Class Meeting: Lectures 19 and 20: Security, SDN

COS 461: Computer Networks
Kyle Jamieson

[Various parts adapted from M. Freedman, J. Rexford]

Today

- Programmable Networks
  - Division of labor: control, data planes
  - Software-defined networking

- Security Intro: Concepts and Applications

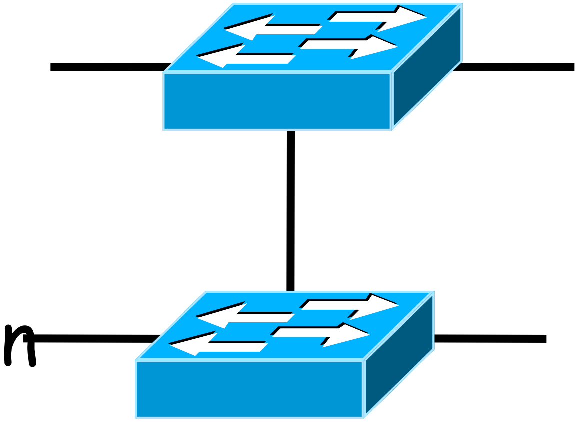
The Internet: A Remarkable Story

- Tremendous success
  - From research experiment to global infrastructure

- Brilliance of under-specifying
  - Network: best-effort packet delivery
  - Hosts: arbitrary applications
- Enables innovation in applications
  - Web, P2P, VoIP, social networks, smart cars, …
- But, change is easy only at the edge… ☹

Inside the 'Net: A Different Story…

- Closed equipment
  - Software bundled with hardware
  - Vendor-specific interfaces
- Over specified
  - Slow protocol standardization
- Few people can innovate
  - Equipment vendors write the code
  - Long delays to introduce new features

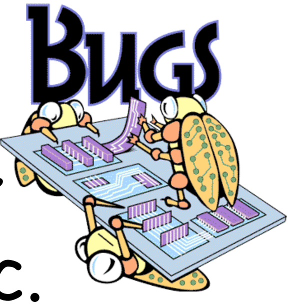


Impacts performance, security, reliability, cost…

Networks are Hard to Manage

- Operating a network is expensive
  - More than half the cost of a network
  - Yet, operator error causes most outages

- Buggy software in the equipment
  - Routers with 20+ million lines of code
  - Cascading failures, vulnerabilities, etc.

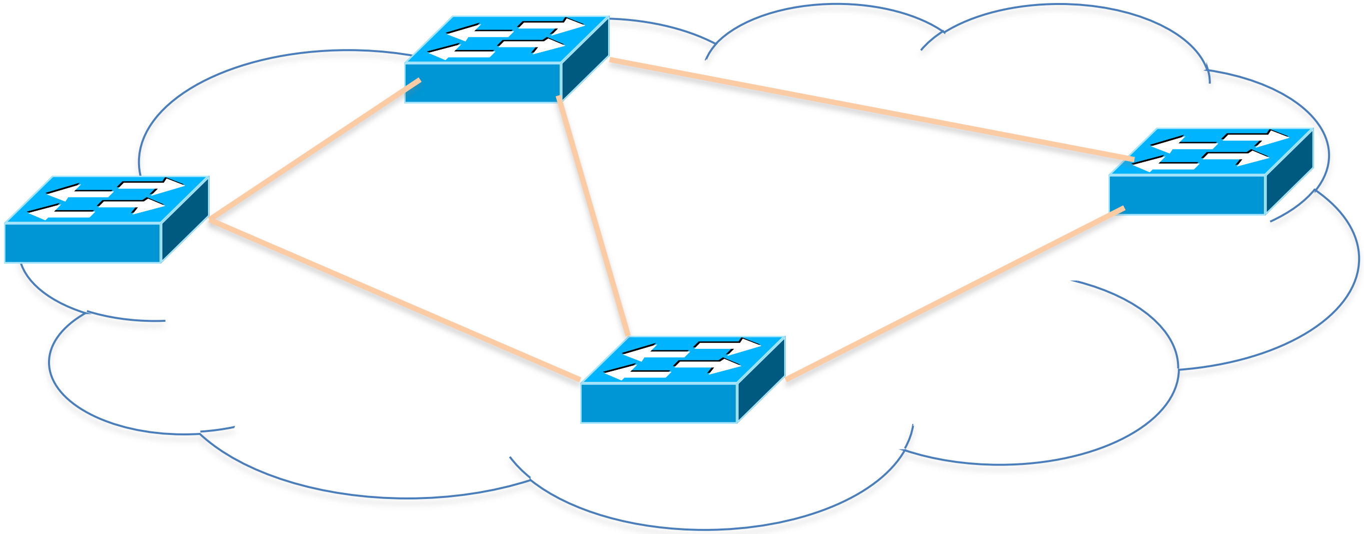


- The network is "in the way"
  - Especially in data centers and the home

Rethinking the “Division of Labor“

Traditional Computer Networks

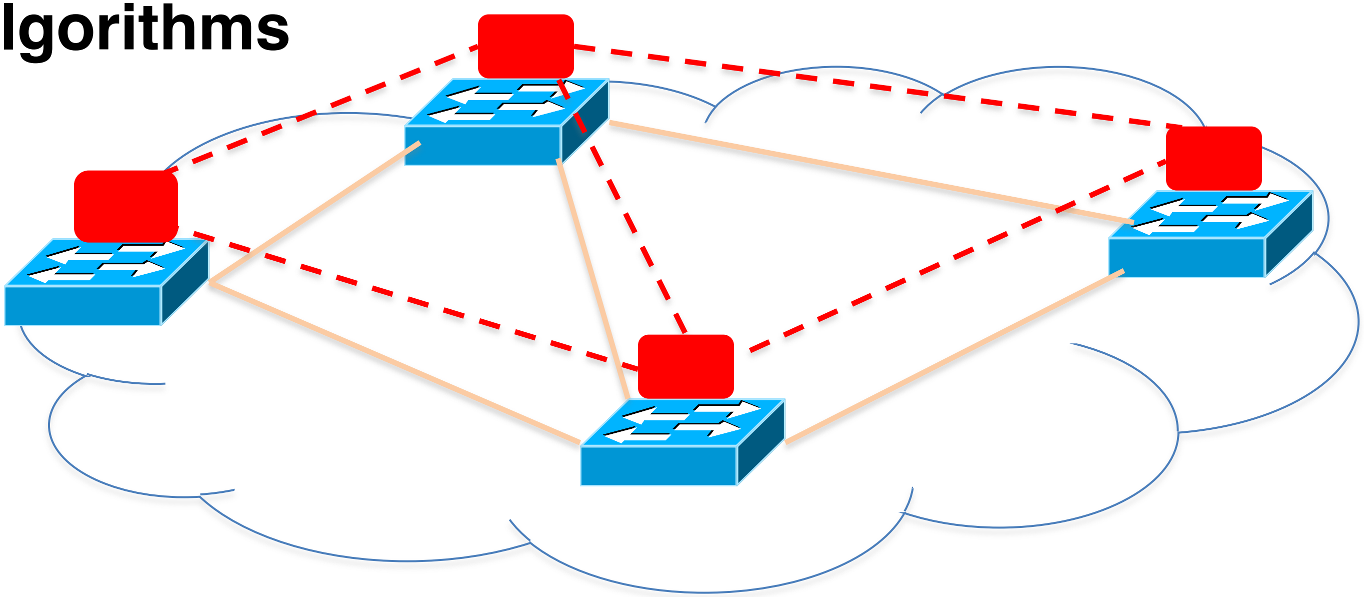
Data plane:
Packet streaming



Forward, filter, buffer, mark, rate-limit, and measure packets

Traditional Computer Networks

Control plane:
Distributed algorithms

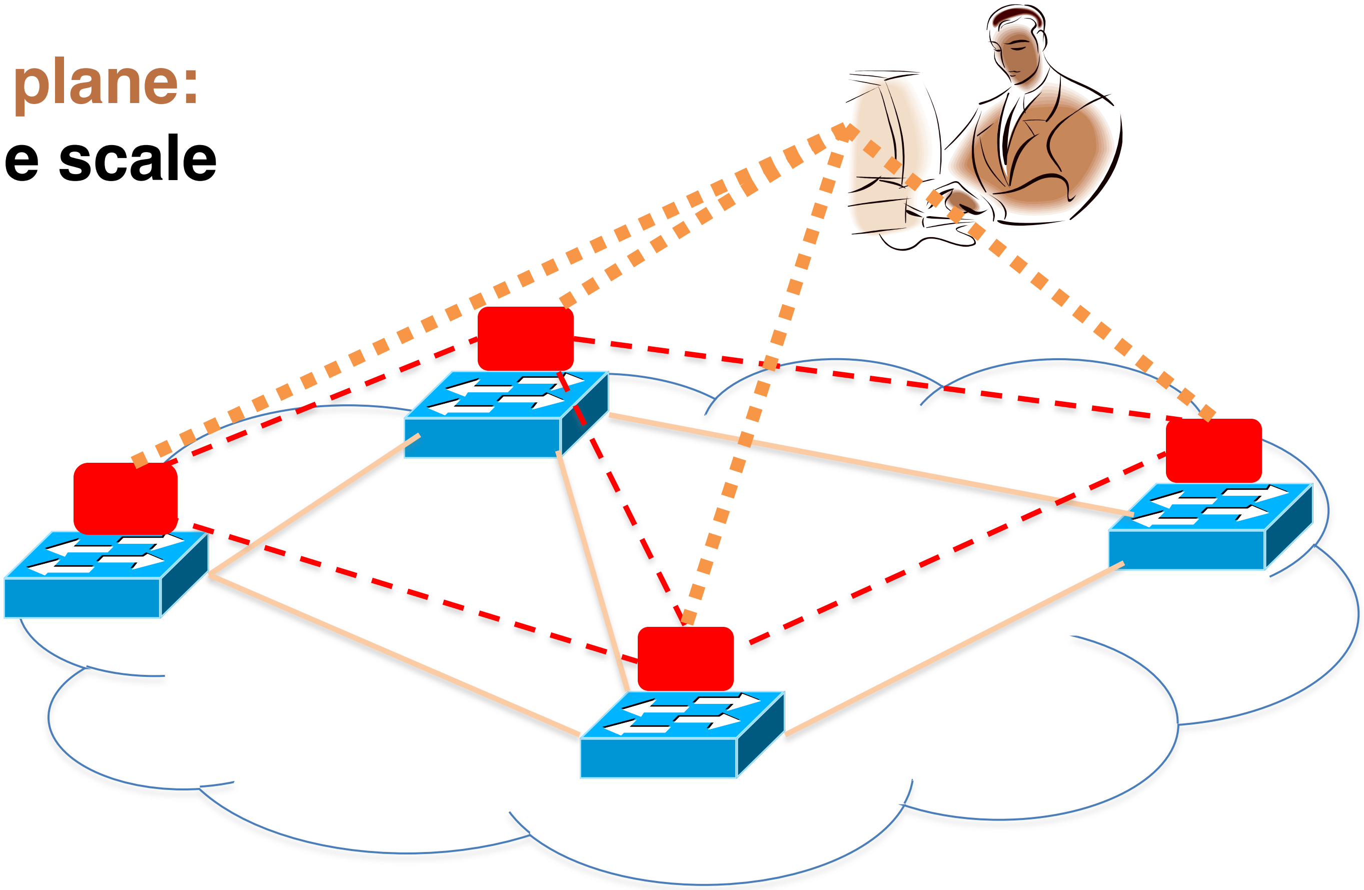


Track topology changes, compute routes, install forwarding rules

Traditional Computer Networks

Management plane:

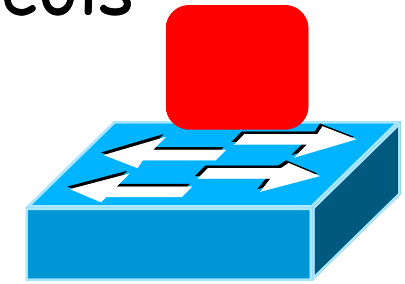
Human time scale



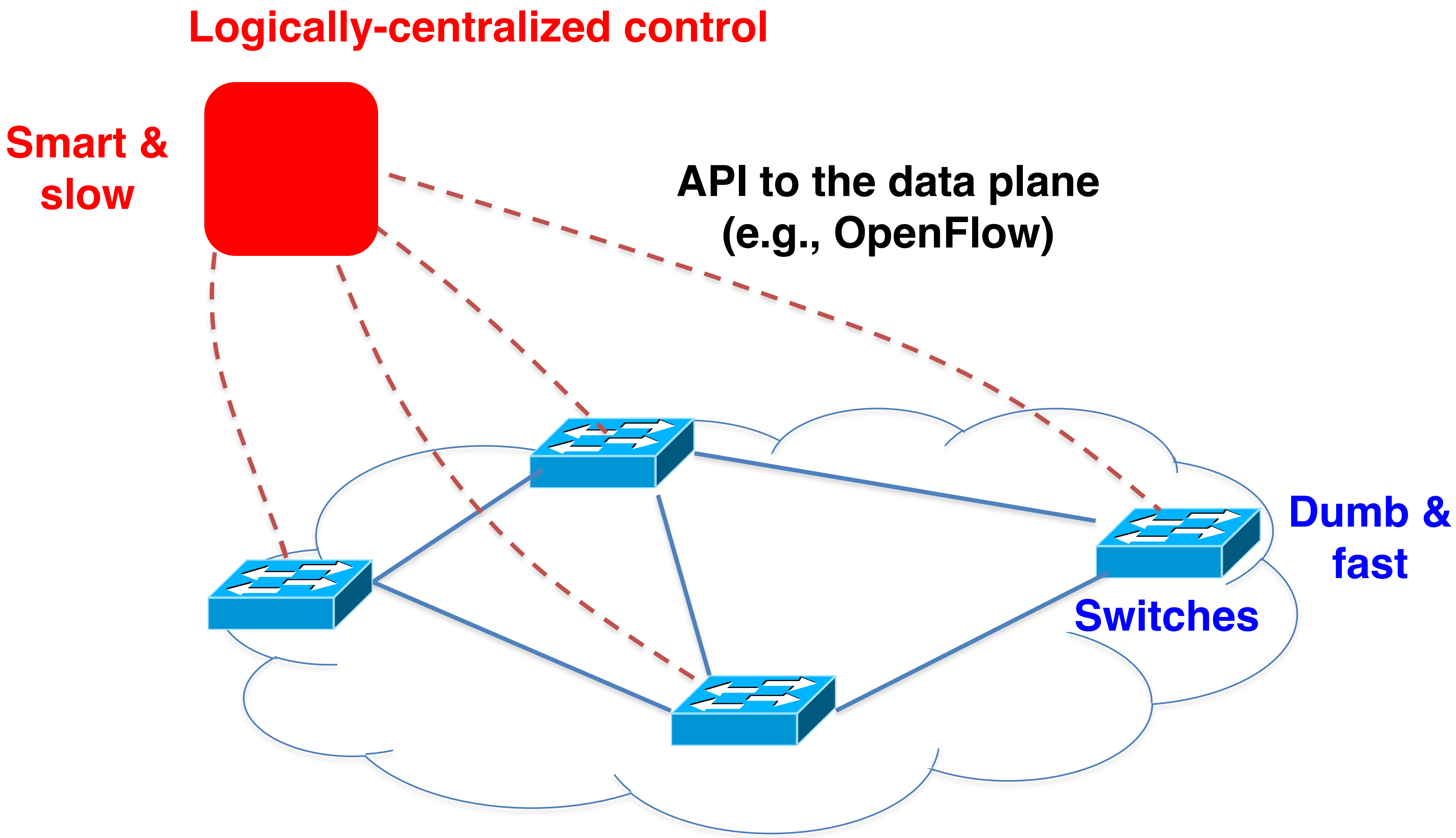
Collect measurements and configure the equipment

Remove that Control Plane!

- Simpler management
  - No need to “invert” control-plane operations
- Faster pace of innovation
  - Less dependence on vendors and standards
- Easier interoperability
  - Compatibility only in “wire” protocols
- Simpler, cheaper equipment
  - Minimal software



Software Defined Networking (SDN)



Logically-centralized control

Smart & slow

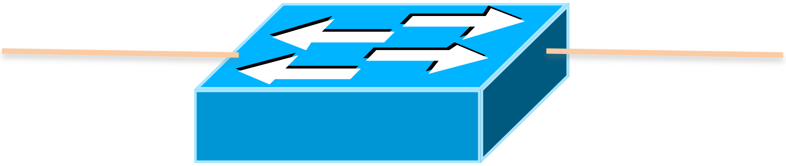
API to the data plane (e.g., OpenFlow)

Dumb & fast

Switches

Data Plane: Simple Packet Handling

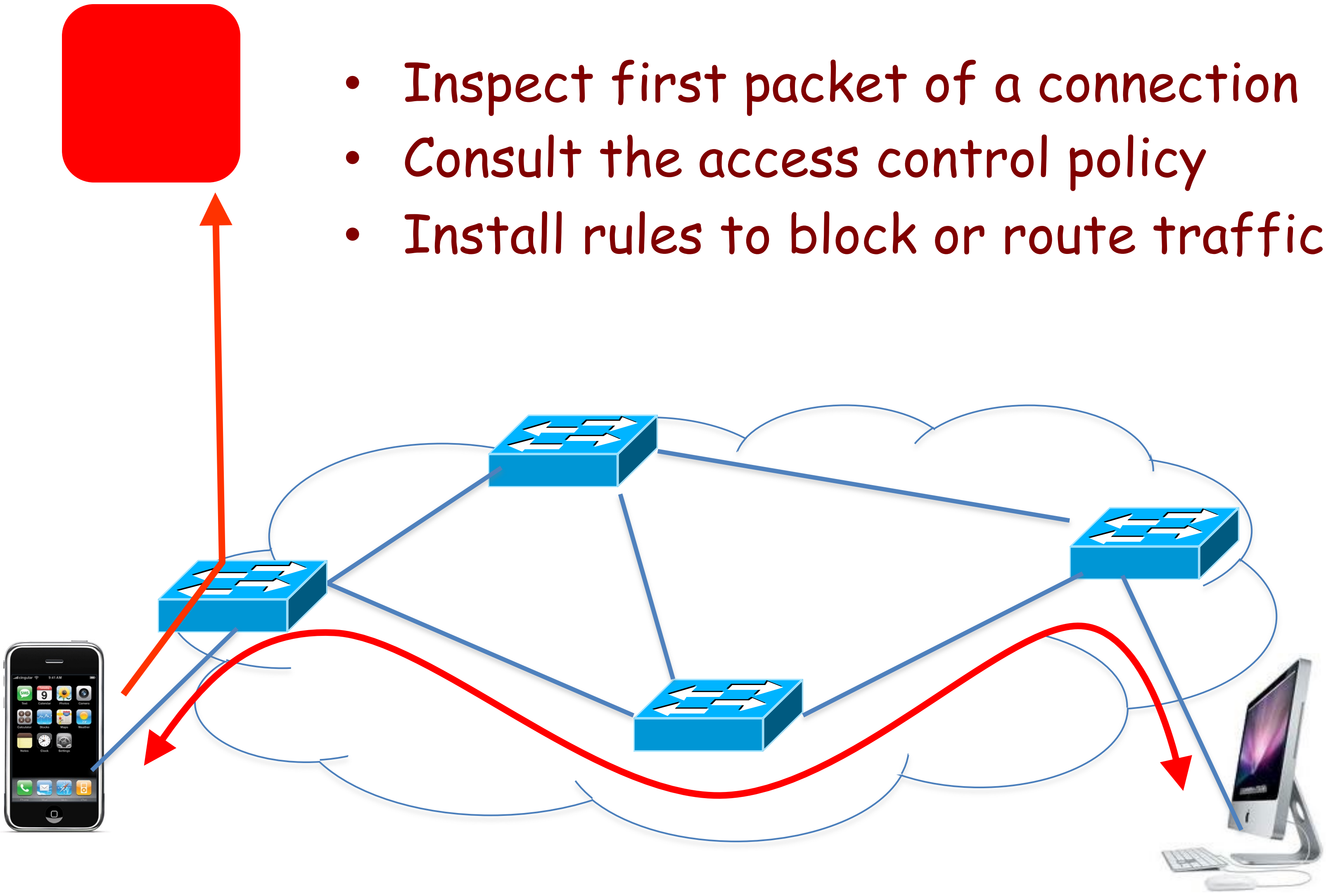
- Simple packet-handling rules
  - Pattern: match packet header bits
  - Actions: drop, forward, modify, send to controller
  - Priority: disambiguate overlapping patterns
  - Counters: #bytes and #packets



1. **src=1.2.*.*, dest=3.4.5.* → drop**
2. **src = *.*.*.*, dest=3.4.*.* → forward(2)**
3. **src=10.1.2.3, dest=*.*.*.* → send to controller**

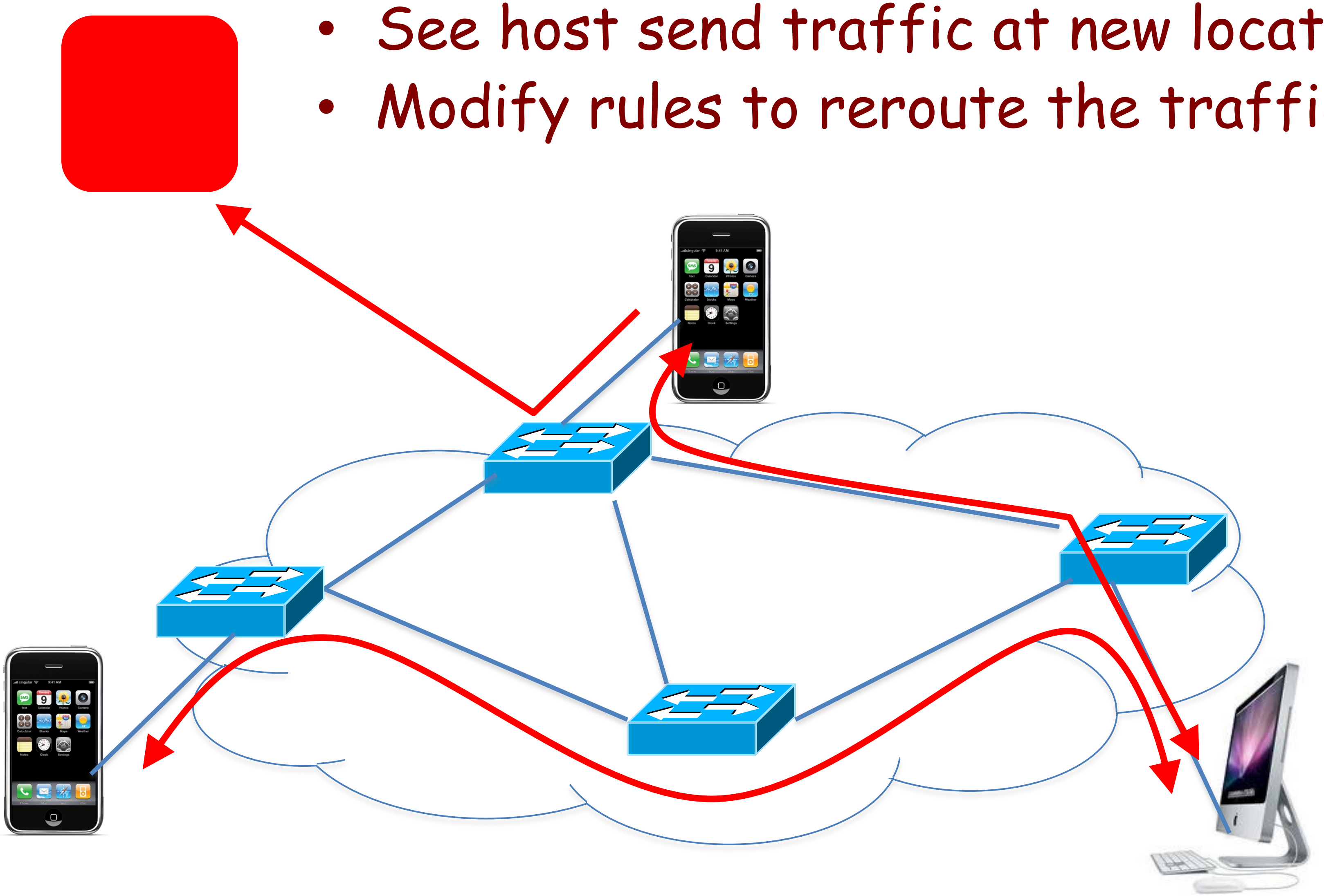
E.g.: Dynamic Access Control

- Inspect first packet of a connection
- Consult the access control policy
- Install rules to block or route traffic



E.g.: Seamless Mobility/Migration

- See host send traffic at new location
- Modify rules to reroute the traffic



SDN: Summary

- Software-Defined Networks: new ways of managing networks
  - New API, OpenFlow, enables new applications

Today

- Programmable Networks
- Security Intro: Concepts and Applications

Internet's Design: Insecure

- Designed for simplicity
- "On by default" design

- Readily available zombie machines
- Attacks look like normal traffic
- Internet's federated operation obstructs cooperation for diagnosis/mitigation

Basic Security Properties

- **Confidentiality:** Concealment of information or resources
- **Authenticity:** Identification & assurance of origin of info
- **Integrity:** Trustworthiness of data/resources; preventing improper/unauthorized changes
- **Availability:** Ability to use desired information/resource
- **Non-repudiation:** Offer of evidence that a party indeed is sender or a receiver of certain information
- **Access control:** Facilities to determine and enforce who is allowed access to what resources (host, software, network, …)

Security protocols at many layers

- Application layer
  - E-mail: PGP, using a web-of-trust
  - Web: HTTP-S, using a certificate hierarchy
- Transport layer
  - Transport Layer Security/ Secure Socket Layer
- Network layer
  - IP Sec
- Network infrastructure
  - DNS-Sec and BGP-Sec

Symmetric vs. Asymmetric Crypto

a.k.a. Secret vs. Public Key Crypto

- Symmetric crypto (all crypto pre 1970s)
  - Sender and recipient share a common key
  - All classical encryption algorithms are private-key
  - Dual use: confidentiality or authentication/integrity
    - Encryption vs. msg authentication code (MAC)
- Public-key crypto
  - (Public, private) key associated w/ea. entity ("Alice")
  - Anybody can encrypt to Alice, anybody can verify Alice's message
  - Only Alice can decrypt, only Alice can "sign"
  - Developed to address "key distribution" problem and "digital signatures" (w/o prior establishment)

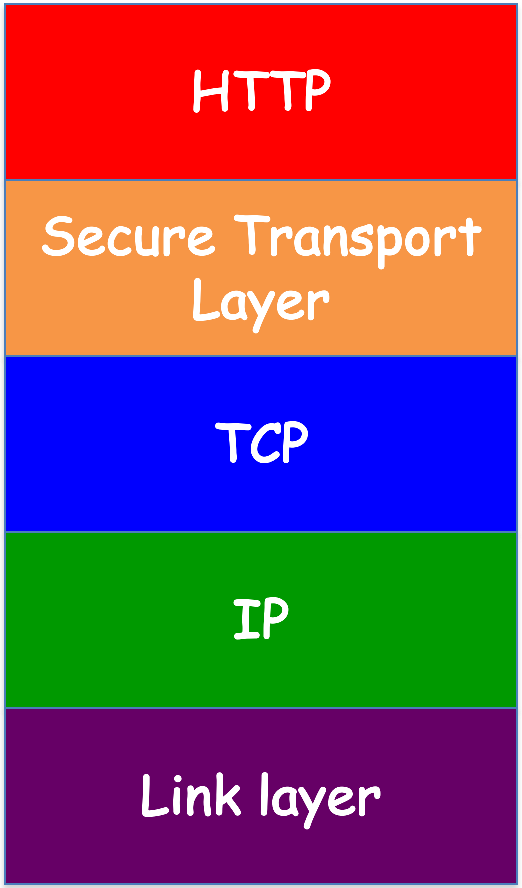
Why still both?

- Symmetric Pros and Cons
  - Simple and very fast (1000-10000x faster than asymmetric)
  - Must agree/distribute the key beforehand
  - AES/CBC (256-bit) → 80 MB/s (*for 2048 bits, .003 ms*)
- Public Key Pros and Cons
  - Easier key pre-distro.: "Public Key Infrastructure" (PKI)
  - Much slower
  - 2048-RSA → 6.1ms Decrypt, 0.16ms Encrypt
- Common "engineering" approach:
  - Best of both worlds via "hybrid" scheme: Use public key to distribute a new random "session" key b/w sender and recipient, then symmetric crypto for remainder of session

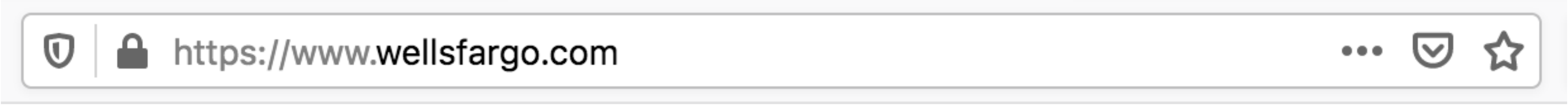
HTTP Security

HTTP-S: Securing HTTP

- HTTP sits on top of secure channel (SSL/TLS)
  - https:// vs. http://
  - TCP port 443 vs. 80
- All (HTTP) bytes encrypted and authenticated
  - No change to HTTP itself!
- Where to get the key???



Learning a Valid Public Key

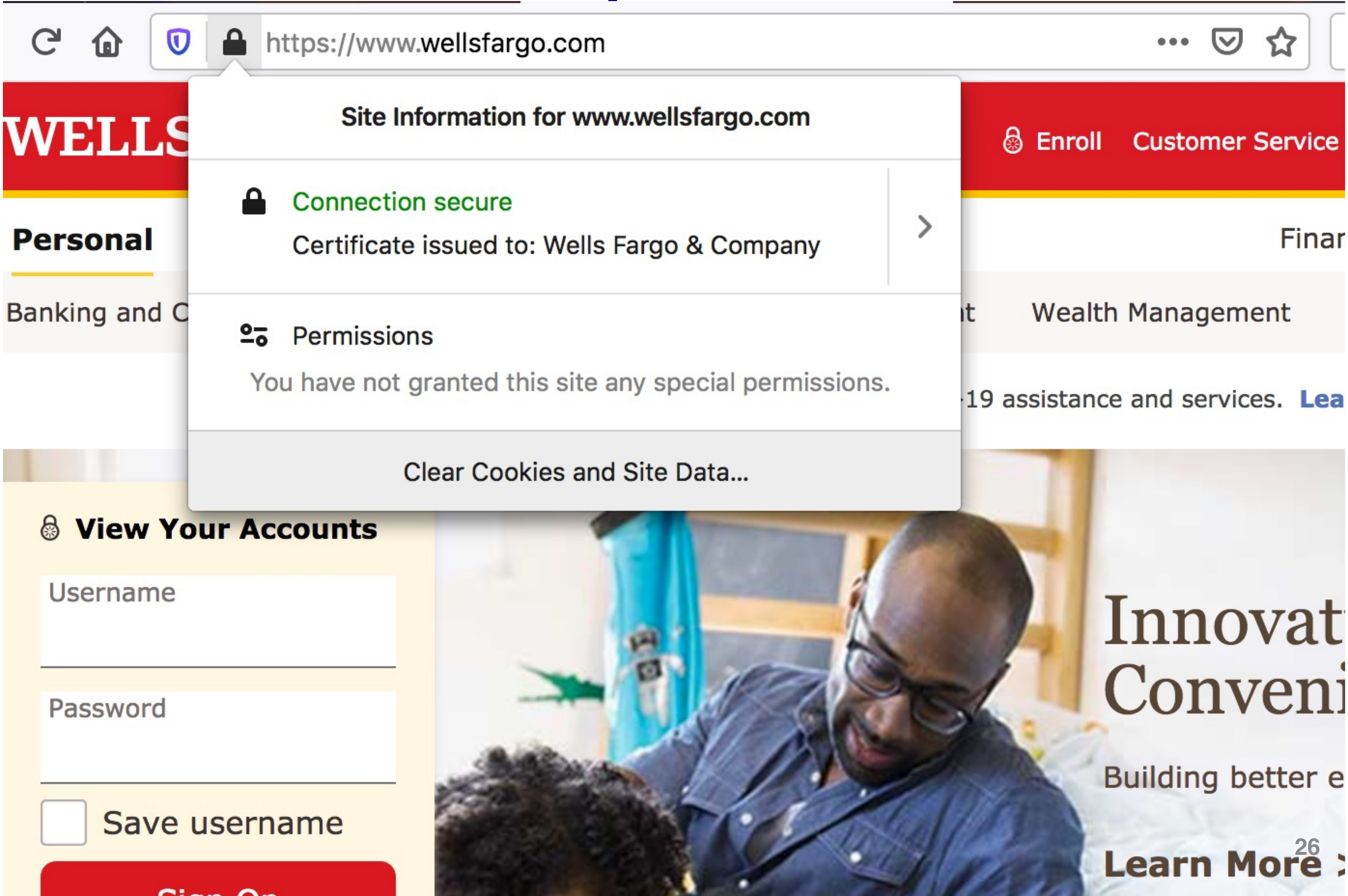

https://www.wellsfargo.com

- What is that lock?
  - Securely binds domain name to public key (PK)
    - If PK is authenticated, then any message signed by that PK cannot be forged by non-authorized party
  - Believable only if you trust the attesting body
    - Bootstrapping problem: Who to trust, and how to tell if this message is actually from them?

Hierarchical Public Key Infrastructure

- Public key certificate
  - Binding between identity and a public key
  - "Identity" is, for example, a domain name
  - Digital signature to ensure integrity
- Certificate authority
  - Issues public key certificates and verifies identities
  - Trusted parties (e.g., VeriSign, GoDaddy, Comodo)
  - Preconfigured certificates in Web browsers

Public Key Certificate



https://www.wellsfargo.com

Site Information for www.wellsfargo.com

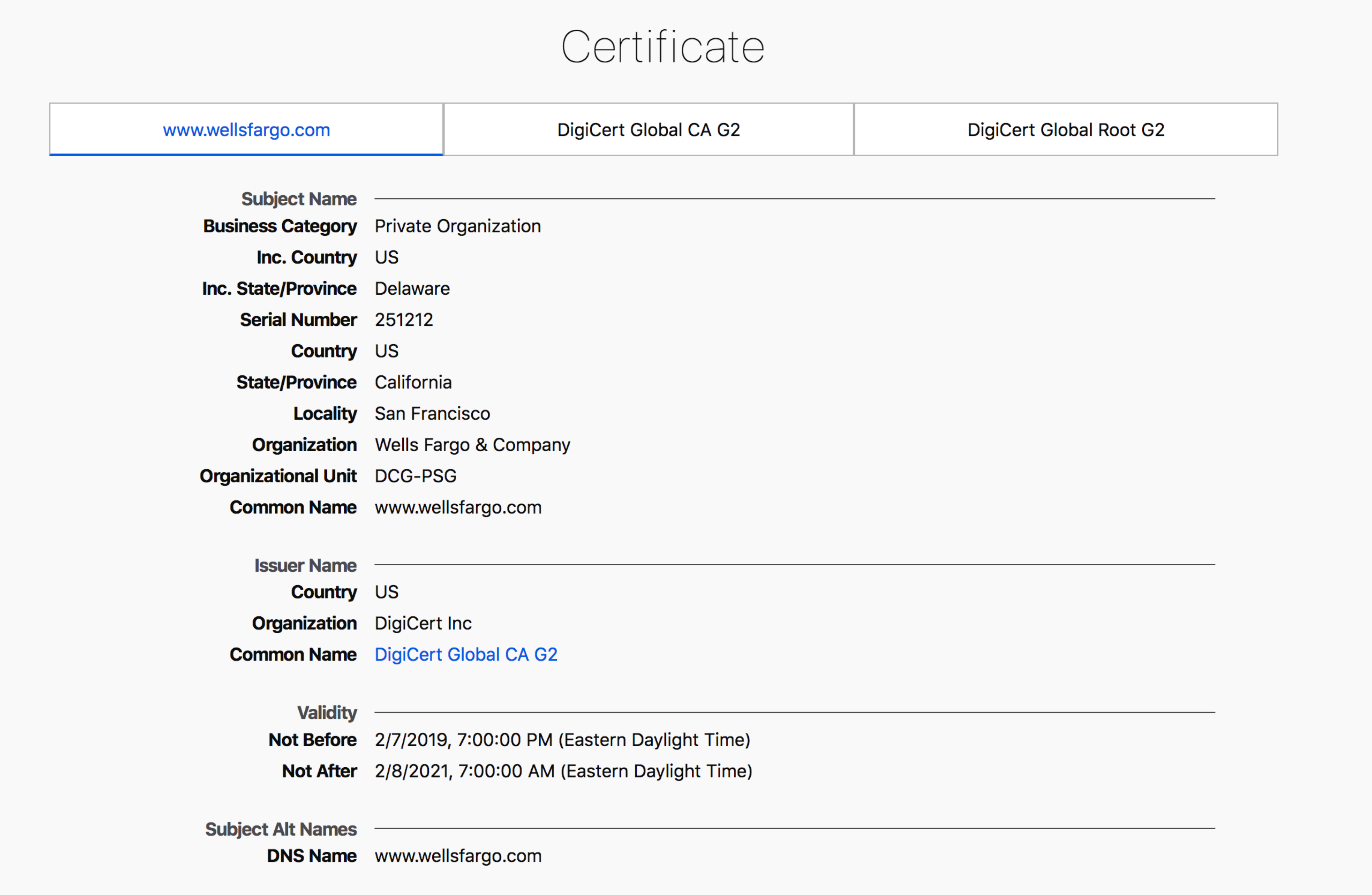
Connection secure

Certificate issued to: Wells Fargo & Company

Permissions

You have not granted this site any special permissions.

Clear Cookies and Site Data...



Certificate

Subject Name

Business Category	Private Organization
Inc. Country	US
Inc. State/Province	Delaware
Serial Number	251212
Country	US
State/Province	California
Locality	San Francisco
Organization	Wells Fargo & Company
Organizational Unit	DCG-PSG
Common Name	www.wellsfargo.com

Issuer Name

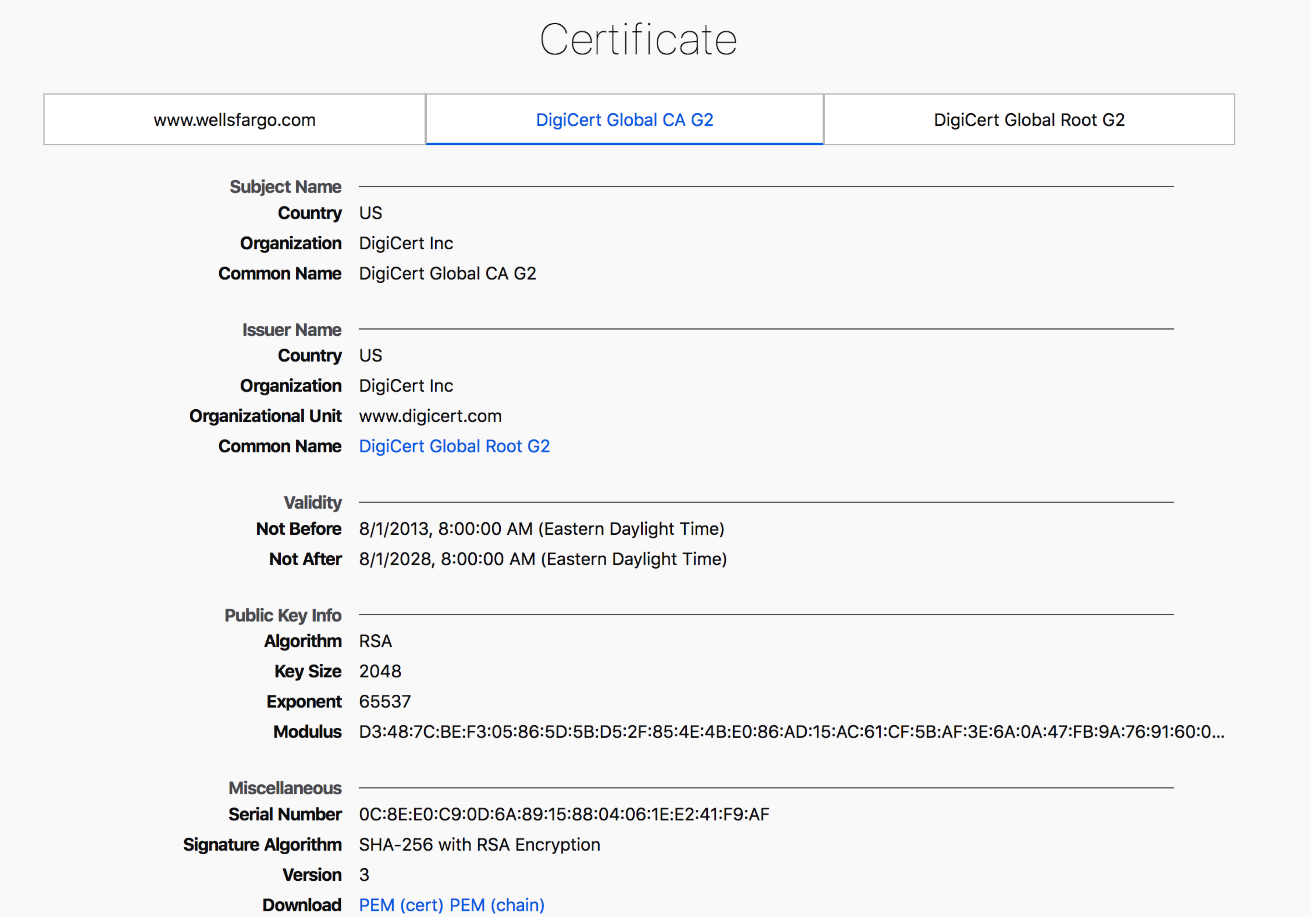
Country	US
Organization	DigiCert Inc
Common Name	DigiCert Global CA G2

Validity

Not Before	2/7/2019, 7:00:00 PM (Eastern Daylight Time)
Not After	2/8/2021, 7:00:00 AM (Eastern Daylight Time)

Subject Alt Names

DNS Name	www.wellsfargo.com



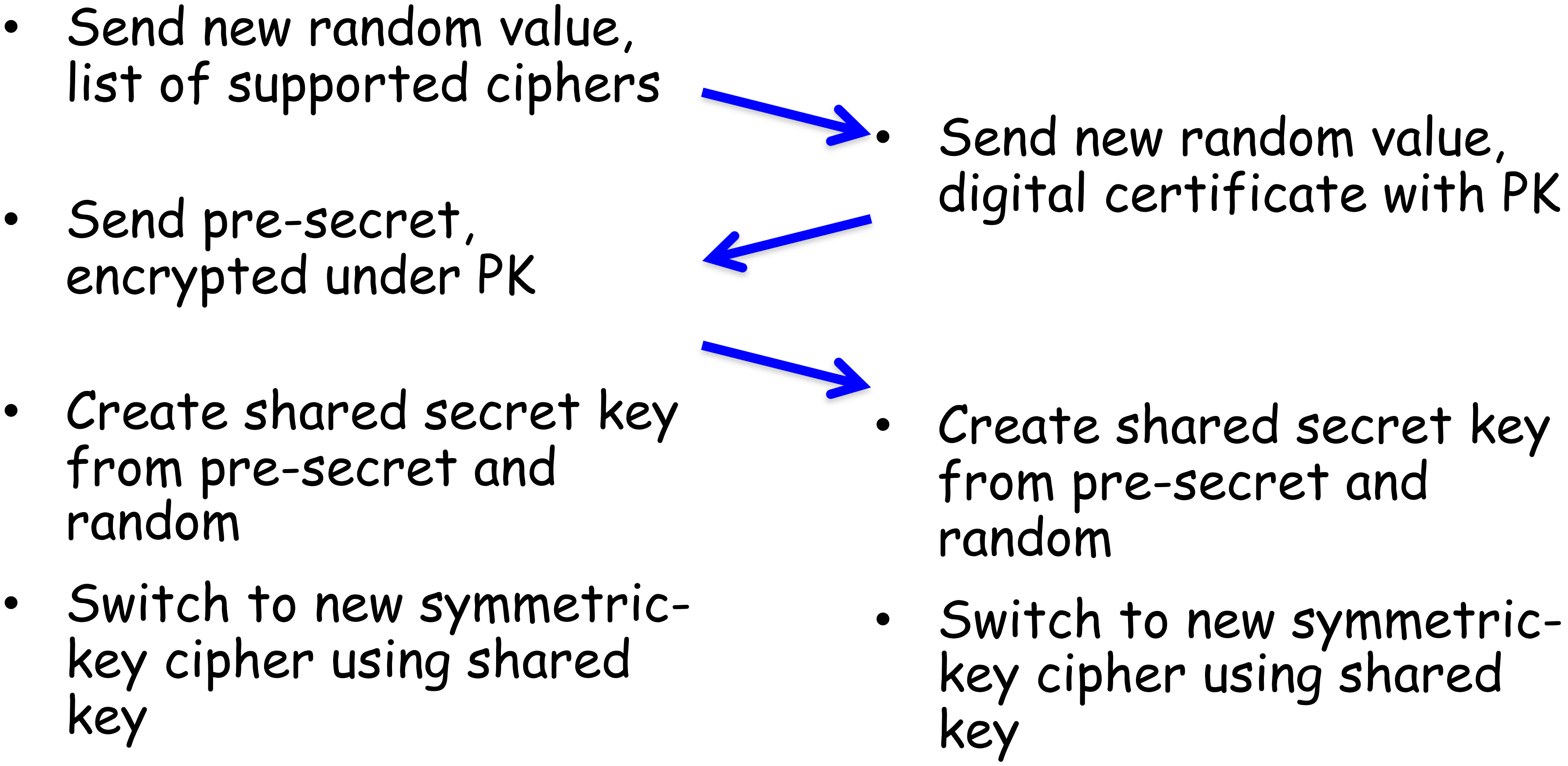
Certificate

Subject Name	
Country	US
Organization	DigiCert Inc
Common Name	DigiCert Global CA G2
Issuer Name	
Country	US
Organization	DigiCert Inc
Organizational Unit	www.digicert.com
Common Name	DigiCert Global Root G2
Validity	
Not Before	8/1/2013, 8:00:00 AM (Eastern Daylight Time)
Not After	8/1/2028, 8:00:00 AM (Eastern Daylight Time)
Public Key Info	
Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	D3:48:7C:BE:F3:05:86:5D:5B:D5:2F:85:4E:4B:E0:86:AD:15:AC:61:CF:5B:AF:3E:6A:0A:47:FB:9A:76:91:60:0...
Miscellaneous	
Serial Number	0C:8E:E0:C9:0D:6A:89:15:88:04:06:1E:E2:41:F9:AF
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)

Transport Layer Security (TLS)

Based on the earlier Secure Socket Layer (SSL) originally developed by Netscape

TLS Handshake Protocol



- Send new random value, list of supported ciphers
- Send new random value, digital certificate with PK
- Send pre-secret, encrypted under PK
- Create shared secret key from pre-secret and random
- Switch to new symmetric-key cipher using shared key
- Create shared secret key from pre-secret and random
- Switch to new symmetric-key cipher using shared key

Comments on HTTPS

- HTTPS authenticates server, not content
  - If CDN (Akamai) serves content over HTTPS, customer must trust Akamai not to change content
- Symmetric-key crypto after public-key ops
  - Handshake protocol using public key crypto
  - Symmetric-key crypto much faster (100-1000x)
- HTTPS on top of TCP, so reliable byte stream
  - Can leverage fact that transmission is reliable to ensure: each data segment received exactly once
  - Adversary can't successfully drop or replay packets

IP Security

IP Security

- There are range of app-specific security mechanisms
  - eg. TLS/HTTPS, S/MIME, PGP, Kerberos, …
- But security concerns that cut across protocol layers
- Implement by the network for all applications?

Enter IPSec!

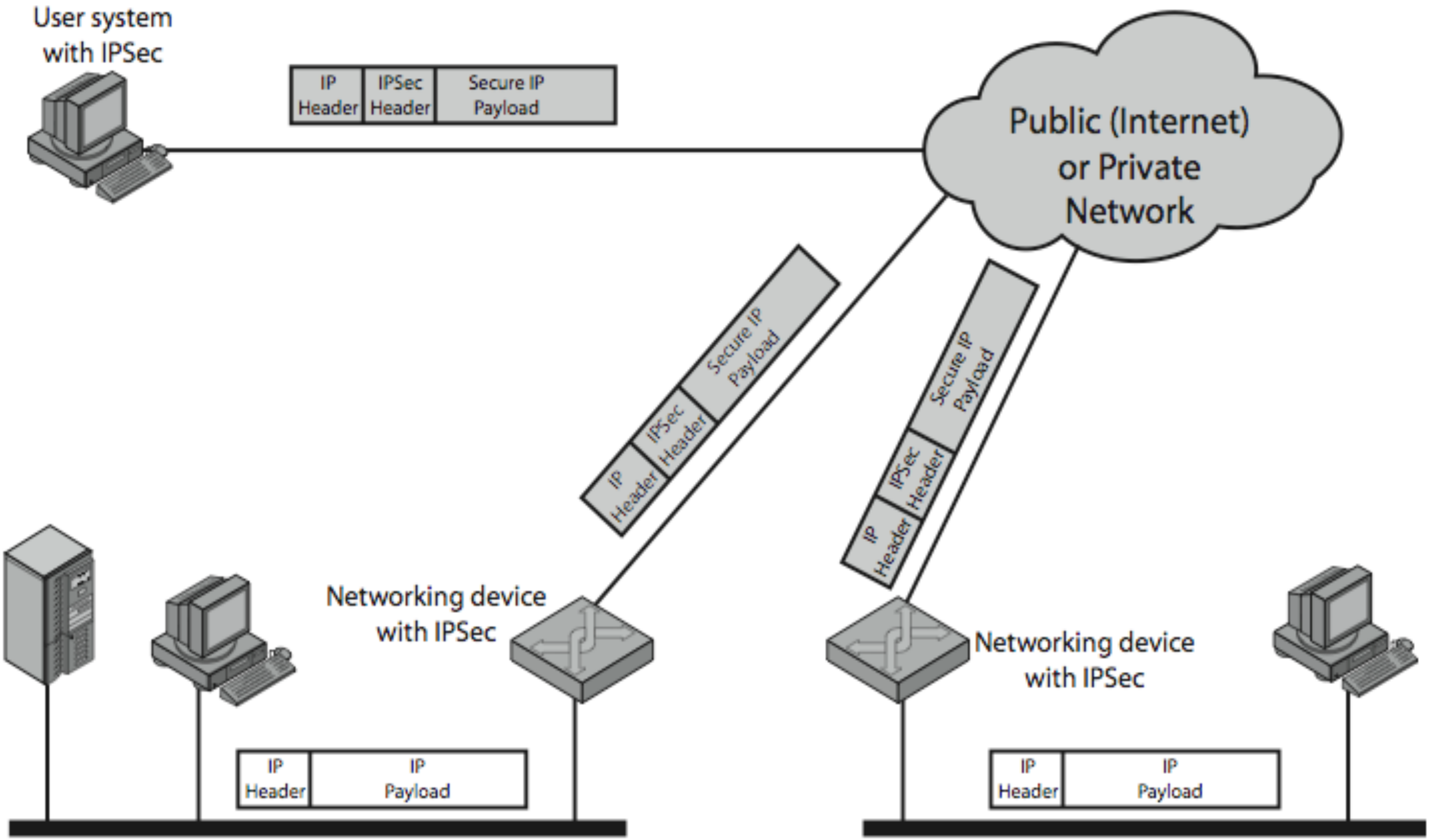
IPSec

- General IP Security framework

- Allows one to provide
  - Access control, integrity, authentication, originality, and confidentiality

- Applicable to different settings
  - Narrow streams: Specific TCP connections
  - Wide streams: All packets between two gateways

IPSec Uses



User system with IPSec
IP Header
IPSec Header
Secure IP Payload
Public (Internet) or Private Network
IP Header
IPSec Header
Secure IP Payload
IP Header
IPSec Header
Secure IP Payload
Networking device with IPSec
Networking device with IPSec
IP Header
IP Payload
IP Header
IP Payload

Benefits of IPSec

- If in a firewall/router:
  - Strong security to all traffic crossing perimeter
  - Resistant to bypass
- Below transport layer
  - Transparent to applications
  - Can be transparent to end users
- Can provide security for individual users

Conclusions: Security

- Security at many layers
  - Application, transport, and network layers
  - Customized to the properties and requirements
- Exchanging keys
  - Public key certificates
  - Certificate authorities vs. Web of trust

Coming Up

- Precept this week- more SDN

- Next week: Data center networks