CSCI 331: Introduction to Computer Security

Lecture 21: How to give a **good** talk / Networks

Instructor: Dan Barowy

Williams

Announcements

CS Holiday Party

Friday, Dec 8 @ 2:35pm
CS Common Room

Join the CS faculty and your peers for an end-of-semester celebration. We will have hot cocoa and treats for you to enjoy. Last gathering of the year!

Your to-dos

1. Final project, **due Sunday, Dec 10 at 10pm.**
2. Optional book report, now due **Sunday, Dec 17**.
3. Resubmissions due **Sunday, Dec 17**.
4. If you want to talk about your project (or anything else), I have office hours:
   - **Thursday**, from 4-5:30pm
   - **Friday**, from 12:30-1:30pm
   - and I can be available during our Tuesday lab period by request.

Topics

Giving a good talk

IP networking primer

Course evaluations

How to give a good talk

Five tips

One: Have a story

Two: Don’t “bury the lede”

THE EXCITING PARTS
“We forgot to tell everyone.”
2023-2023

Three: Don’t make your audience read

Four: Use examples

Five: Stay on script

Six (oops!): Finish on time

Sample talk

Your Presentation

Your final presentation should be **no more than 10 minutes in length**, and it should have no more than 5-10 slides. It should

1. describe the history and significance of your attack,
2. how it works,
3. should include a short demo (if possible),
4. and conclude by briefly discussing defenses against such an attack (or the converse if your project is about a defense)

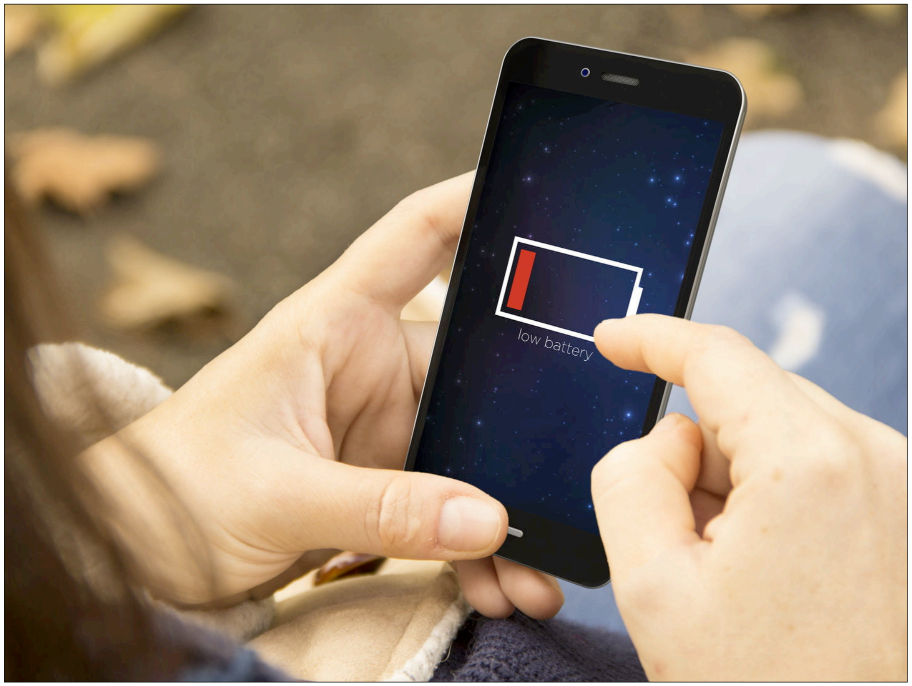
Remember, you only have 10 minutes to give your talk, so please keep it high-level and concise. Think of your talk as an advertisement for your paper. **Practice your talk**, and remember, we can read your paper if we want to know more.

Juice Jacking

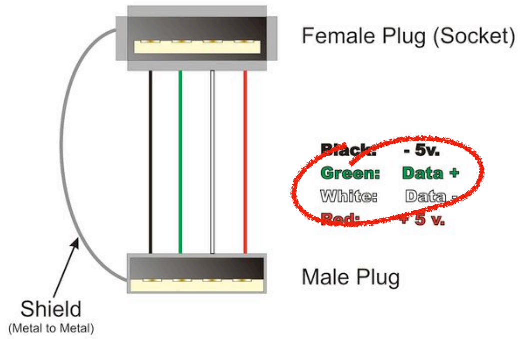
The hidden dangers of a USB charging jack.

"Don't use that juice!"

Dan Barowy



USB Type A Connectors



Black:	- 5v.
Green:	Data +
White:	Data -
Red:	+ 5 v.

USB charge rates advertised over data wires.

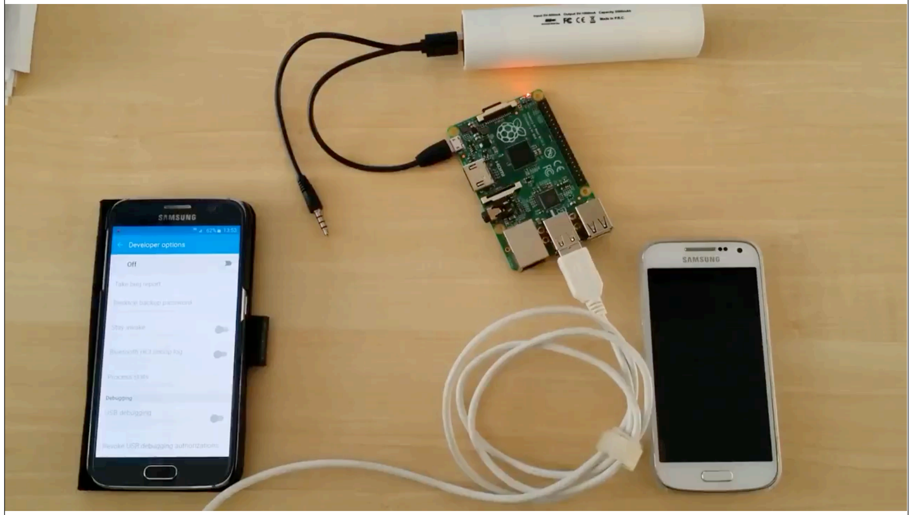
“juice jacking”

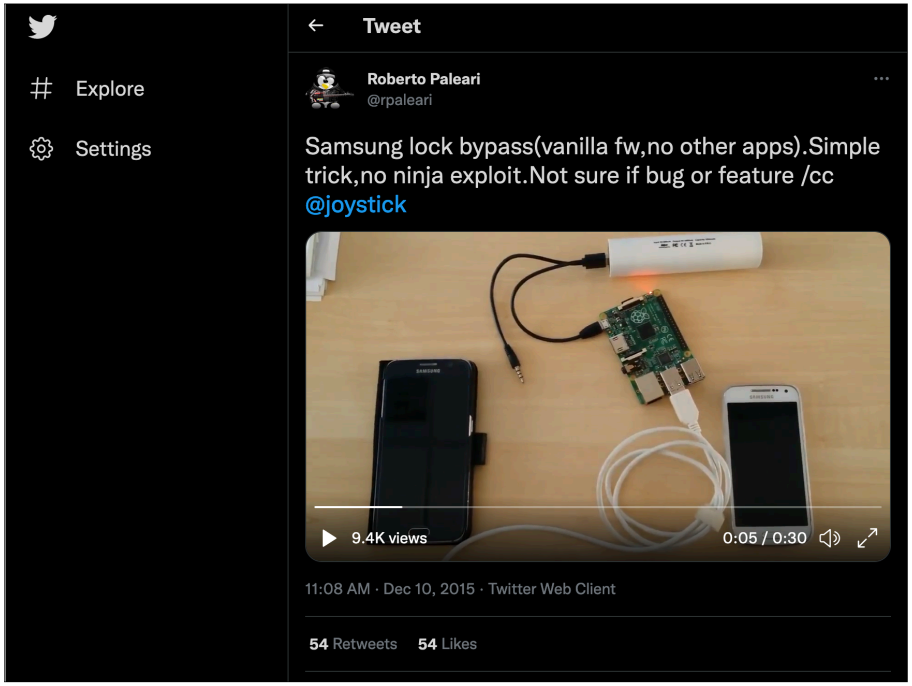
DEFCON 2011, “Wall of Sheep”
(Brian Markus, Joseph Mlodzianowski, and Robert Rowley)

YOU SHOULD NOT TRUST PUBLIC KIOSKS WITH YOUR SMART PHONE.

INFORMATION CAN BE RETRIEVED OR DOWNLOADED WITHOUT YOUR CONSENT. LUCKILY FOR YOU, THIS STATION HAS TAKEN THE ETHICAL ROUTE AND YOUR DATA IS SAFE. ENJOY THE FREE CHARGE!

2011, “Wall of Sheep”
Mlodzianowski, and Robert Rowley)



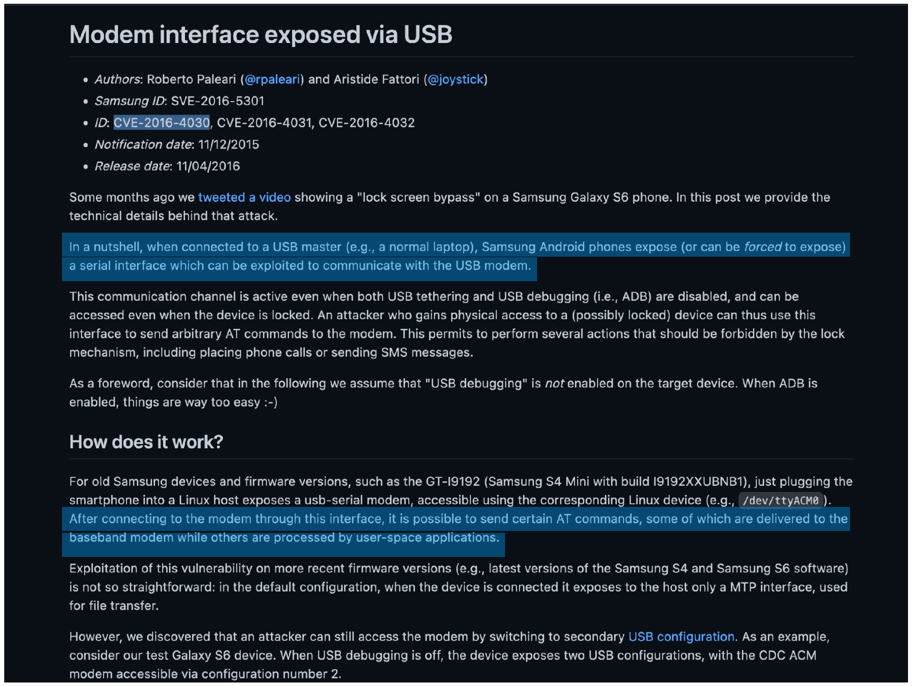


Roberto Paleari
@rpaleari

Samsung lock bypass(vanilla fw,no other apps).Simple trick,no ninja exploit.Not sure if bug or feature /cc @joystick

11:08 AM · Dec 10, 2015 · Twitter Web Client

54 Retweets 54 Likes



Modem interface exposed via USB

- *Authors*: Roberto Paleari (@rpaleari) and Aristide Fattori (@joystick)
- *Samsung ID*: SVE-2016-5301
- *ID*: CVE-2016-4030, CVE-2016-4031, CVE-2016-4032
- *Notification date*: 11/12/2015
- *Release date*: 11/04/2016

Some months ago we tweeted a video showing a "lock screen bypass" on a Samsung Galaxy S6 phone. In this post we provide the technical details behind that attack.

In a nutshell, when connected to a USB master (e.g., a normal laptop), Samsung Android phones expose (or can be *forced* to expose) a serial interface which can be exploited to communicate with the USB modem.

This communication channel is active even when both USB tethering and USB debugging (i.e., ADB) are disabled, and can be accessed even when the device is locked. An attacker who gains physical access to a (possibly locked) device can thus use this interface to send arbitrary AT commands to the modem. This permits to perform several actions that should be forbidden by the lock mechanism, including placing phone calls or sending SMS messages.

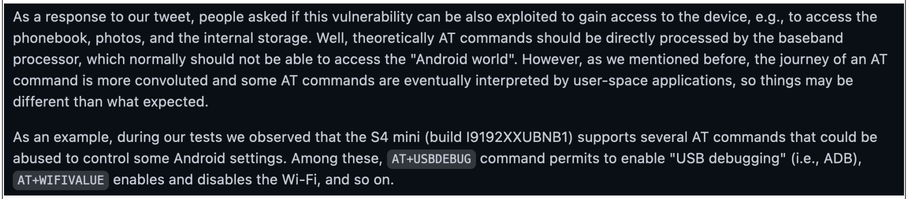
As a foreword, consider that in the following we assume that "USB debugging" is *not* enabled on the target device. When ADB is enabled, things are way too easy :-)

How does it work?

For old Samsung devices and firmware versions, such as the GT-I9192 (Samsung S4 Mini with build I9192XXUBNB1), just plugging the smartphone into a Linux host exposes a usb-serial modem, accessible using the corresponding Linux device (e.g., `/dev/ttyACM0`). After connecting to the modem through this interface, it is possible to send certain AT commands, some of which are delivered to the baseband modem while others are processed by user-space applications.

Exploitation of this vulnerability on more recent firmware versions (e.g., latest versions of the Samsung S4 and Samsung S6 software) is not so straightforward: in the default configuration, when the device is connected it exposes to the host only a MTP interface, used for file transfer.

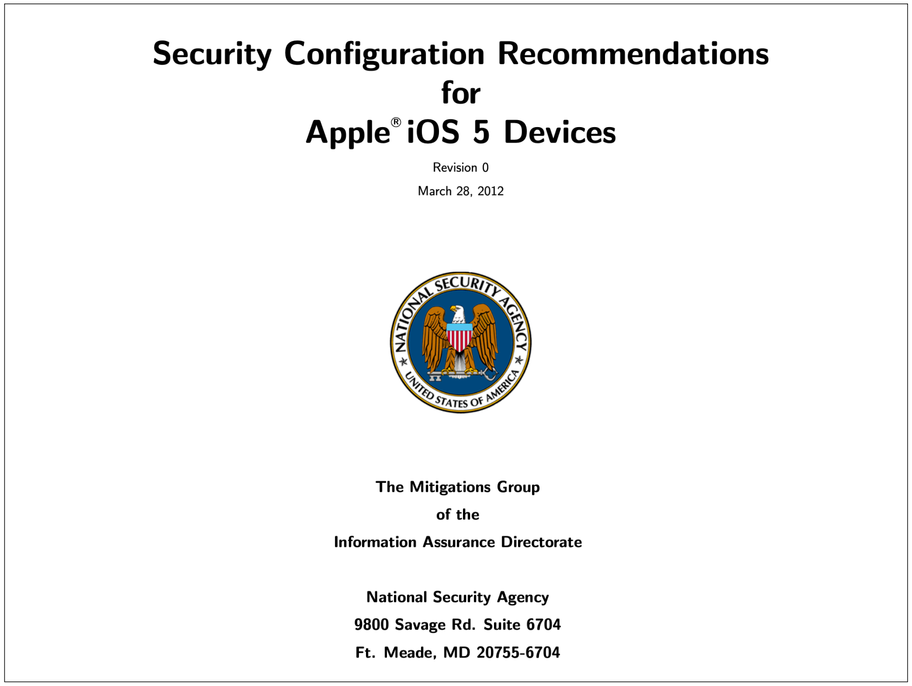
However, we discovered that an attacker can still access the modem by switching to secondary USB configuration. As an example, consider our test Galaxy S6 device. When USB debugging is off, the device exposes two USB configurations, with the CDC ACM modem accessible via configuration number 2.



As a response to our tweet, people asked if this vulnerability can be also exploited to gain access to the device, e.g., to access the phonebook, photos, and the internal storage. Well, theoretically AT commands should be directly processed by the baseband processor, which normally should not be able to access the "Android world". However, as we mentioned before, the journey of an AT command is more convoluted and some AT commands are eventually interpreted by user-space applications, so things may be different than what expected.

As an example, during our tests we observed that the S4 mini (build I9192XXUBNB1) supports several AT commands that could be abused to control some Android settings. Among these, `AT+USBDEBUG` command permits to enable "USB debugging" (i.e., ADB), `AT+WIFIVALUE` enables and disables the Wi-Fi, and so on.

USB debugging = pwned



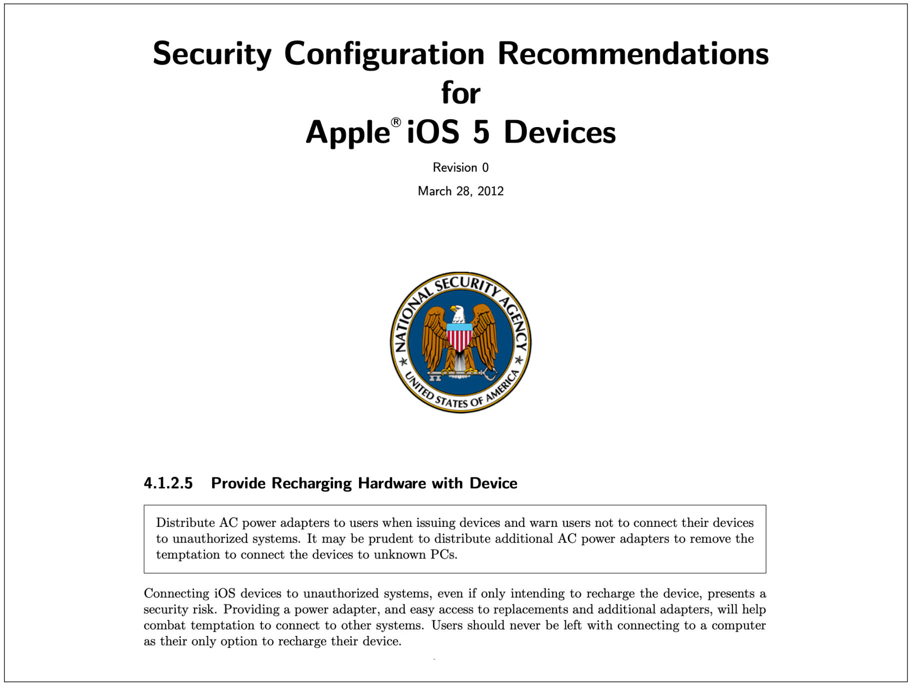
Security Configuration Recommendations for Apple® iOS 5 Devices

Revision 0

March 28, 2012

The Mitigations Group
of the
Information Assurance Directorate

National Security Agency
9800 Savage Rd. Suite 6704
Ft. Meade, MD 20755-6704



Security Configuration Recommendations for Apple® iOS 5 Devices

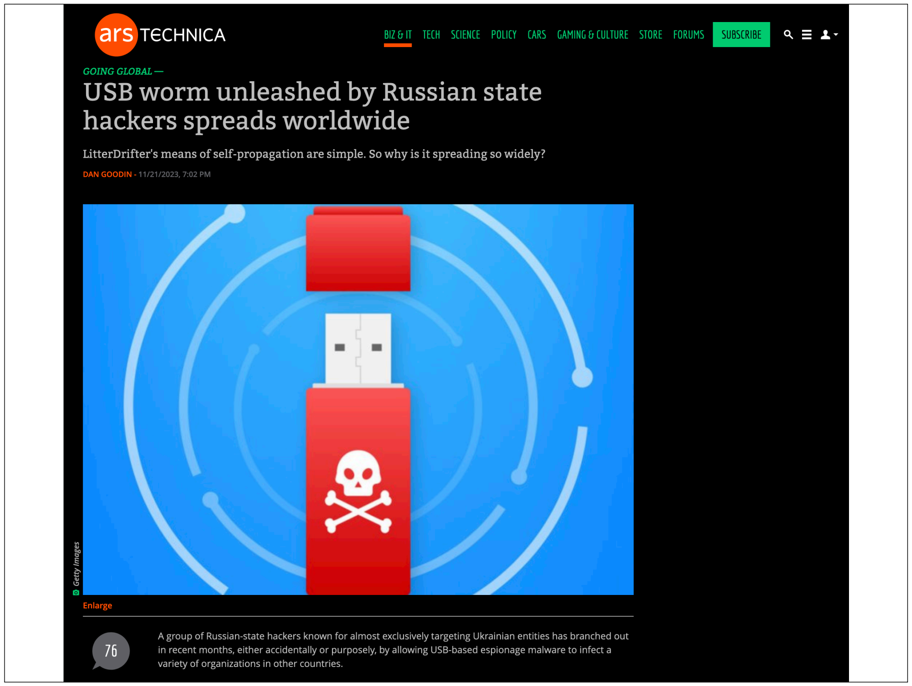
Revision 0

March 28, 2012

4.1.2.5 Provide Recharging Hardware with Device

> Distribute AC power adapters to users when issuing devices and warn users not to connect their devices to unauthorized systems. It may be prudent to distribute additional AC power adapters to remove the temptation to connect the devices to unknown PCs.

Connecting iOS devices to unauthorized systems, even if only intending to recharge the device, presents a security risk. Providing a power adapter, and easy access to replacements and additional adapters, will help combat temptation to connect to other systems. Users should never be left with connecting to a computer as their only option to recharge their device.



GOING GLOBAL —

USB worm unleashed by Russian state hackers spreads worldwide

LitterDrifter's means of self-propagation are simple. So why is it spreading so widely?

DAN GOODIN - 11/21/2023, 7:02 PM

A group of Russian-state hackers known for almost exclusively targeting Ukrainian entities has branched out in recent months, either accidentally or purposely, by allowing USB-based espionage malware to infect a variety of organizations in other countries.

GOING GLOBAL —

USB worm unleashed by Ru
hackers spreads worldwide

LitterDrifter's means of self-propagation are simple. So why

DAN GOODIN - 11/21/2023, 7:02 PM

Mitigations

Juice Jacking

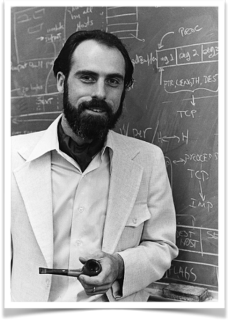
Thanks!

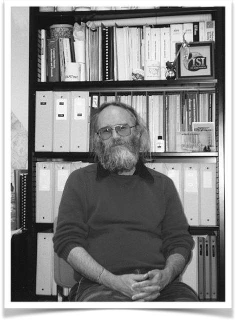
Dan Barowy

Williams

IP networking

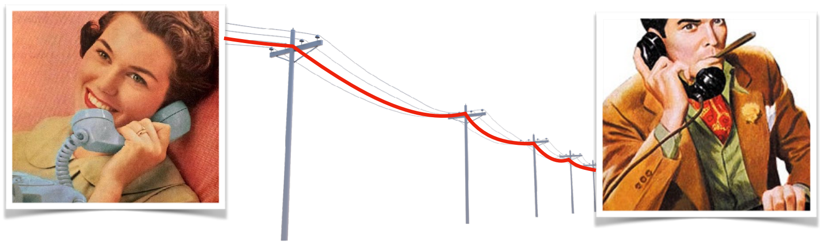
IP networking





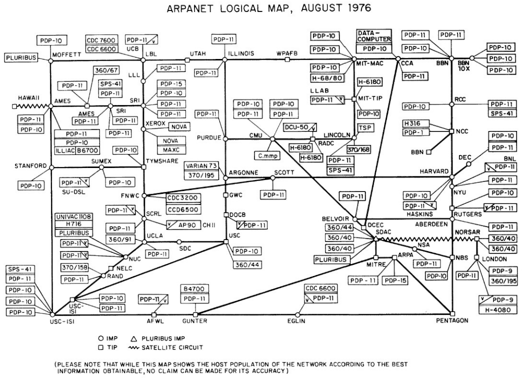
- Invented in 1974 by Vint Cerf (Stanford), Bob Kahn (BBN), and Jon Postel (UCLA).
- **IP** (Internet Protocol) was a **radical** departure from existing networking, inspired by the experimental CYCLADES network.
- IP was built on a **connectionless** **packet-switched** architecture instead of a **connection-oriented** architecture like **telephony**.

Connection-oriented communication



- Tech. behind **original telephone network** ("POTS": 1876-1988).
- During a call, a **physical circuit** is closed between two endpoints.
- The line is "**reserved**" for those two callers.
- Anyone else wanting to make a call needs to **reserve another line** or **wait**.
- Highly reliable; **less than 5 minutes outage per year** ("five nines").
- Relatively **simple** technology.
- **Major drawback**: adding capacity is very expensive. You need to add physical wires!

The ARPANet



- **Predecessor** to the modern Internet.
- Largely built by **BBN** and funded by **DARPA** in the 1960's.
- Problem: building network using connection-oriented architecture was **too expensive**.
- Decided to **go connectionless**.

Connectionless communication

- Uses a technique called "**packet switching**."
- Messages are **broken into little pieces** ("packets" or "datagrams")
- Network reserves resources **just long enough** to send one piece.
- It is the **sender's/receiver's responsibility to ensure data is delivered reliably**, not the network's.
- Instead of reliability guarantees, network ensures "**best effort**."
- Makes **better utilization** of shared resources.
- Many messages can then be **multiplexed** onto the network.
- Key takeaway: **don't need more wires**!

Pooled vs Static Buffers

- From Denning, Peter. "A Statistical Model for Console Behavior in Multiuser Computers" CACM, Vol.11, No.9 p. 605, Sept 1968.
- For 50 users and a ratio of characters/interrupt = 10.

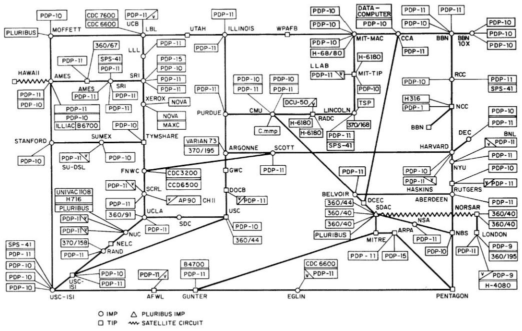
Total Buffer Size	**Probability of Overflow**	
(in bytes)	**Pooled**	**Static**
750	.006	.90
1000	10^{-6}	.76
1500		.44
2000		.22
2500		.10
3000		.05
3500		.02
4000		.01
4500		.004

- This result is completely general for static vs pooled resources. It is really a no-brainer.
  - Values for the blanks in the pooled column were too small to represent on the computer Denning used.

(slide courtesy of Prof. John Day at Boston U.)

Connectionless communication

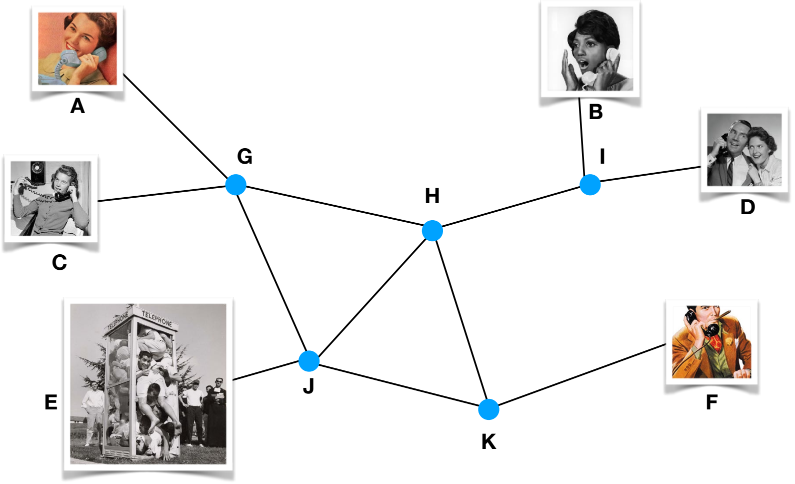
ARPANET LOGICAL MAP, AUGUST 1976



(PLEASE NOTE THAT WHILE THIS MAP SHOWS THE HOST POPULATION OF THE NETWORK ACCORDING TO THE BEST INFORMATION OBTAINABLE, NO CLAIM CAN BE MADE FOR ITS ACCURACY)

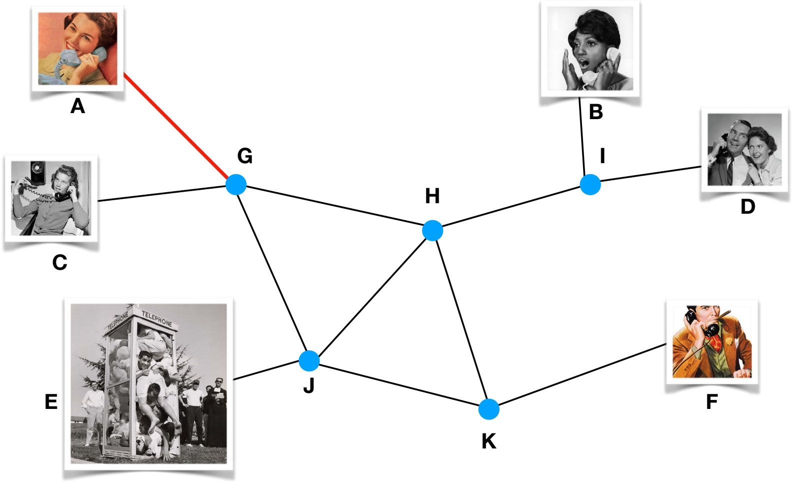
- Major downside: **pushed complexity** onto sender/receiver.
- The ARPANet was **an experiment** to figure out how to do this.
- More importantly, how to do it **reliably**.
- Cert, Kahn, and Postel's Internet Protocol **addressed reliability problems** and was **quickly adopted** for use on the ARPANet.

How IP works



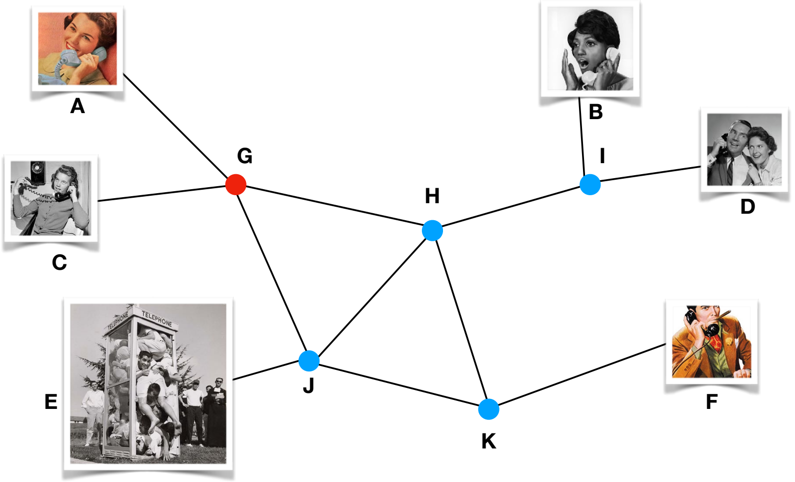
- **A** wants to send data to **F**.

How IP works

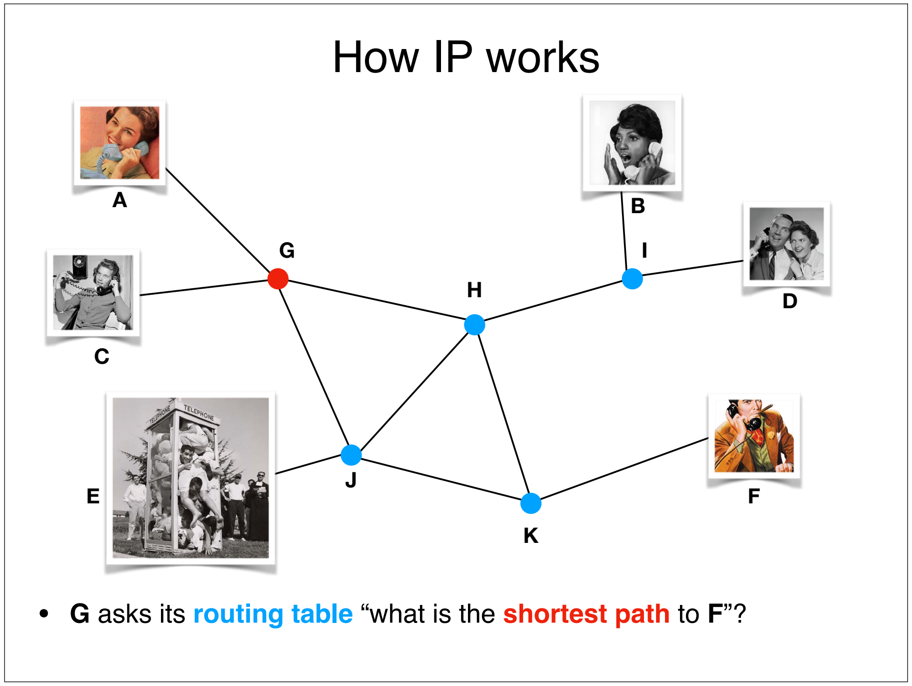


- **A makes a connection** and sends its packet(s) to its **gateway**, the **router**, **G**.

How IP works

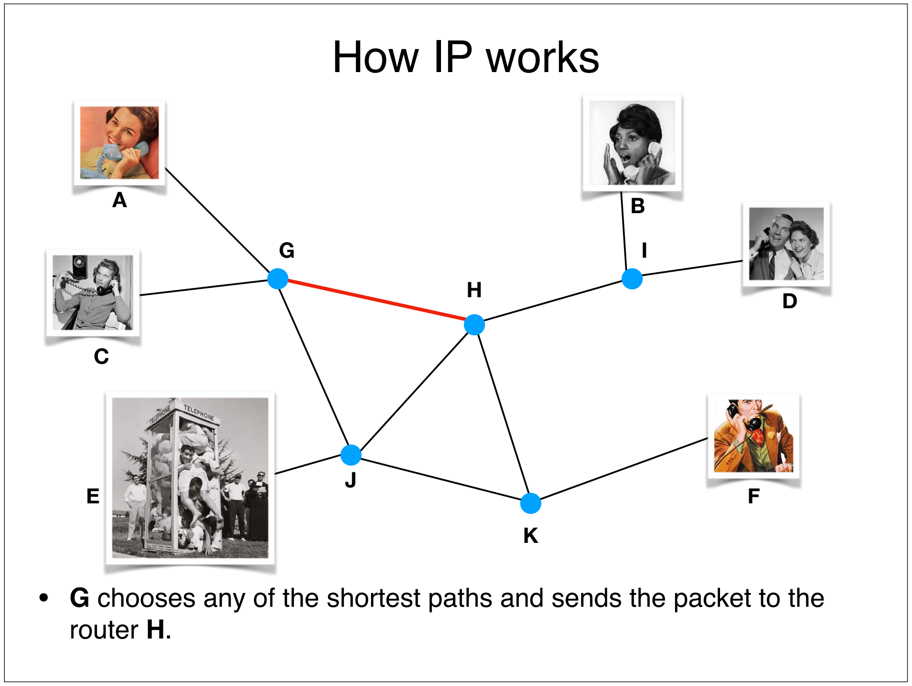


- **G** stores the packet and closes the connection to **A**.



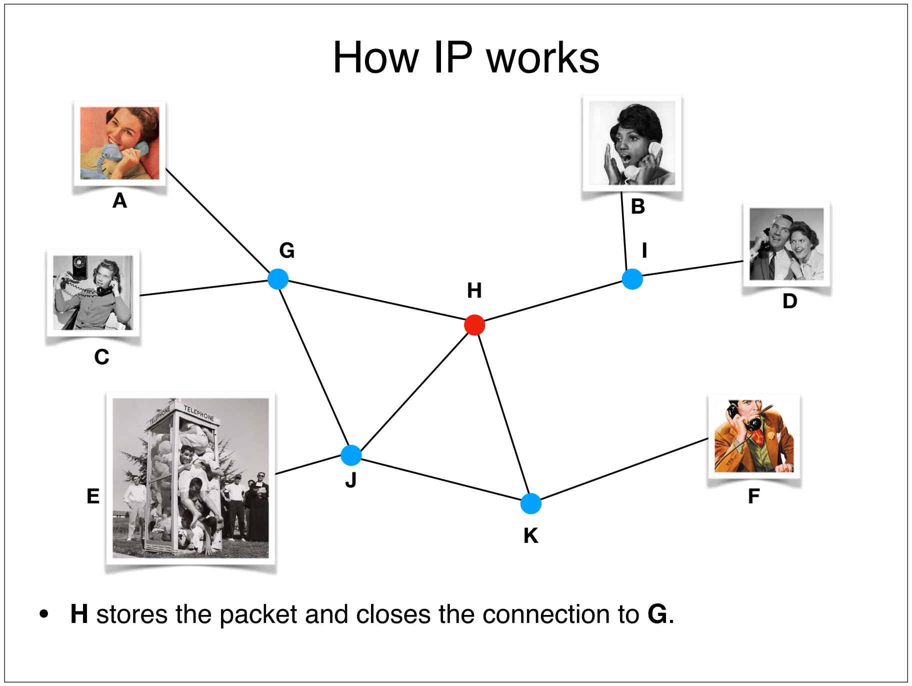
How IP works

- **G** asks its routing table “what is the shortest path to **F**”?



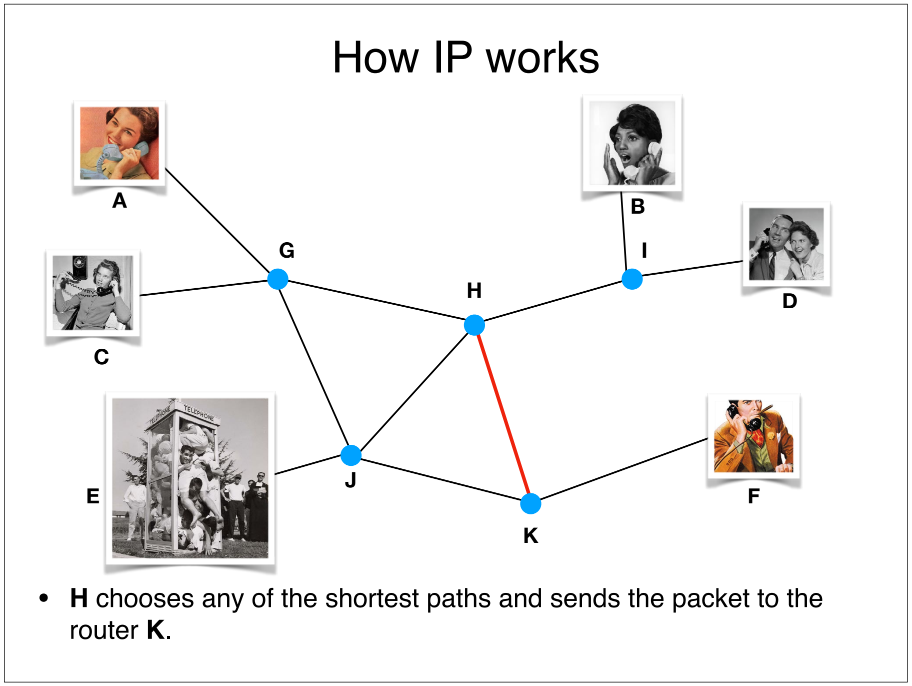
How IP works

- **G** chooses any of the shortest paths and sends the packet to the router **H**.



How IP works

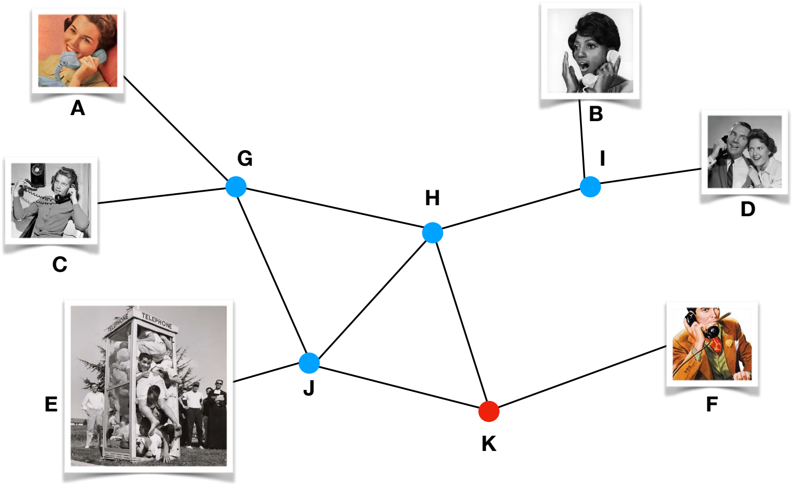
- **H** stores the packet and closes the connection to **G**.



How IP works

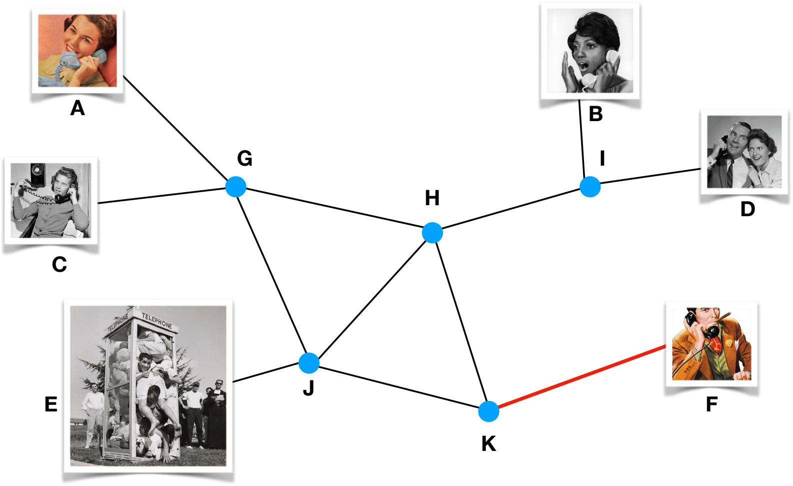
- **H** chooses any of the shortest paths and sends the packet to the router **K**.

How IP works



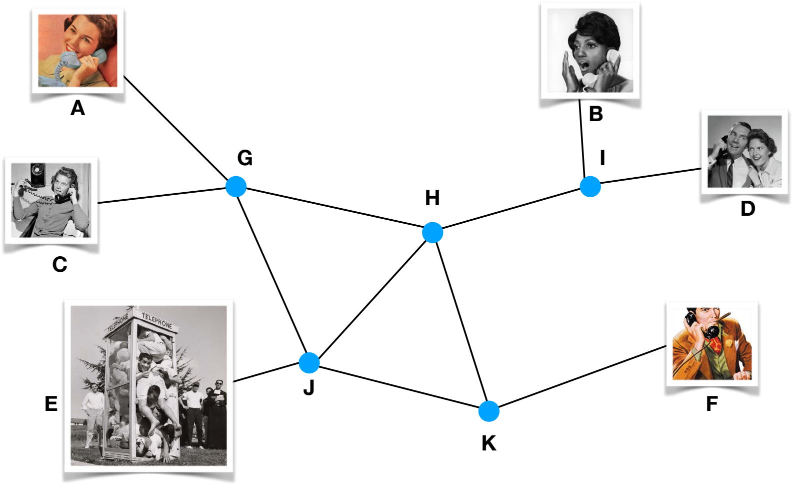
- **K** stores the packet and closes the connection to **H**.

How IP works



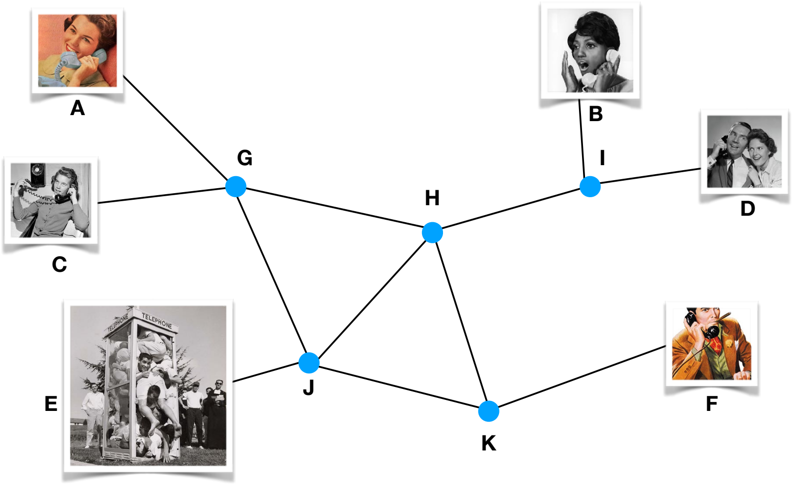
- **J** chooses any of the shortest paths and sends the packet to the receiver **F**.

How IP works

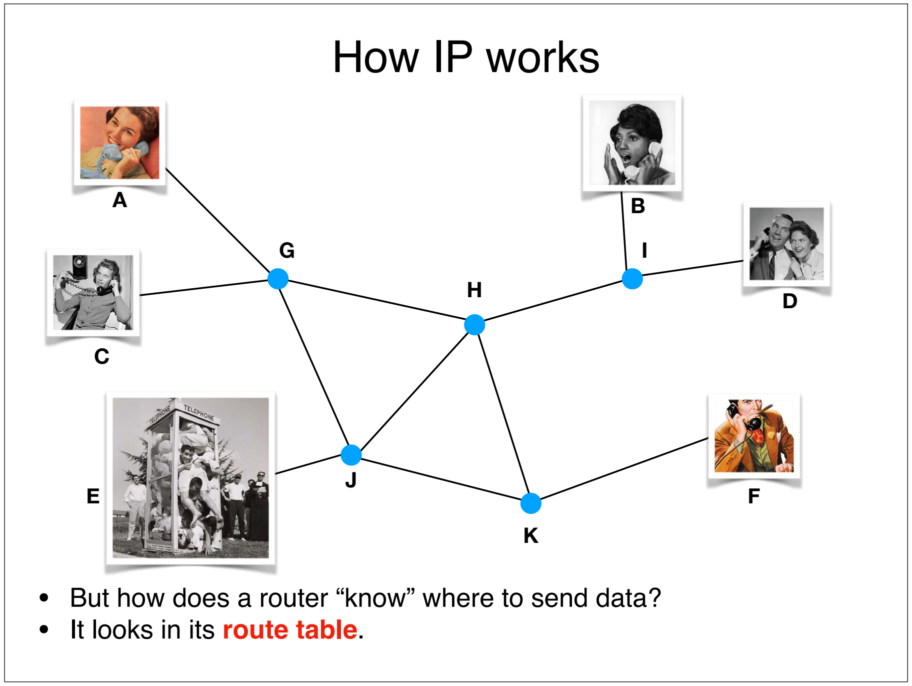


- **F** stores the packet and closes the connection to **K**.

How IP works

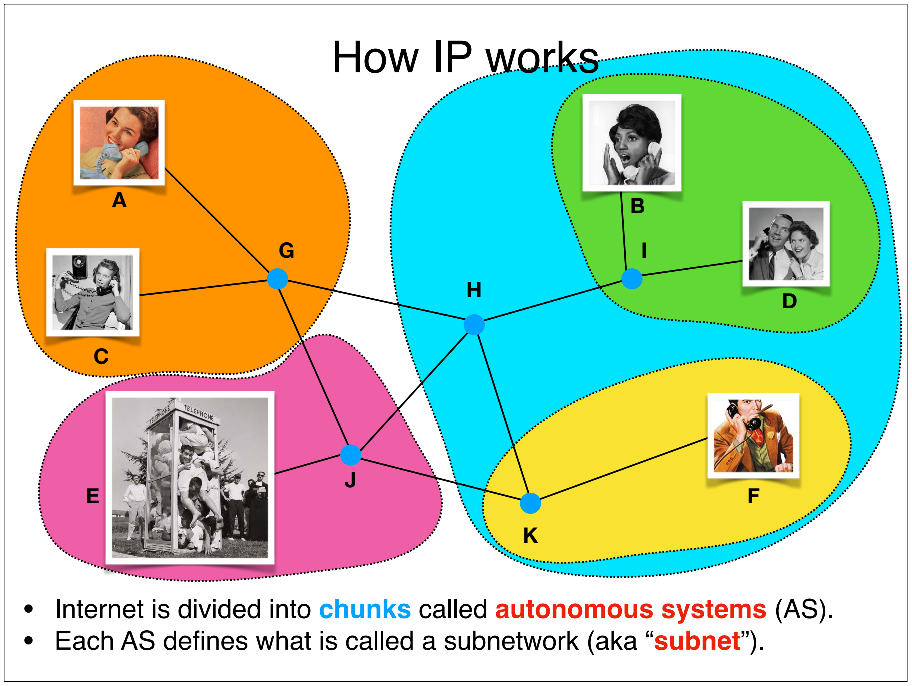


- Notice that at any point, only a small fraction of network resources are used.



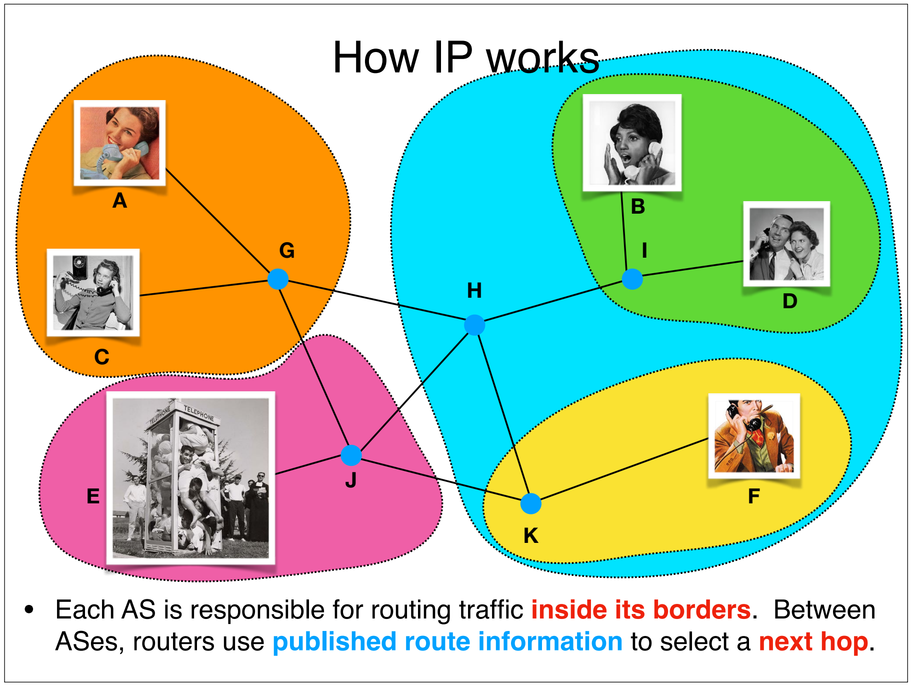
How IP works

- But how does a router “know” where to send data?
- It looks in its **route table**.



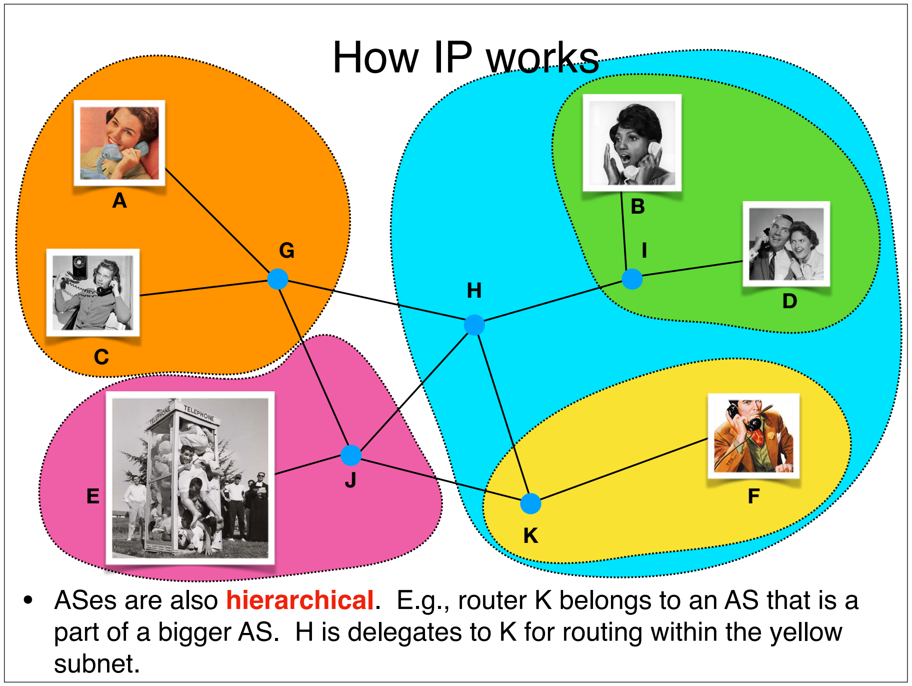
How IP works

- Internet is divided into **chunks** called **autonomous systems** (AS).
- Each AS defines what is called a subnetwork (aka “**subnet**”).



How IP works

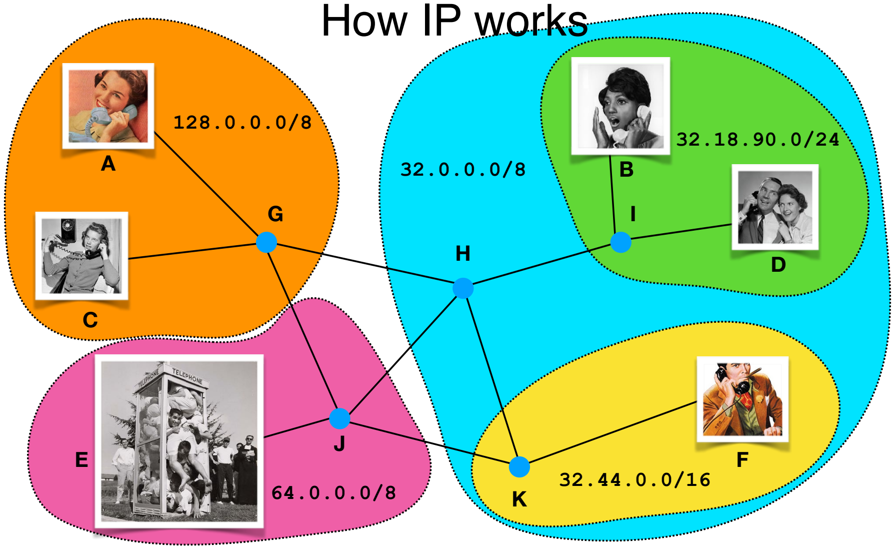
- Each AS is responsible for routing traffic **inside its borders**. Between ASes, routers use **published route information** to select a **next hop**.



How IP works

- ASes are also **hierarchical**. E.g., router K belongs to an AS that is a part of a bigger AS. H is delegates to K for routing within the yellow subnet.

How IP works



- Subnets are defined by contiguous blocks of addresses.

IPv4 address

It's like a **mailing address** for the **Earth**.

32.45.8.12

Each byte ("octet") is between 0 and 255 (0 to $2^8 - 1$).

This is actually just a 32-bit number split into 4 pieces.

```
0|0|1|0|0|0|0|0|0|0|1|0|1|1|0|1|0|0|0|0|1|0|0|0|0|0|0|0|1|1|0|0
      32              45              8               12
```

CIDR

Classless Interdomain Routing ("cider")

$$\underbrace{32.0.0.0}_{\text{address prefix}}/\underbrace{8}_{\text{subnet mask}}$$

```
addr 0|0|1|0|0|0|0|0|0|0|1|0|1|1|0|1|0|0|0|0|1|0|0|0|0|0|0|0|1|1|0|0
mask ■■■■■■■■□□□□□□□□□□□□□□□□□□□□□□□□
```

- The subnet mask says which part of the address is fixed, and which part is variable.
- An AS is responsible for routing the variable part.
- In this example, any router knows that the AS for 32.0.0.0/8 is responsible for routing any packet with an address starting with 32.

Recap & Next Class

Today we learned:

How to give a good talk

IP networking

Next class:

A little more IP networking

Retrospective

What I do

Evaluation Forms

(all of these are anonymous)

We care a lot about what you say in these forms. Please **take your time** and **write thoughtful responses**.

I changed parts of the course this semester **based on prior feedback**.

Your feedback is **valuable to me.** It will help me decide whether these changes were **good** or **bad**.

Purpose of Blue Sheets

Student comments on the blue sheets […] are solely for your benefit. They are not made available to department or program chairs, the Dean of the Faculty, or the CAP for evaluation purposes.

—Office of the Provost, Williams College

Purpose of SCS Forms

“[T]he SCS provides instructors with feedback regarding their courses and teaching. The faculty legislation governing the SCS provides that SCS results are made available to the appropriate department chair, the Dean of the Faculty, and at appropriate times, to members of the Committee on Appointments and Promotions (CAP). The results are considered in matters of faculty reappointment, tenure, and promotion.”

—Office of the Provost, Williams College

“Blue Sheet” Prompts

* What course topic did you **enjoy** the most?

* Are there course topics that you **did not like**? If so, was the issue with **presentation** or **importance**?

* Did you **look forward** to attending class?

* Please comment on **other aspects** of the course and feel free to **suggest alternatives**. E.g., office hours, TAs, assignments, course structure, meeting times, etc.