



The Beauty and Joy of Computing

Internet II



UC Berkeley EECS
Lecturer
Gerald Friedland

Motorola aims at Smartphones
with interchangeable parts

Good: See IBM PC 1980s
Bad: See IBM PC 1980s



[http://www.usatoday.com/story/tech/personal/
2013/10/29/motorola-project-ara/3296887/](http://www.usatoday.com/story/tech/personal/2013/10/29/motorola-project-ara/3296887/)



Components of the Internet: Physical



Client



Server

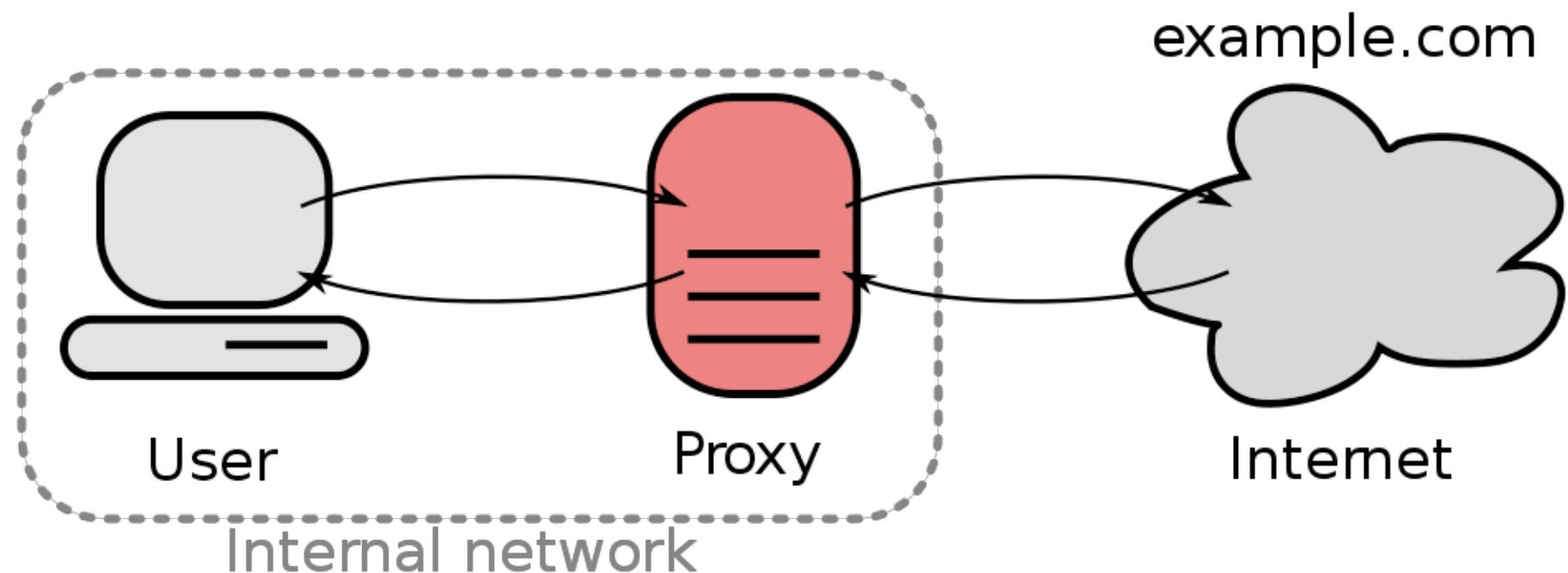


Router





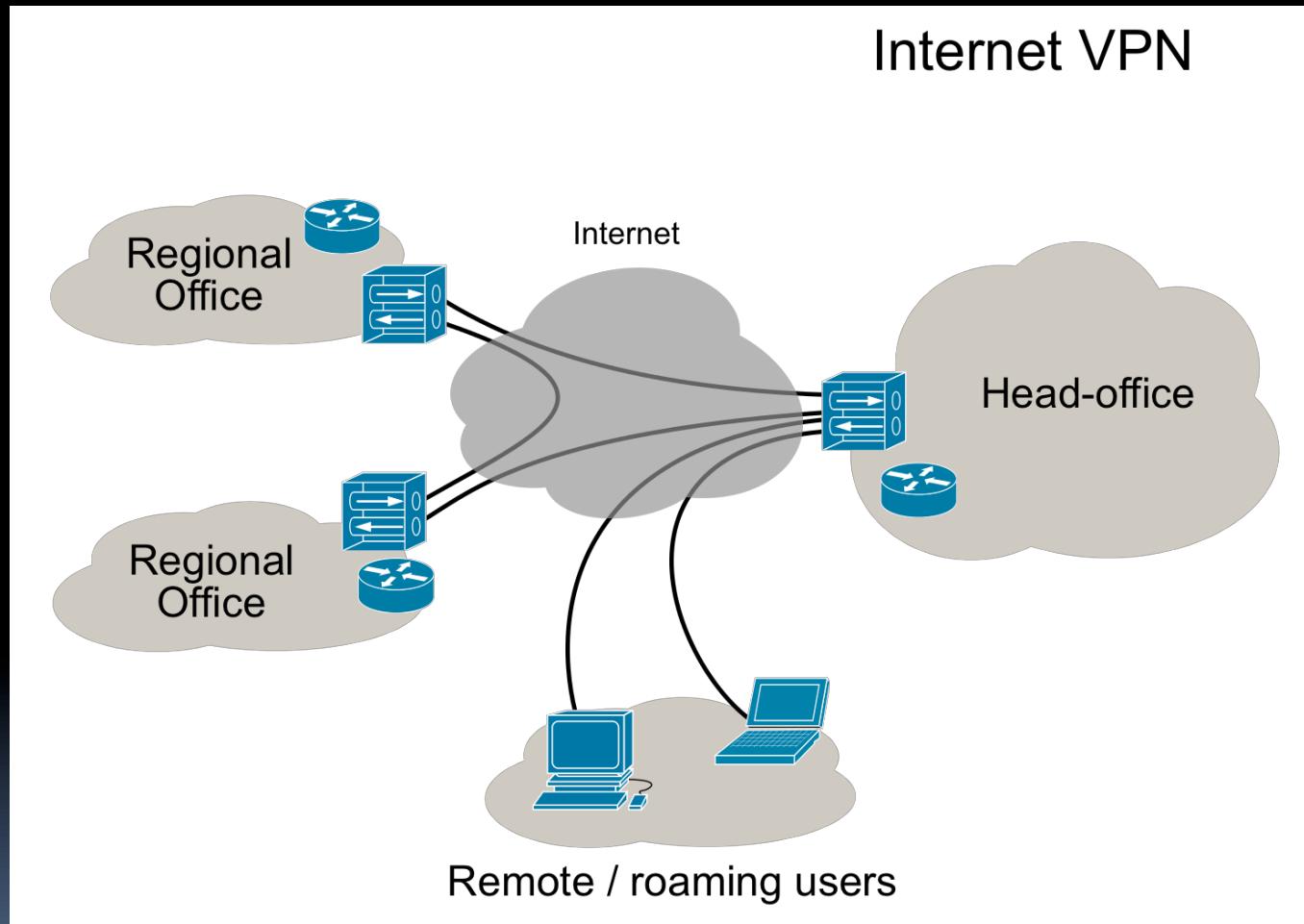
Virtual Components: Proxy



Proxy



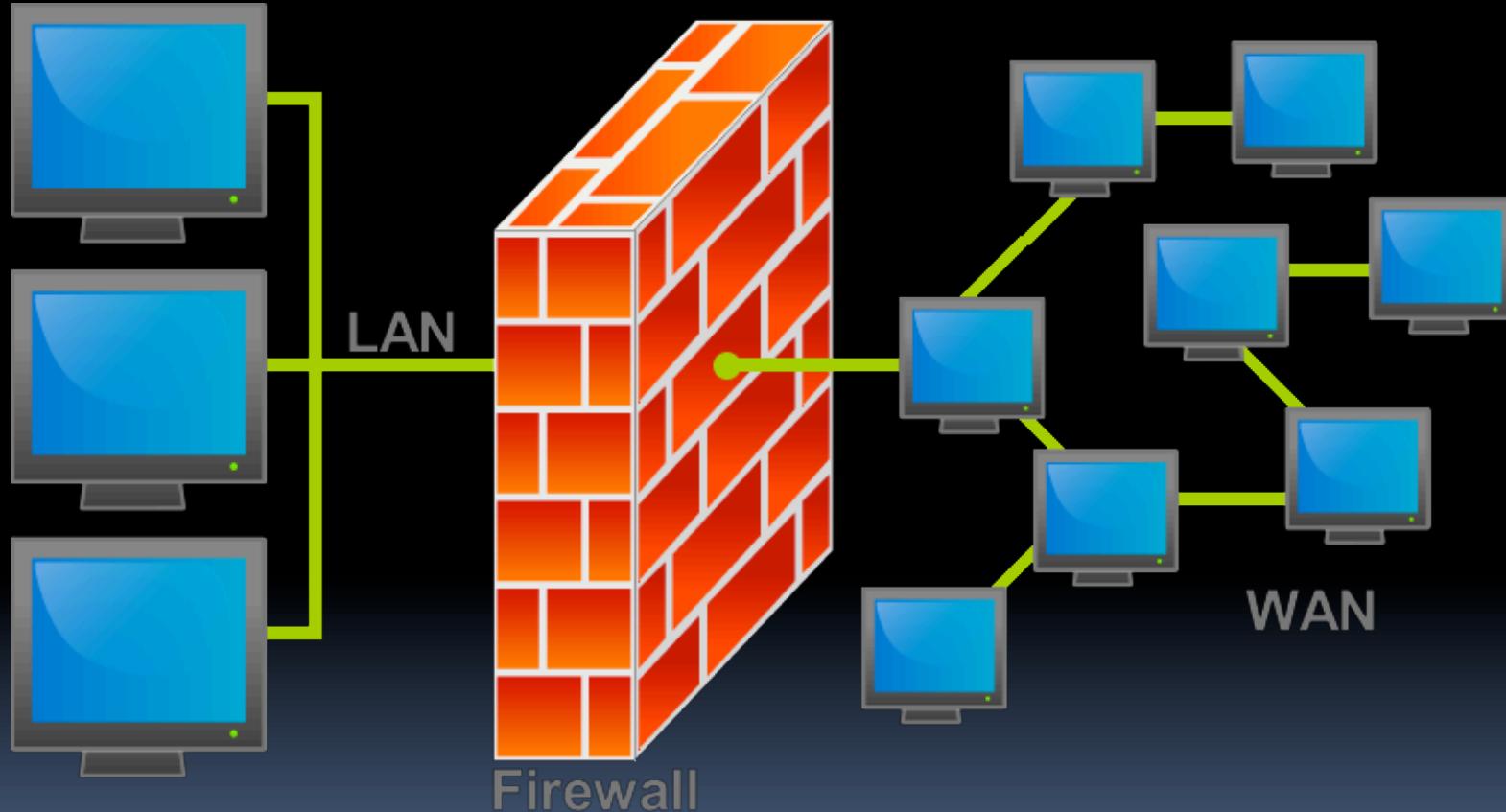
Virtual Components: VPN



Virtual Private Networks



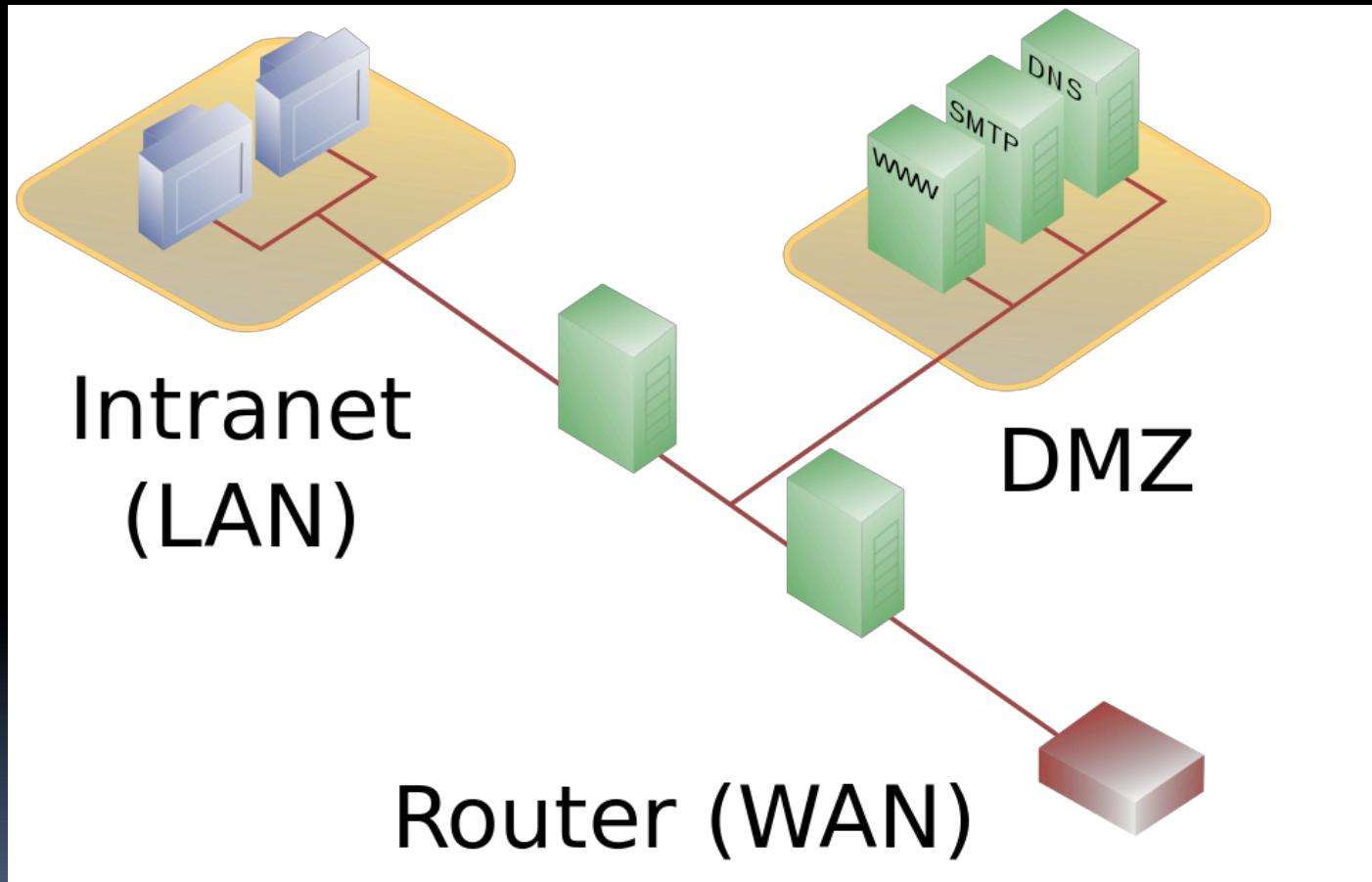
Virtual Components: Firewall



Firewall



Virtual Components: DMZ



Demilitarized Zone





Protocols

Protocol = Language of the Internet

Examples:

- **Hypertext Transfer Protocol (HTTP)**
- **File Transfer Protocol (FTP)**
- **Simple Mail Transfer Protocol (SMTP)**
- **Transfer Control Protocol (TCP)**





Protocols

```
S: 220 smtp.example.com ESMTP Postfix
C: HELO relay.example.org
S: 250 Hello relay.example.org, I am glad to meet you
C: MAIL FROM:<bob@example.org>
S: 250 Ok
C: RCPT TO:<alice@example.com>
S: 250 Ok
C: RCPT TO:<theboss@example.com>
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>. <CR><LF>
C: From: "Bob Example" <bob@example.org>
C: To: "Alice Example" <alice@example.com>
C: Cc: theboss@example.com
C: Date: Tue, 15 January 2008 16:02:43 -0500
C: Subject: Test message
C:
C: Hello Alice.
C: This is a test message with 5 header fields and 4 lines in the message body.
C: Your friend,
C: Bob
C: .
S: 250 Ok: queued as 12345
C: QUIT
S: 221 Bye
{The server closes the connection}
```



Friedland



Protocol stack: Open Systems Interconnection

OSI Model			
	Data unit	Layer	Function
Host layers	Data	7. Application	Network process to application
		6. Presentation	Data representation, encryption and decryption, convert machine dependent data to machine independent data
		5. Session	Interhost communication, managing sessions between applications
	Segments	4. Transport	Reliable delivery of packets between points on a network.
Media layers	Packet/Datagram	3. Network	Addressing, routing and (not necessarily reliable) delivery of datagrams between points on a network.
	Bit/Frame	2. Data link	A reliable direct point-to-point data connection.
	Bit	1. Physical	A (not necessarily reliable) direct point-to-point data connection.





Encryption

Encryption is the essential security component of the Internet. Common protocols:

- PGP for e-mail
- https:// for http://
- SSH for remote shells (instead of telnet)
- SCP and SFTP for file transfer (replaces rcp and ftp)
- DES for passwords

Adds itself into OSI layer.





Question

Have you ever used encryption for your e-mails?

- a) No
- b) Yes, using PGP
- c) Yes, using other than PGP





Encryption: How it works

Two types of encryption:

- **Symmetric (Shared Key)**
 - Issue: Key needs to be send over Internet... (not a solution)
- **Asymmetric**
 - Used by secure protocols today





Encryption: How to not send keys

<http://www.youtube.com/watch?v=3QnD2c4Xovk>



UC Berkeley "The Beauty and Joy of Computing" : Internet II (13)

Friedland





Question

Does encryption help with privacy issues?





Speed Metrics

- **Latency = Time to establish connection**
 - Also called ping time
 - Usually in ms range
 - Additive with route length
 - Hardware dependent
- **Throughput = Information per second transferred**
 - Measured in bits/sec
 - Slowest connection in route dictates throughput
 - Hardware dependent





Threats to the Internet

- **Internet is vulnerable at bottlenecks**
- **Computers are vulnerable and attackable**
 - Malware (Virus, Worms, etc)
 - Denial of Service (DOS) Attacks
- **Internet is vulnerable to monopolization (e.g. switch from E-mail to Facebook)**





Threats to Society

- **Dependence on the Internet by**
 - Individuals
 - Economy
 - Governments

creates possibility for Cyberwar (see discussion)

- **Uncontrollable availability of information creates threats to some individuals, societies, governments**
- **Data-driven economy changes privacy configuration of society**





Internet Economy impacts Privacy



<http://www.tacma.net>

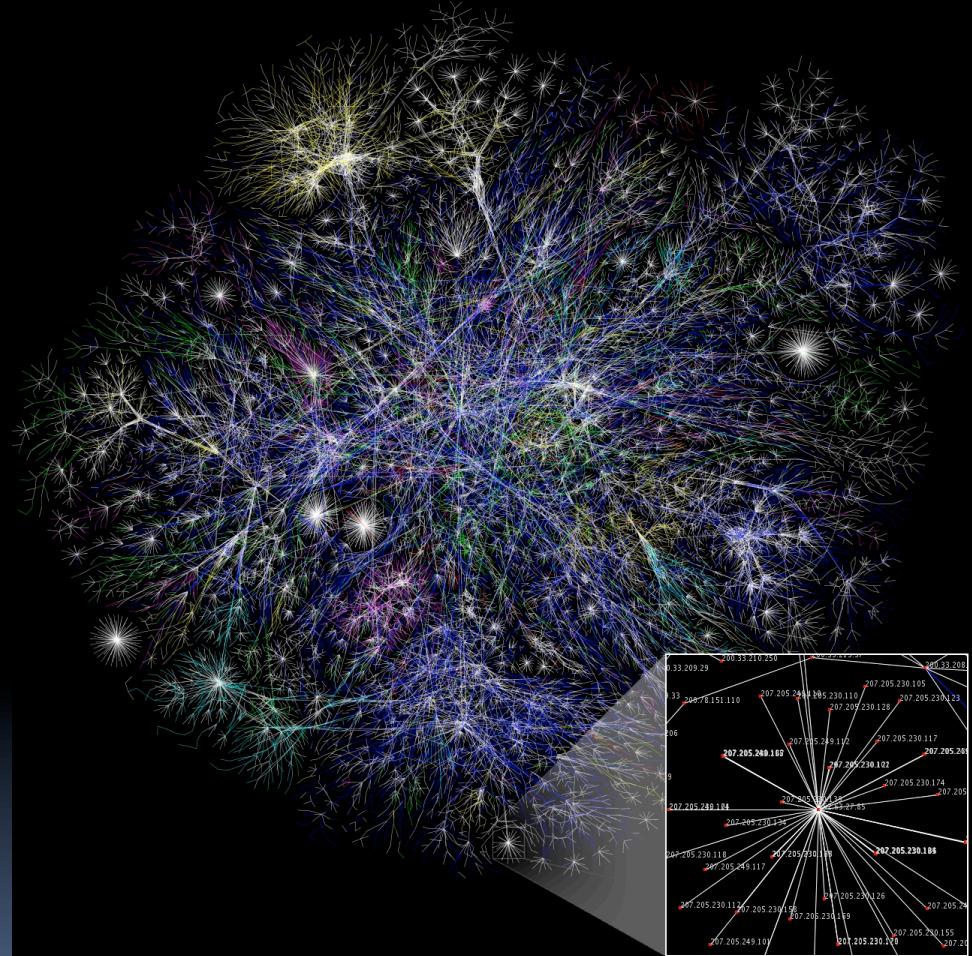
UC Berkeley "The Beauty and Joy of Computing" : Internet II (18)

Friedland



Summary

- The Internet has physical and virtual building pieces and uses protocols
- Encryption schemes allow safer point-to-point communication
- The Internet is vulnerable as is society



[http://commons.wikimedia.org/
wiki/File:Internet_map_1024.jpg](http://commons.wikimedia.org/wiki/File:Internet_map_1024.jpg)

Friedland

