – Inventors of TCP/IP

Week 10



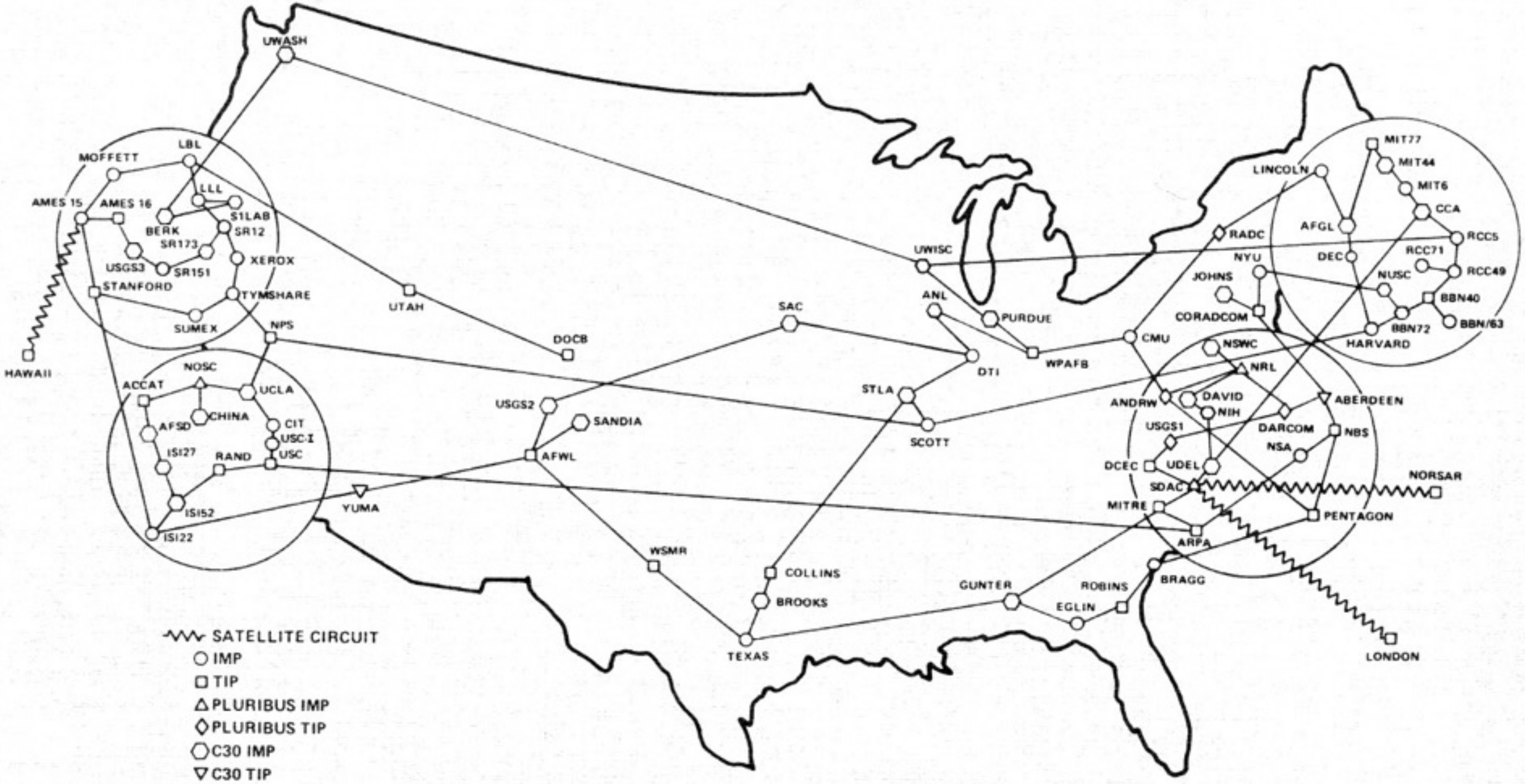
Internet 1969



Internet 1973

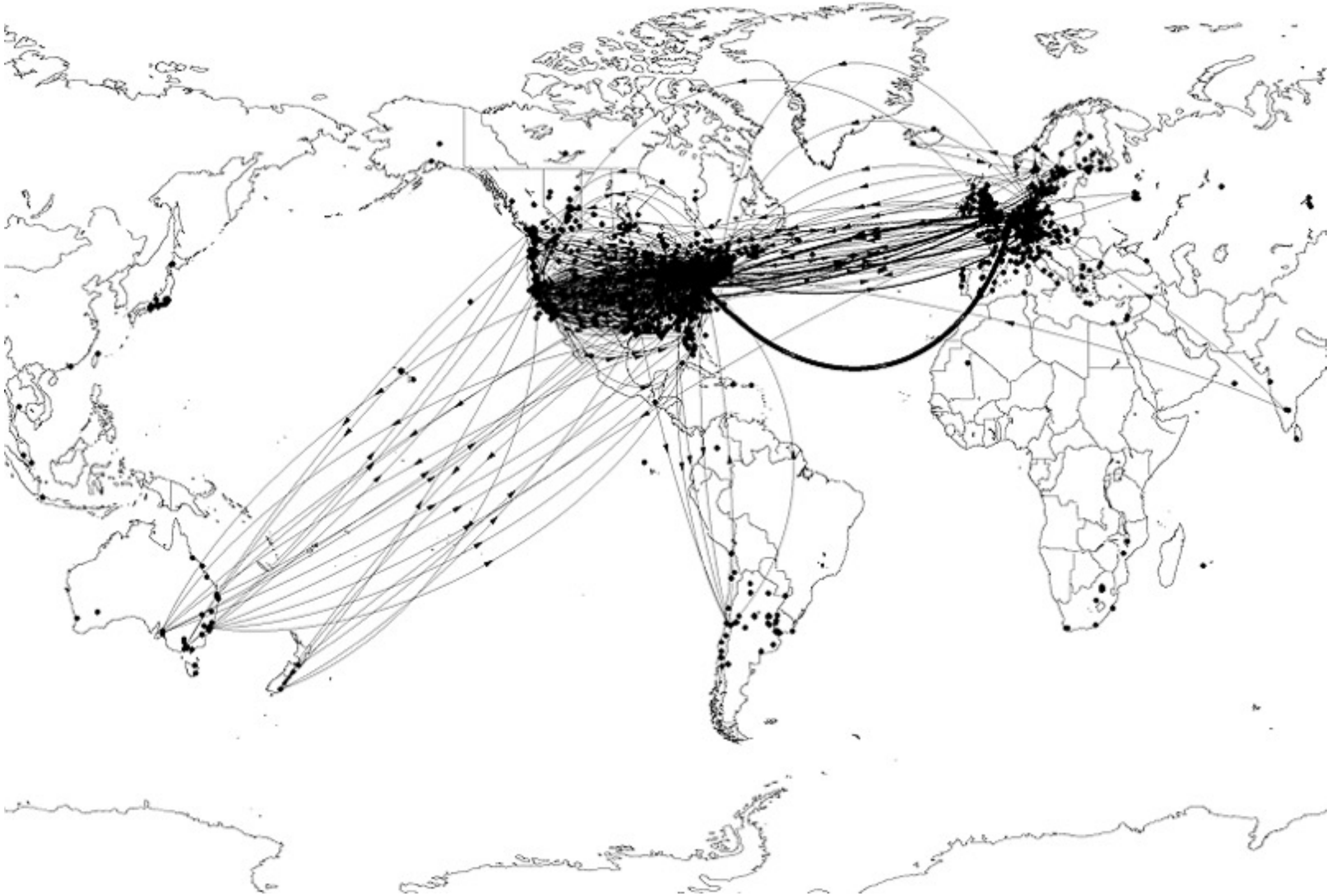
Week 10

ARPANET GEOGRAPHIC MAP, FEBRUARY 1982



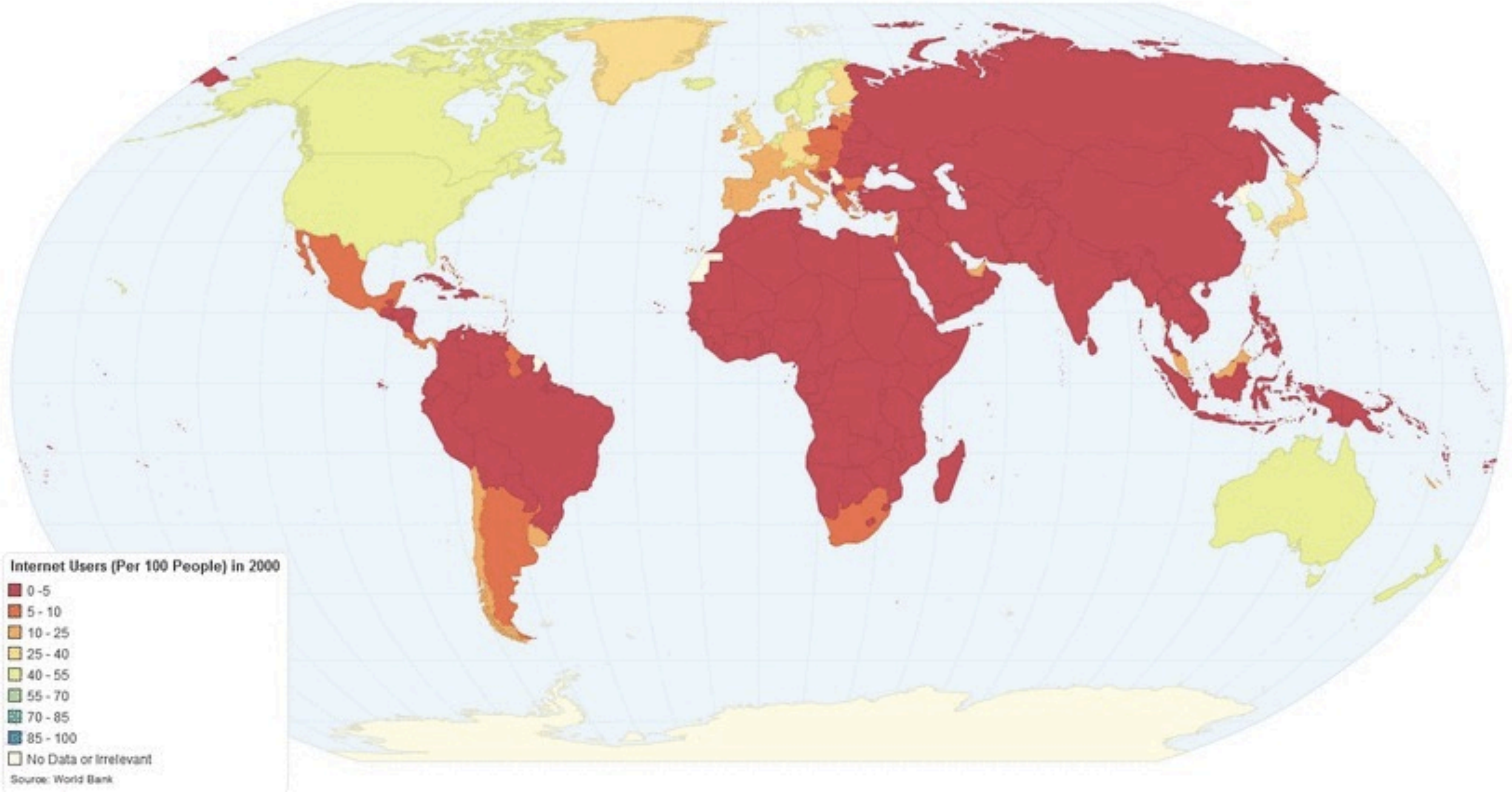
(NOTE: THIS MAP DOES NOT SHOW ARPA'S EXPERIMENTAL SATELLITE CONNECTIONS)
NAMES SHOWN ARE IMP NAMES, NOT (NECESSARILY) HOST NAMES

Internet 1982



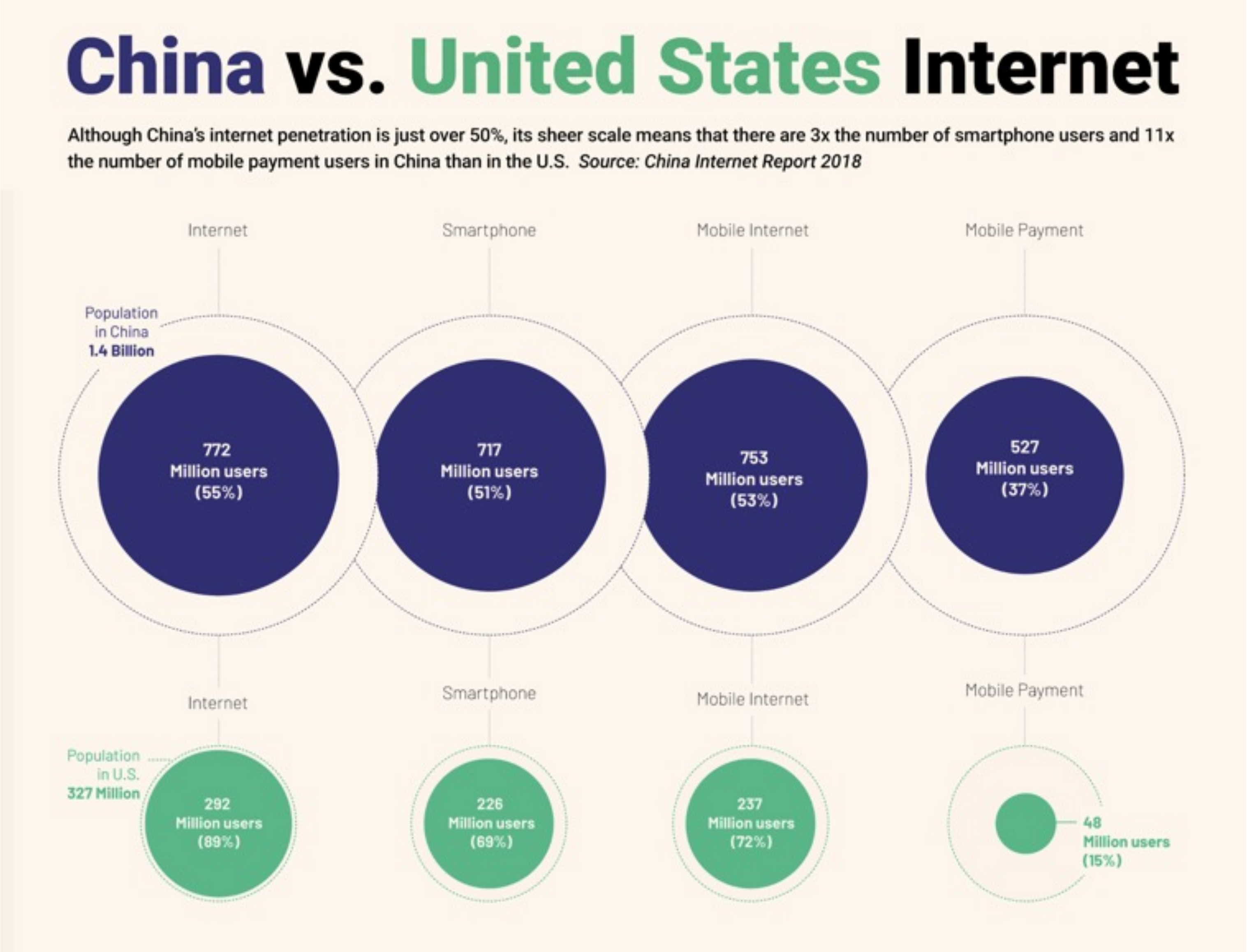
Internet 1993

Week 10



Internet 2000

Week 10



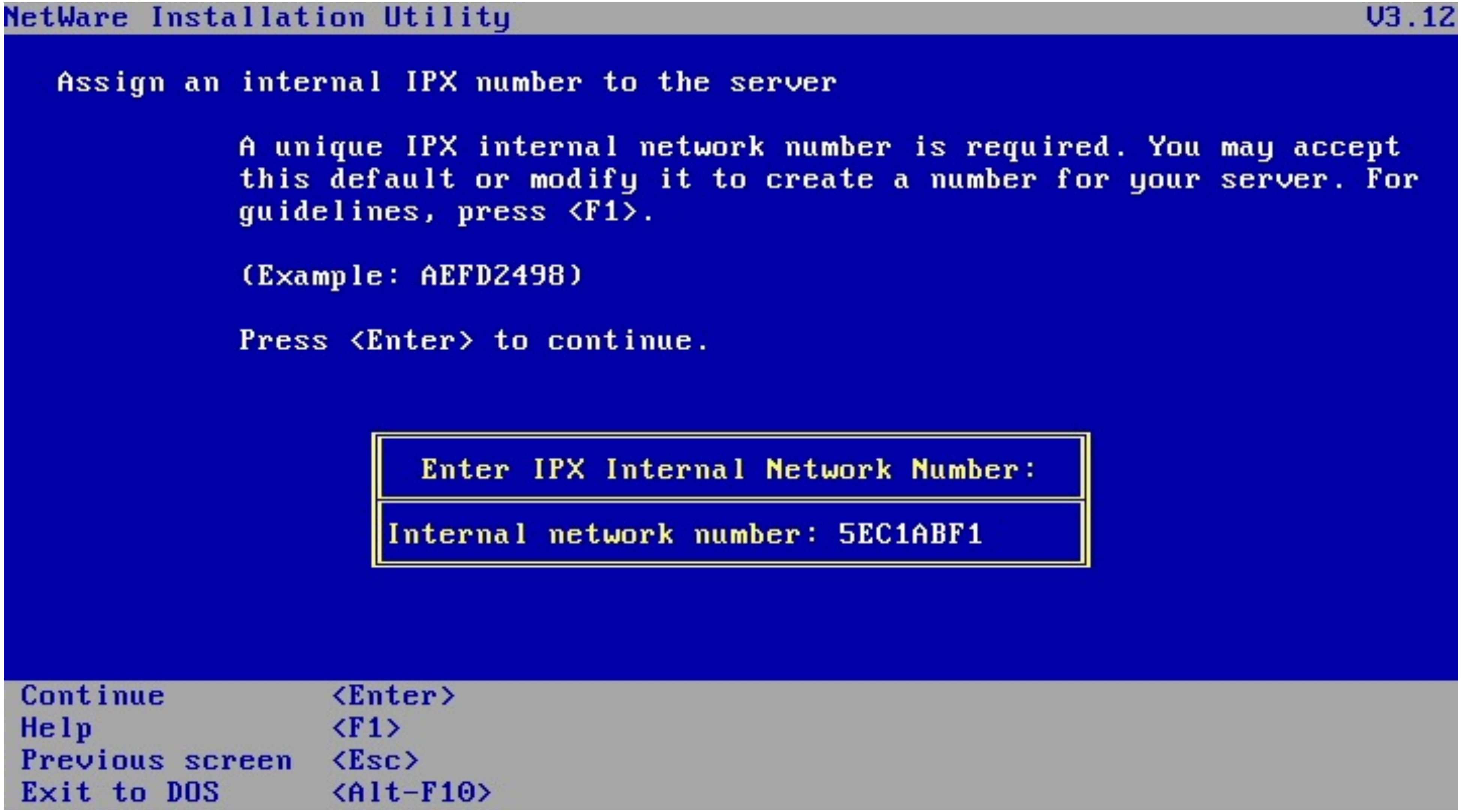
China vs. United States Internet

Although China's internet penetration is just over 50%, its sheer scale means that there are 3x the number of smartphone users and 11x the number of mobile payment users in China than in the U.S. *Source: China Internet Report 2018*

Internet 2018

How Have Networks Evolved?

Week 10



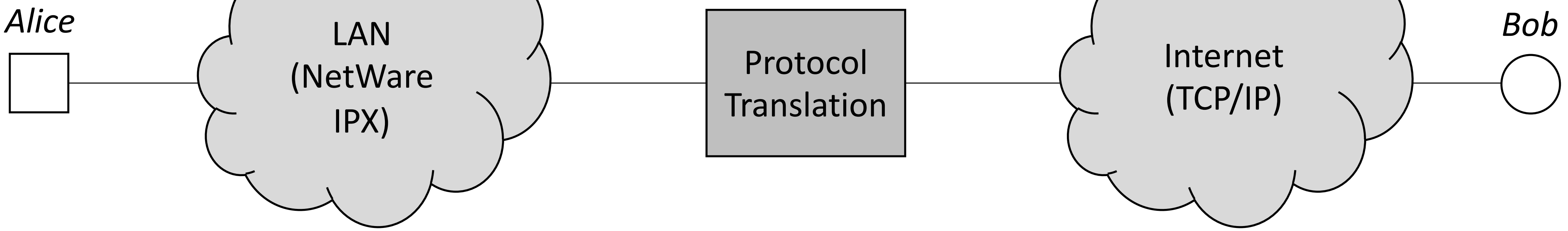
```
NetWare Installation Utility                                          V3.12

  Assign an internal IPX number to the server

            A unique IPX internal network number is required. You may accept
            this default or modify it to create a number for your server. For
            guidelines, press <F1>.

            (Example: AEFD2498)

            Press <Enter> to continue.


                    Enter IPX Internal Network Number:

                    Internal network number: 5EC1ABF1

 Continue          <Enter>
 Help              <F1>
 Previous screen   <Esc>
 Exit to DOS       <Alt-F10>
```

Novell NetWare – IPX Protocol (70% of LAN Market in 90’s)

Week 10

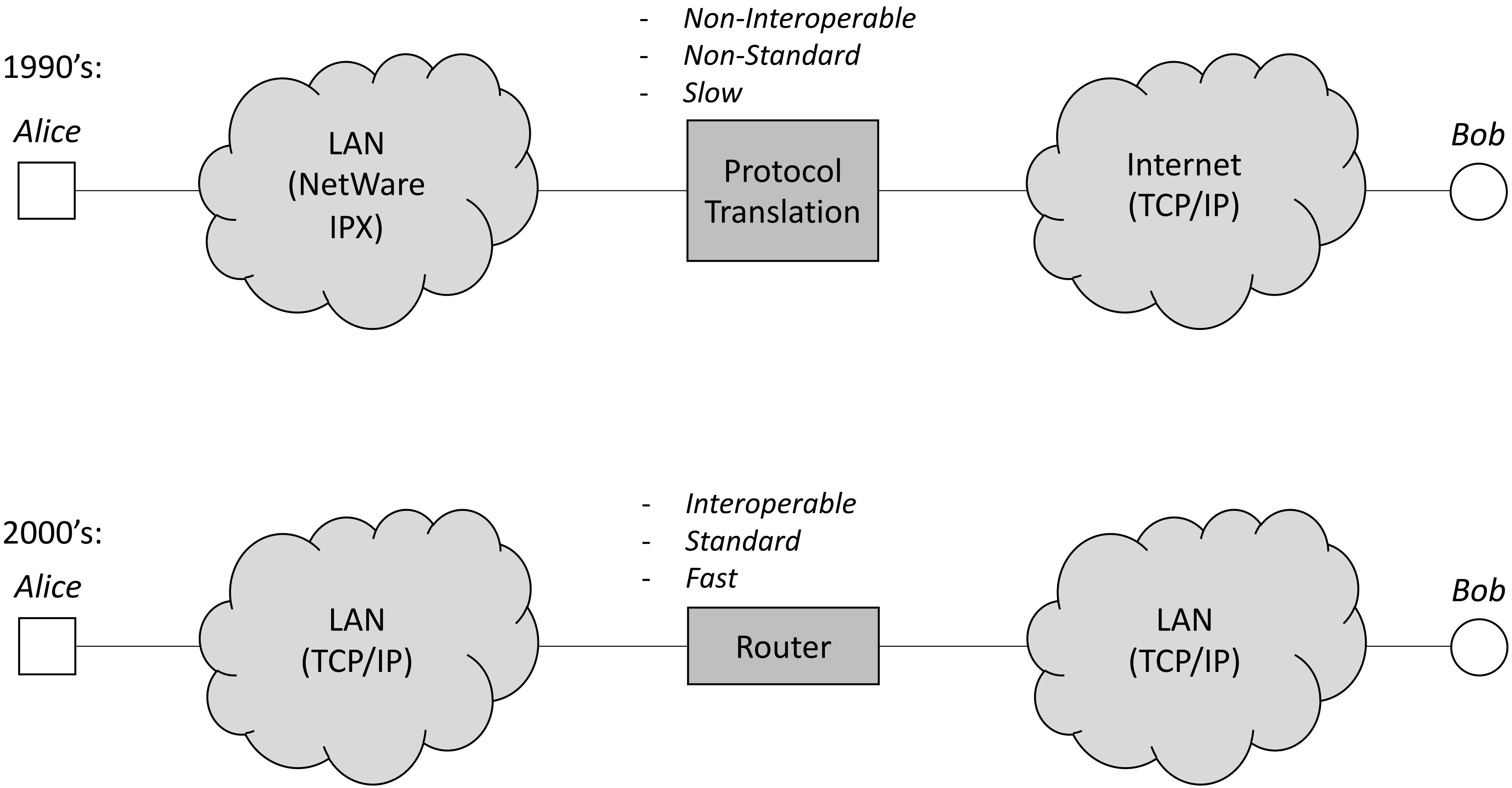
1990's:

- *Non-Interoperable*
- *Non-Standard*
- *Slow*



LAN Protocol Evolution to TCP/IP

Week 10



1990’s:

Alice

LAN
(NetWare
IPX)

- *Non-Interoperable*
- *Non-Standard*
- *Slow*

Protocol
Translation

Internet
(TCP/IP)

Bob

2000’s:

Alice

LAN
(TCP/IP)

- *Interoperable*
- *Standard*
- *Fast*

Router

LAN
(TCP/IP)

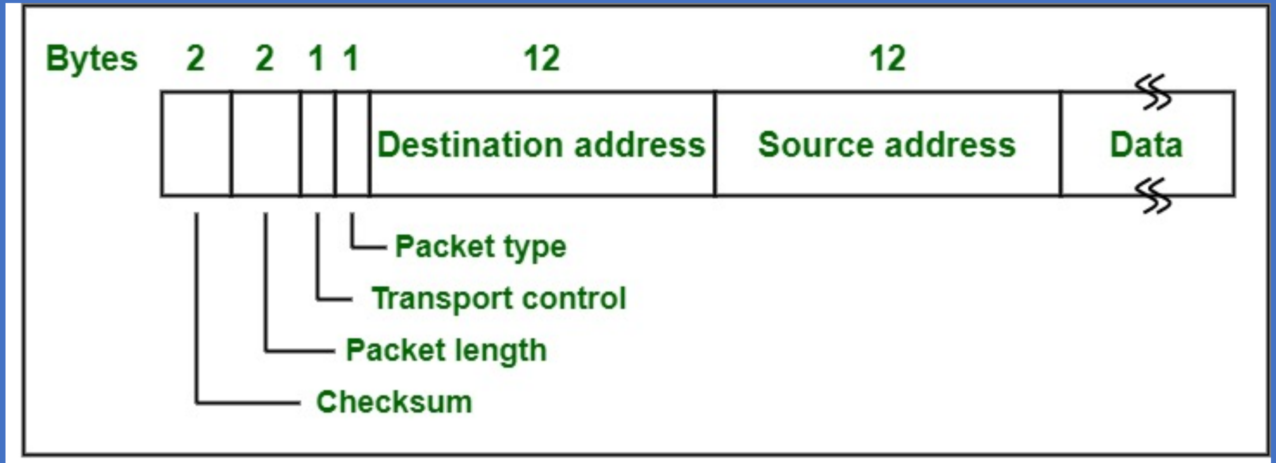
Bob

LAN Protocol Evolution to TCP/IP

Week 10

Local Netware IPX Dissolved into Native IP Networks

Making Analyst Predictions . . .

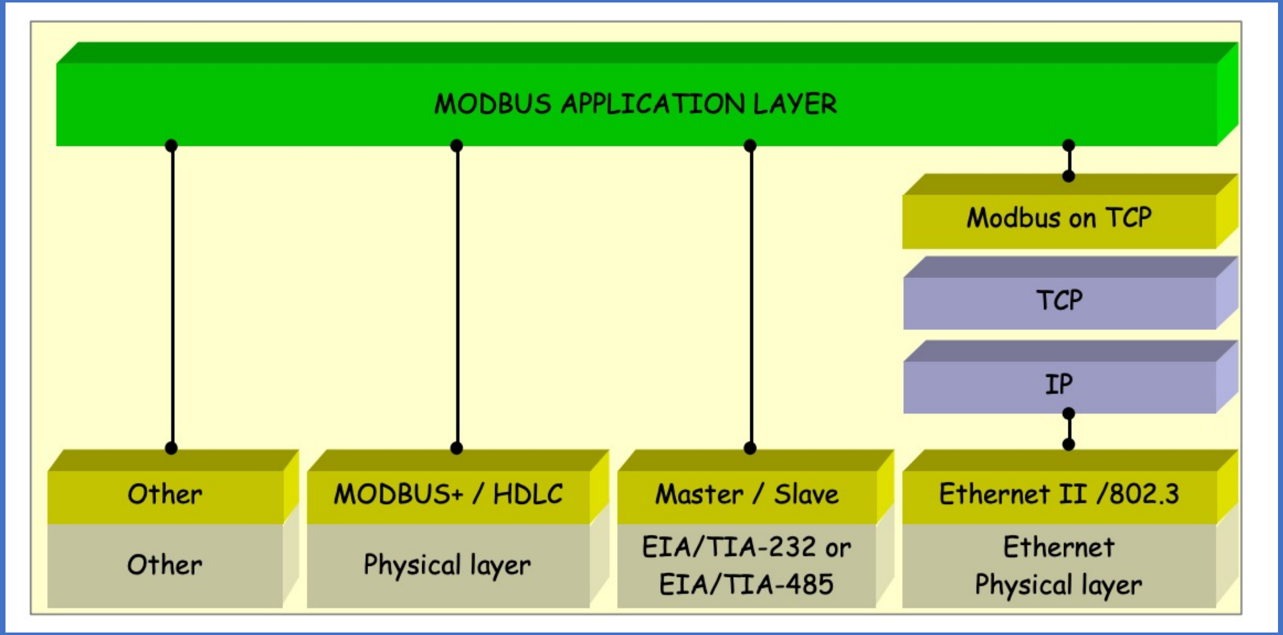


A Novell NetWare IPX Packet

Week 10

OT Networks Will Dissolve into Native IT Networks

Making Analyst Predictions . . .



MODBUS APPLICATION LAYER

Modbus on TCP

TCP

IP

Other

Other

MODBUS+ / HDLC

Physical layer

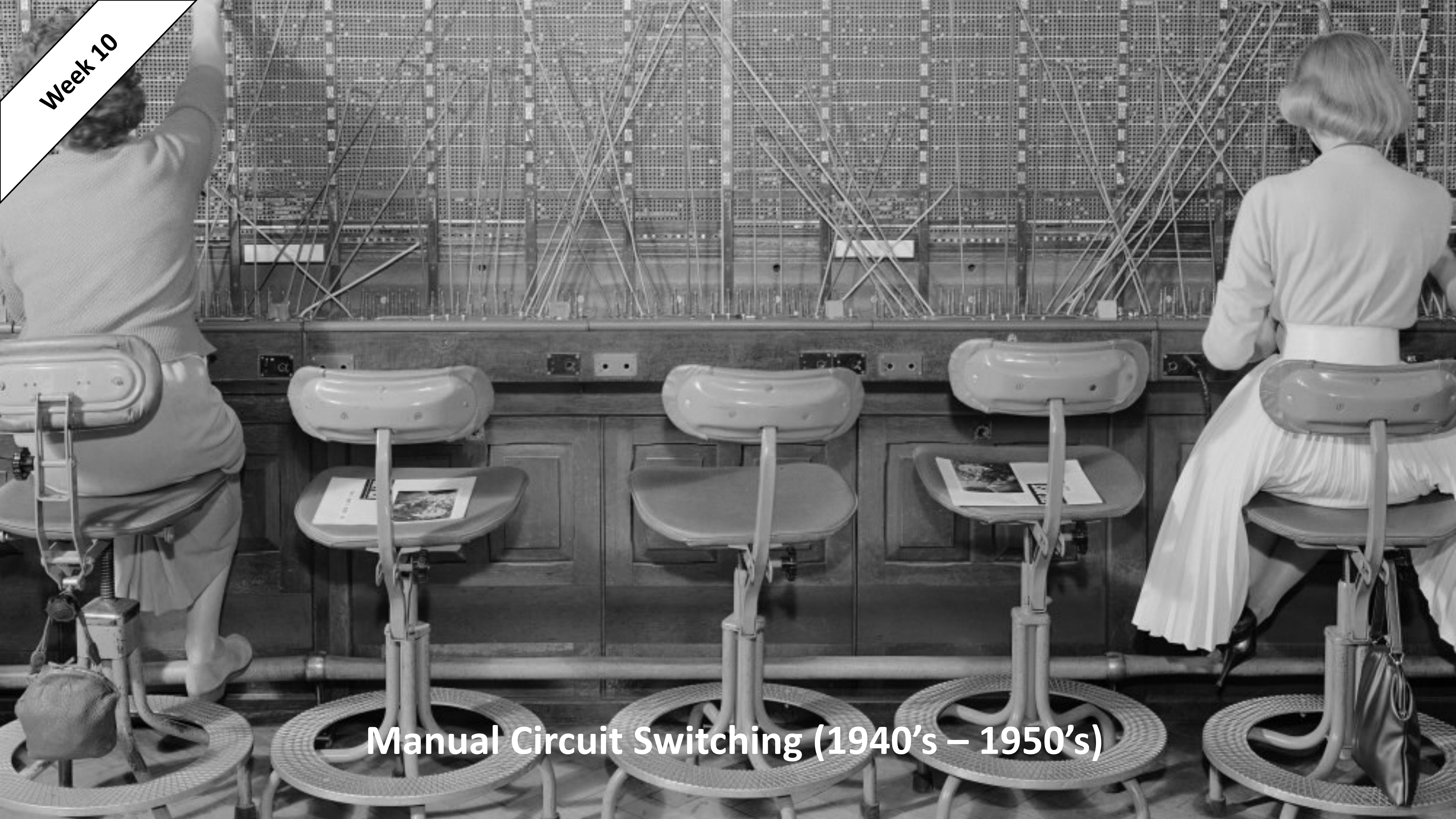
Master / Slave

EIA/TIA-232 or EIA/TIA-485

Ethernet II /802.3

Ethernet Physical layer

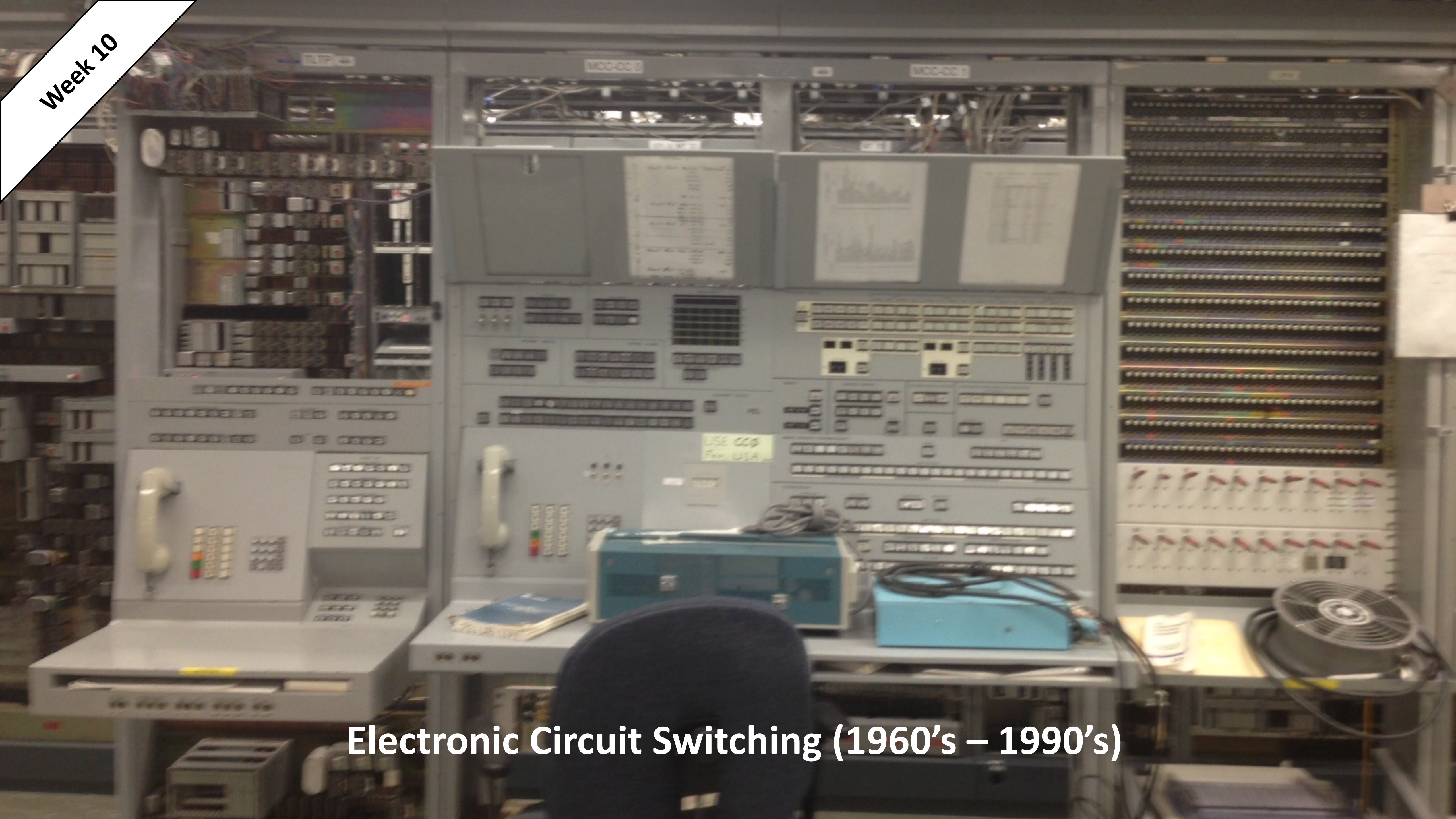
What is Circuit Switching?



Week 10

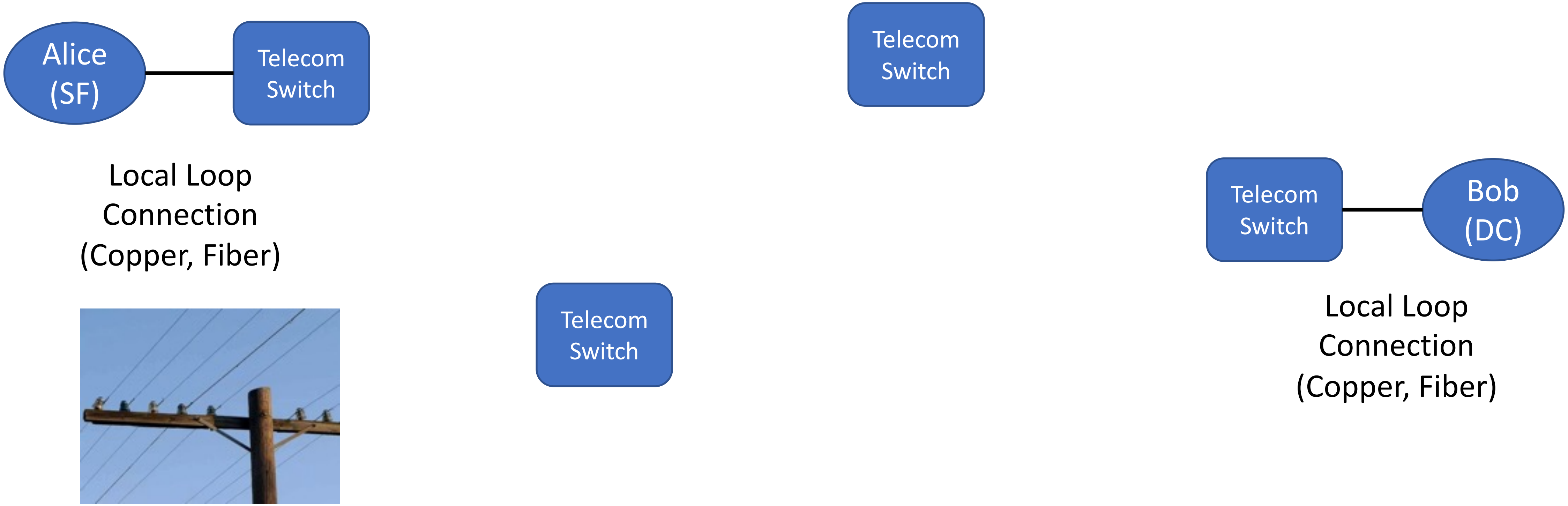
Manual Circuit Switching (1940’s – 1950’s)

Week 10



Electronic Circuit Switching (1960’s – 1990’s)

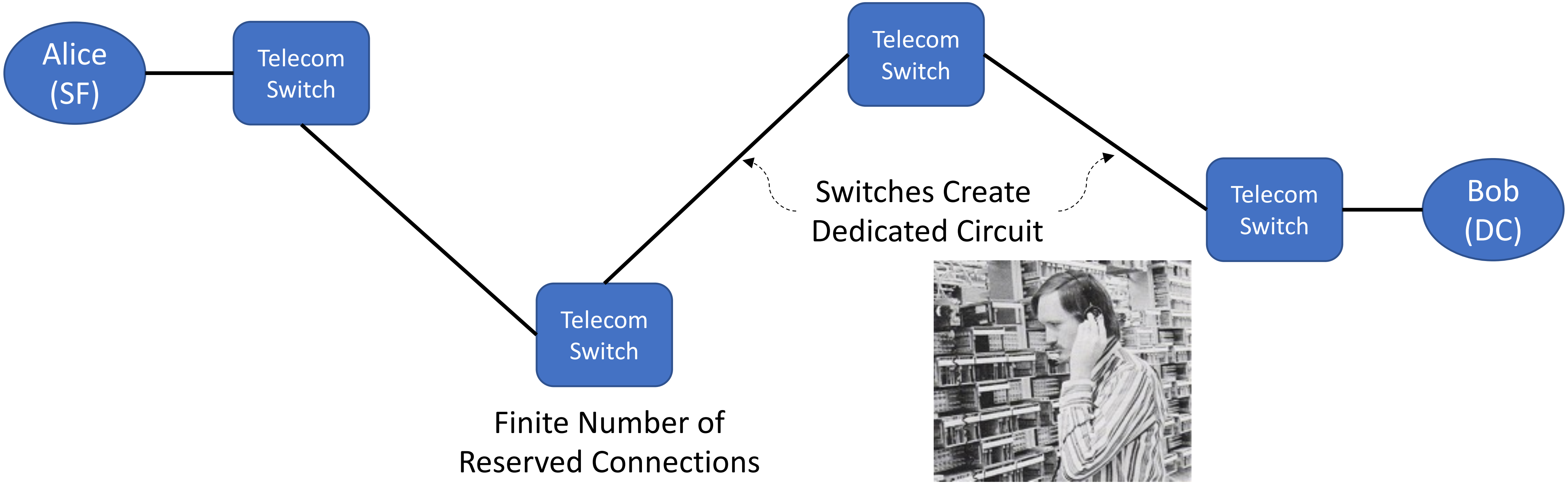
Week 10



Local Loop
Connection
(Copper, Fiber)

Local Loop
Connection
(Copper, Fiber)

Circuit-Switched Networks (1960 – 2000)



Alice (SF)

Telecom Switch

Telecom Switch

Telecom Switch

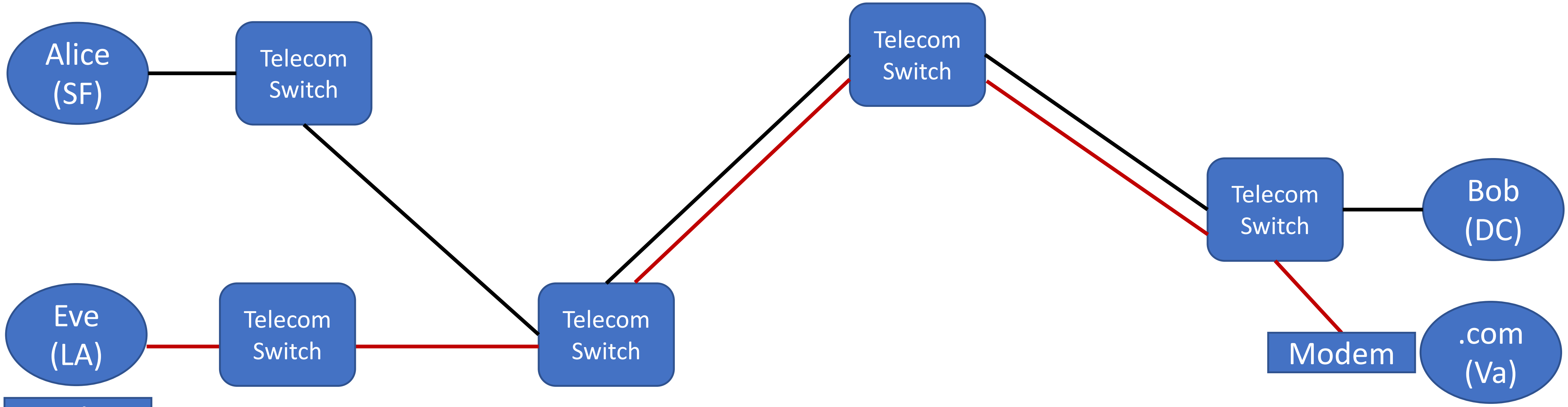
Telecom Switch

Bob (DC)

Switches Create Dedicated Circuit

Finite Number of Reserved Connections

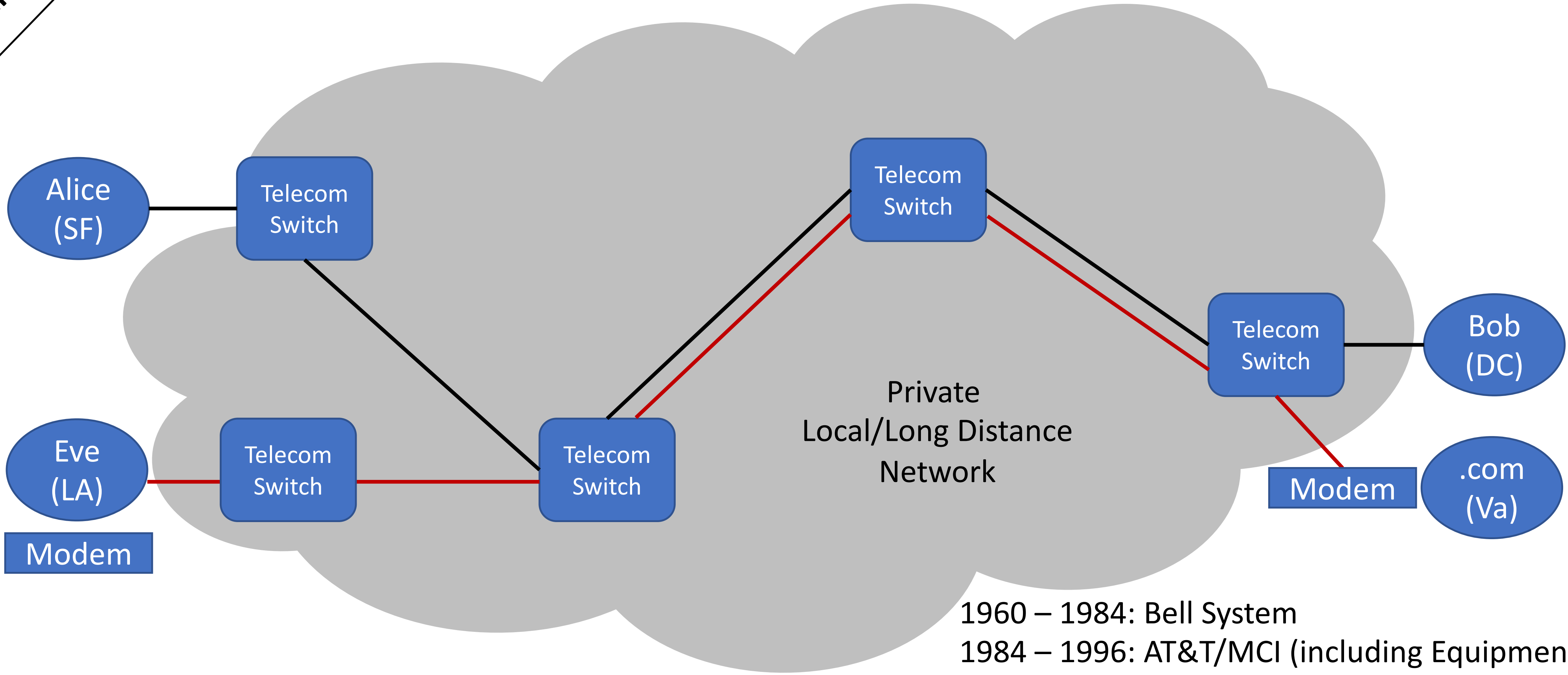
Circuit-Switched Networks – Point-to-Point Connection



Modem

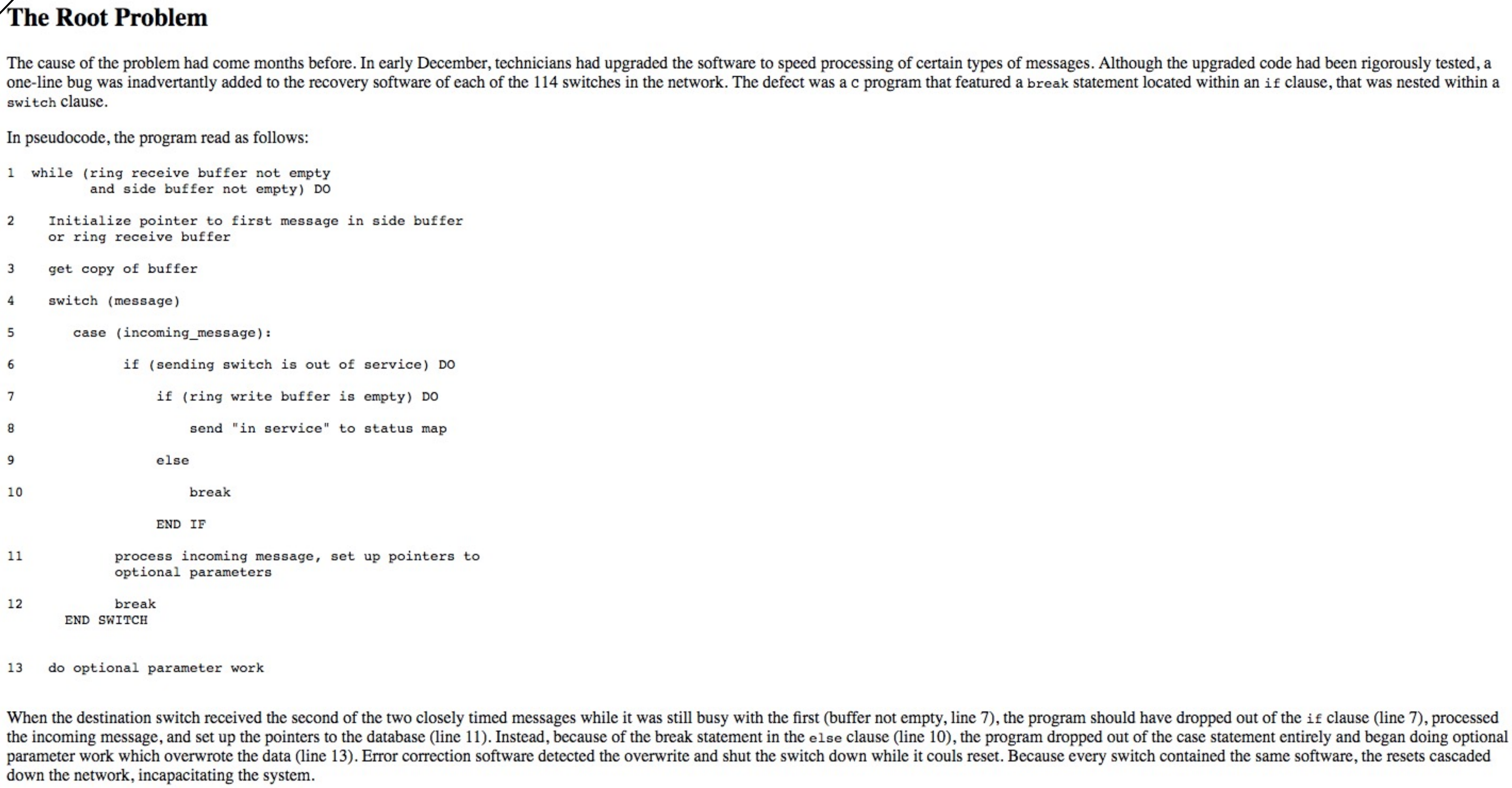
Circuit-Switched Network – Circuit Sharing

Week 10



1960 – 1984: Bell System
1984 – 1996: AT&T/MCI (including Equipment)
1996 – Present: Separate Network from Equipment

Circuit-Switched Network – Long Distance Network



The Root Problem

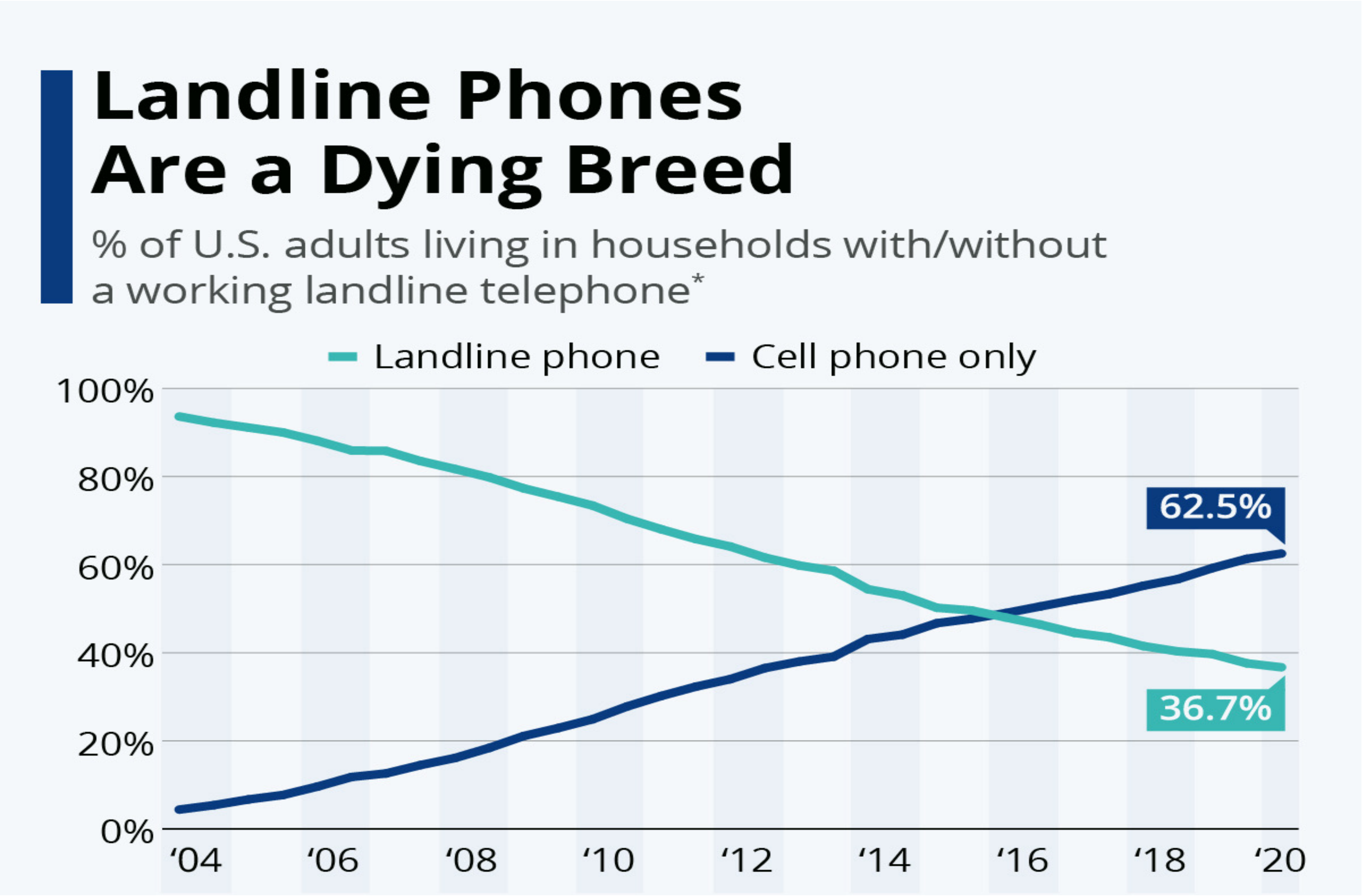
The cause of the problem had come months before. In early December, technicians had upgraded the software to speed processing of certain types of messages. Although the upgraded code had been rigorously tested, a one-line bug was inadvertantly added to the recovery software of each of the 114 switches in the network. The defect was a `C` program that featured a `break` statement located within an `if` clause, that was nested within a `switch` clause.

In pseudocode, the program read as follows:

```
1  while (ring receive buffer not empty
          and side buffer not empty) DO

2    Initialize pointer to first message in side buffer
     or ring receive buffer

3    get copy of buffer

4    switch (message)

5       case (incoming_message):

6              if (sending switch is out of service) DO

7                  if (ring write buffer is empty) DO

8                      send "in service" to status map

9                  else

10                     break

                   END IF

11           process incoming message, set up pointers to
             optional parameters

12           break
       END SWITCH


13   do optional parameter work
```

When the destination switch received the second of the two closely timed messages while it was still busy with the first (buffer not empty, line 7), the program should have dropped out of the `if` clause (line 7), processed the incoming message, and set up the pointers to the database (line 11). Instead, because of the break statement in the `else` clause (line 10), the program dropped out of the case statement entirely and began doing optional parameter work which overwrote the data (line 13). Error correction software detected the overwrite and shut the switch down while it couls reset. Because every switch contained the same software, the resets cascaded down the network, incapacitating the system.

January 15, 1990 – Nationwide AT&T Outage

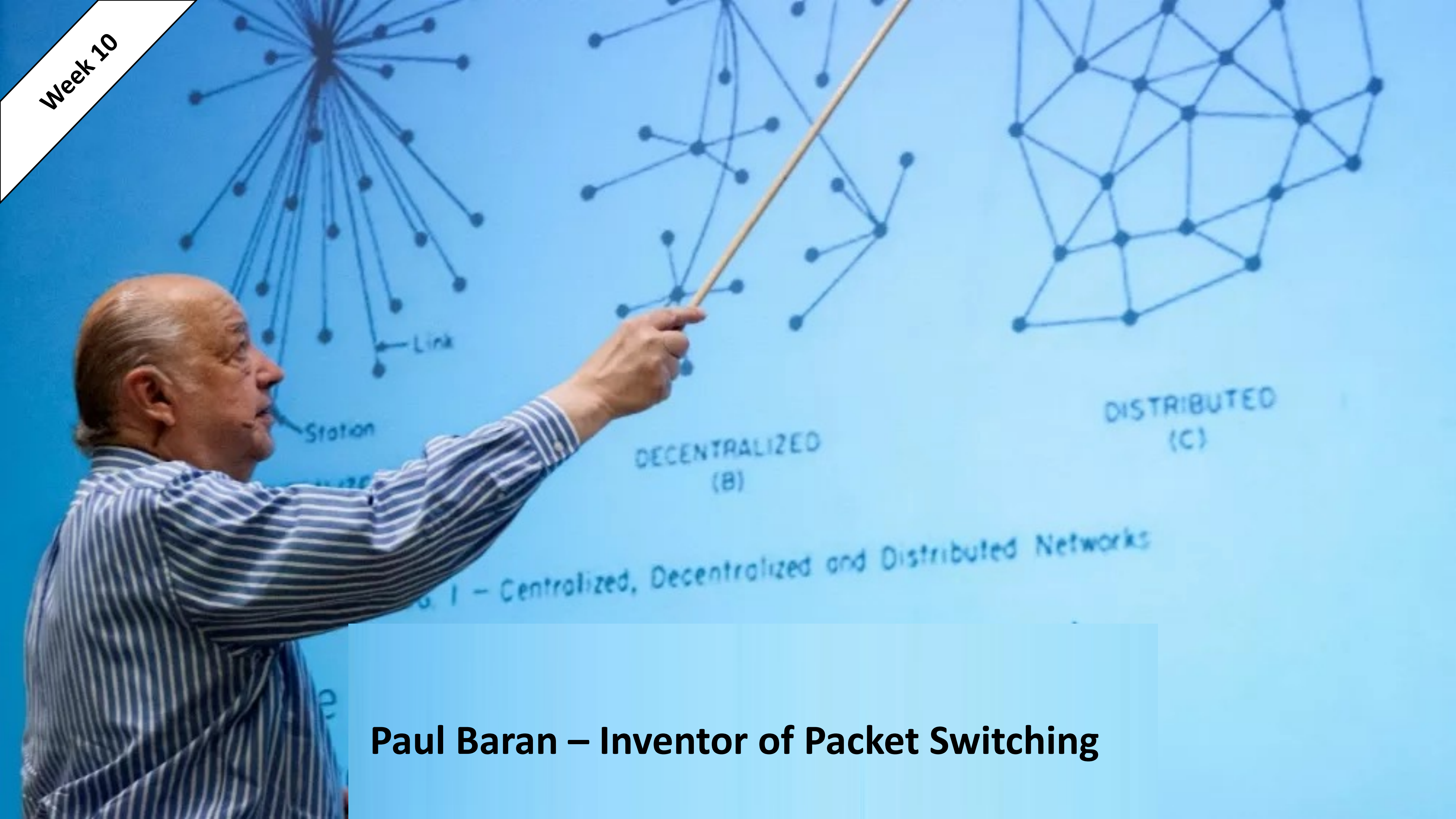


Landline Phones Are a Dying Breed

% of U.S. adults living in households with/without a working landline telephone*

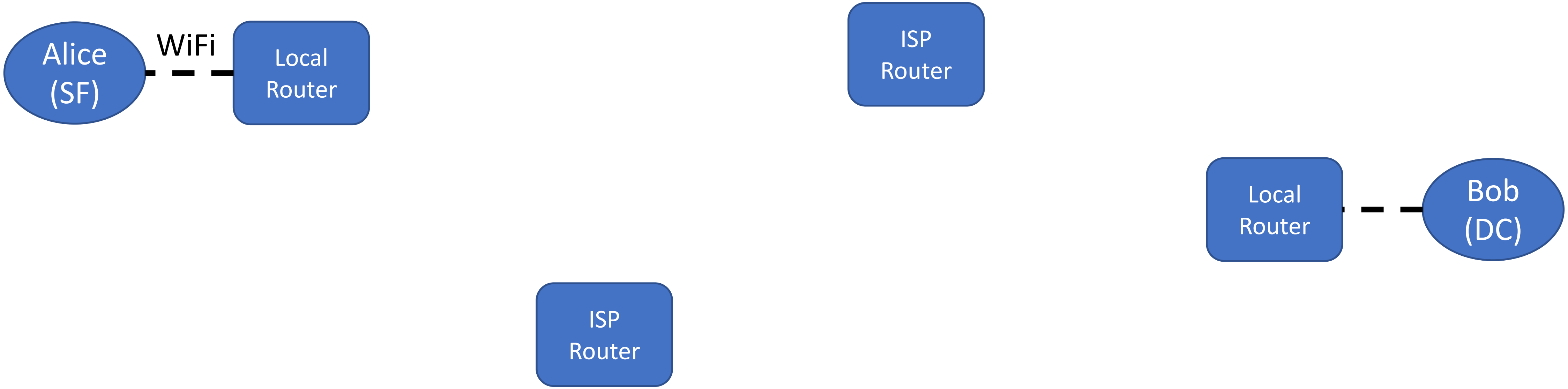
Death of Landline Phones

What is Packet Switching and How is it Used for Wide Area Networks (WANs)?

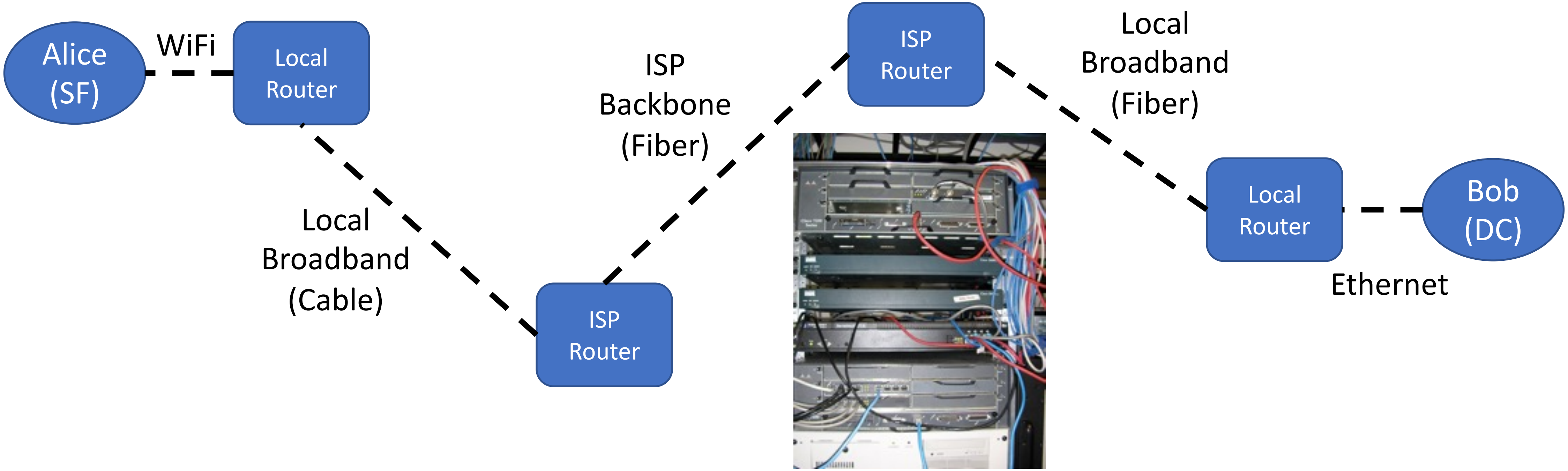


Paul Baran – Inventor of Packet Switching

Week 10

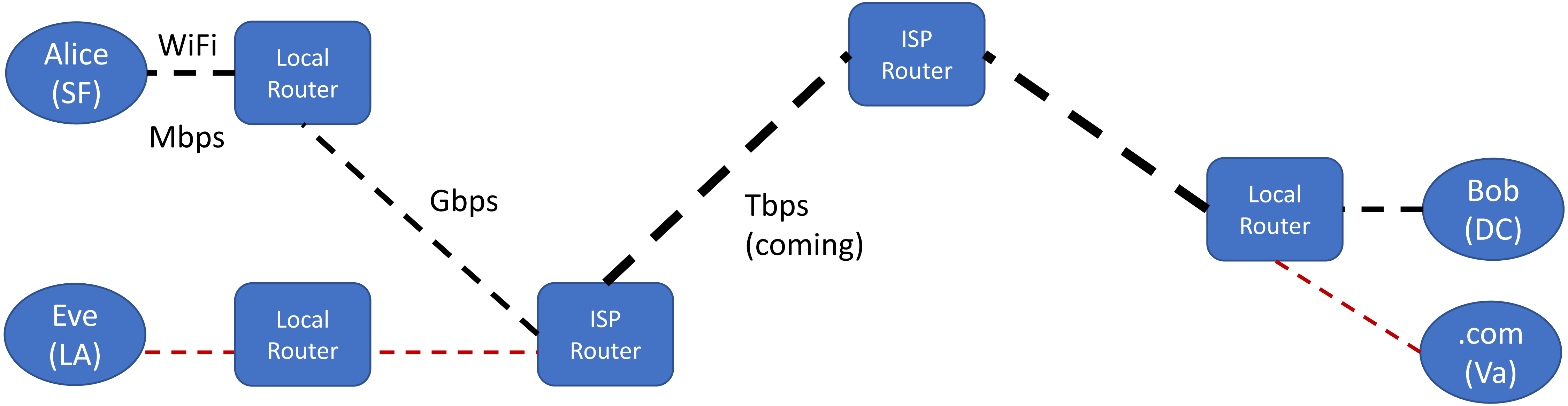


Packet Switching



Packet Switching – Stream of Packets

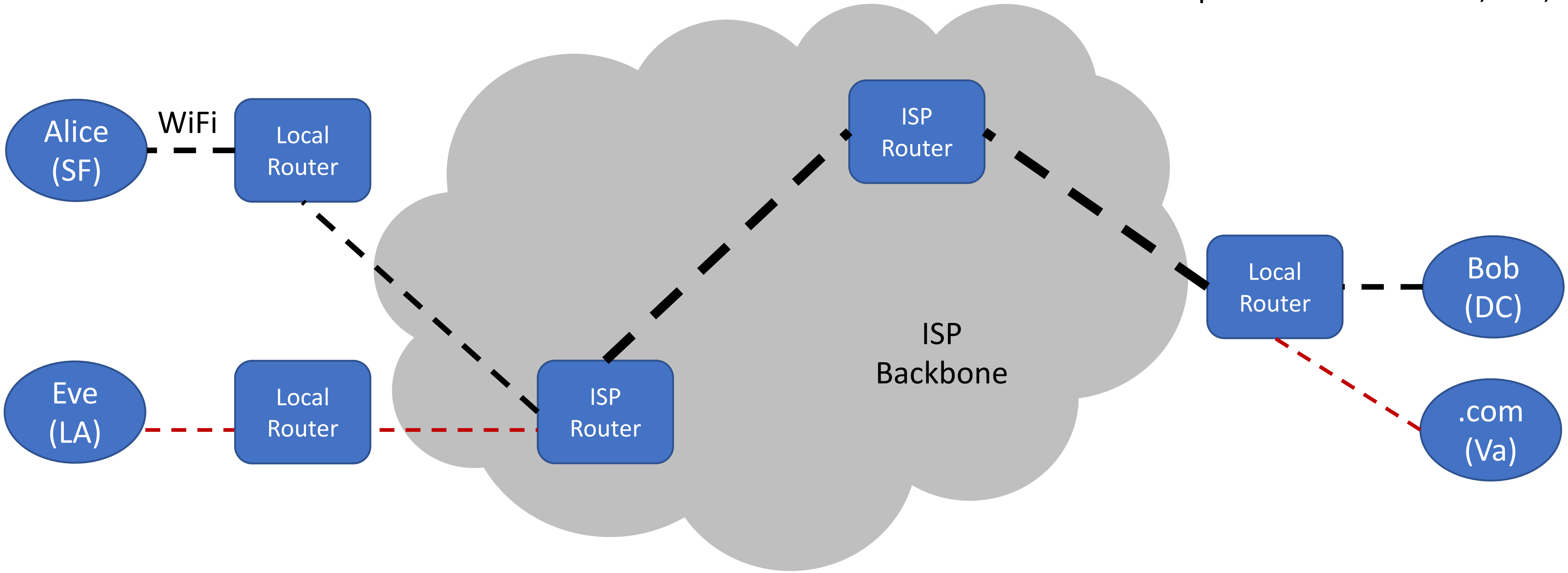
Week 10



Packet Switching – Varying Capacities

Week 10

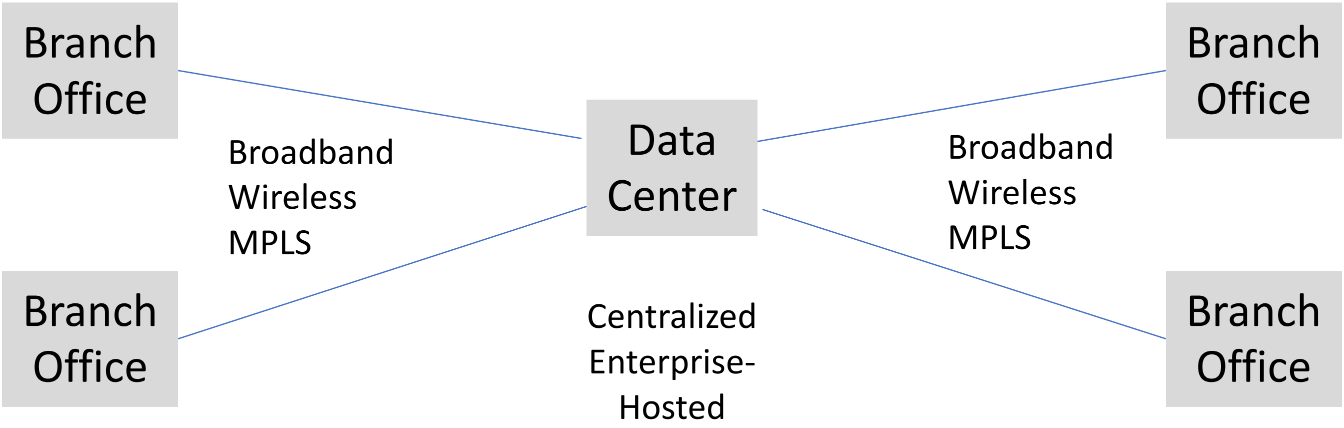
1980’s – 1990’s: Cisco, Lucent, Juniper
1990’s – 2000’s: add Ericsson, Nokia
2000’s – present: add Huawei, ZTE, others



Packet Switching – ISP Backbones

Week 10

Traditional Branch Office WAN – Basic Configuration



Branch Office

Branch Office

Broadband
Wireless
MPLS

Data Center

Centralized
Enterprise-
Hosted

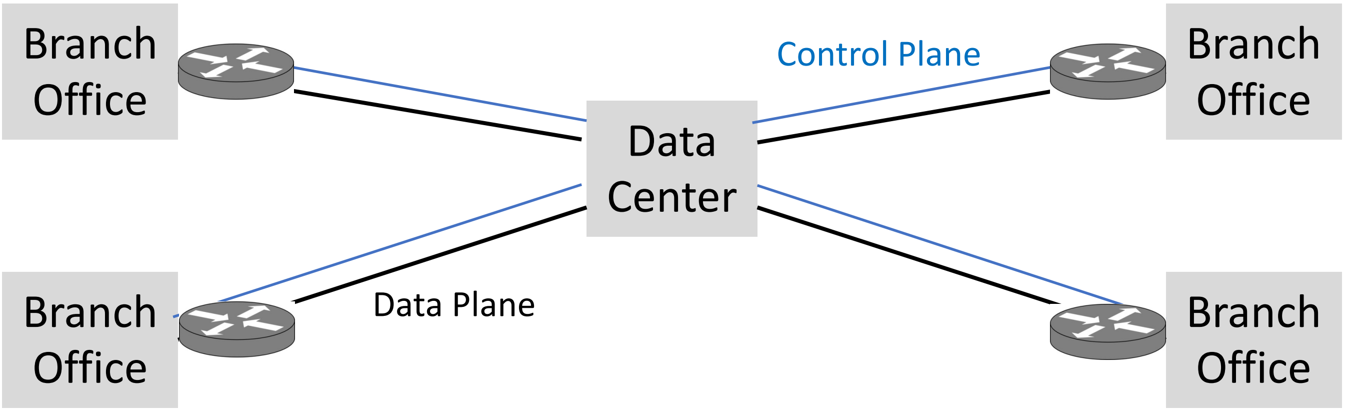
Broadband
Wireless
MPLS

Branch Office

Branch Office

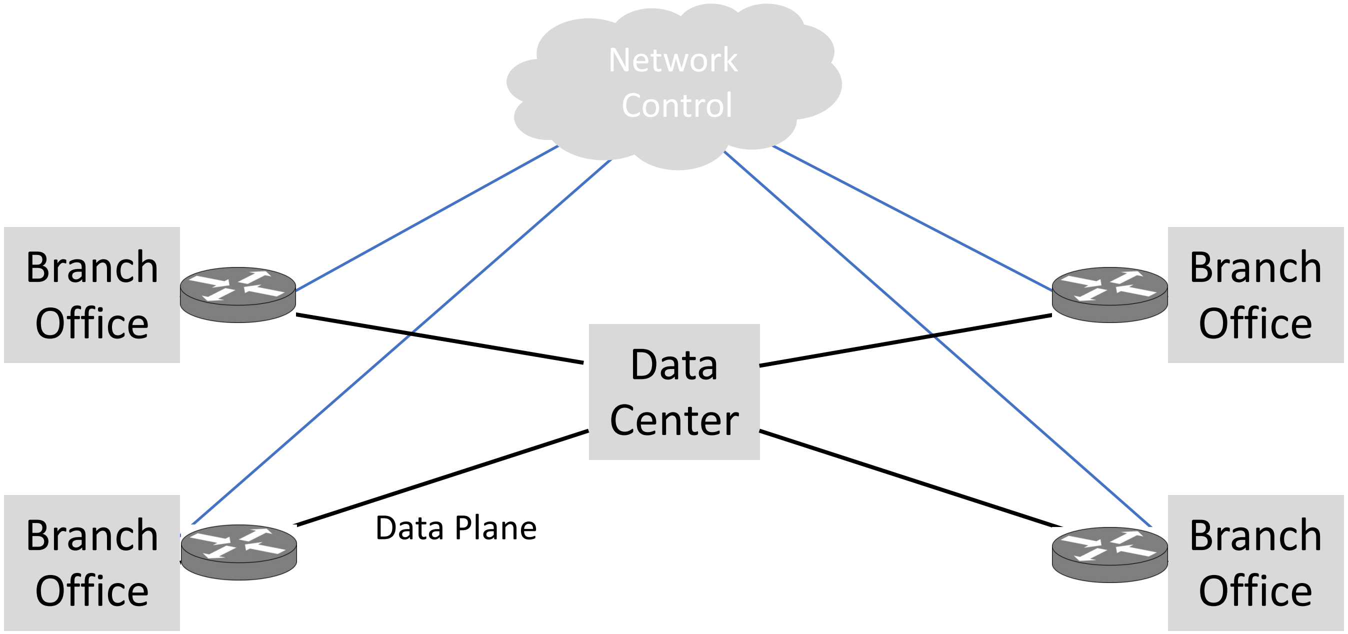
Week 10

Traditional Branch Office WAN – Control and Data Plane Separation



Week 10

Traditional Branch Office WAN – Cloud-Based Network Control

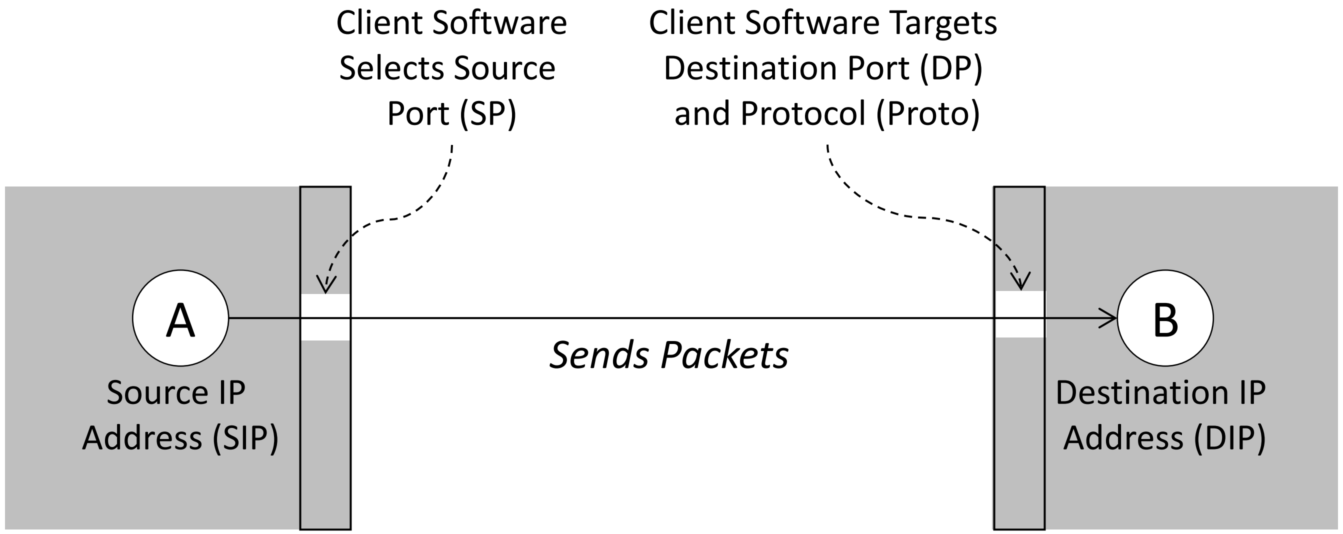


How Does TCP/IP Work?

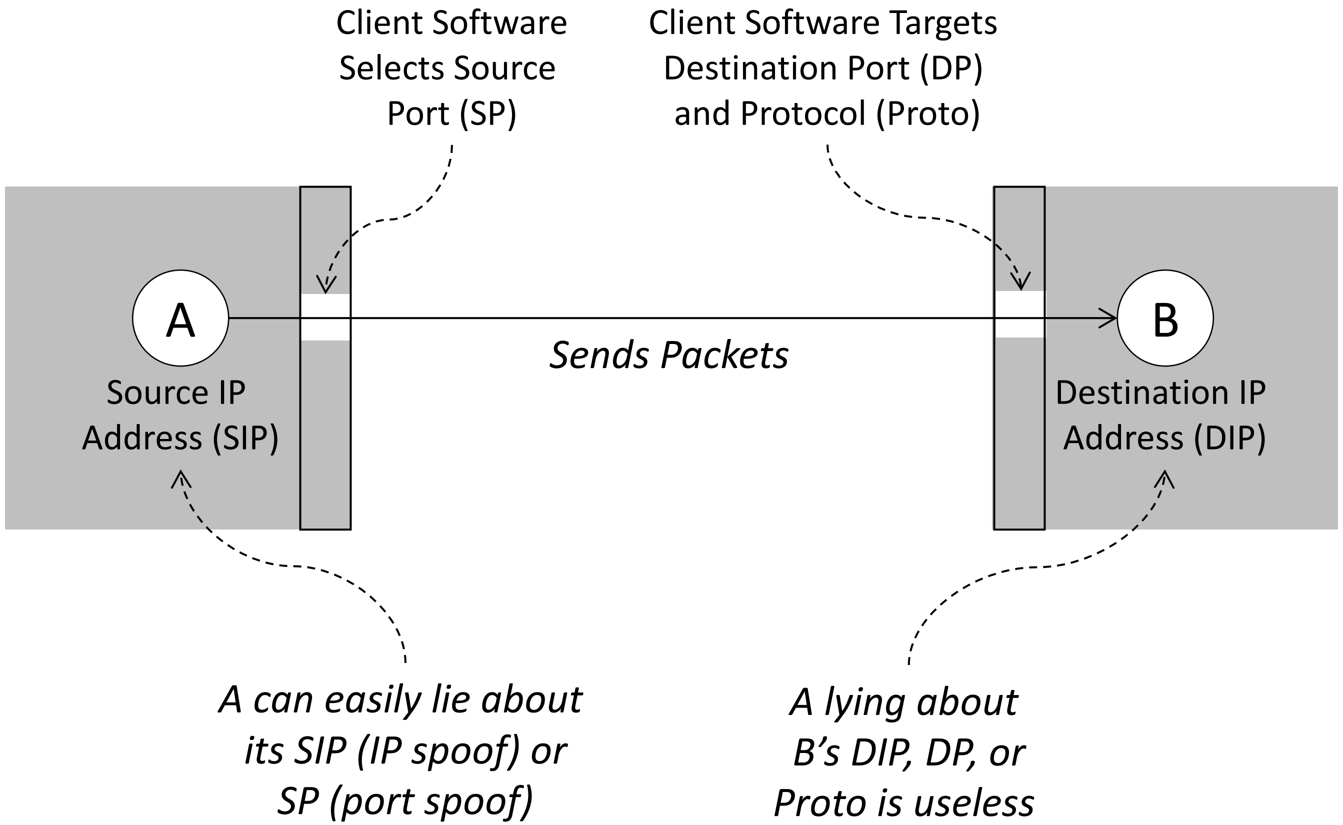
Week 10

A
Source IP Address (SIP)
B
Destination IP Address (DIP)

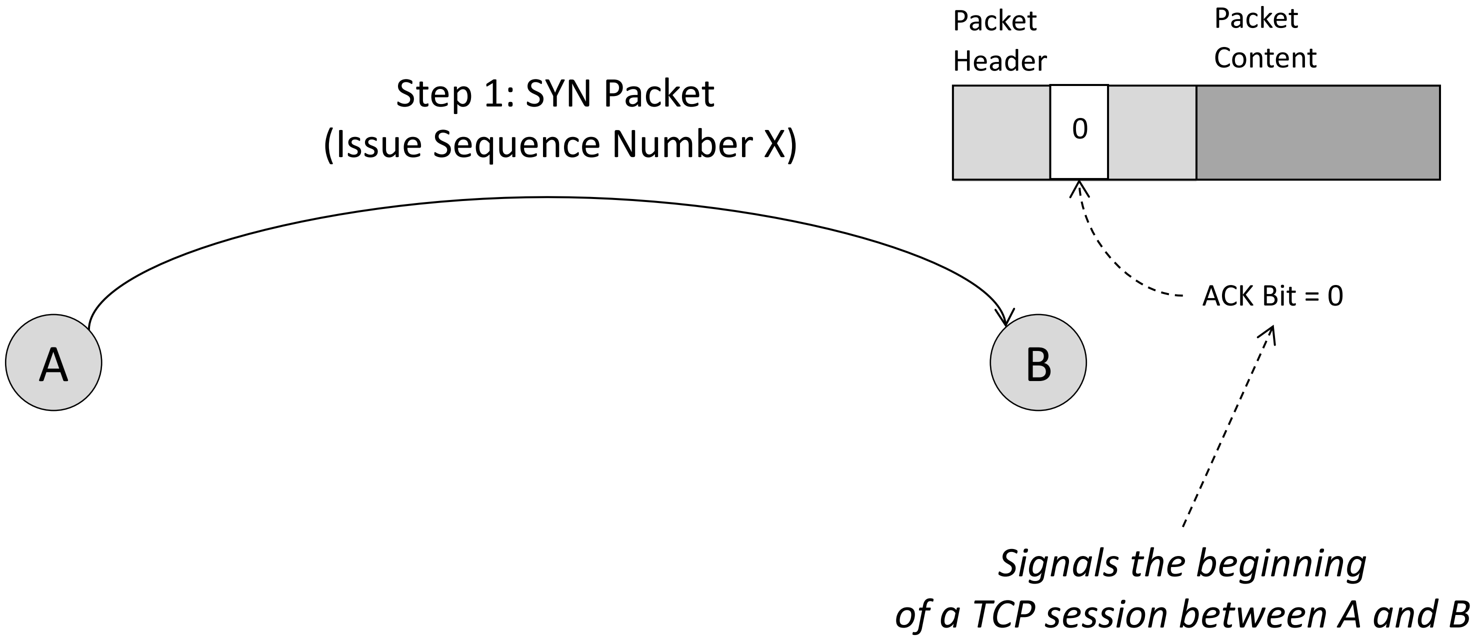
TCP/IP Basics



TCP/IP Basics



TCP/IP Basics

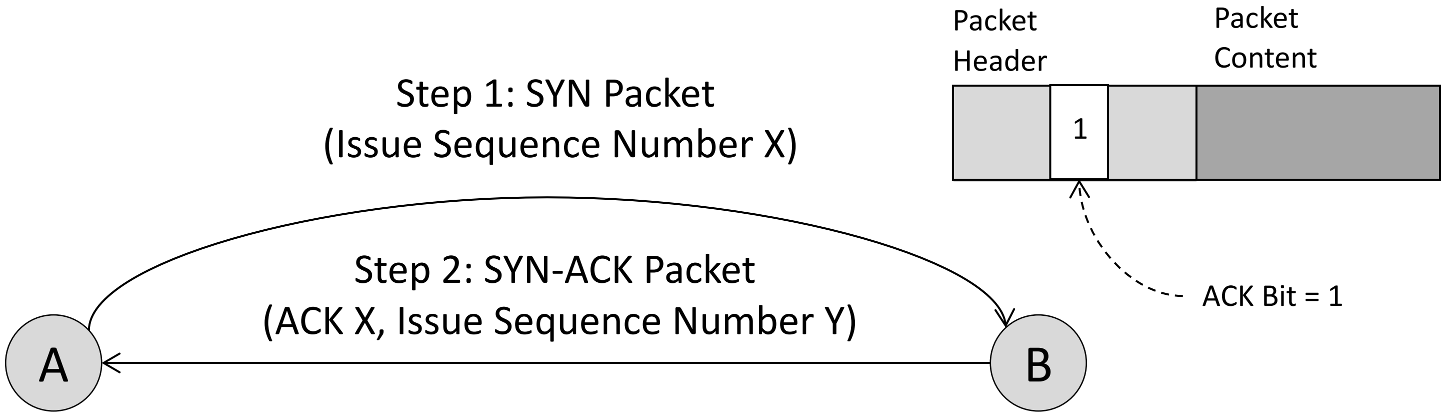


Step 1: SYN Packet
(Issue Sequence Number X)

Signals the beginning of a TCP session between A and B

Three-Step TCP Handshake

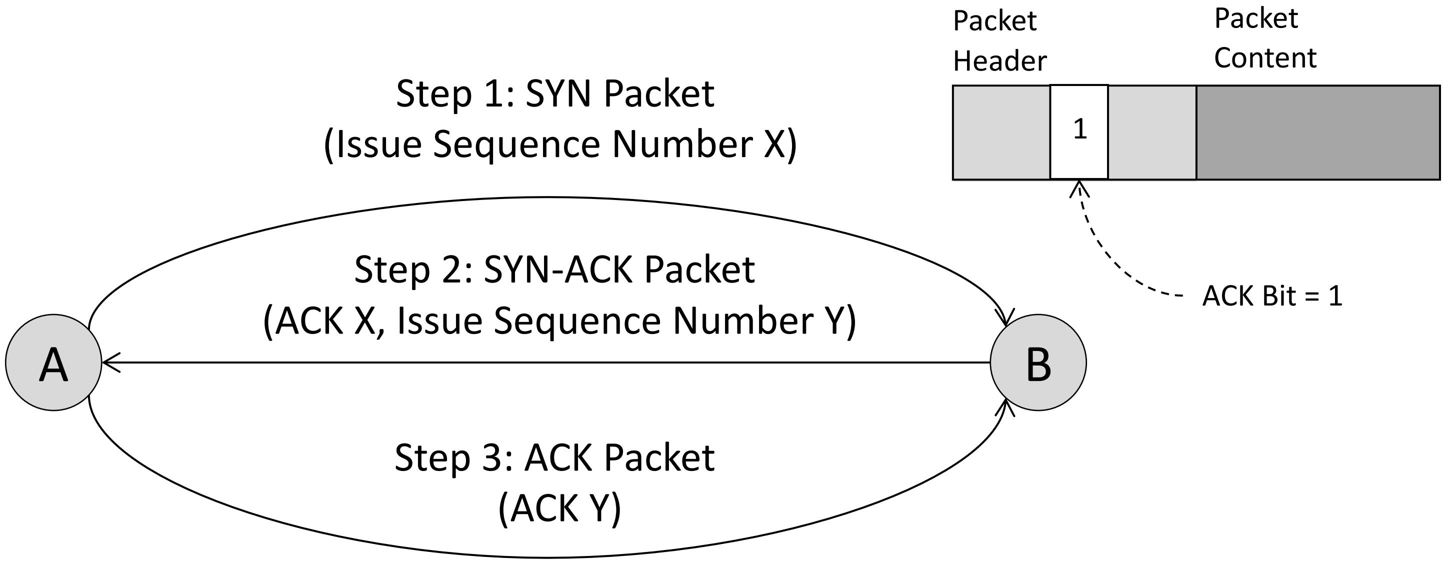
Week 10



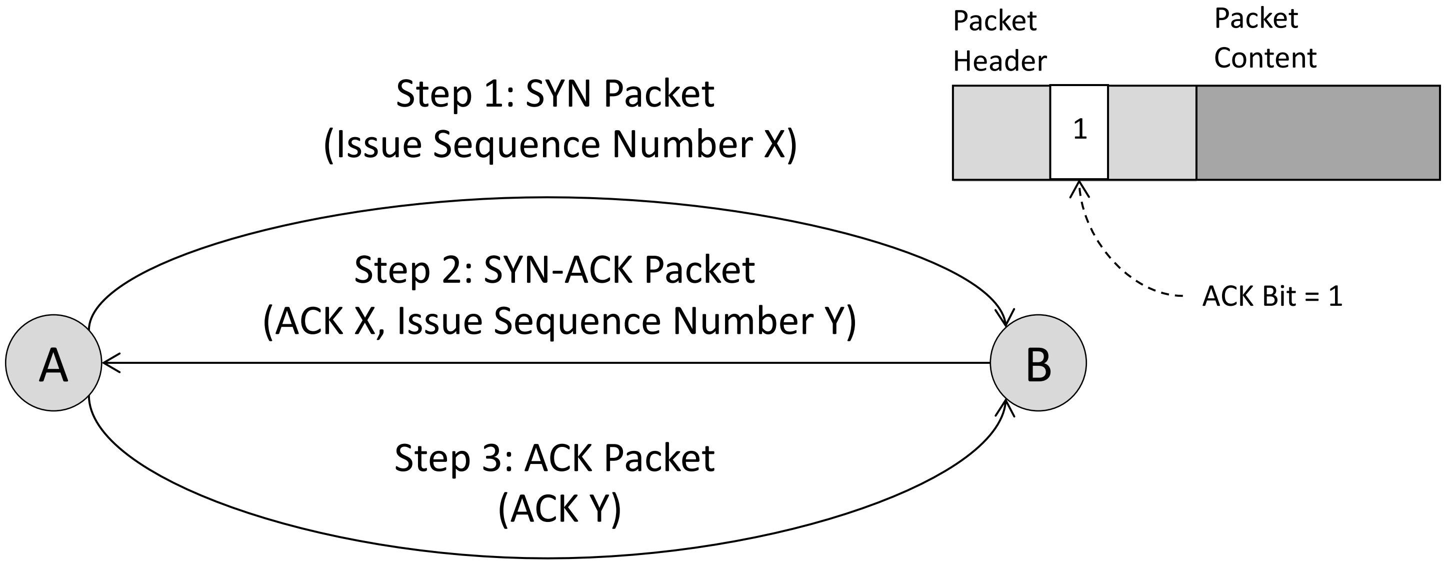
Step 1: SYN Packet
(Issue Sequence Number X)

Step 2: SYN-ACK Packet
(ACK X, Issue Sequence Number Y)

Three-Step TCP Handshake



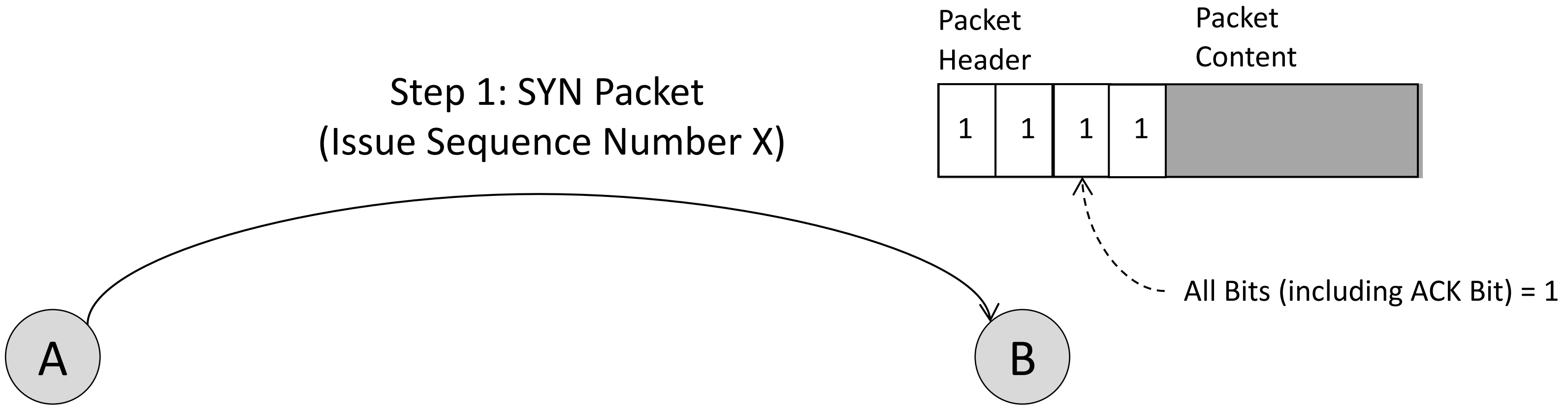
Three-Step TCP Handshake



These are sufficient conditions for data transfer and session traffic between A and B, until the decision is made to terminate the session.

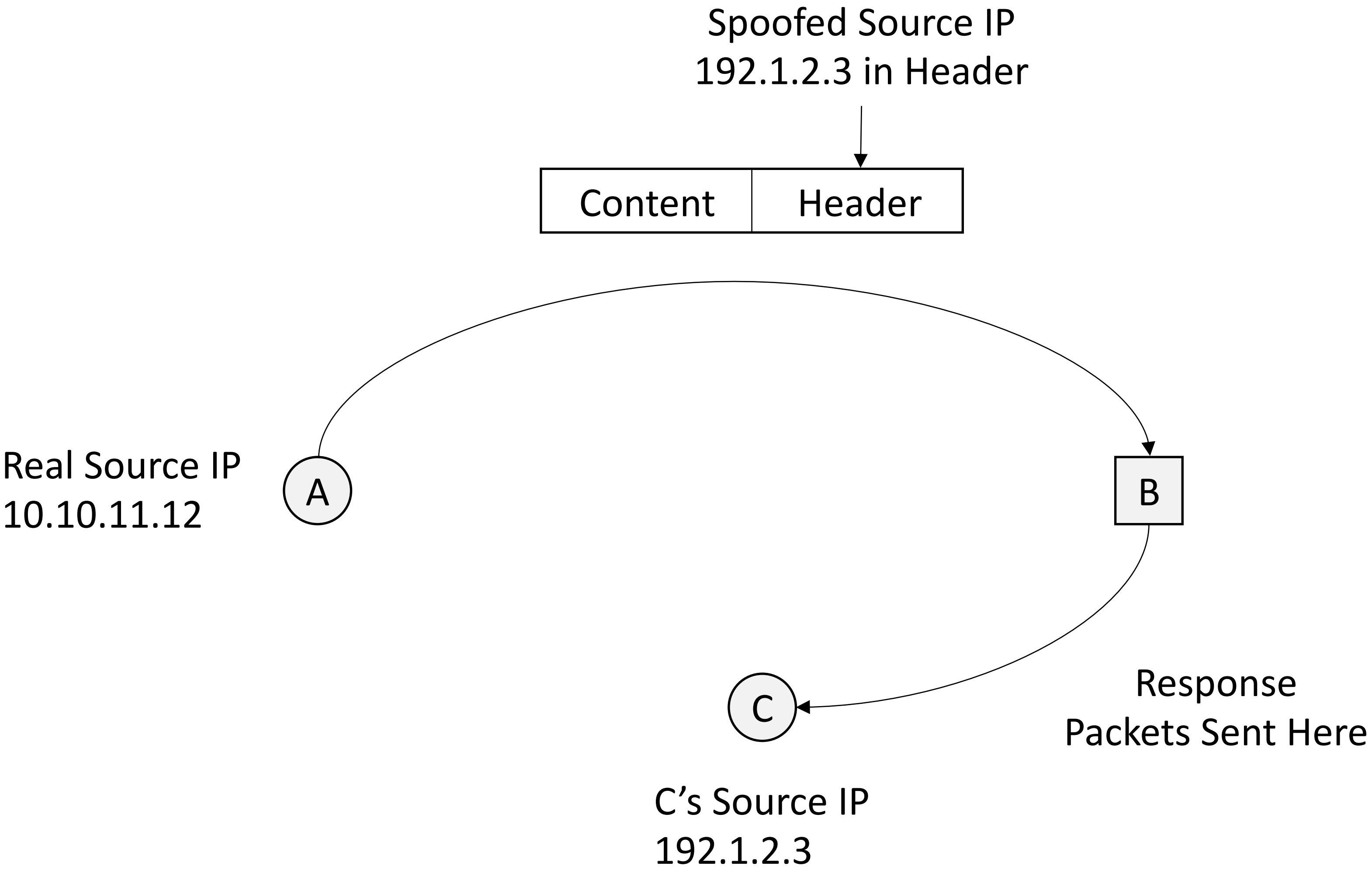
Three-Step TCP Handshake

What are Some Basic TCP/IP Hacks?



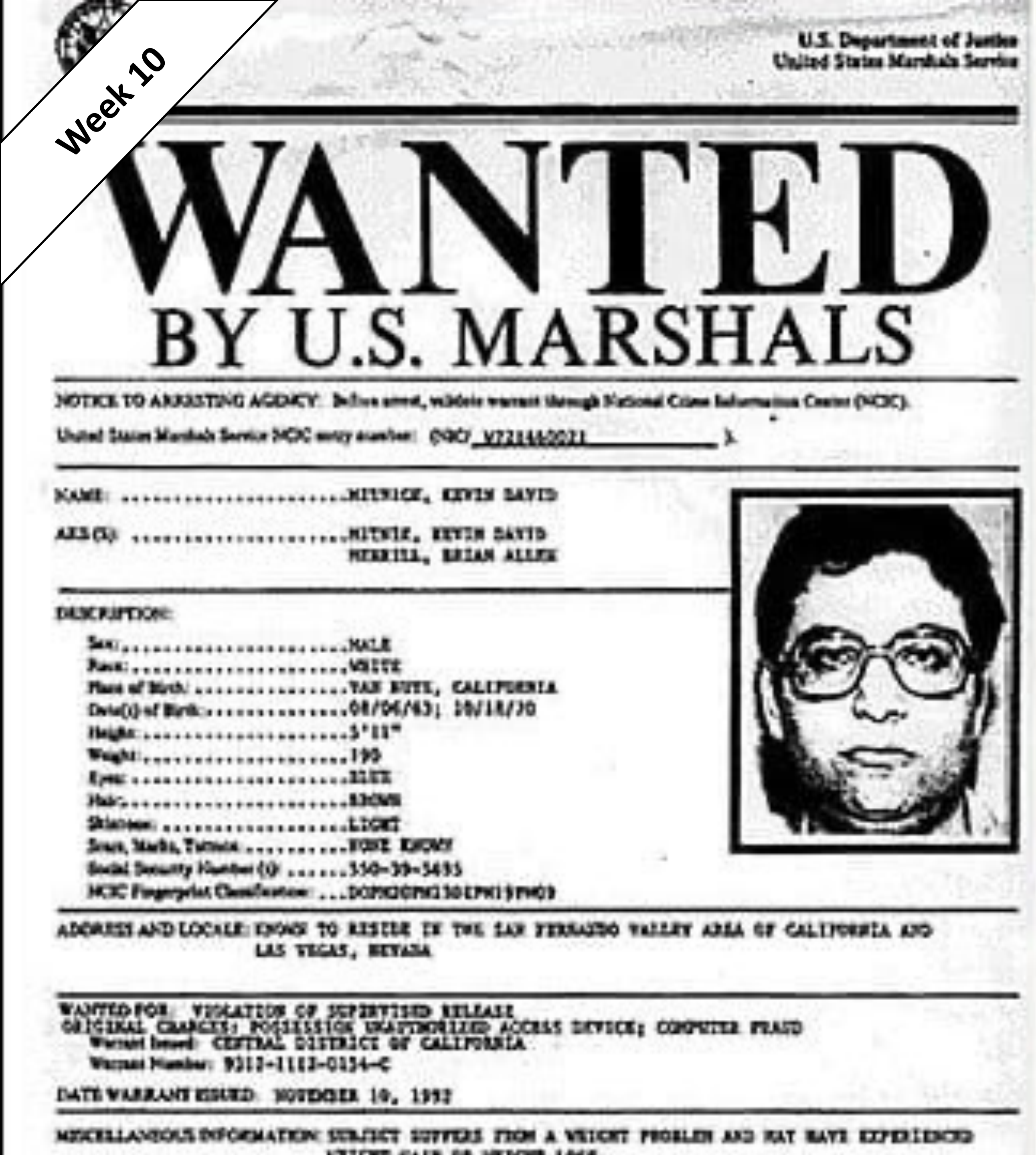
Xmas Tree Packet Attack

Week 10



Spoofed Source Packet Redirection Attack

Week 10



U.S. Department of Justice
United States Marshals Service

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).

United States Marshals Service NCIC entry number: (NIC/ W721460021).

NAME: ....MITNICK, KEVIN DAVID

AKA(S): ....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:

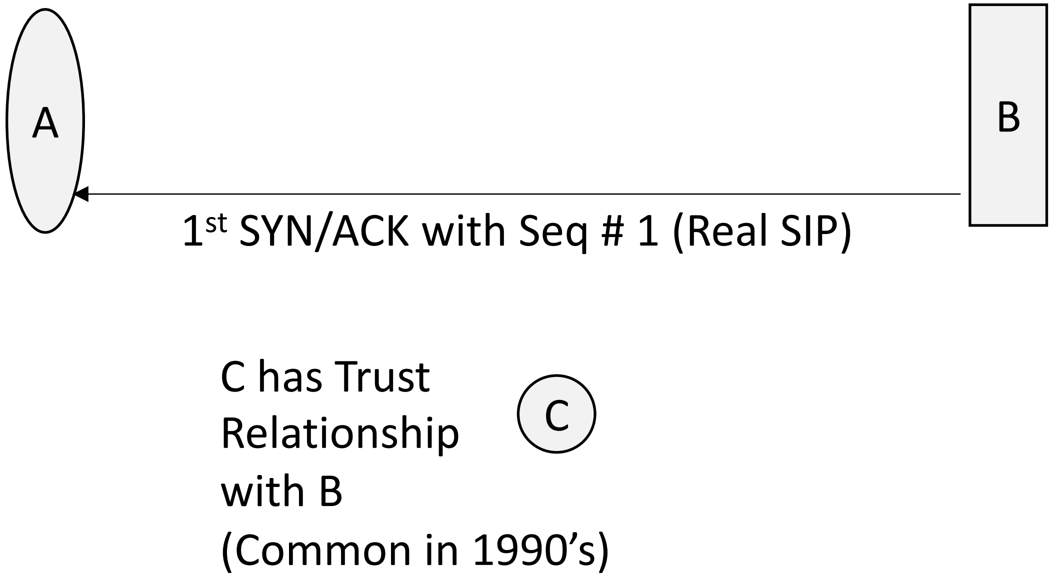
Sex:..........................MALE
Race:.........................WHITE
Place of Birth: ....VAN NUYS, CALIFORNIA
Date(s) of Birth:.............08/06/63; 10/18/70
Height:.......................5'11"
Weight:.......................190
Eyes: ....BLUE
Hair:.........................BROWN
Skintone: ....LIGHT
Scars, Marks, Tattoos.........NONE KNOWN
Social Security Number (s) 350-39-5435
NCIC Fingerprint Classification: ...DOPM20PM13DIPM19PM09

ADDRESS AND LOCALE: KNOWN TO RESIDE IN THE SAN FERNANDO VALLEY AREA OF CALIFORNIA AND
LAS VEGAS, NEVADA

WANTED FOR: VIOLATION OF SUPERVISED RELEASE
ORIGINAL CHARGES: POSSESSION UNAUTHORIZED ACCESS DEVICE; COMPUTER FRAUD
Warrant Issued: CENTRAL DISTRICT OF CALIFORNIA
Warrant Number: 9212-1112-0154-C

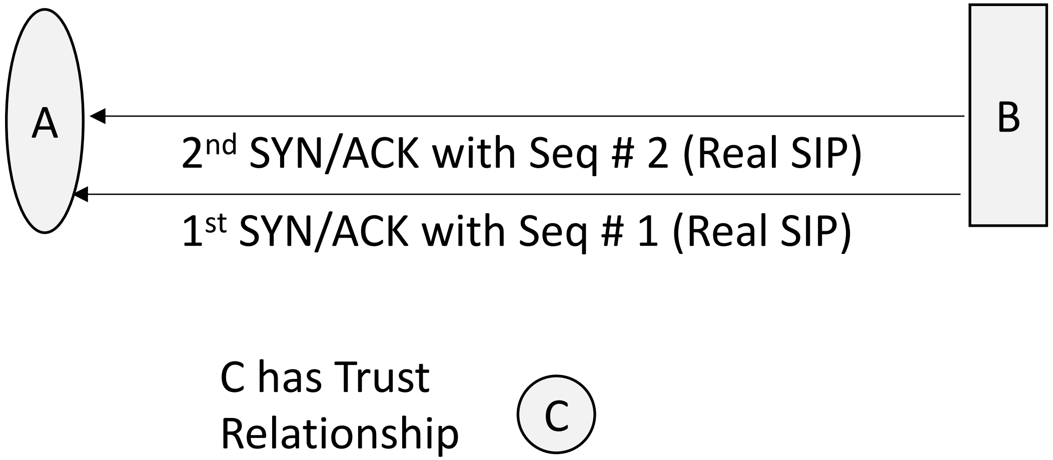
DATE WARRANT ISSUED: NOVEMBER 10, 1992

MISCELLANEOUS INFORMATION: SUBJECT SUFFERS FROM A WEIGHT PROBLEM AND MAY HAVE EXPERIENCED
WEIGHT GAIN OR WEIGHT LOSS



C has Trust
Relationship
with B
(Common in 1990's)

Sequence Number Guessing Attack



A

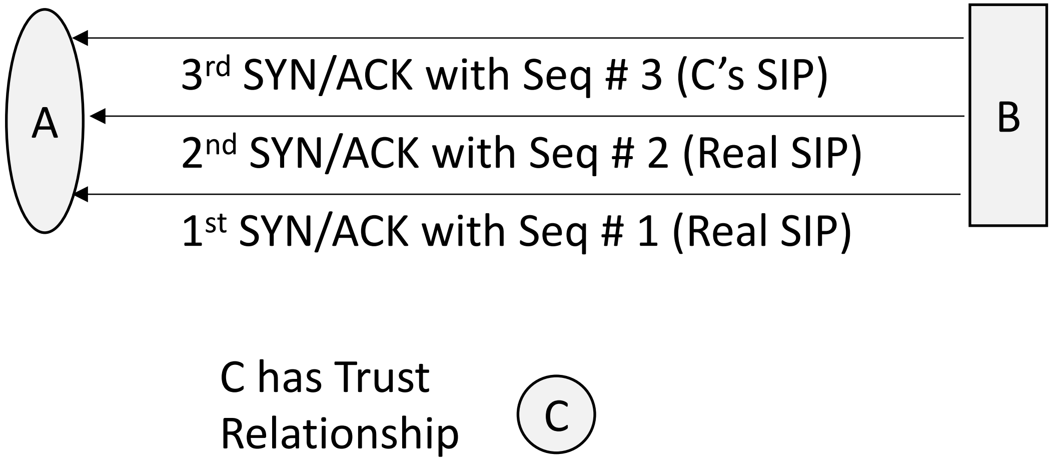
B

2nd SYN/ACK with Seq # 2 (Real SIP)

1st SYN/ACK with Seq # 1 (Real SIP)

C has Trust Relationship with B (Common in 1990’s)

Sequence Number Guessing Attack



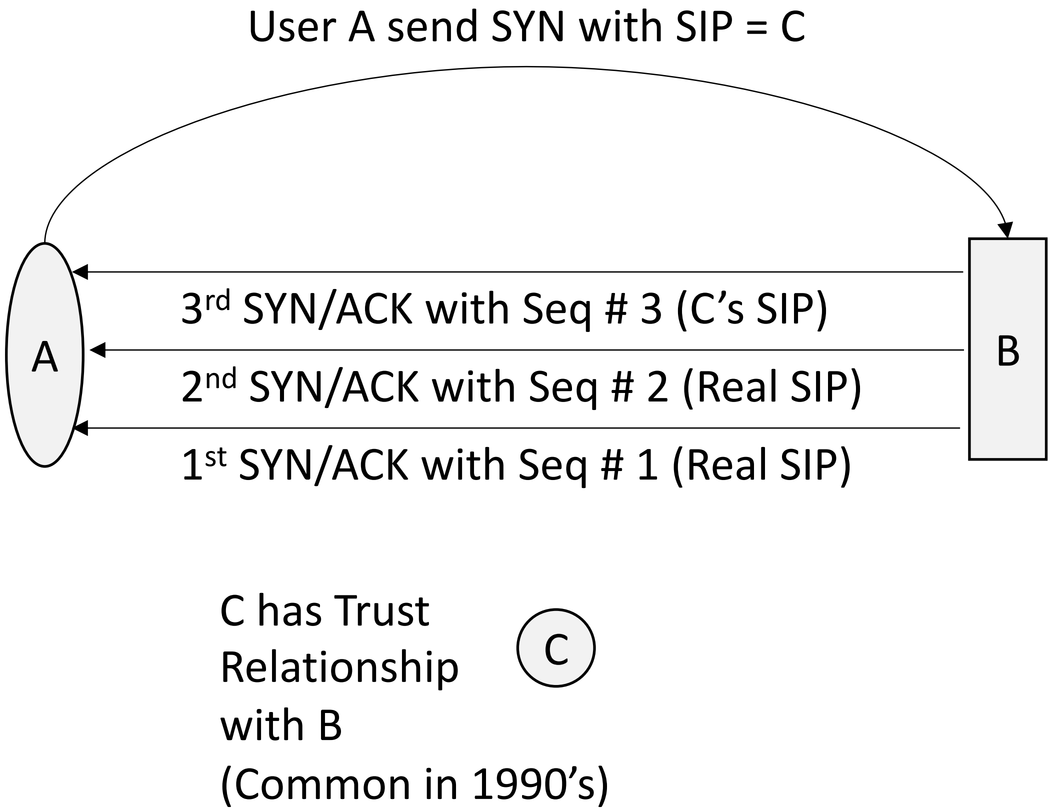
3rd SYN/ACK with Seq # 3 (C's SIP)

2nd SYN/ACK with Seq # 2 (Real SIP)

1st SYN/ACK with Seq # 1 (Real SIP)

C has Trust
Relationship
with B
(Common in 1990's)

Sequence Number Guessing Attack



User A send SYN with SIP = C

A

B

3rd SYN/ACK with Seq # 3 (C’s SIP)

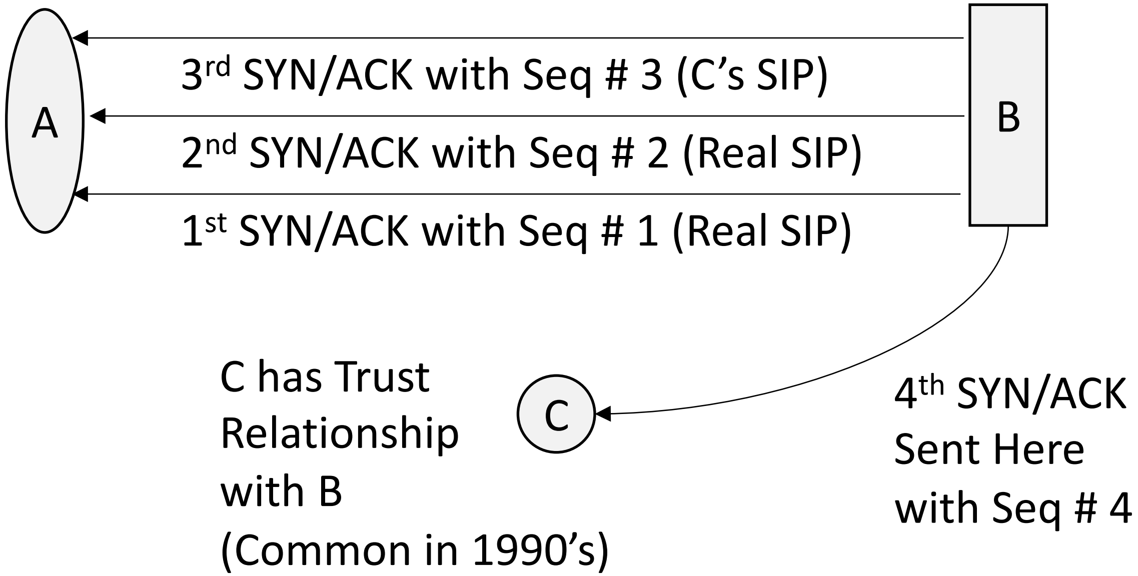
2nd SYN/ACK with Seq # 2 (Real SIP)

1st SYN/ACK with Seq # 1 (Real SIP)

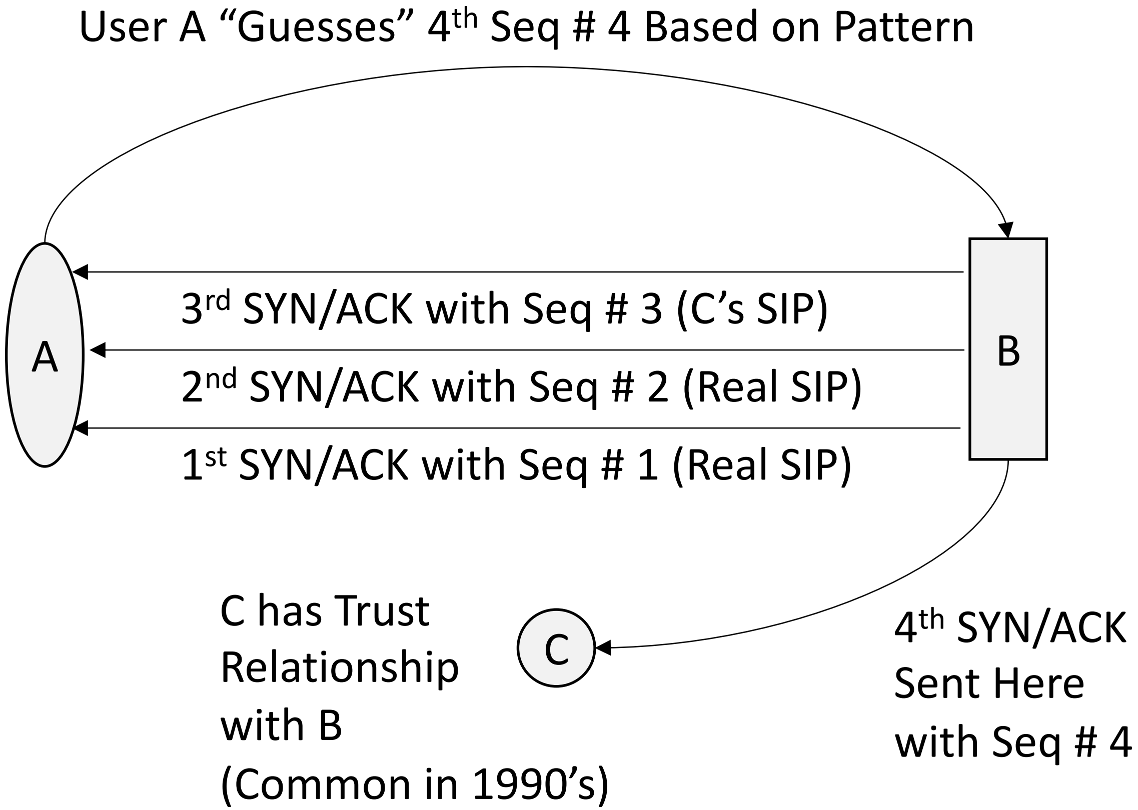
C has Trust
Relationship
with B
(Common in 1990’s)

C

Sequence Number Guessing Attack


A
B
3rd SYN/ACK with Seq # 3 (C's SIP)
2nd SYN/ACK with Seq # 2 (Real SIP)
1st SYN/ACK with Seq # 1 (Real SIP)
C
C has Trust Relationship with B (Common in 1990's)
4th SYN/ACK Sent Here with Seq # 4

Sequence Number Guessing Attack



User A "Guesses" 4th Seq # 4 Based on Pattern

3rd SYN/ACK with Seq # 3 (C's SIP)

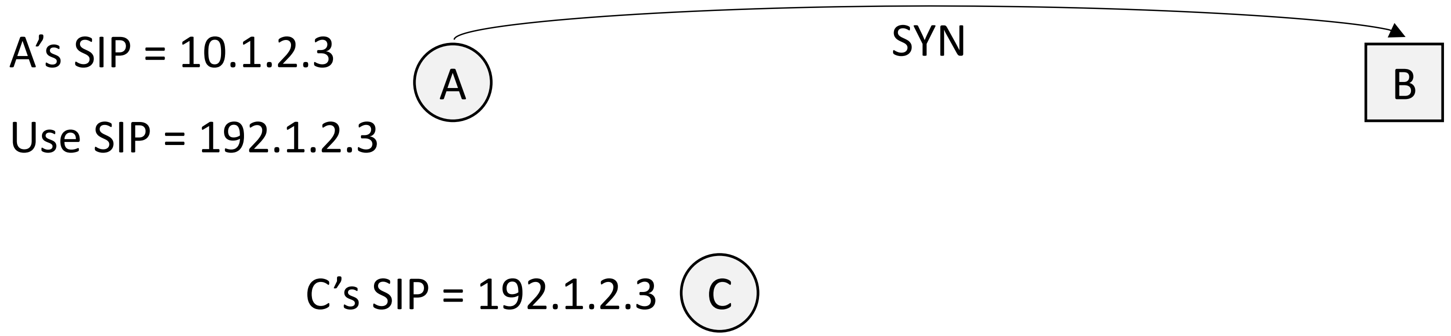
2nd SYN/ACK with Seq # 2 (Real SIP)

1st SYN/ACK with Seq # 1 (Real SIP)

C has Trust Relationship with B (Common in 1990's)

4th SYN/ACK Sent Here with Seq # 4

Sequence Number Guessing Attack

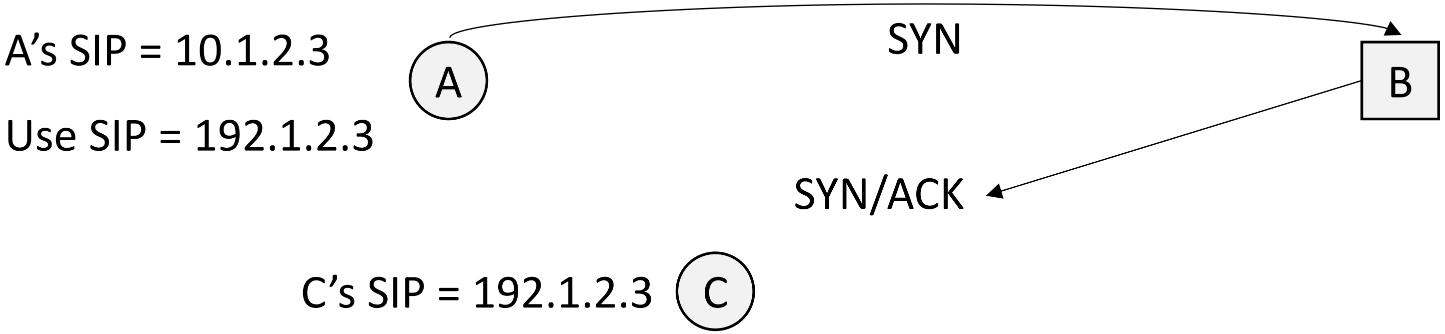


A’s SIP = 10.1.2.3

Use SIP = 192.1.2.3

C’s SIP = 192.1.2.3

SYN Packet Flood Attack



A's SIP = 10.1.2.3

Use SIP = 192.1.2.3

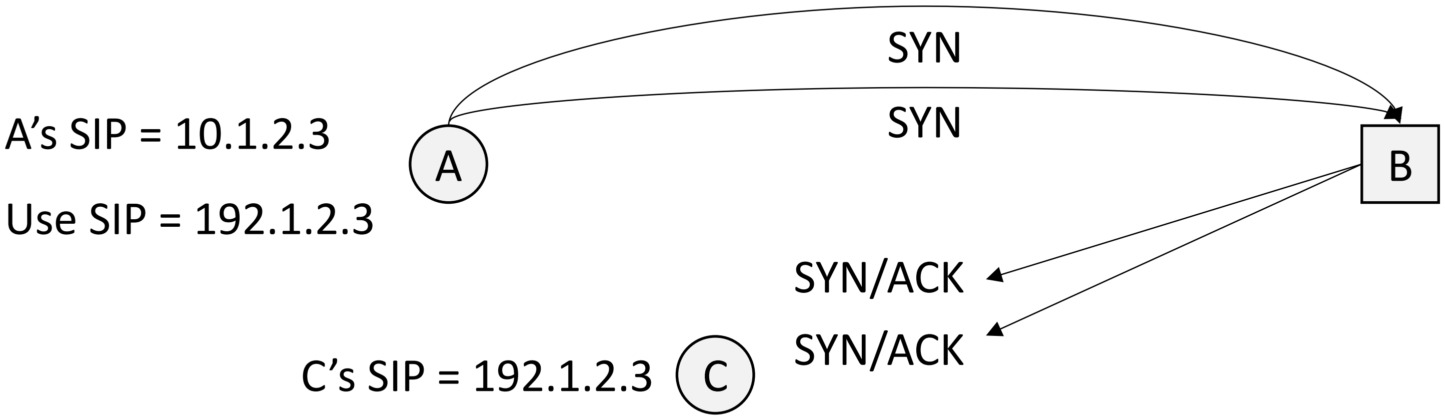
C's SIP = 192.1.2.3

SYN

SYN/ACK

SYN Packet Flood Attack

Week 10



SYN

SYN

A's SIP = 10.1.2.3

Use SIP = 192.1.2.3

A

B

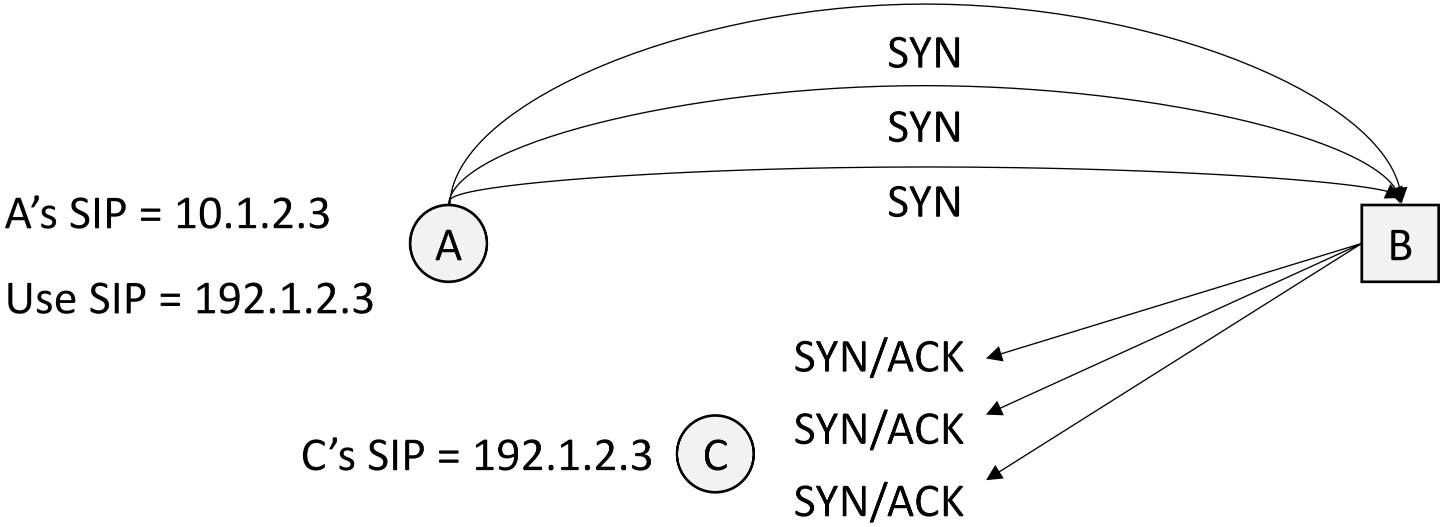
SYN/ACK

SYN/ACK

C's SIP = 192.1.2.3

C

SYN Packet Flood Attack

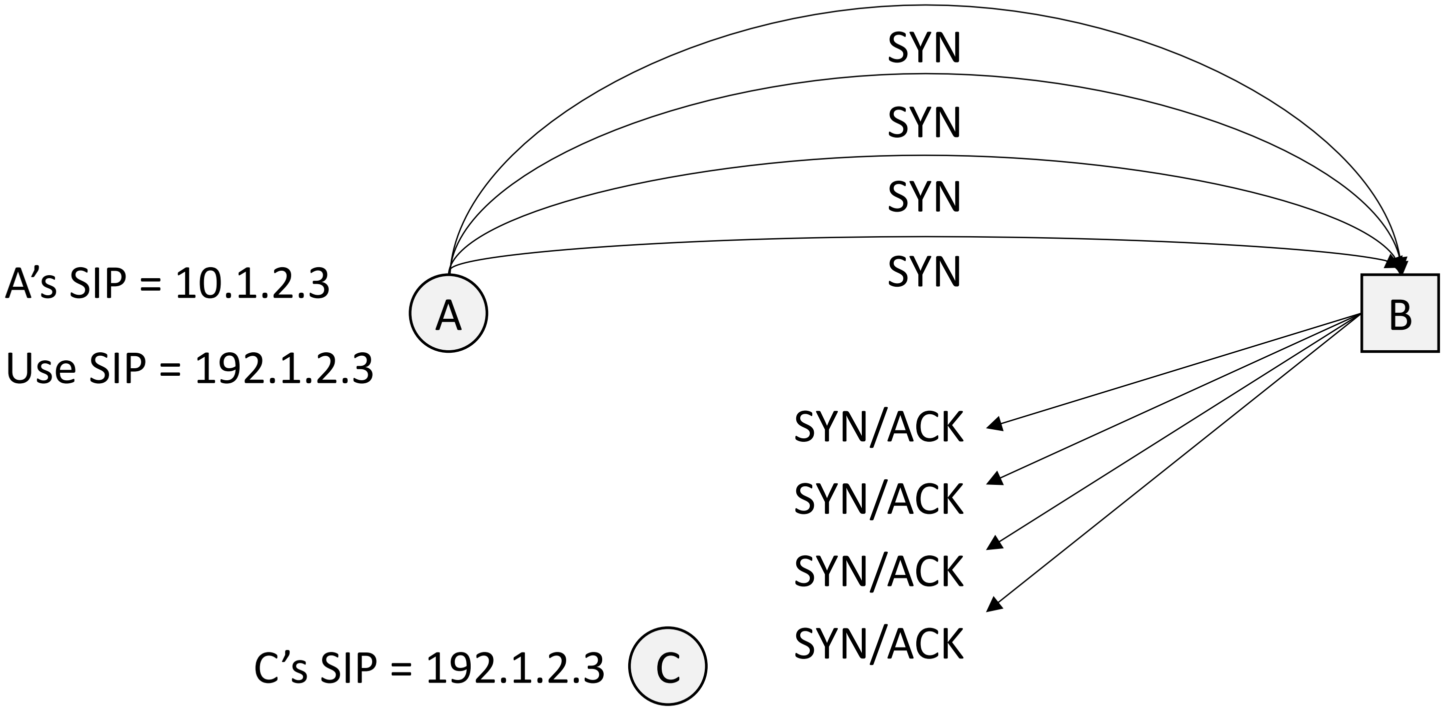


A's SIP = 10.1.2.3

Use SIP = 192.1.2.3

C's SIP = 192.1.2.3

SYN Packet Flood Attack



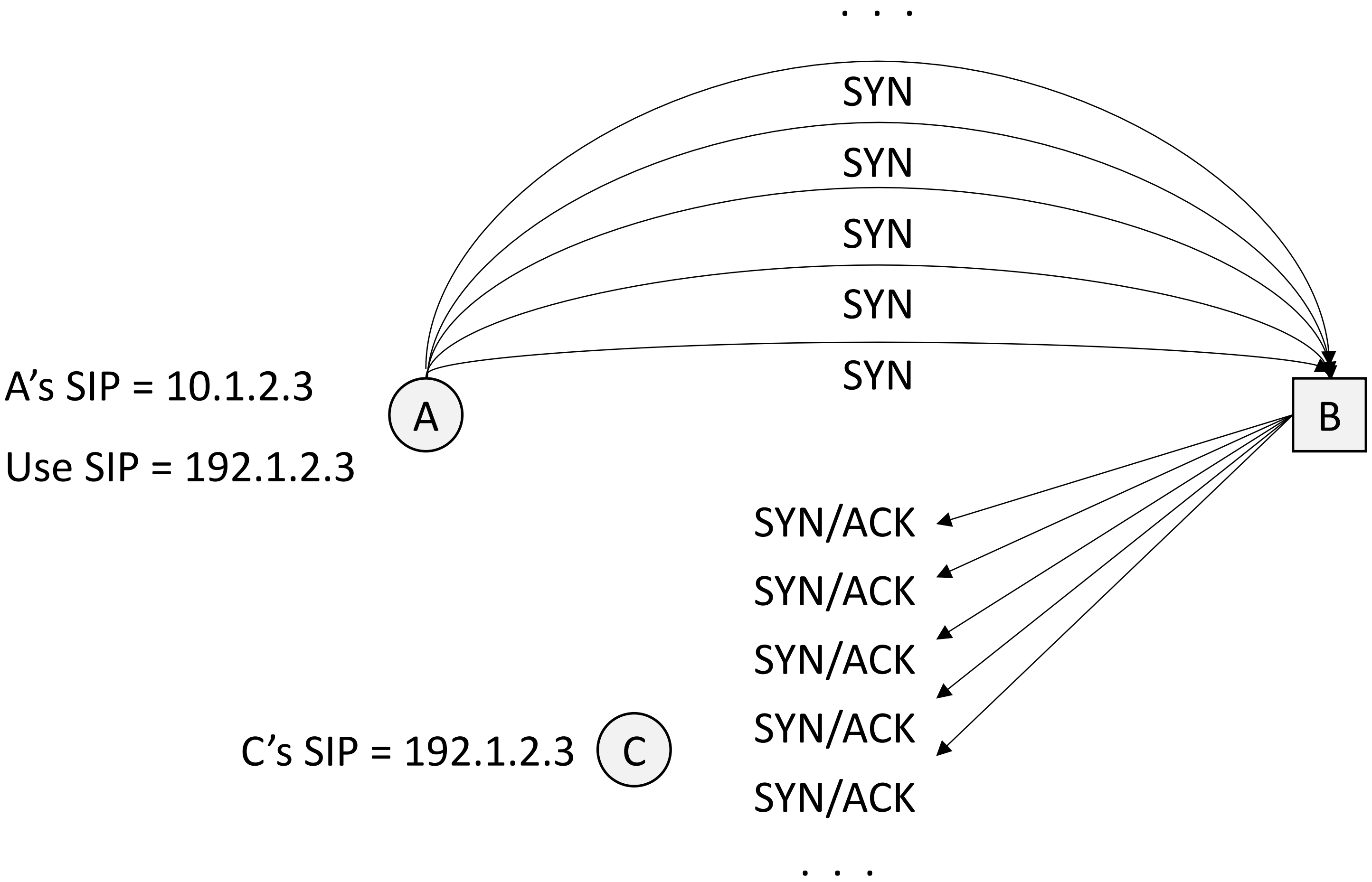
A's SIP = 10.1.2.3

Use SIP = 192.1.2.3

C's SIP = 192.1.2.3

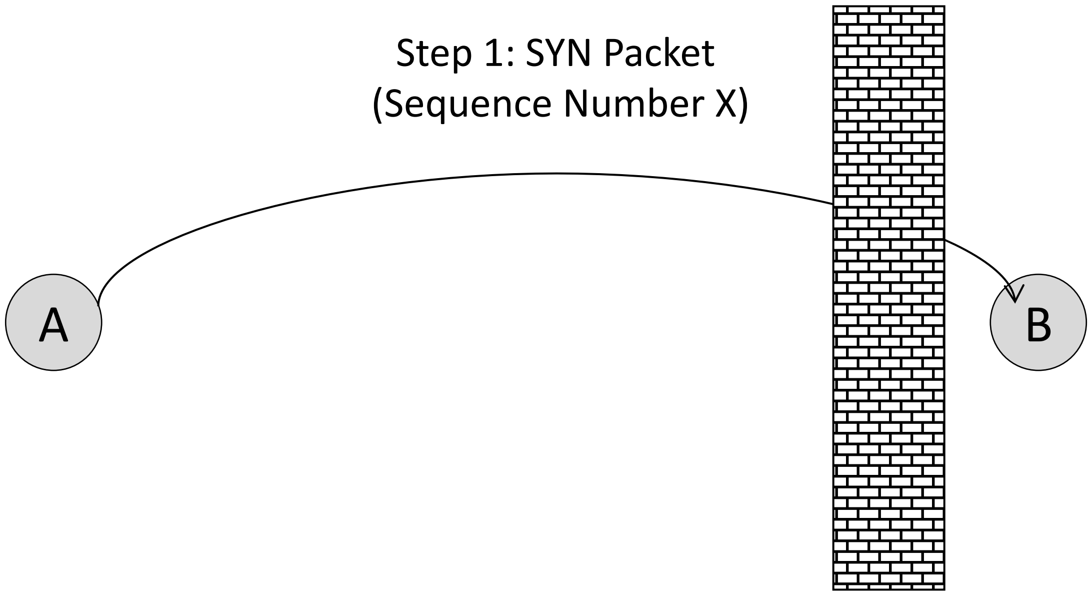
SYN Packet Flood Attack

Week 10

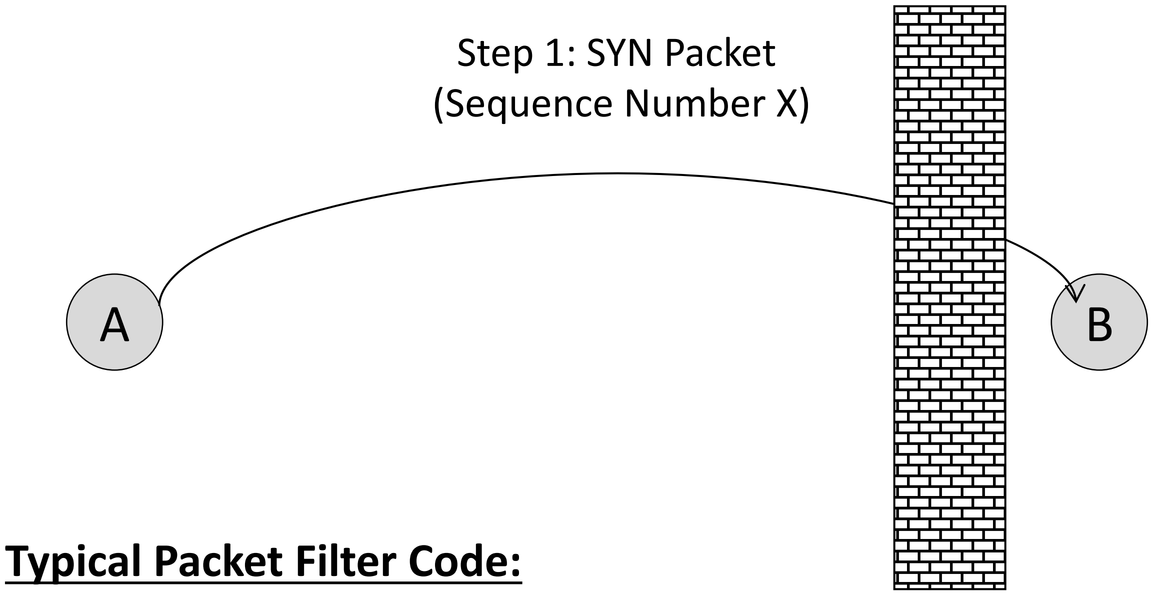


SYN Packet Flood Attack

How Does Packet Filtering Work?
(Hint: Most Basic Firewall)



Basis for Packet Filtering Firewall



Typical Packet Filter Code:

```
if packet header ACK bit = 0 then
      examine SIP, SP, DIP, and DP
      and determine if allow or block
else
      allow packet (ACK bit = 1)
fi
```

Might make network vulnerable to scanning

Basis for Packet Filtering Firewall

Week 10

In
Network
(Trusted)
Out
Network
(Untrusted)

Packet Filtering Firewall – Factors (GUI)

Packet Filtering Firewall – Factors (GUI)

Rule	SIP	SP	DIP	DP	Prot	ACK	Dir	Action
Name of the firewall rule	Source IP address of initiator	Source port of initiator	Destination IP address of initiator	Destination port of initiator	Protocol used by initiator	Value of the ACK bit for TCP only	Physical direction of packet	Block, allow, or divert

GUI for packet filter to protect *In* Network

In
Network
(Trusted)
Out
Network
(Untrusted)

Week 10

Rule	SIP	DIP	SP	DP	Prot	ACK	Dir	Action
Rule 1								
Rule 2								
Rule 3								
Rule 4								
. . .								
Default Rule	*	*	*	*	*	*	**Block**	

*Star * matches on any packet value*

Packet Filtering Firewall – Rule Processing

Week 10

Rule	SIP	DIP	SP	DP	Prot	ACK	Dir	Action
Rule 1								
Rule 2								
Rule 3								
Rule 4								
.								
.								
.								
Default Rule	*	*	*	*	*	*	**Block**	

Firewall Operational Process:

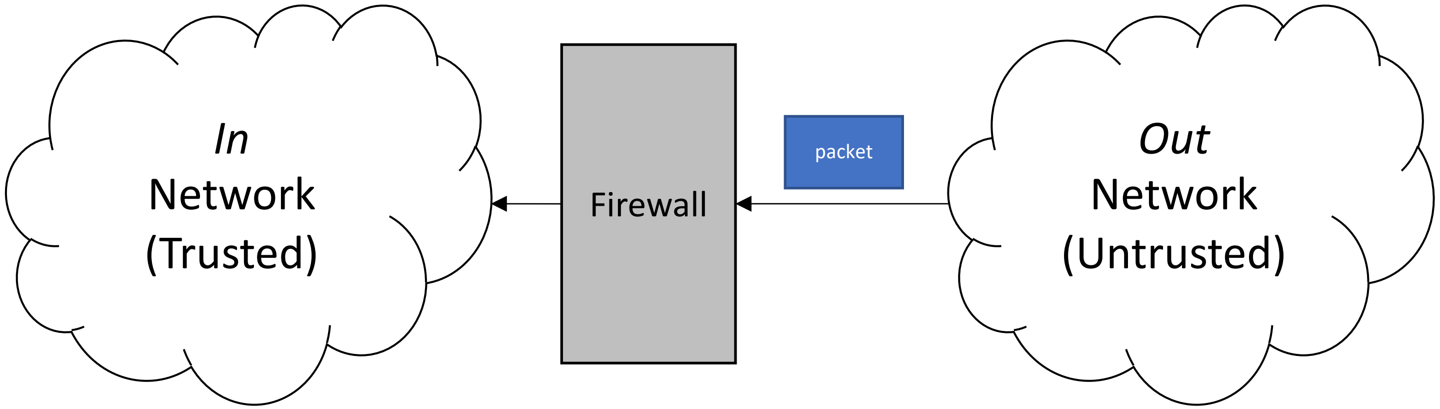
First check to see if Rule 1 matches the packet
Then check to see if Rule 2 matches the packet
Then check to see if Rule 3 matches the packet
And so on

If none of the rules match the packet,
then apply the default rule

*Star * matches on*
any packet value

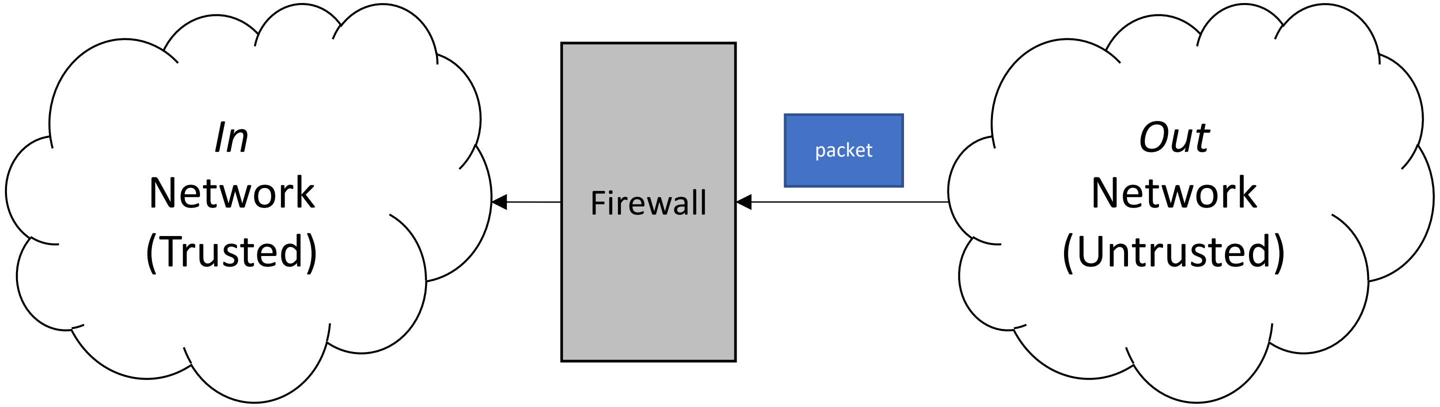
Packet Filtering Firewall – Rule Processing

Week 10

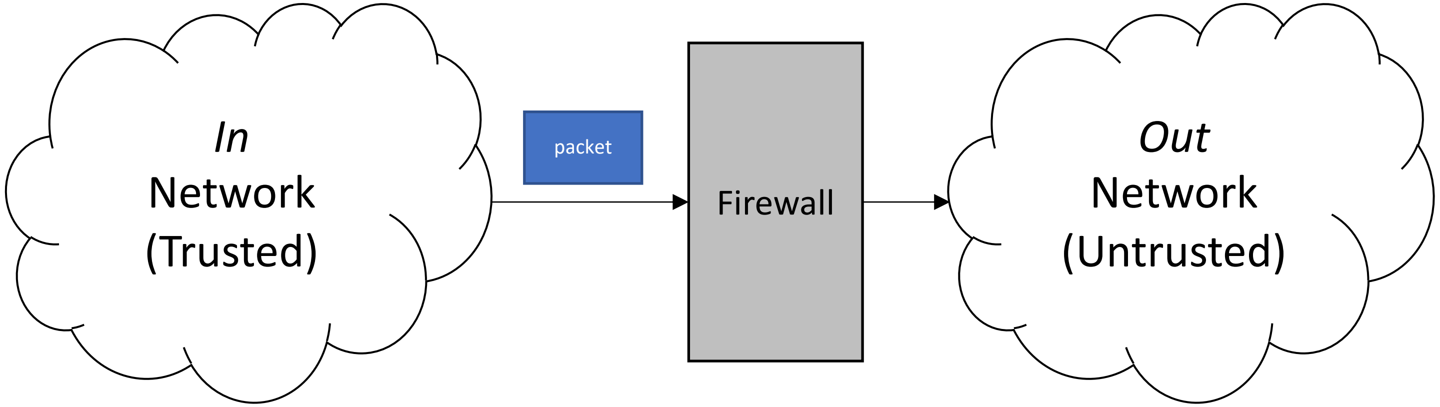


Packet Filtering Firewall – Inbound Spoof

Rule	SIP	SP	DIP	DP	Prot	ACK	Dir	Action
Spoof Block (inbound)	In	*	*	*	TCP	0 (first TCP Packet)	Inbound	Block (Makes no sense)



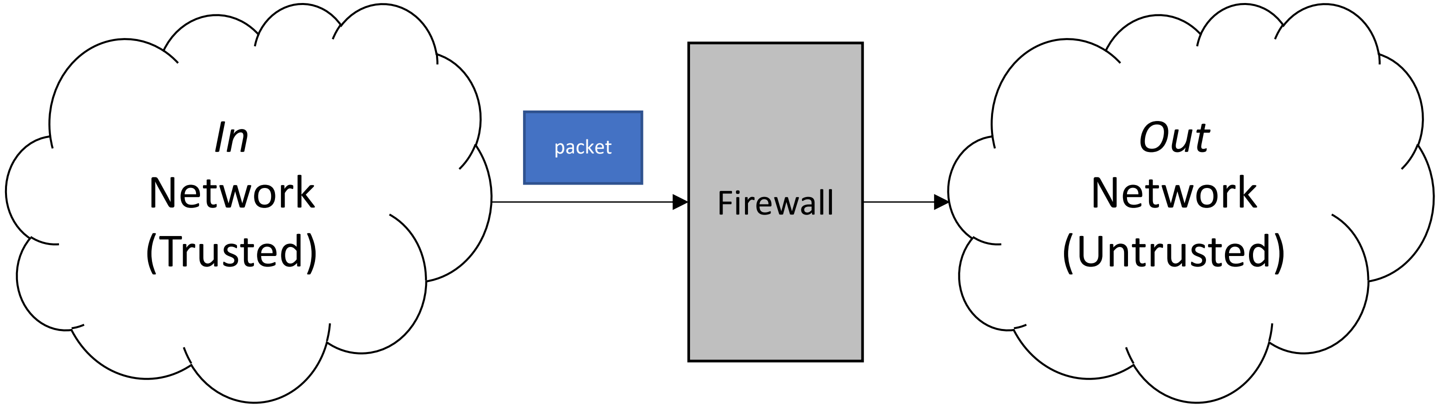
Packet Filtering Firewall – Inbound Spoof



Packet Filtering Firewall – Outbound Spoof

Week 10

Rule	SIP	SP	DIP	DP	Prot	ACK	Dir	Action
Spoof Block (outbound)	Out	*	*	*	TCP	0 (first TCP Packet)	Outbound	Block (Makes no sense)



Packet Filtering Firewall – Outbound Spoof

Week 10

Rule	SIP	SP	DP	DIP	Prot	ACK	Dir	Action
Rule 1	X	Y	Z	A	B	C	D	Block
Rule 2	X	Y’	Z’	A’	B’	C’	D’	Block
Rule 3	X’’	Y’	Z’’	A’’	B’’	C’’	D’’	Block
Rule 4	X’’’	Y’’’	Z’’’	A’’’	B’’’	C’’’	D’’’	Block
. . .								
Rule n	X^{n-1}	Y^{n-1}	Z^{n-1}	A^{n-1}	B^{n-1}	C^{n-1}	D^{n-1}	**Allow**

This is called a *default allow* “blacklist”. It requires that you include every signature for every possible bad action.

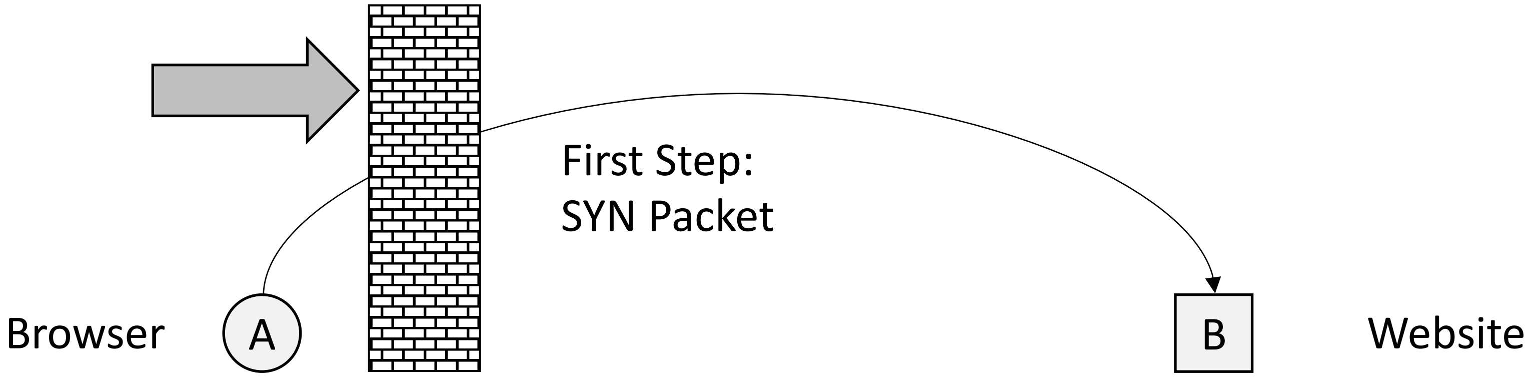
Packet Filtering Firewall – Default Allow “Signatures”

Rule	SIP	SP	DP	DIP	Prot	ACK	Dir	Action
Rule 1	X	Y	Z	A	B	C	D	Allow
Rule 2	X	Y’	Z’	A’	B’	C’	D’	Allow
Rule 3	X’’	Y’	Z’’	A’’	B’’	C’’	D’’	Allow
Rule 4	X’’’	Y’’’	Z’’’	A’’’	B’’’	C’’’	D’’’	Allow
. . .								
Rule n	X^{n-1}	Y^{n-1}	Z^{n-1}	A^{n-1}	B^{n-1}	C^{n-1}	D^{n-1}	**Block**

This is called a *default block* “whitelist”. It requires that you think of every possible service required for the organization.

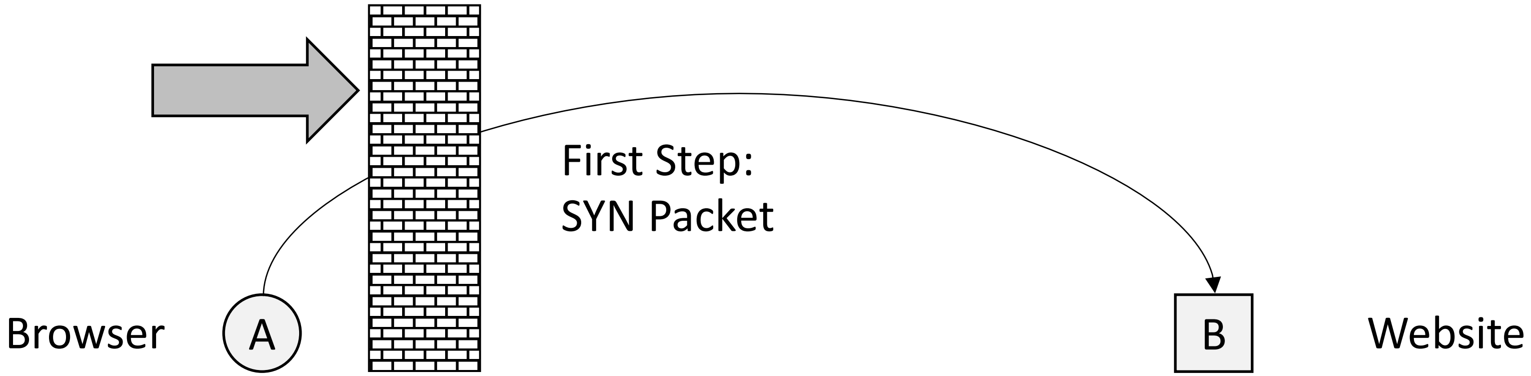
Packet Filtering Firewall – Default Block “Rules”

How Are Firewall Rules Established to Filter Services?



Packet Filtering Firewall – Allow Outbound Web Browsing

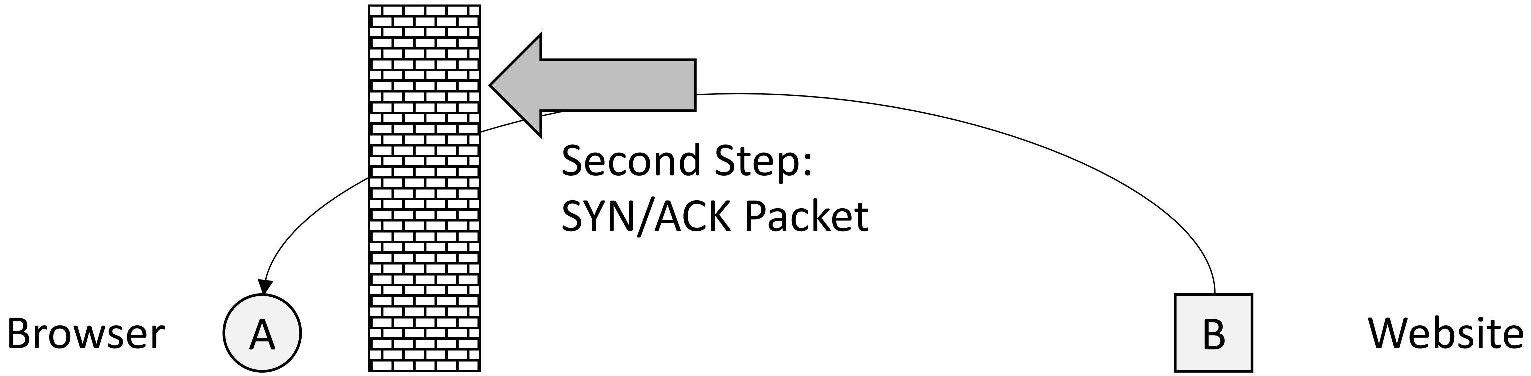
Rule	SIP	DIP	SP	DP	Prot	ACK	Dir	Action
Allow Outbound HTTP (SYN Packet)	In Address	Out Address	> 1023	80 (HTTP)	TCP	0	Outbound	Allow



Packet Filtering Firewall – Allow Outbound Web Browsing

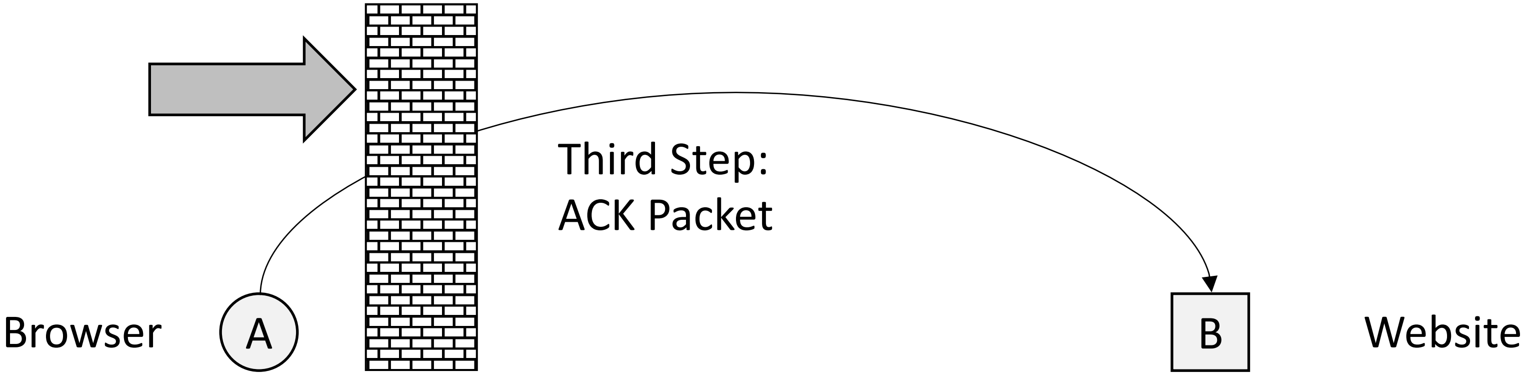
Week 10

Rule	SIP	DIP	SP	DP	Prot	ACK	Dir	Action
Allow Outbound HTTP (SYN Packet)	In Address	Out Address	> 1023	80 (HTTP)	TCP	0	Outbound	Allow
Allow Outbound HTTP (SYN/ACK Resp)	Out Address	In Address	80 (HTTP)	> 1023	TCP	1	Inbound	Allow



Packet Filtering Firewall – Allow Outbound Web Browsing

Rule	SIP	DIP	SP	DP	Prot	ACK	Dir	Action
Allow Outbound HTTP (SYN Packet)	In Address	Out Address	> 1023	80 (HTTP)	TCP	0	Outbound	Allow
Allow Outbound HTTP (SYN/ACK Resp)	Out Address	In Address	80 (HTTP)	> 1023	TCP	1	Inbound	Allow
Allow Outbound HTTP (ACK Packet)	In Address	Out Address	> 1023	80 (HTTP)	TCP	1	Outbound	Allow



Packet Filtering Firewall – Allow Outbound Web Browsing

Rule	SIP	DIP	SP	DP	Prot	ACK	Dir	Action
Allow Outbound HTTP (SYN Packet)	In Address	Out Address	> 1023	80 (HTTP)	TCP	0	Outbound	Allow
Allow Outbound HTTP (SYN/ACK Resp)	Out Address	In Address	80 (HTTP)	> 1023	TCP	1	Inbound	Allow
Allow Outbound HTTP (ACK Packet)	In Address	Out Address	> 1023	80 (HTTP)	TCP	1	Outbound	Allow

TCP/Port 80 = HTTP

Packet Filtering Firewall – Port 80 Corresponds to HTTP

Rule	SIP	DIP	SP	DP	Prot	ACK	Dir	Action
Allow Outbound Telnet (SYN Packet)	In Address	Out Address	> 1023	23 (Telnet)	TCP	0	Outbound	Allow
Allow Outbound Telnet (SYN/ACK Resp)	Out Address	In Address	23 (Telnet)	> 1023	TCP	1	Inbound	Allow
Allow Outbound Telnet (ACK Packet)	In Address	Out Address	> 1023	23 (Telnet)	TCP	1	Outbound	Allow

TCP/Port 23 = Telnet

Packet Filtering Firewall – Port 23 Corresponds to Telnet

Week 10

Rule	SIP	DIP	SP	DP	Prot	ACK	Dir	Action
Allow Outbound SMTP (SYN Packet)	In Address	Out Address	> 1023	25 (SMTP)	TCP	0	Outbound	Allow
Allow Outbound SMTP (SYN/ACK Resp)	Out Address	In Address	25 (SMTP)	> 1023	TCP	1	Inbound	Allow
Allow Outbound SMTP (ACK Packet)	In Address	Out Address	> 1023	25 (SMTP)	TCP	1	Outbound	Allow

TCP/Port 25 = SMTP

Packet Filtering Firewall – Port 25 Corresponds to SMTP

Rule	SIP	DIP	SP	DP	Prot	ACK	Dir	Action
Allow Outbound SMTP (SYN Packet)	In Address	Out Address	> 1023	25 (SMTP)	TCP	**0**	Outbound	Allow
Allow Outbound SMTP (SYN/ACK Resp)	Out Address	In Address	25 (SMTP)	> 1023	TCP	1	Inbound	Allow
Allow Outbound SMTP (ACK Packet)	In Address	Out Address	> 1023	25 (SMTP)	TCP	**1**	Outbound	Allow

These rules only differ in ACK value

Packet Filtering Firewall – Rule Optimization

Week 10

Rule	SIP	DIP	SP	DP	Prot	ACK	Dir	Action
Allow Outbound SMTP (SYN Packet)	In Address	Out Address	> 1023	25 (SMTP)	TCP	*	Outbound	Allow
Allow Outbound SMTP (SYN/ACK Resp)	Out Address	In Address	25 (SMTP)	> 1023	TCP	1	Inbound	Allow

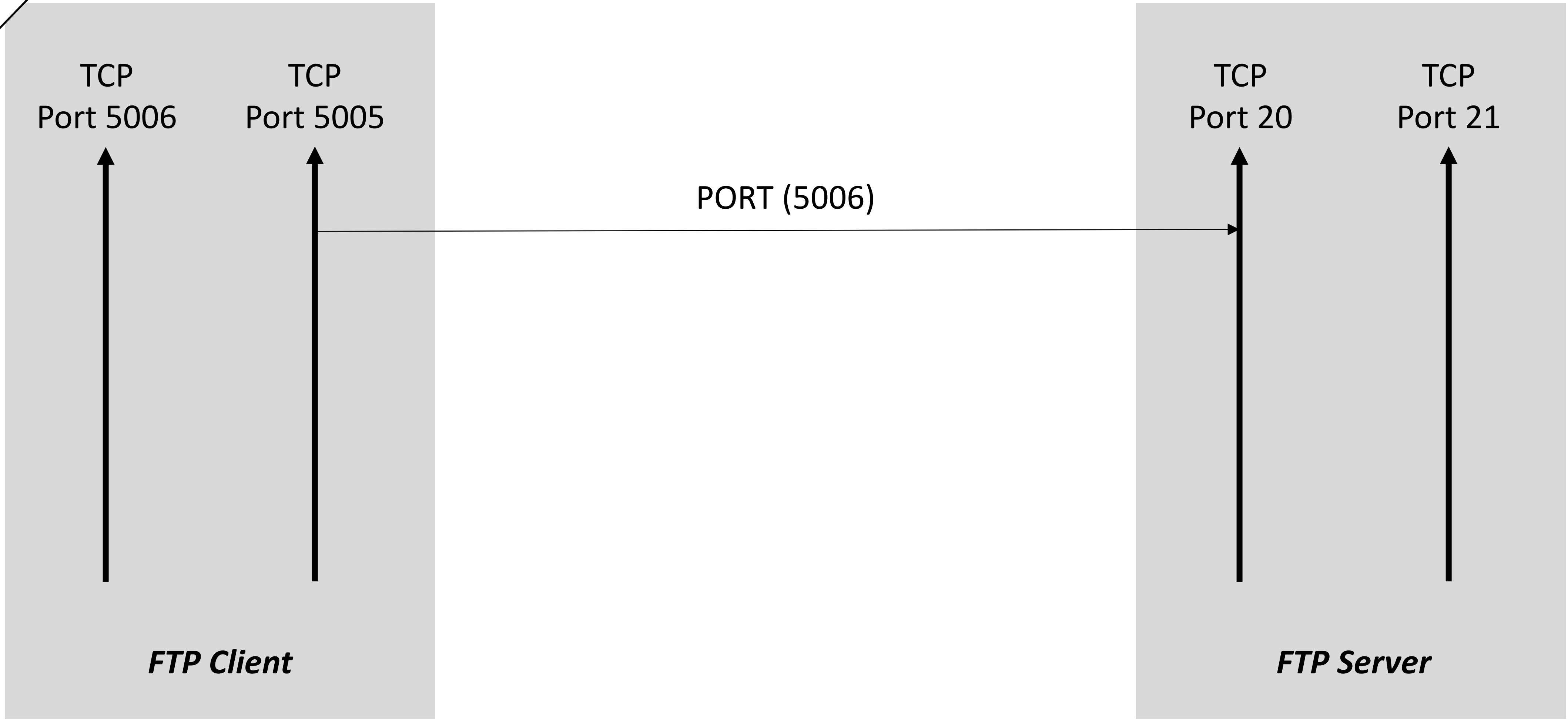
Packet Filtering Firewall – Rule Optimization

What are Some Application-Level and Network Architecture-Based Firewall Issues?

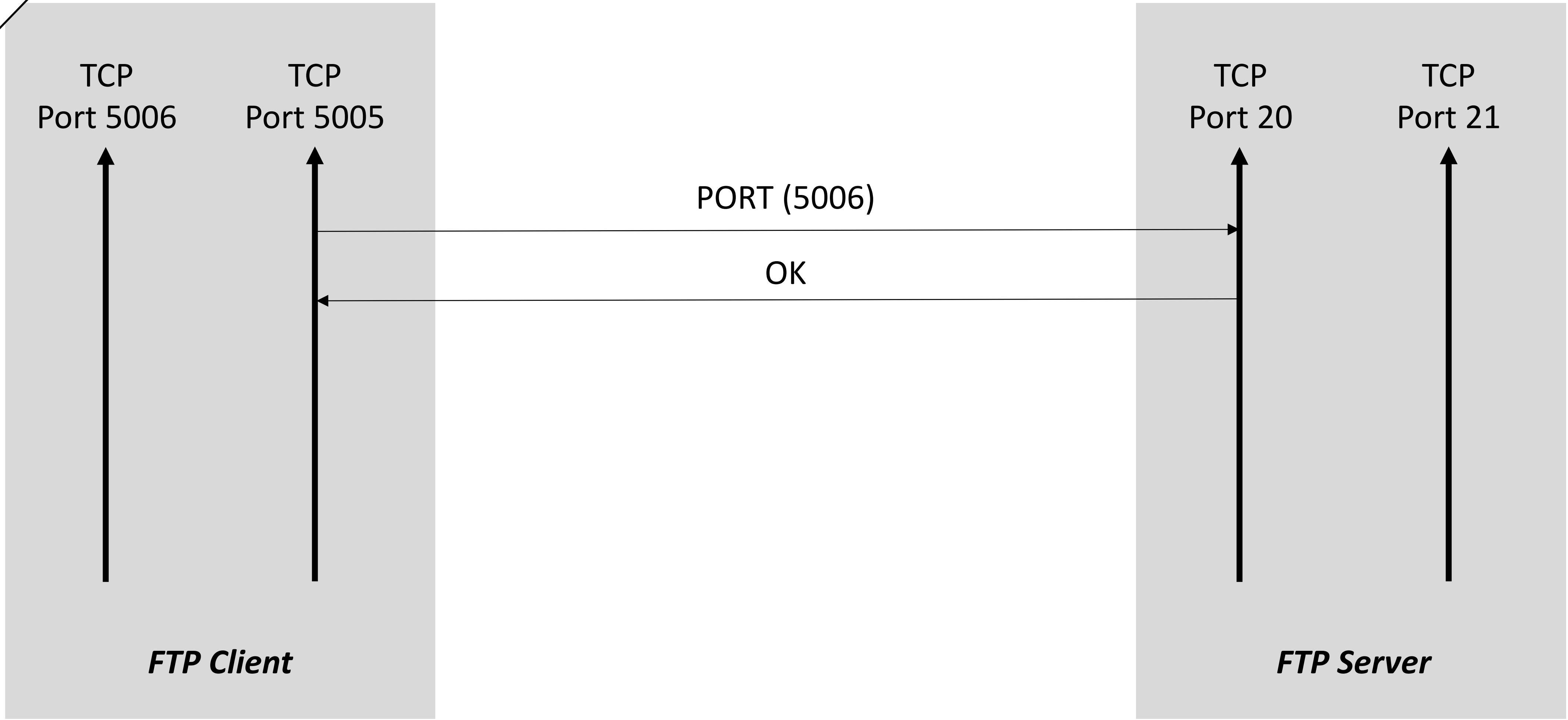
Week 10

	Web Services	*Email Services*	*Remote Access*	. . .
Inbound	*Only to Corporate Web Site*	*Only to Corporate Email Server*	*Only to Corporate RA Server*	
Outbound	*Only to Approved Web Sites*	*Unrestricted*	*Unrestricted*	

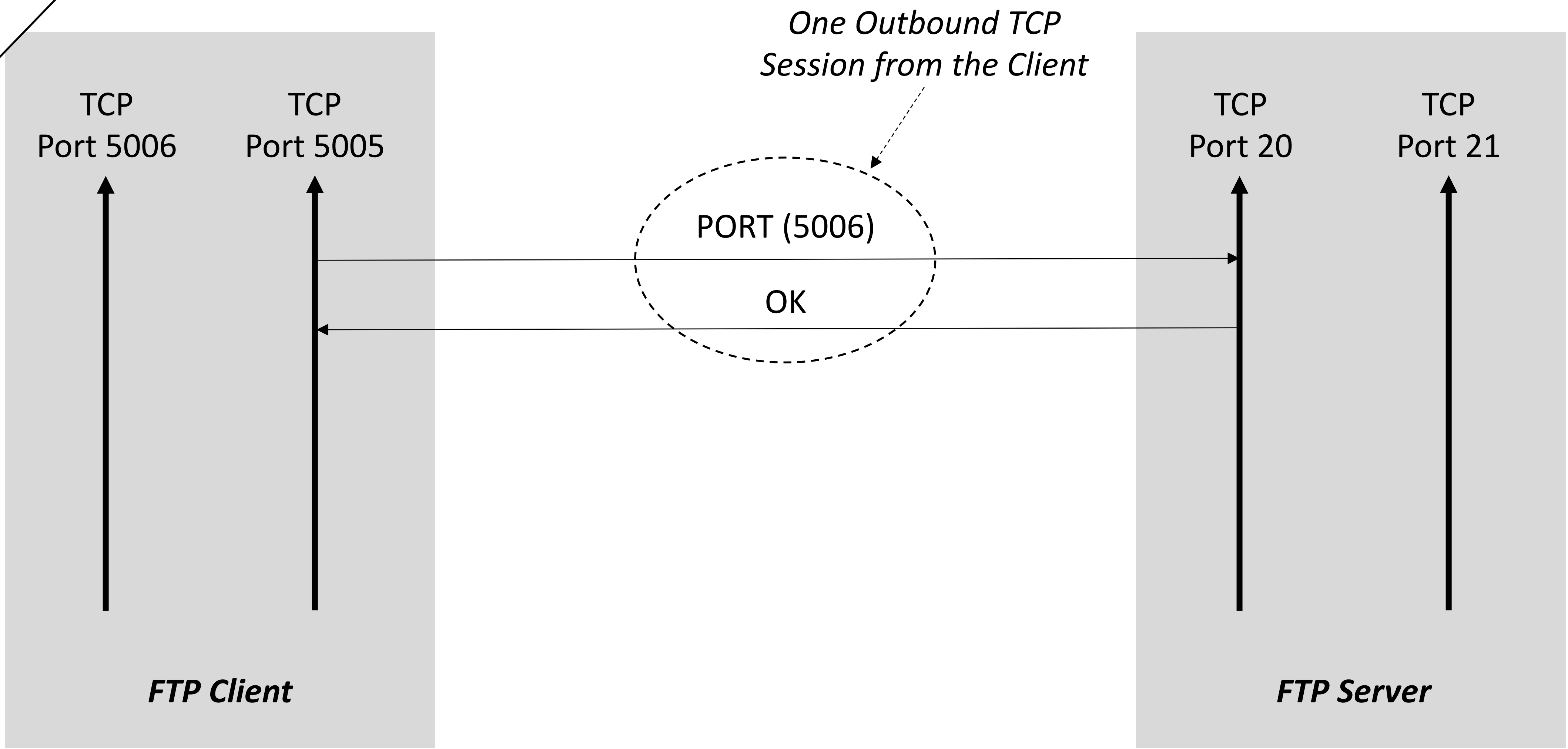
Firewall – Policy Rules Decisions



Packet Filtering Firewall – FTP

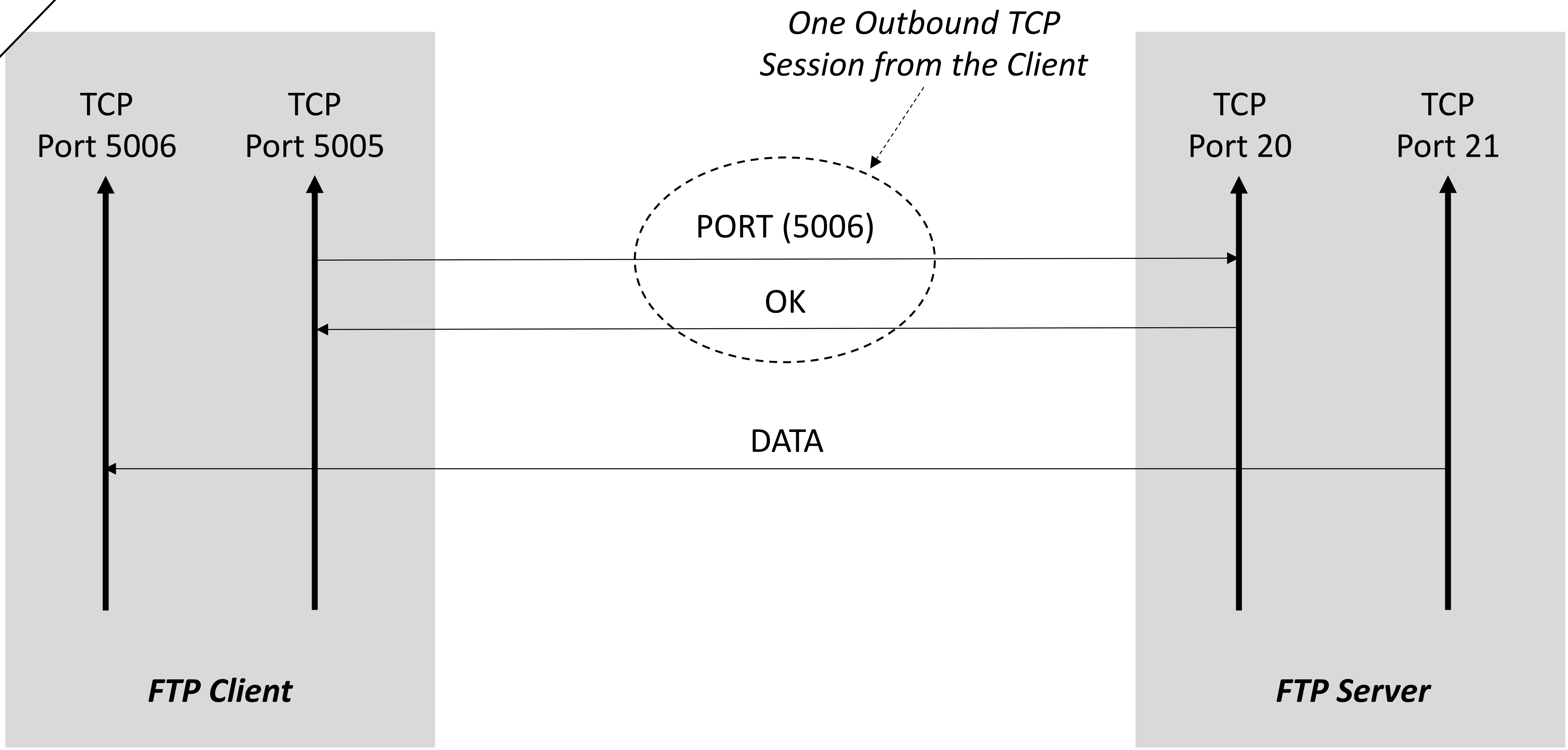


Packet Filtering Firewall – FTP

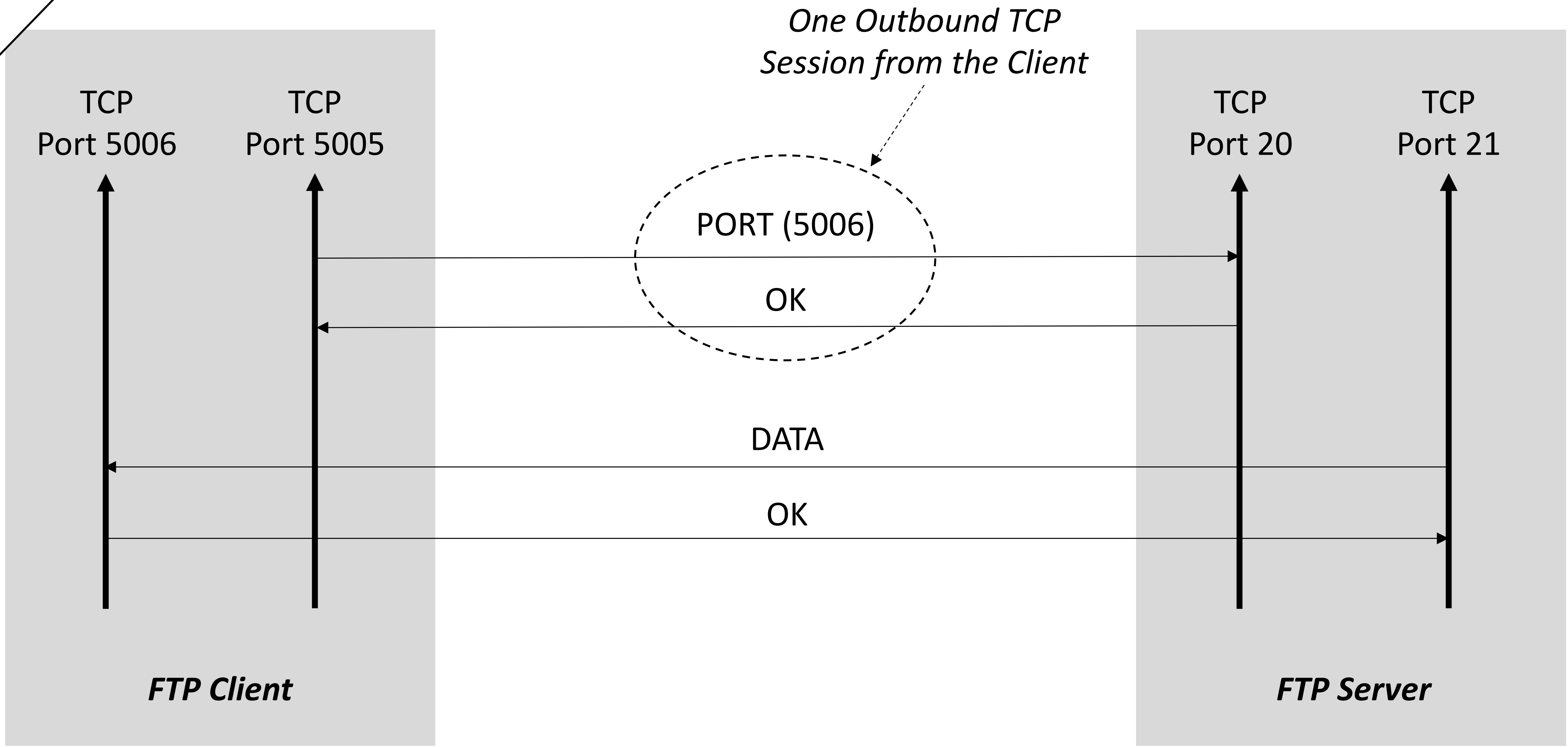


Packet Filtering Firewall – FTP

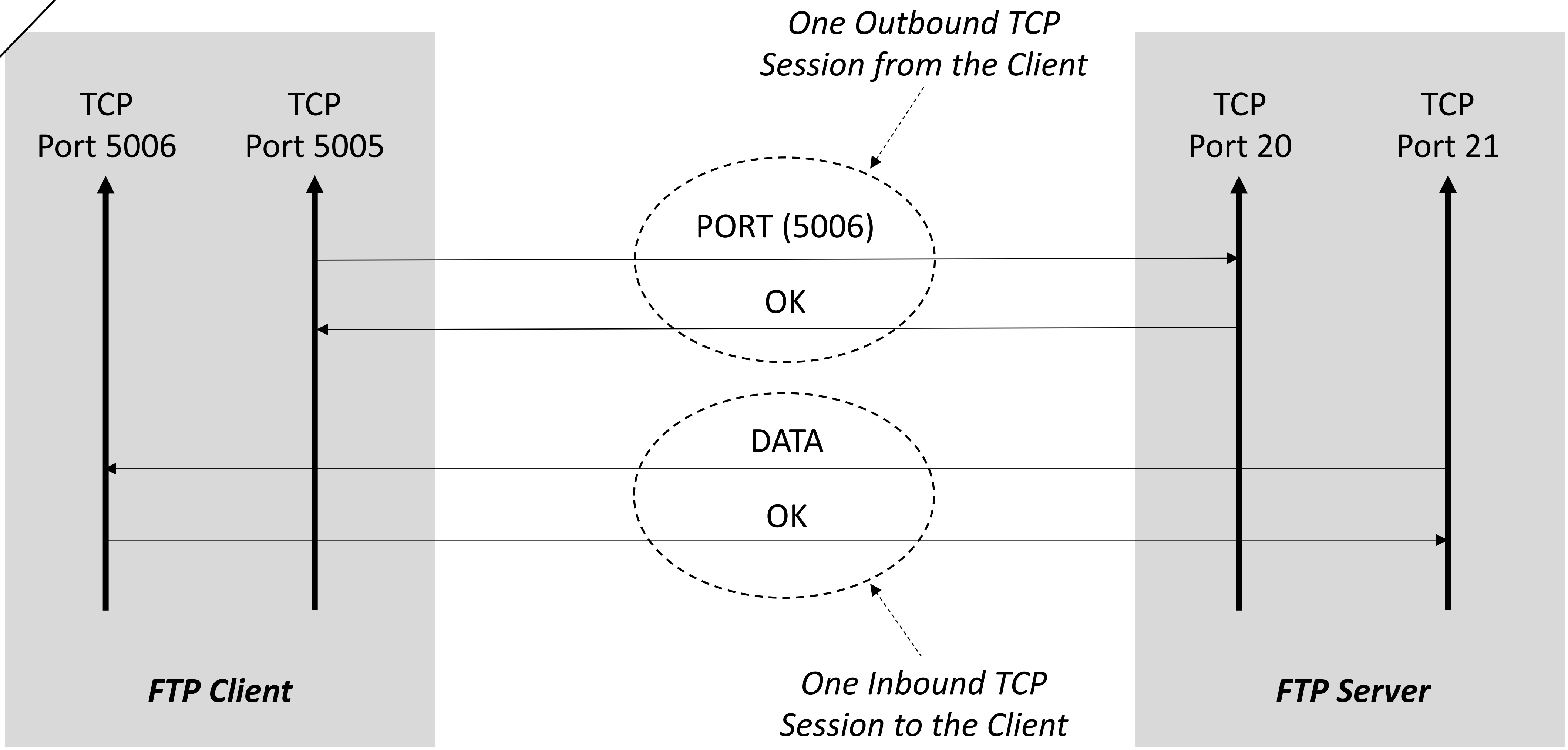
Week 10



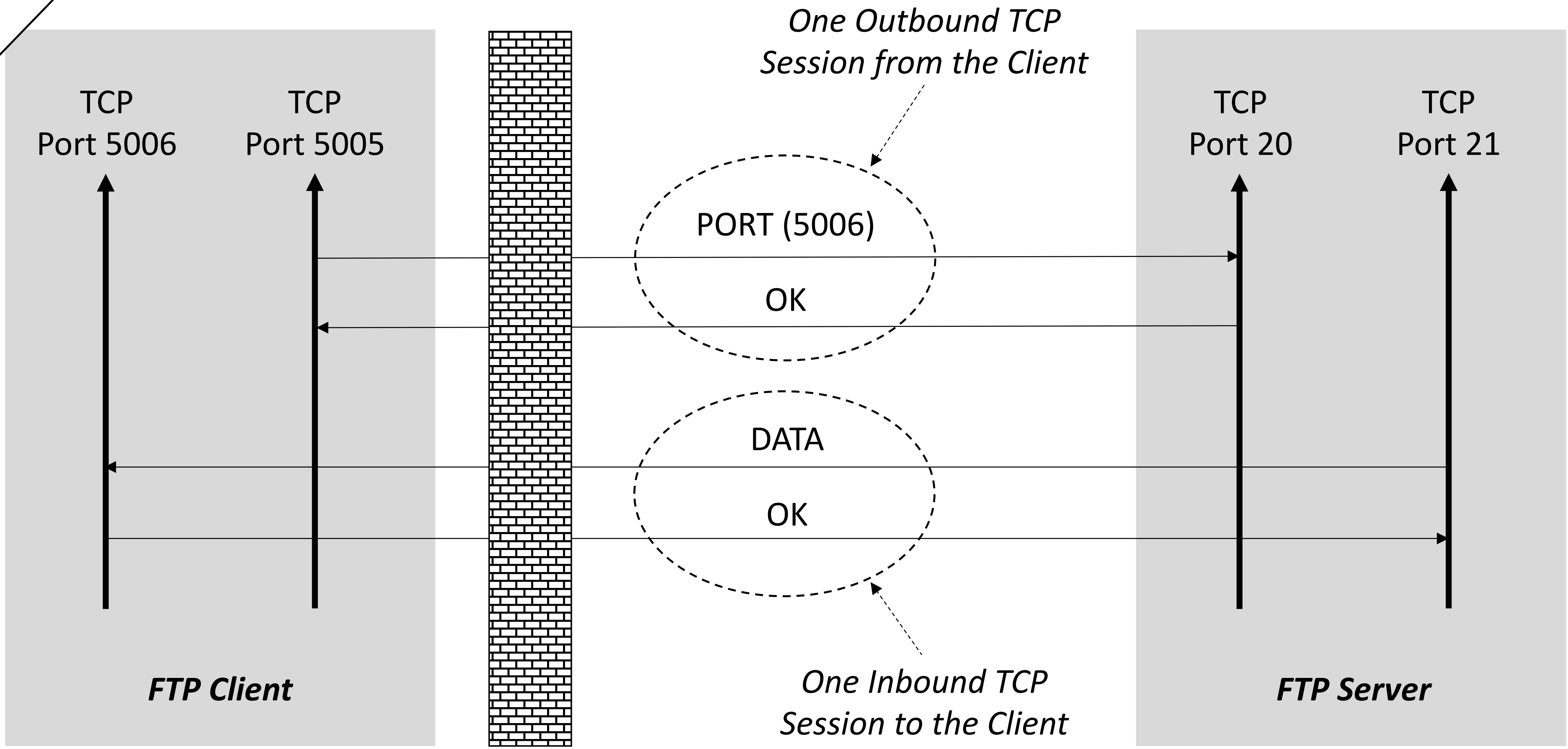
Packet Filtering Firewall – FTP



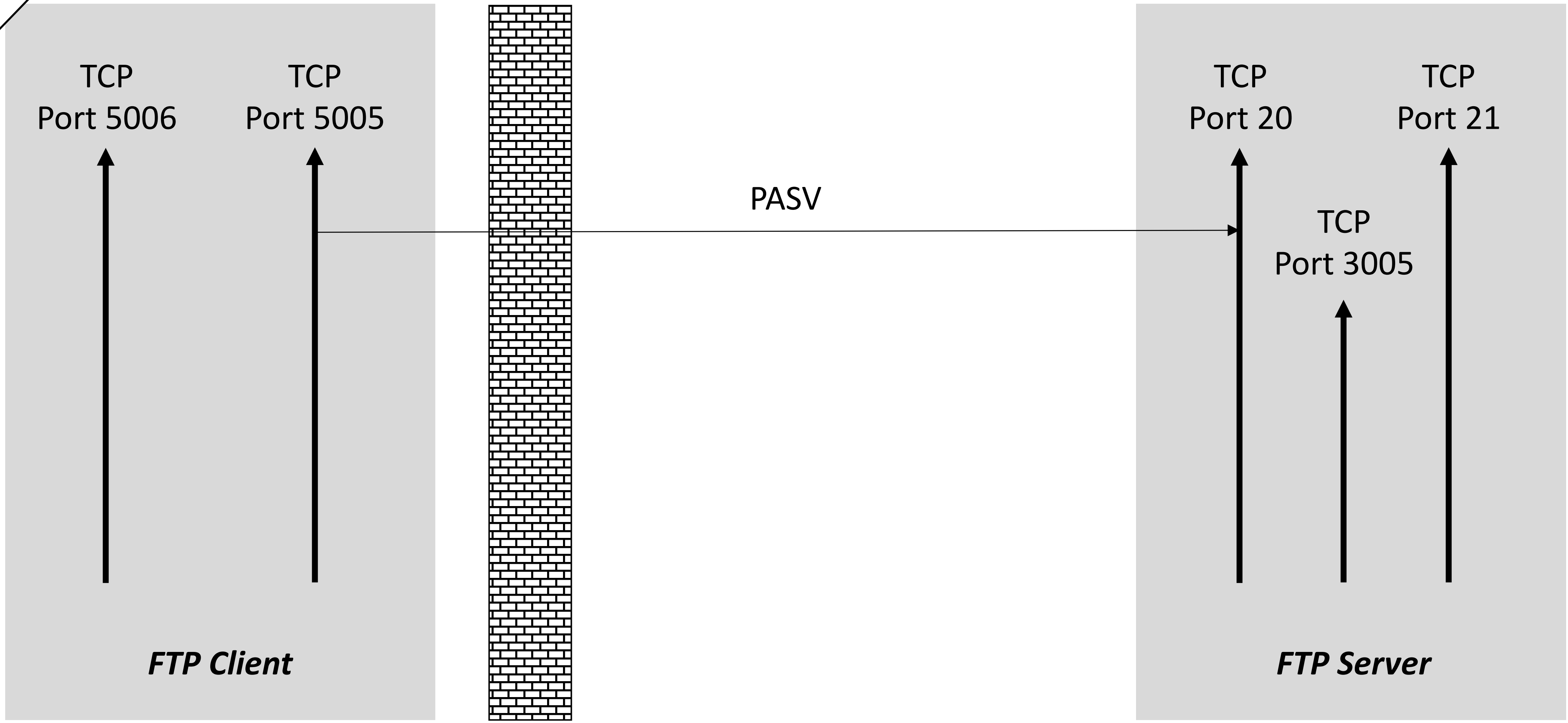
Packet Filtering Firewall – FTP



Packet Filtering Firewall – FTP

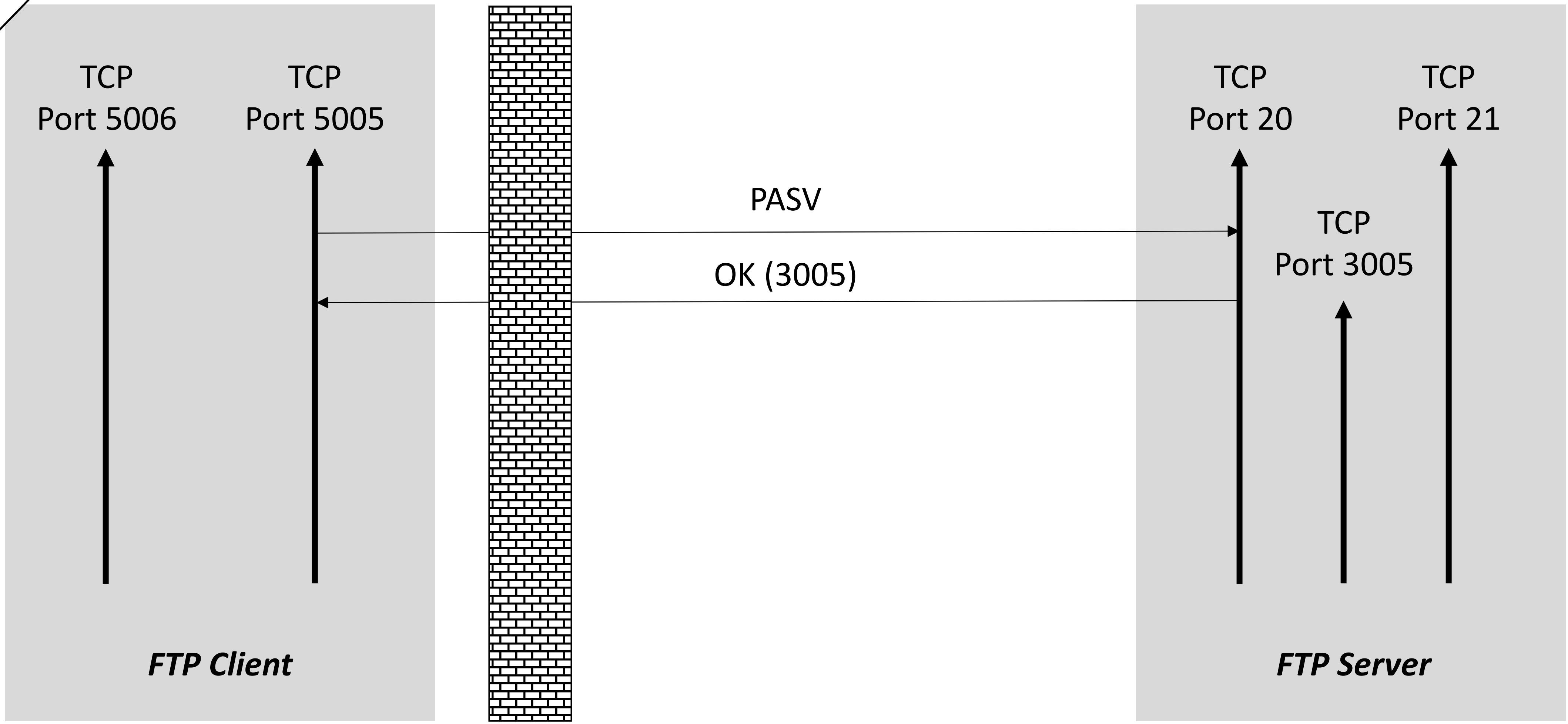


Packet Filtering Firewall – FTP Firewall Weakness



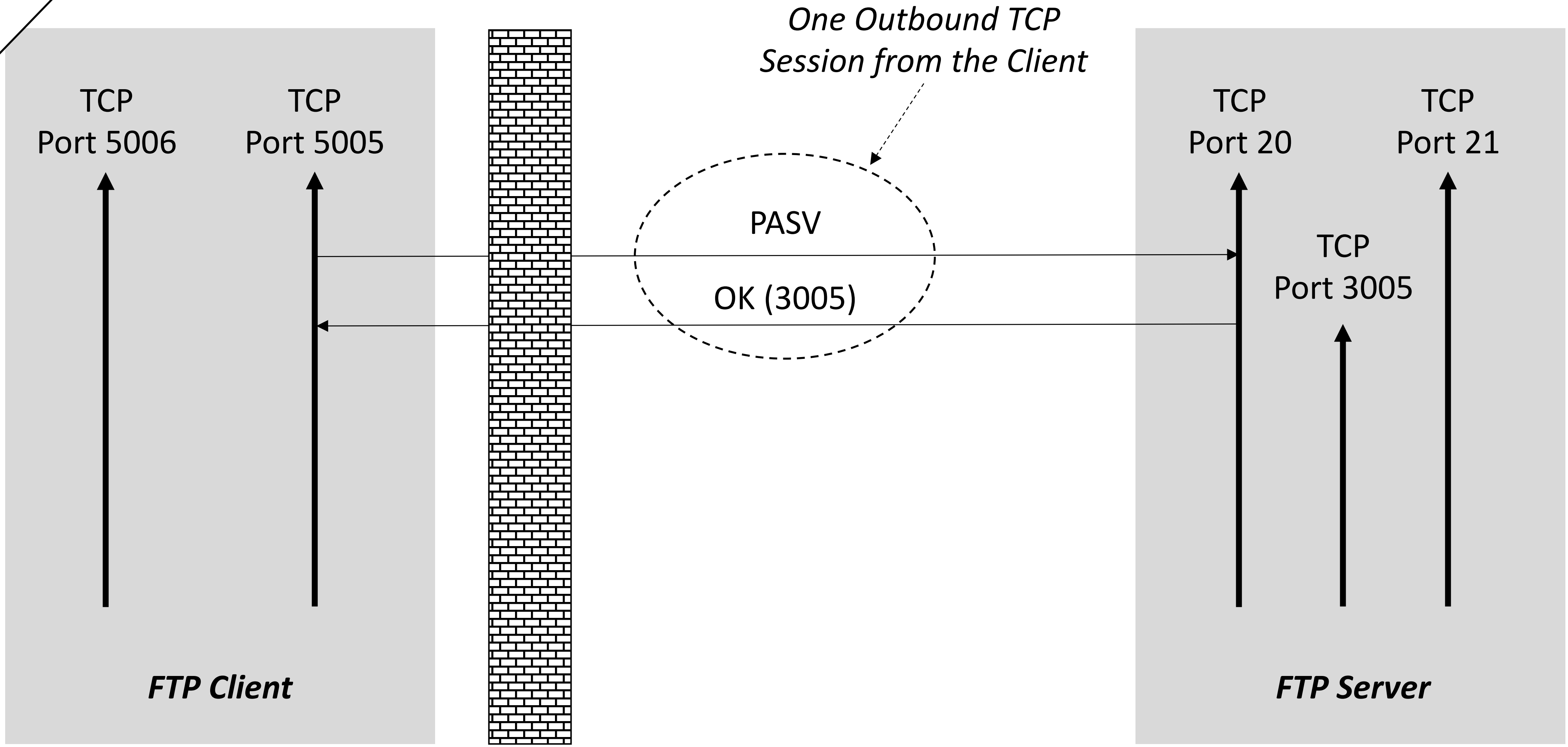
Firewall Must Allow only Outbound TCP Connections

Packet Filtering Firewall – PASV Mode FTP



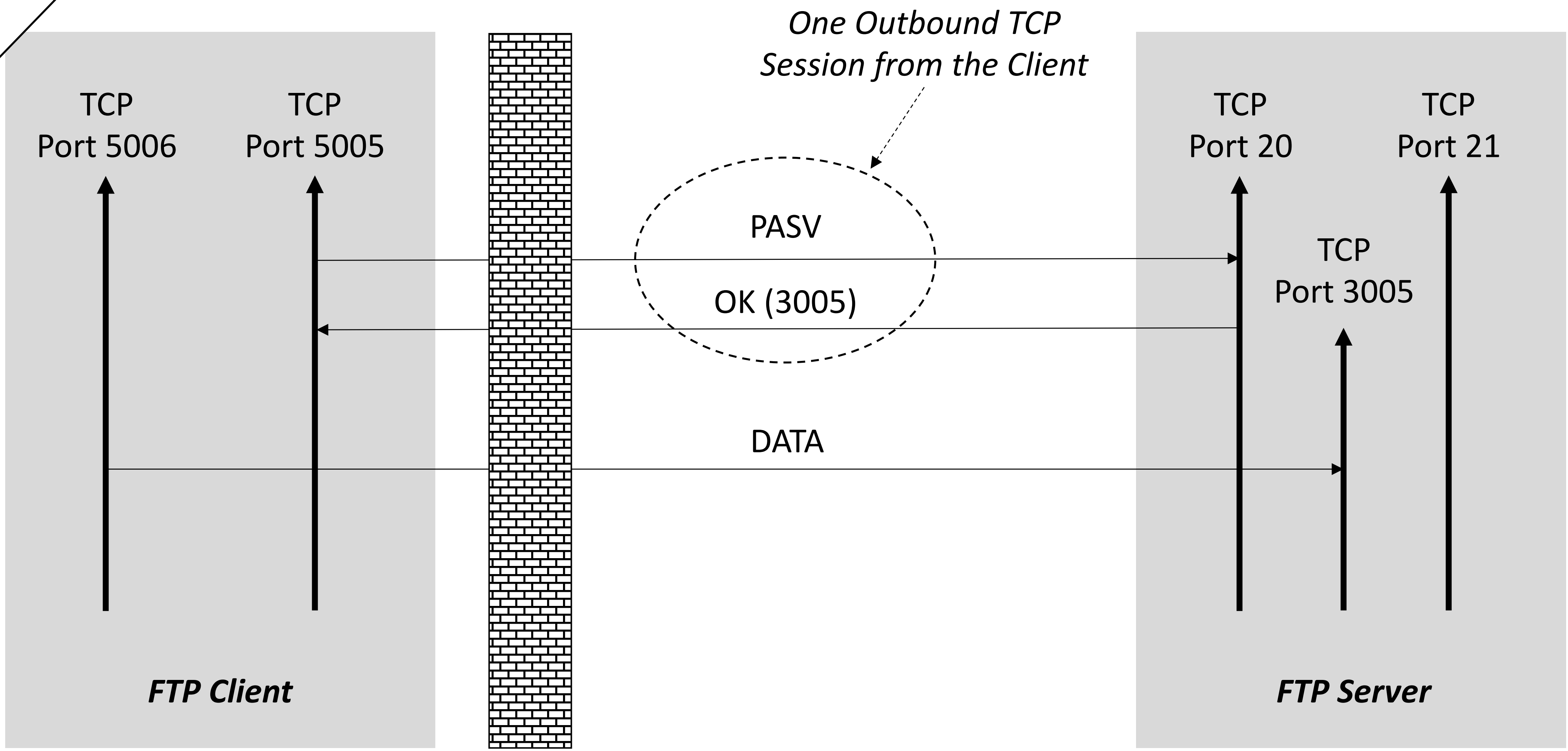
Firewall Must Allow only Outbound TCP Connections

Packet Filtering Firewall – PASV Mode FTP



Firewall Must Allow only Outbound TCP Connections

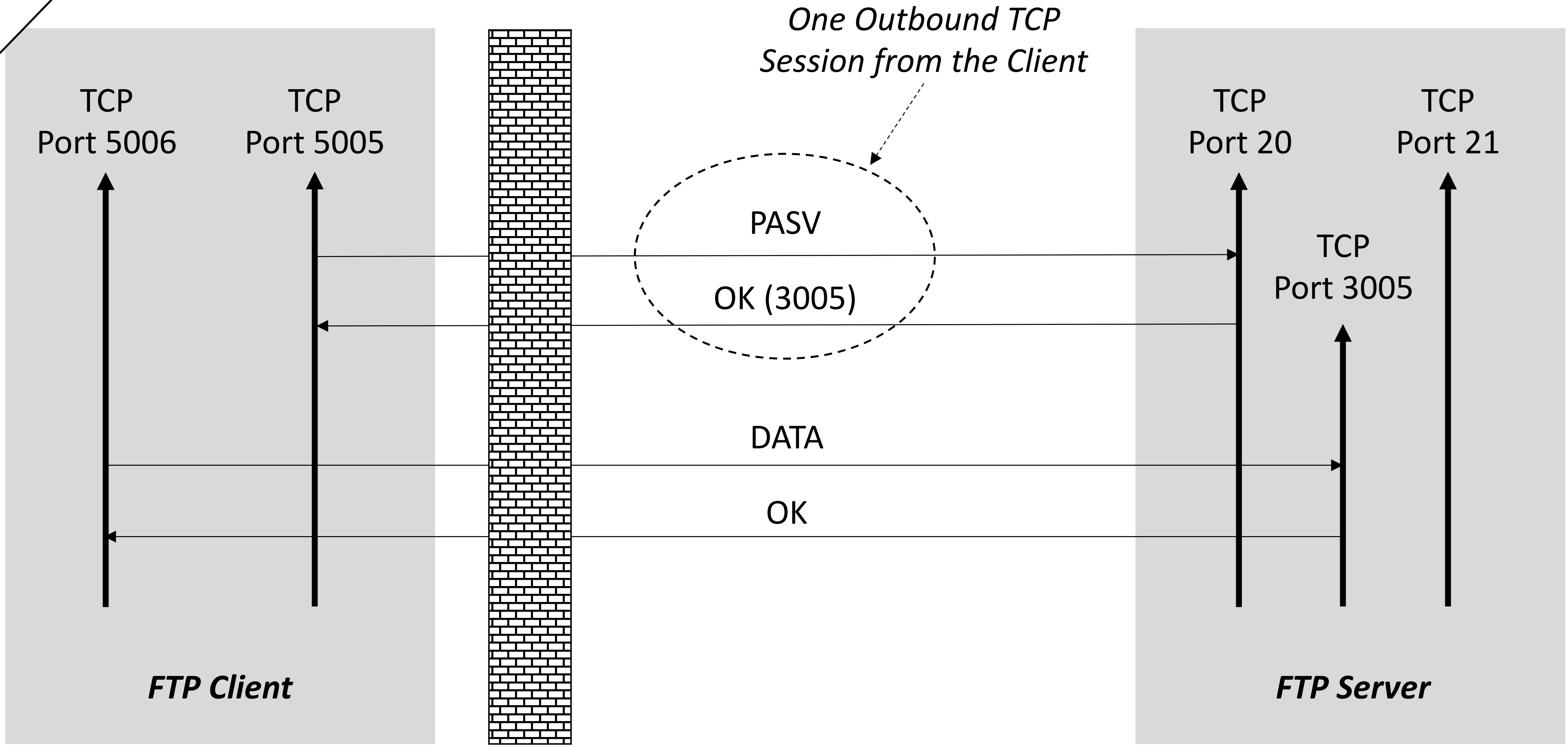
Packet Filtering Firewall – PASV Mode FTP



Firewall Must Allow only Outbound TCP Connections

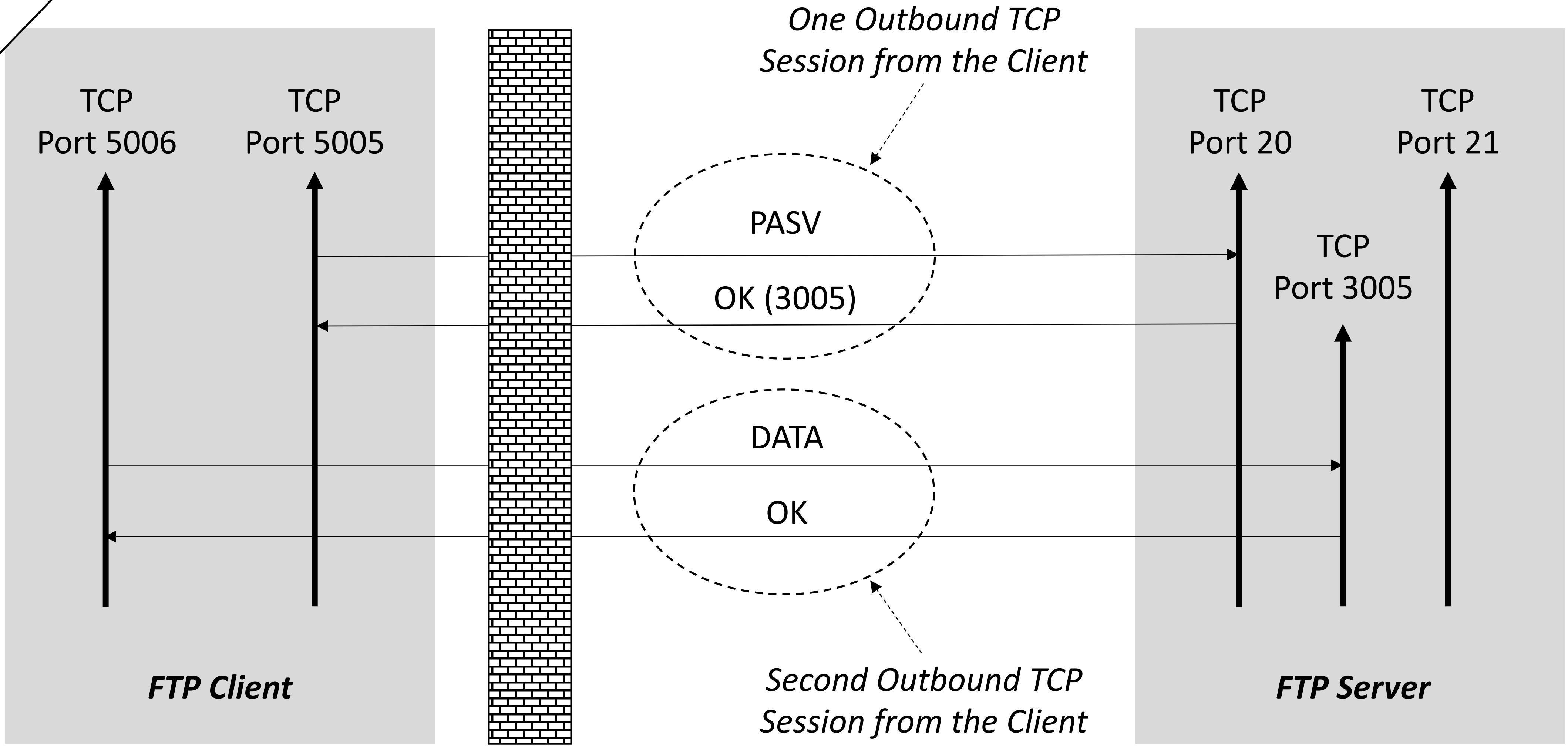
Packet Filtering Firewall – PASV Mode FTP

Week 10



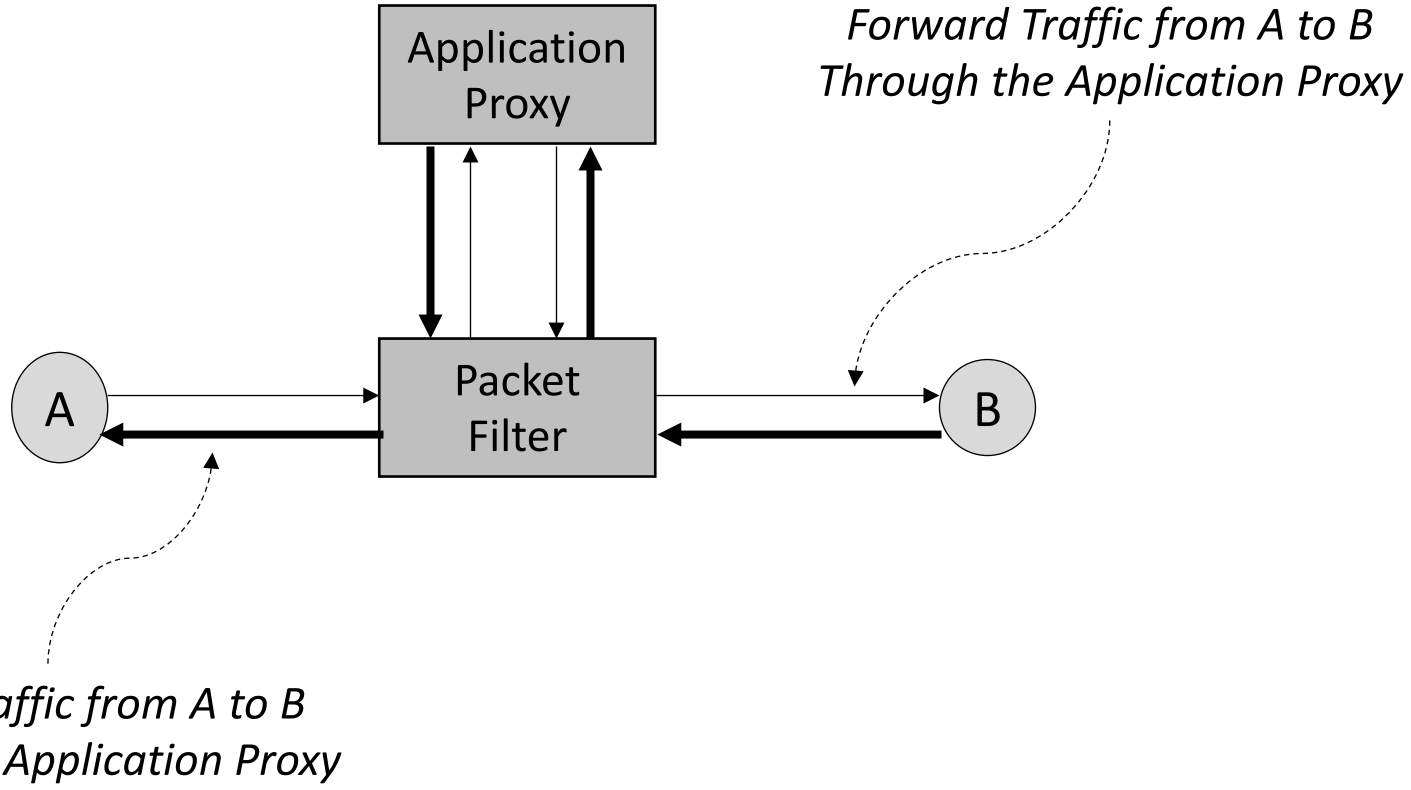
Firewall Must Allow only Outbound TCP Connections

Packet Filtering Firewall – PASV Mode FTP



Firewall Must Allow only Outbound TCP Connections

Packet Filtering Firewall – PASV Mode FTP

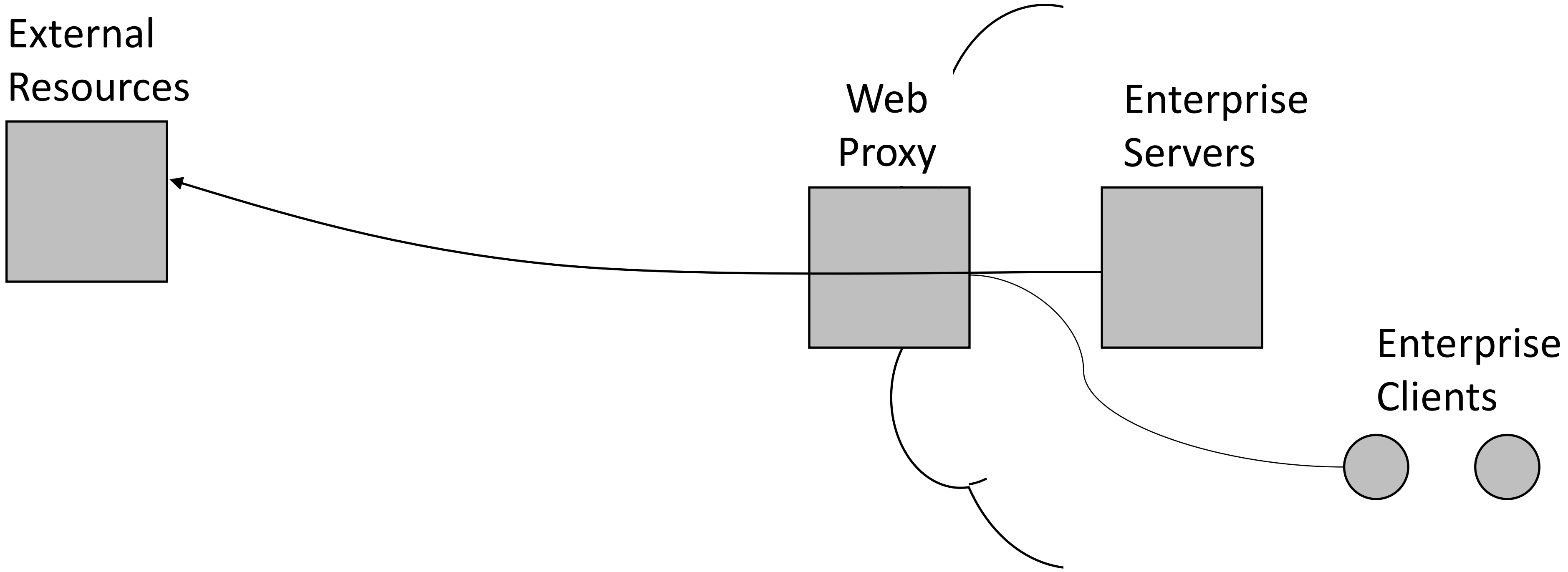


Forward Traffic from A to B Through the Application Proxy

Reverse Traffic from A to B Through the Application Proxy

Application Proxy Firewall

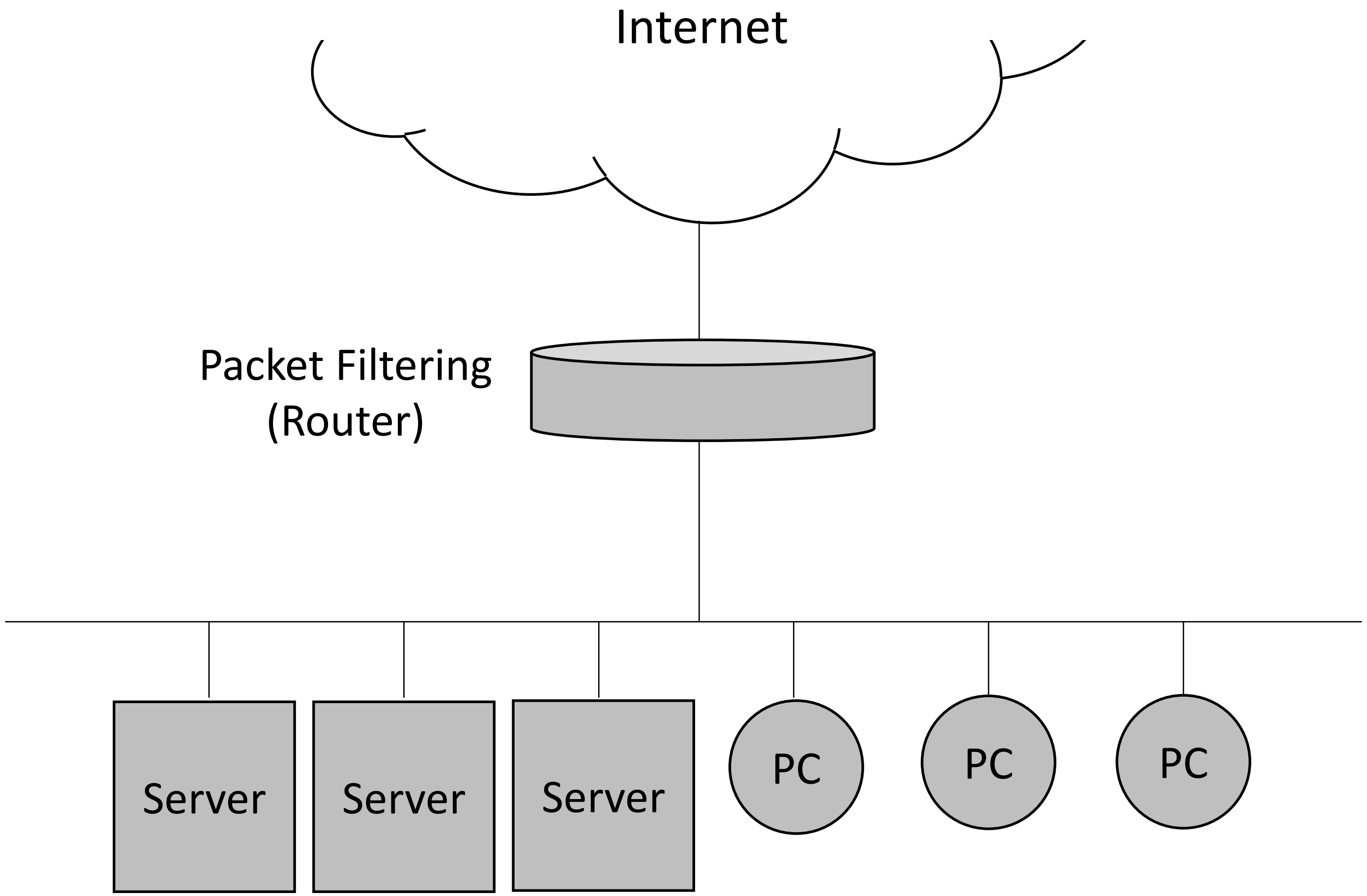
Week 10



Proxy for Enterprise Protection (Outbound URL Filters)

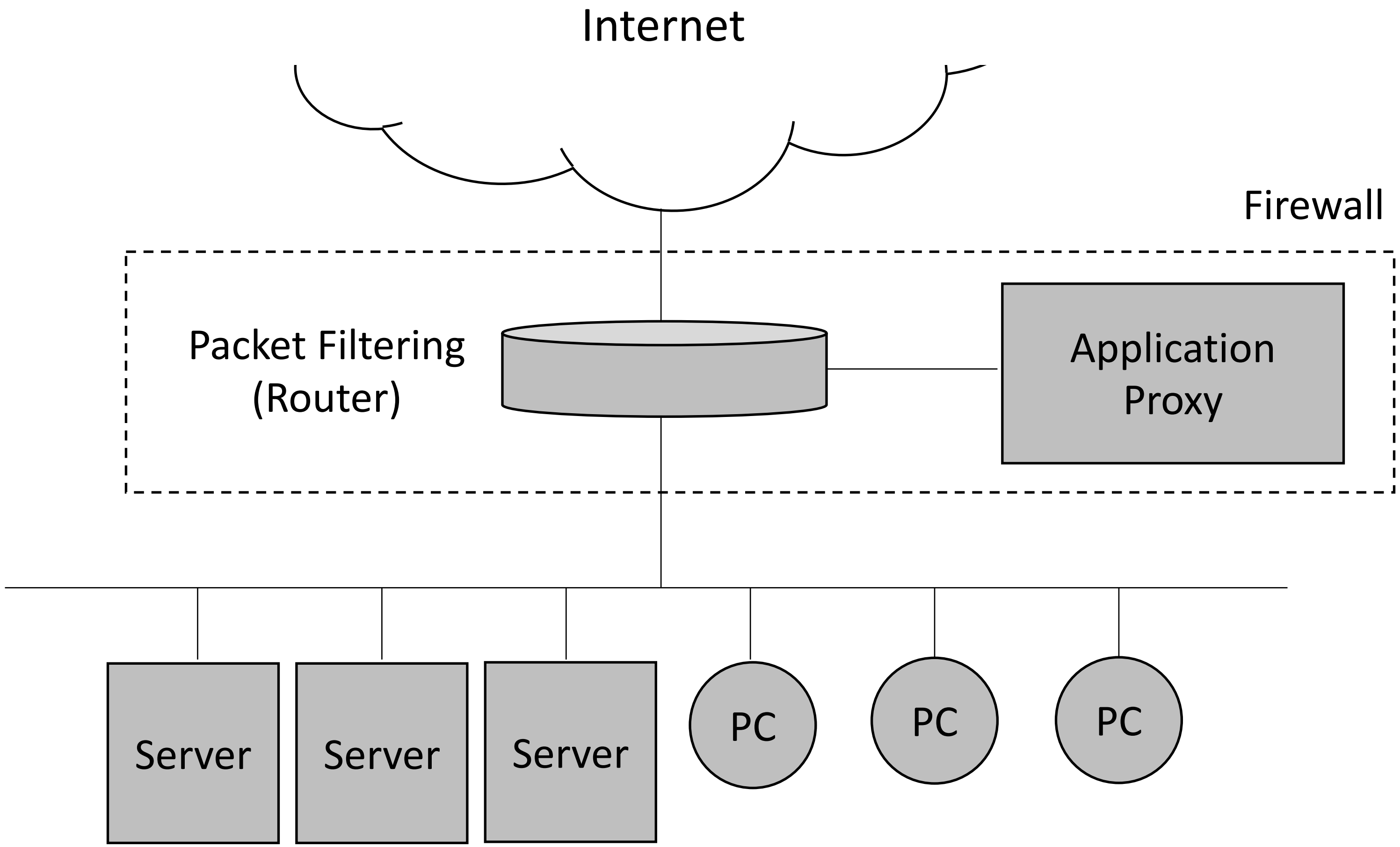
Week 10

Pros: Simple, Inexpensive
Cons: Only Simple Rules



Simple Packet Filtering Architecture for Enterprise

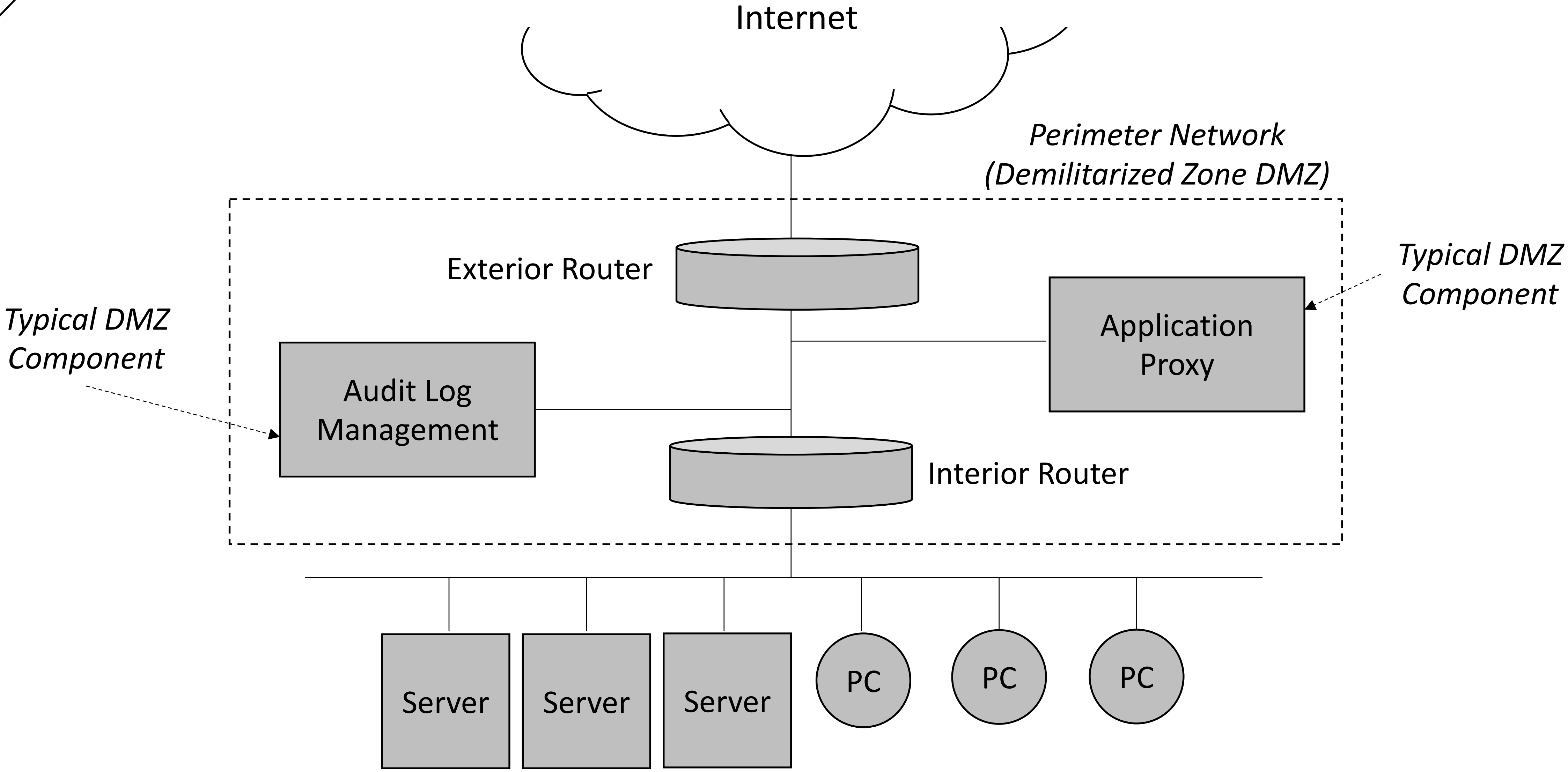
Pros: Increased Capability
Cons: Slightly Higher Cost



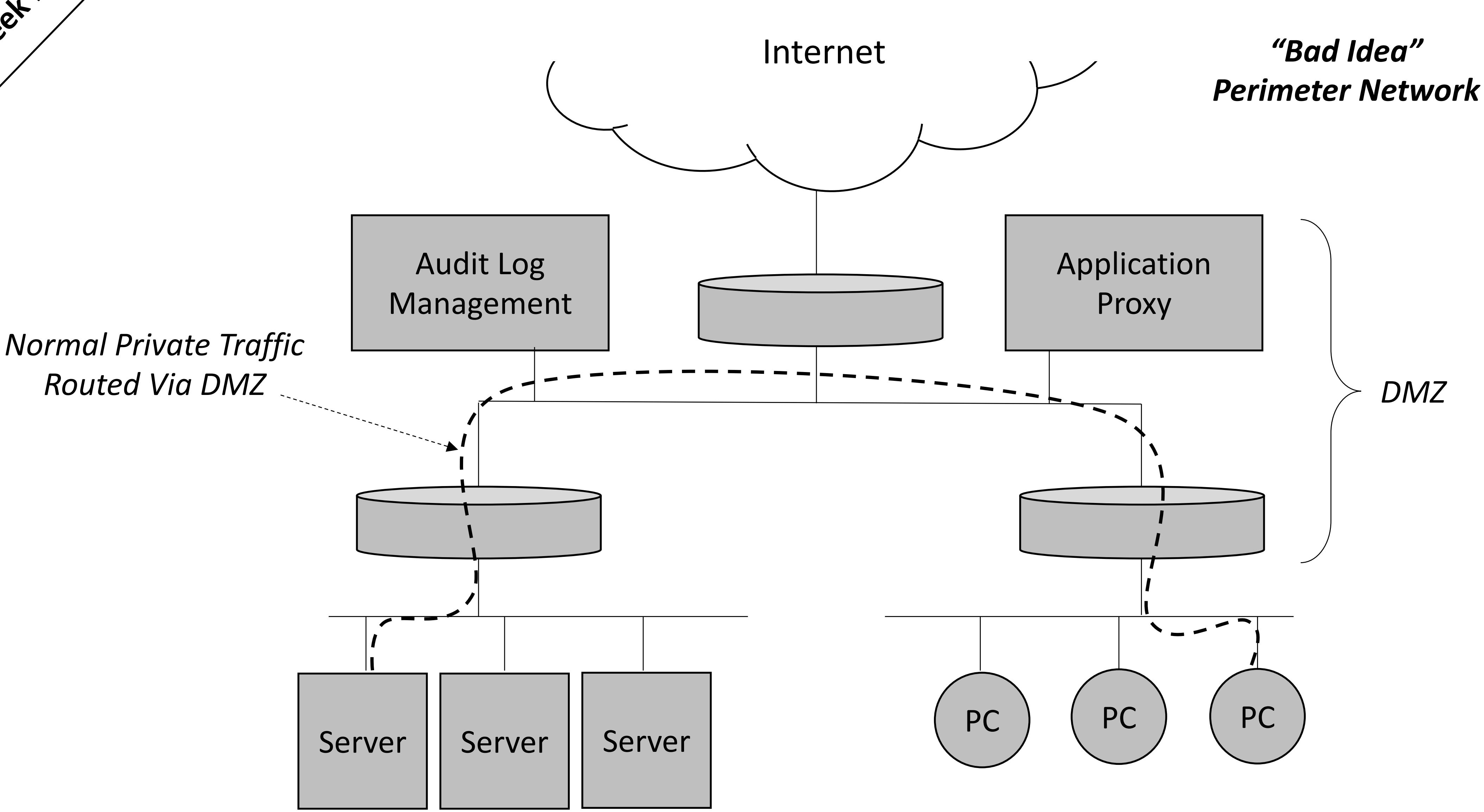
Simple Packet Filtering Architecture Plus Application Proxy for Enterprise

Week 10

Pros: Highest Capability
Cons: Highest Cost



Enterprise DMZ



"Bad Idea" Perimeter Network

Firewall Configuration – Not Recommended