Anatomy of a Communications Outage

4 April 2016

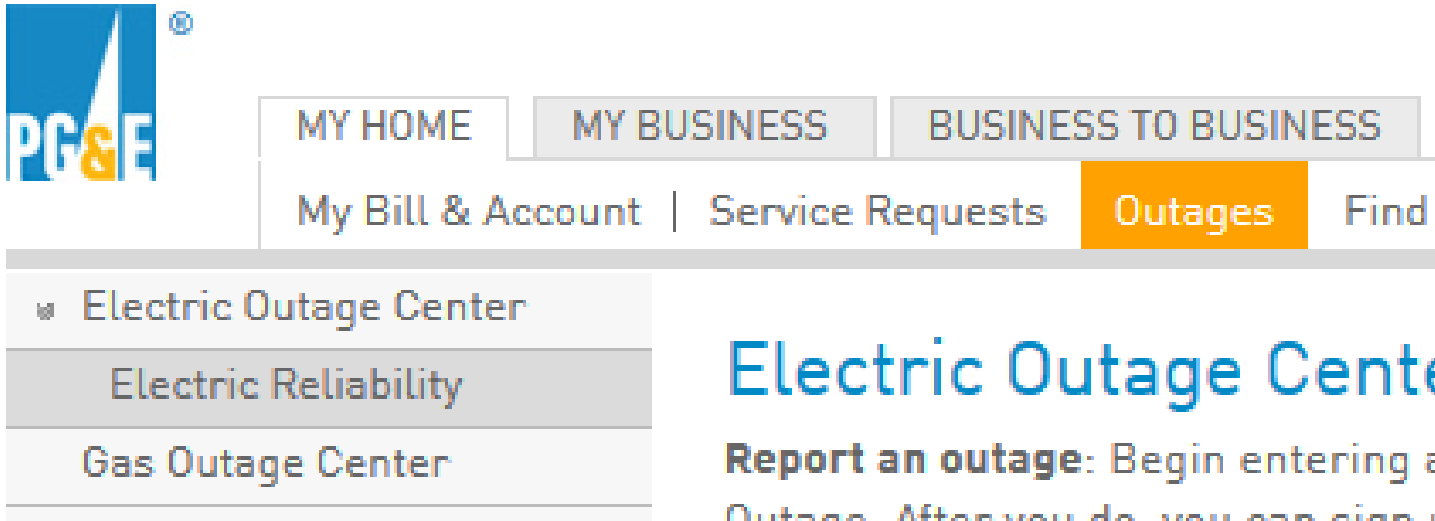
Jim Oberhofer KN6PE

Thursday morning, 8:00am

Bay Area power outage

Almost all of the Bay Area woke up (late) with no power.

As people scrambled to find their smartphones or battery-powered AM Radios, they learned that as massive power failure occurred sometime early Thursday morning, about 2:15am, that took out most of northern California's power system. PG&E and CAISO issued press releases saying that finding and fixing the cause of the outage is in progress.



Thursday afternoon, 1:00pm

Bay Area power outage

10 hours into the blackout.

PG&E reported that some unidentified fault was hampering them from bringing up the power grid per their usual procedures.

- The ***good news*** is that they isolated the source of the problem to the Cortina Substation, about 73 miles north of Sacramento.
- The ***bad news*** is that the cause is still unknown.

Friday morning, 8:00am

Bay Area power outage

30 hours into the blackout.

County OES holds a press conference:

- Essential services remain in operation throughout most of the bay area. Some backup power systems failed.
- Telephone networks are operational, but an increased demand left many circuits overloaded.
- Water systems in a few cities lost pressure forcing boil-water advisories to be put into effect.
- Cellular service is spotty due to call volume.
- Major cellular providers are now on backup power.
- Most Commercial TV, radio stations are still on the air.

Friday afternoon, 3:00pm

Bay Area power outage

38 hours into the blackout.

A joint press conference was held with County OES, PG&E, and several telephone/internet carriers. The news is not good.

- Still no exact cause for the problem, but they now suspect a software bug or worse… a worm or virus.
- Attempts to bring up the grid have failed; PG&E thinks this could go on for another 24 hours.
- AT&T and other carriers state that their networks continue to be overloaded, long delays getting a dial tone, and some backup power systems have started to fail.
- Wireline services are working, but most VRAD backup batteries will run down tonight.

Friday afternoon, 4:00pm

Bay Area power outage

39 hours into the blackout.

The Cupertino City Manager requested ARES and CERT teams to activate Saturday *if they wake up to no telephone service at home*. The request is to do the following:

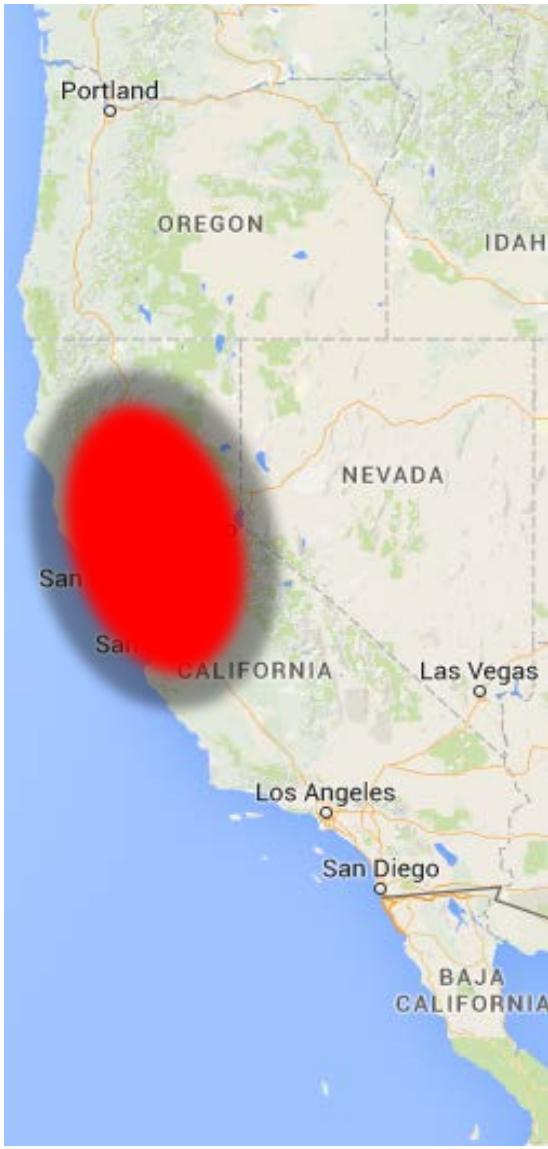
- Set up communications outreach locations throughout the City to pass on information and relay resident requests for help.
- Support the EOC.

Saturday early morning, 1:30am

Bay Area power outage

Almost 48 hours into the blackout.

- Wireline and cell phone communications fail throughout all of Santa Clara County.
- No dial tones were heard on picking up the telephone handset.
- Placing 911 calls is no longer possible.



Is this scenario likely?

San Jose Mercury News
BUSINESS

Internet infrastructure is vulnerable to attacks that can cause prolonged outages

By Felicia Fonseca and David A. Lieb | *Associated Press*

POSTED: 03/27/2015 12:24:22 PM PDT | UPDATED: 10 MONTHS AGO 2 COMMENTS

FLAGSTAFF, Ariz. -- When vandals sliced a fiber-optic cable in the Arizona desert last month, they did more than time-warp thousands of people back to an era before computers, credit cards or even phones. They exposed a glaring vulnerability in the nation's Internet infrastructure: no backup systems in many places.

San Jose Mercury News

BUSINESS

Internet infrastructure is vulnerable to attacks that can cause prolonged outages

By Felicia Fonseca and David A. Lieb | *Associated Press*

POSTED: 03/27/2015 12:24:22 PM PDT | UPDATED: 10 MONTHS AGO 2 COMMENTS

…vandals sliced a fiber-optic cables…

…accidental fiber-optic line cuts…

…underwater fiber-optic cable breaks…

…warnings about such vulnerabilities made two decades ago

Could this happen here?

Looking for the background

- National Infrastructure Protection Plan (NIPP)
  - FEMA, 2006, Risk Management Framework to address pre-existing threats that may occur from natural disasters, cyber-attacks, and terrorism.

Critical Infrastructure Sectors

1. Chemical
2. Commercial Facilities
3. Communication
4. Critical Manufacturing
5. Dam
6. Defense Industrial Base
7. Emergency Services
8. Energy
9. Finance Services
10. Food and Agriculture
11. Government Facilities
12. Healthcare and Pub Health
13. Information Technology
14. Nuclear Reactor, Mat'ls, Waste
15. Transportation Systems
16. Water and Wastewater

Could this happen here?

Looking for the background

- National Infrastructure Protection Plan
- *Communications Sector-Specific Plan (CSSP)*

Developing a view for a local risk assessment

Potentially impacted systems

- Telephony
- Internet
- Radio
- Messaging
- Video

Impacting Events

- Loss of Power
- Loss of Connectivity
- System Overload

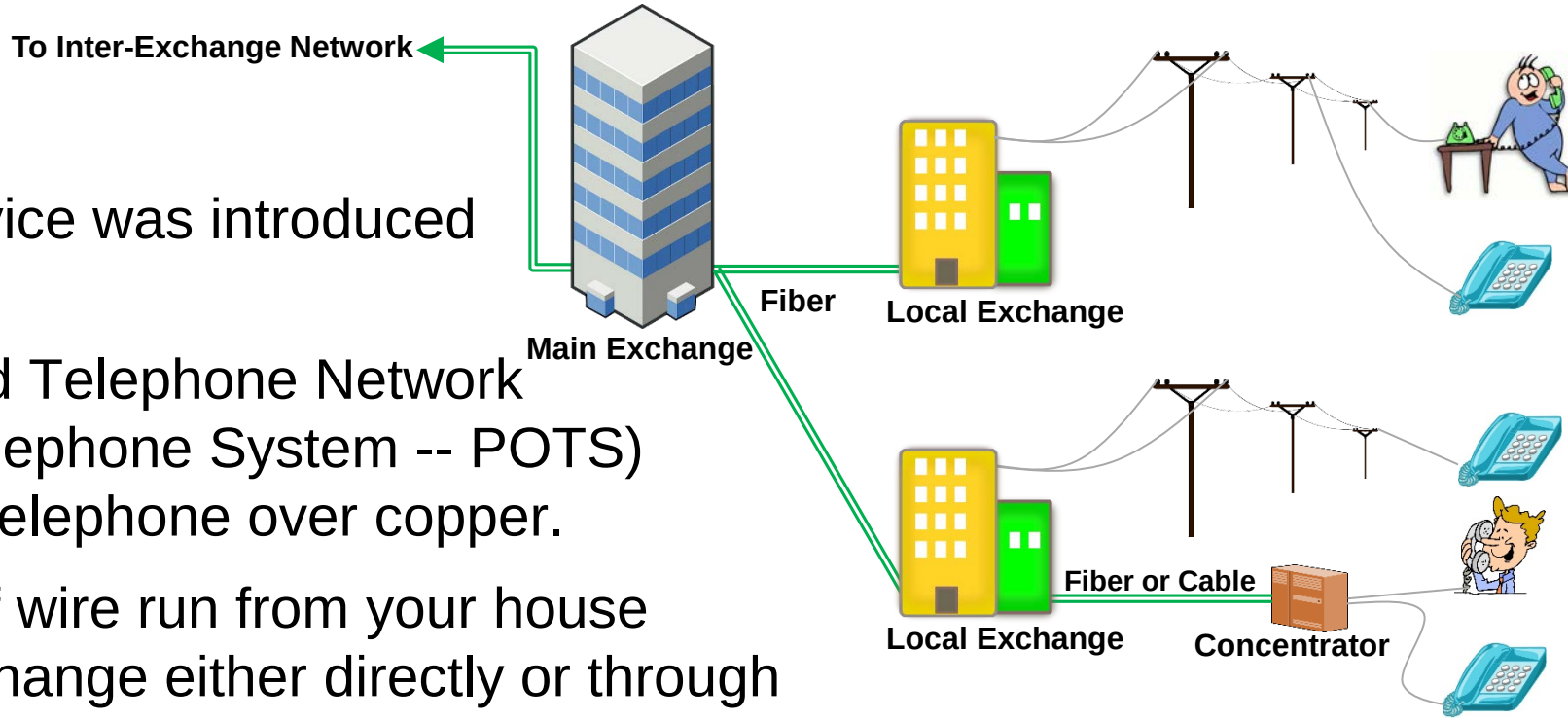
Risks (& recommendations)

What could fail?

What could cause a failure?

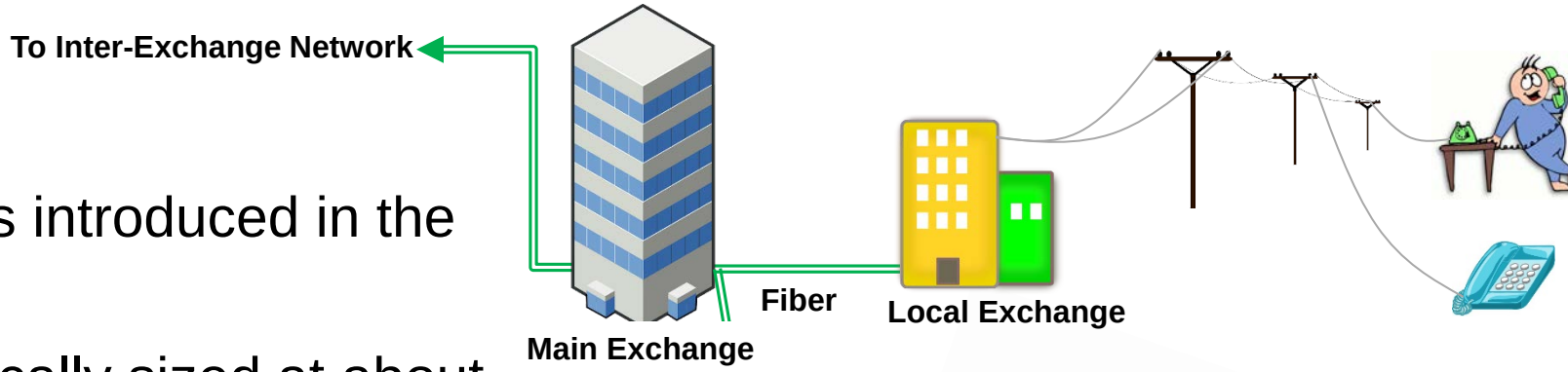
How likely, and the impact, if a failure does occur?

Landline Telephone Network

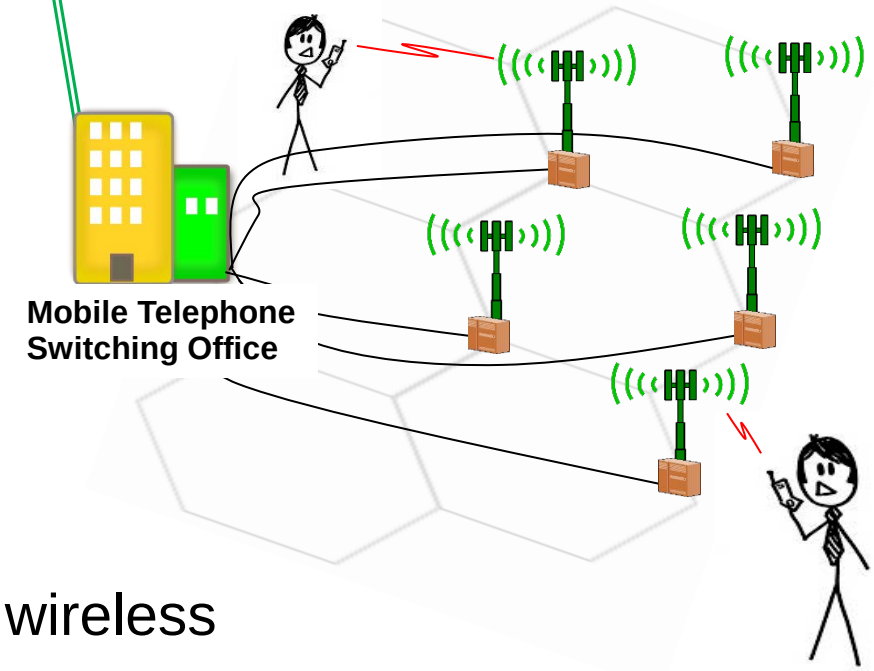


1. Telephone service was introduced in 1876.
2. Public Switched Telephone Network (or Plain Ol' Telephone System -- POTS) is voice-grade telephone over copper.
3. Copper pairs of wire run from your house to the local exchange either directly or through a digital concentrator.
4. Local calls are kept local; Out of area calls are switched to the Inter-exchange Network.
5. In 2013, there were 1.16 billion landline subscribers worldwide.

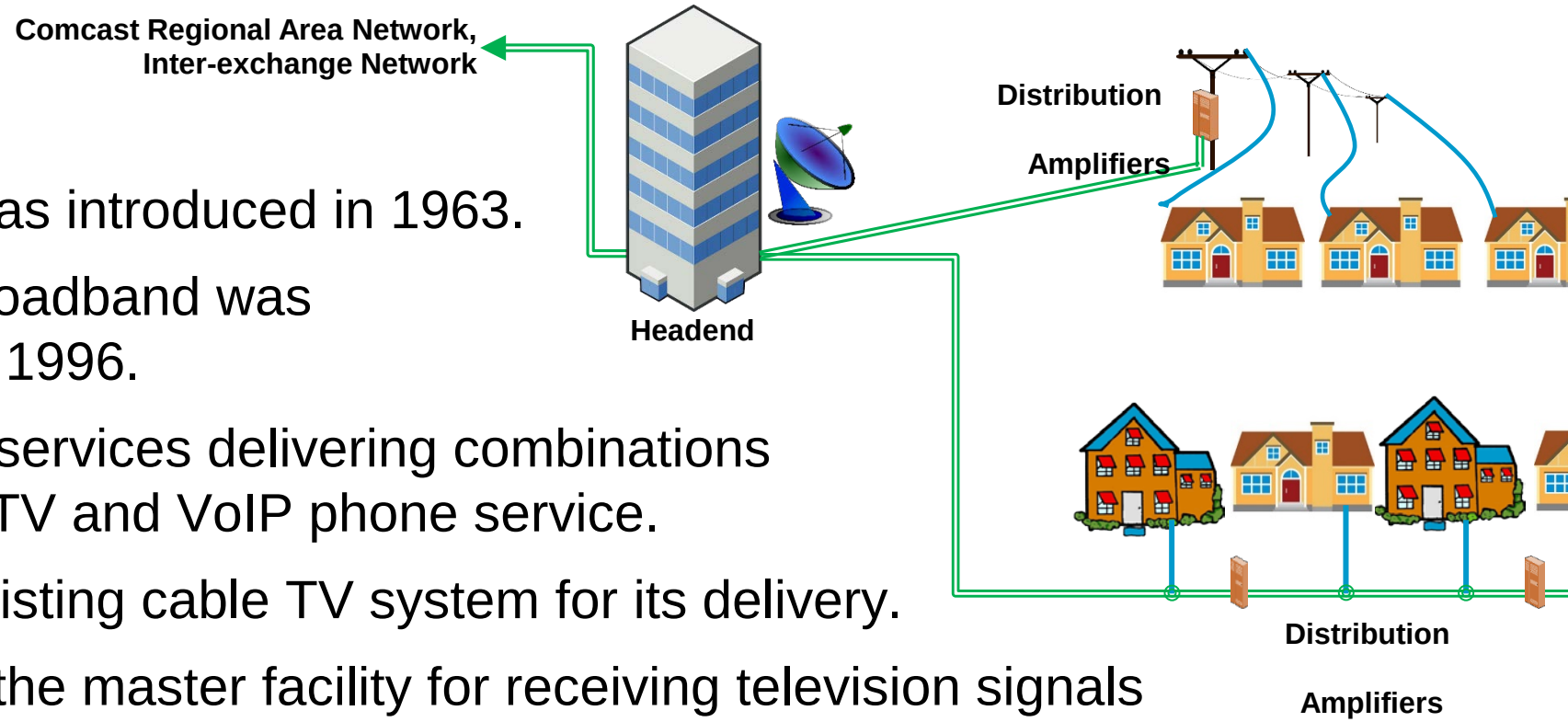
Cellular Telephone Network



1. Cell service was introduced in the U.S. in 1983.
2. Each cell is typically sized at about 10 square miles.
3. Cell phones and base stations use low-power transmitters, thereby allowing the same frequencies can be reused in nonadjacent cells.
4. Most cell sites are powered by commercial power or generators at remote locations.
5. In 2012, 38% of U.S. households had only wireless phones, up to 41% in 2013.

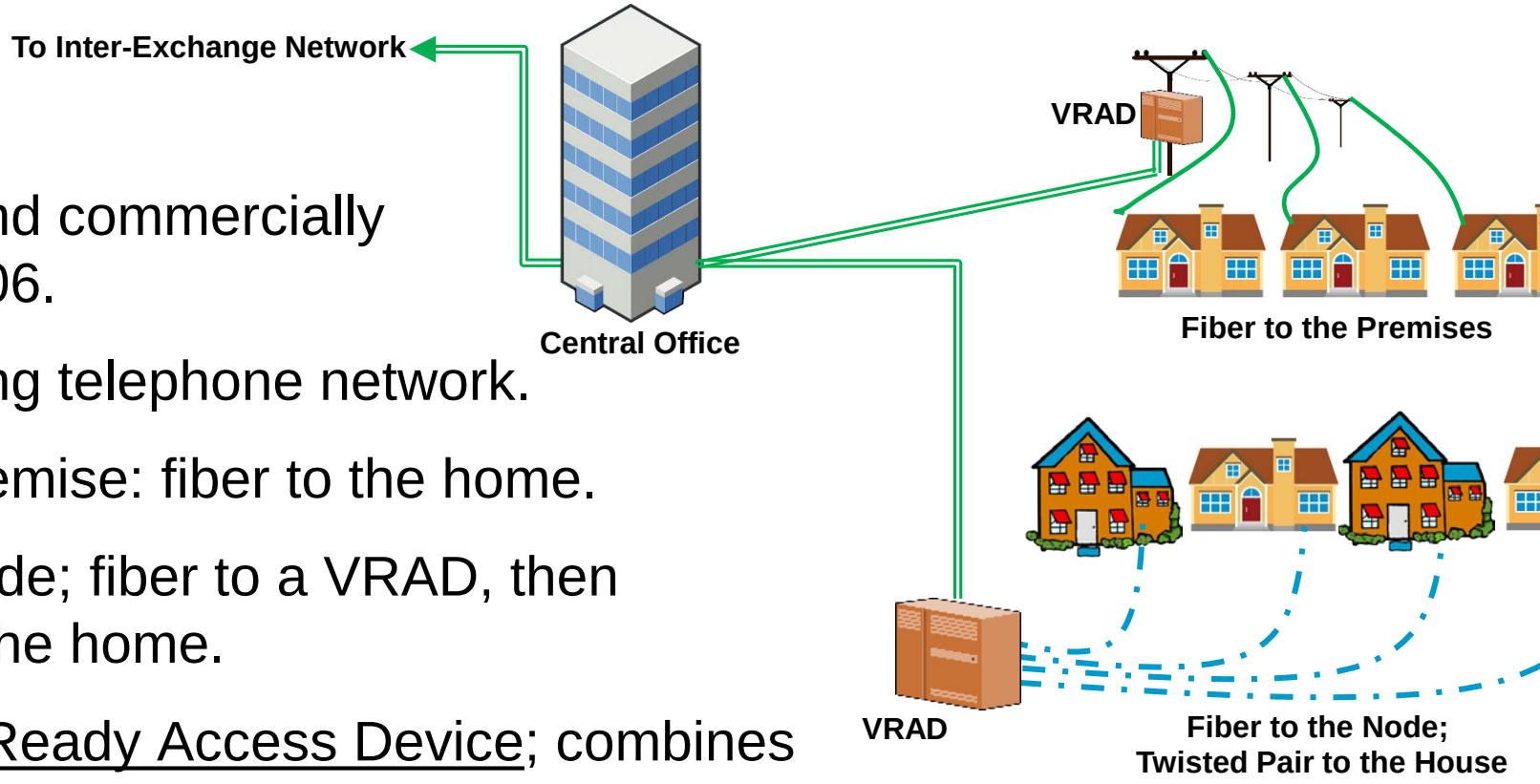


Digital Telephone, Cable Data Network



1. Cable TV was introduced in 1963.
2. Comcast broadband was launched in 1996.
3. Broadband services delivering combinations of Internet, TV and VoIP phone service.
4. Uses the existing cable TV system for its delivery.
5. **Headend:** the master facility for receiving television signals for processing and distribution over a cable television system.
6. **Distribution Amplifiers:** ensures a sufficient signal level down the path.
7. **Coax Splitter:** splits signal for TV, Internet, and Phone.

Digital Telephone, DSL Data Network



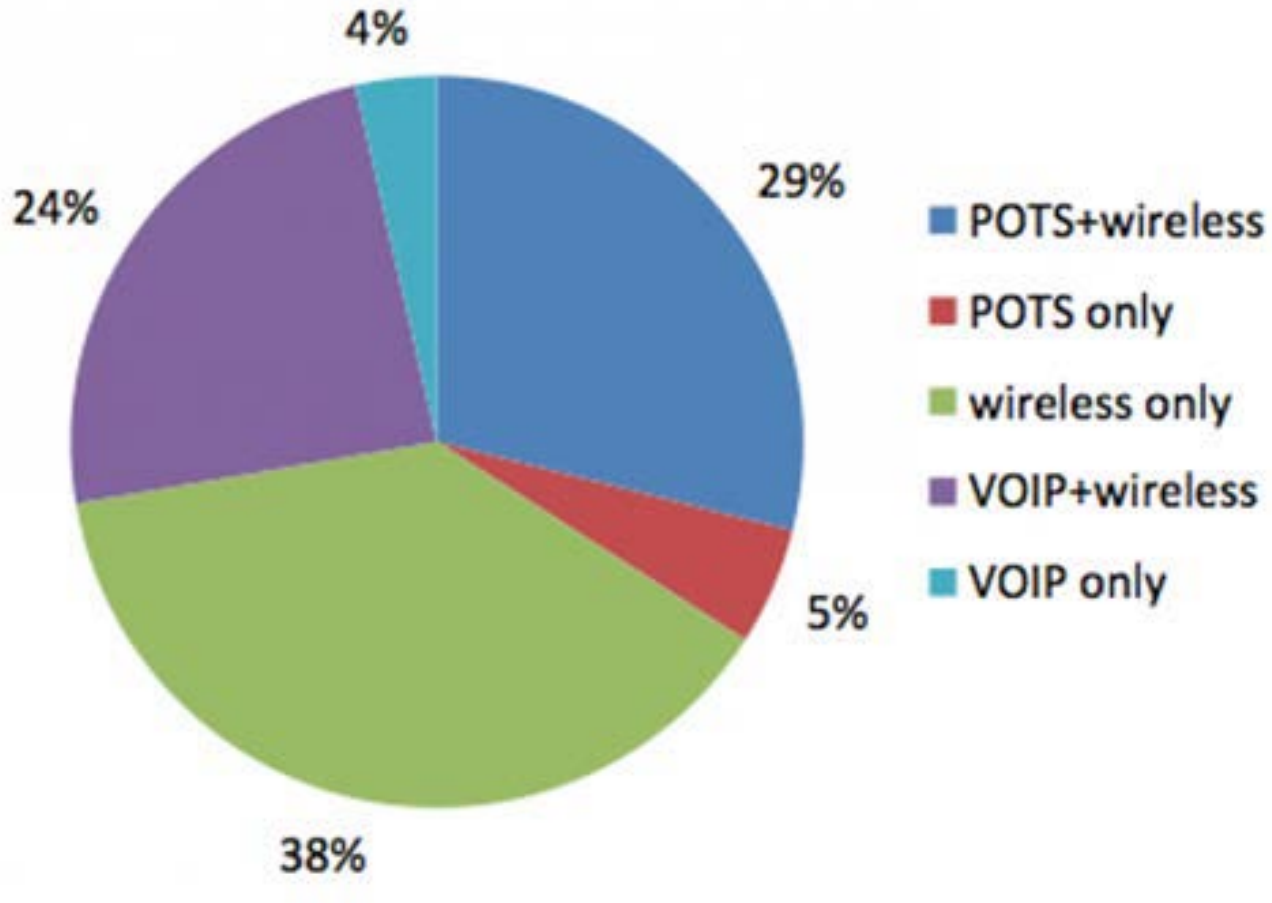
1. AT&T broadband commercially launched in 2006.
2. Uses the existing telephone network.
3. Fiber-to-the-Premise: fiber to the home.
4. Fiber-to-the-Node; fiber to a VRAD, then twisted pair to the home.
5. **VRAD**: Video Ready Access Device; combines voice and data (DSLAM) with the TV stream to the home.

DSLAM: Digital Subscriber Line Access Multiplexer; combines end voice and data traffic into one signal; at the Central Offices or VRADs.

Telephone use… by the numbers

Who's using what?

- In 2012, the CDC estimated that only 38% of U.S. households had only wireless at home.
- Households with a **POTS-only wireline service** decreased from **88%** to **5%** between 2002 and 2012.



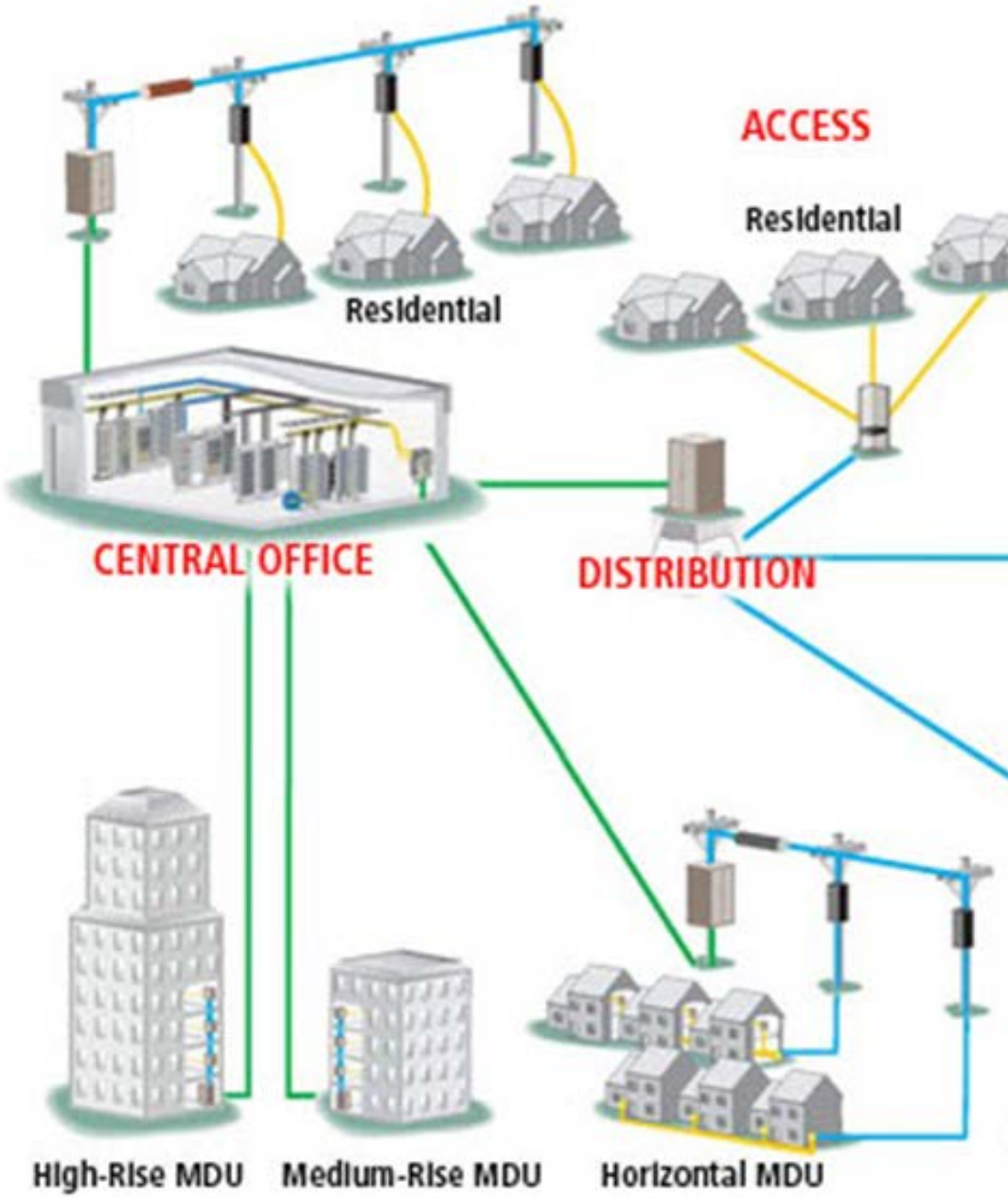
What do they all have in common?

Connectivity…

1. **Almost everything connects together**

   …in the physical world of wire, cable, or fiber sooner or later.

   1. Wired Telephone
   2. Cellular phone
   3. AT&T, Comcast, Sprint, Verizon, other carriers



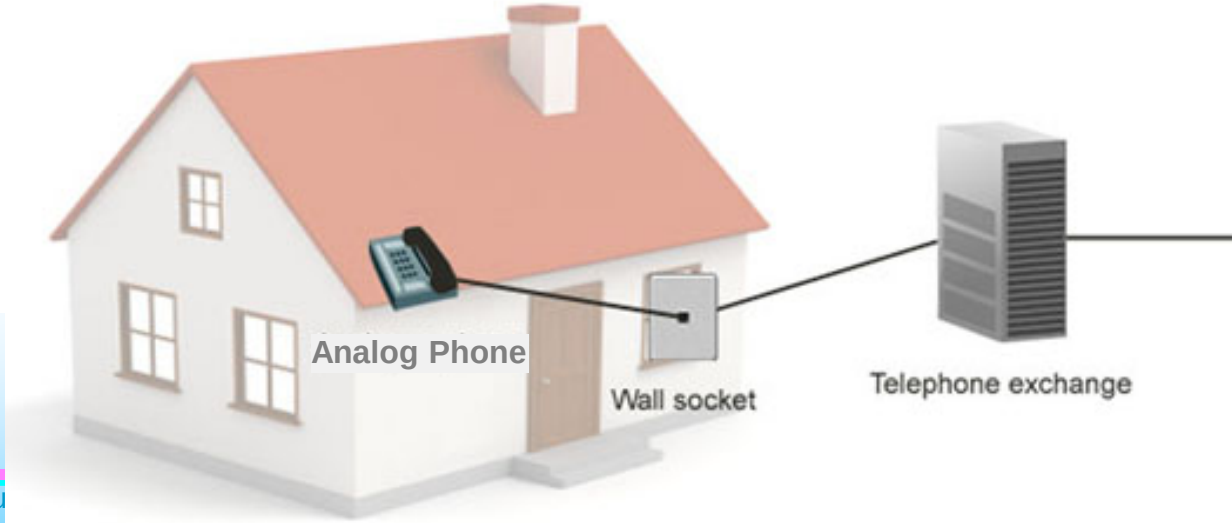
What do they all have in common?

…and Power

2. All require power to operate

Landline Telephone Network

1. The Phone company maintains an extensive battery system with backup generators at Local Exchange offices.
2. Operates at 6 to 12 volts DC, ~30ma.
3. 90VAC for the ring signal, as provided by the Local Exchange.
4. During a power failure, wired phones will continue to work,
5. … assuming at least one is a “corded” phone.



What do they all have in common?

…and Power

2. All require power to operate

Cellular Telephone Network

1. Towers, controllers fed from commercial power.
2. Backup batteries are built into most standard power systems.
3. Batteries can last from 2 to 8 hours, depending on their configuration.
4. Generators are also used to avoid service interruption.

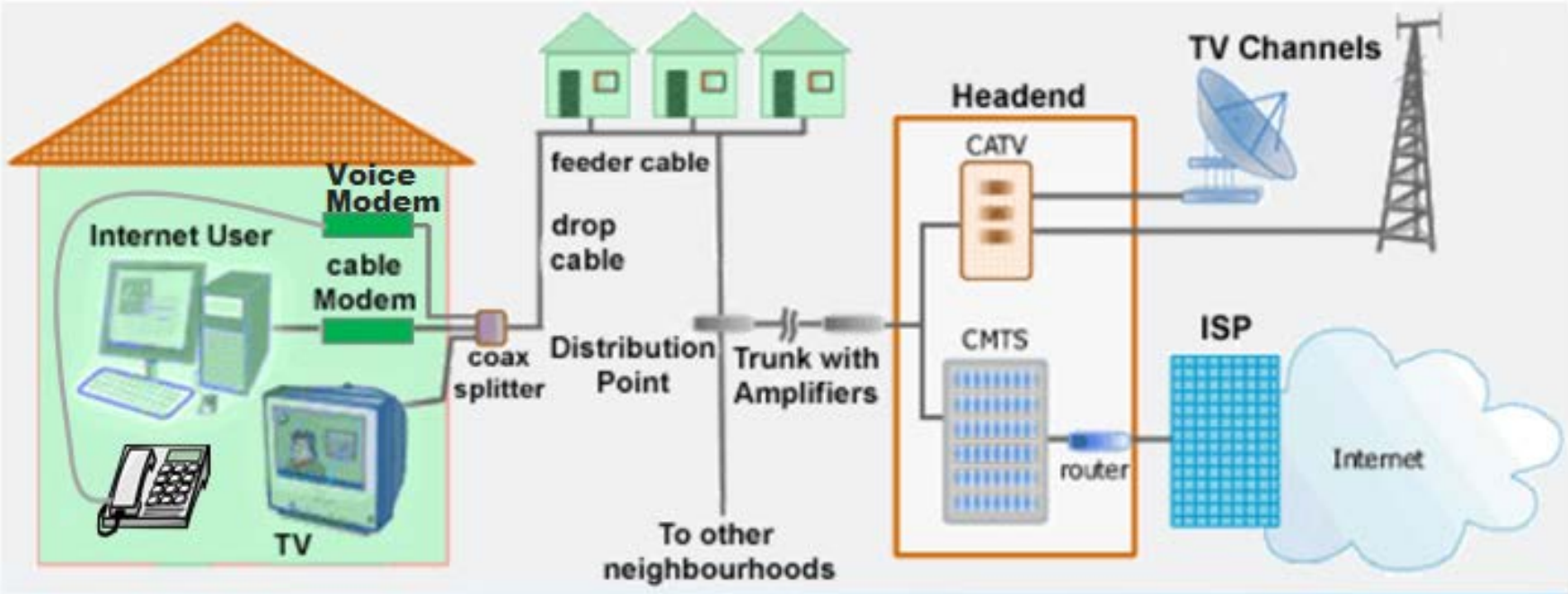
What do they all have in common?

…and Power

2. All require power to operate

Comcast Digital Network

1. Central Office / Headend: backup generators, batteries.
2. The *voice phone modem* requires a ***backup battery*** to ensure telephone service remains operational during a power outage.

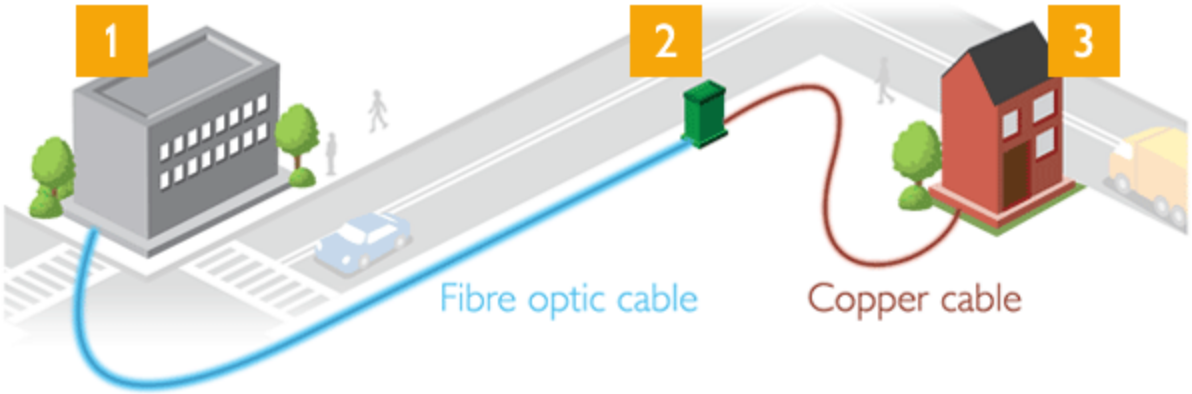


What do they all have in common?

…and Power

2. All require power to operate

AT&T Digital Network



1. Central Office: gen & battery backup.
2. VRAD Neighborhood boxes; backup NiMH batteries, 2-4 days of power.
3. Wi-Fi Resident Gateway; with phone service, add a Belkin 12V, 7Ah SLA.

What could cause communications outages?

- **Loss of Power**
  - Power failures – accidental, natural, intentional
- **Loss of Connectivity**
  - Cable breaks – accidental, natural, intentional
- **System Overload**
  - Some out-of-the-ordinary event that causes a lot of people to use the phone at the same time
- **Solar Storms, Solar Flares**

Is this scenario likely?

Loss of Power

Date	Event	Duration	Impact
Accidental			
November 1965	Northeast Blackout	13 hours	30,000,000
October 2003	Northeast Blackout	1-2 days	55,000,000
September 2011	Pacific Southwest	12 hours	7,000,000
Natural…			
October 1989	Loma Prieta Earthquake	2-3 days	1,400,000
January 1994	Northridge Earthquake	1 week	300,000
September 2005	Katrina	Weeks	3,900,000
Intentional…			
April 2013	Metcalf Sniper Attack	27 days	None

Is this scenario likely?

Loss of Power

Intentional

April 16, 2013, San Jose Mercury, *WSJ*.
Assault on California Power Station Raises Alarm on Potential for Terrorism.

- telephone cables were cut.
- 20 minutes of shooting at the Station.
- 17 transformers were knocked out.
- 27 days to make repairs.

*"If it was widely replicated across the country, [an event like this] could take down the U.S. electric grid and black out much of the country"; **loss of communications would follow**.*

Shots in the Dark

A look at the April 16 attack on PG&E's Metcalf Transmission Substation

1	2	3	4	5
12:58 a.m., 1:07 a.m. Attackers cut telephone cables	**1:31 a.m.** Attackers open fire on substation	**1:41 a.m.** First 911 call from power plant operator	**1:45 a.m.** Transformers all over the substation start crashing	**1:50 a.m.** Attack end and gunme leave

Sources: PG&E; Santa Clara County Sheriff's Dept.; California Independent System Operator; California
The Wall Street Journal

Is this scenario likely?

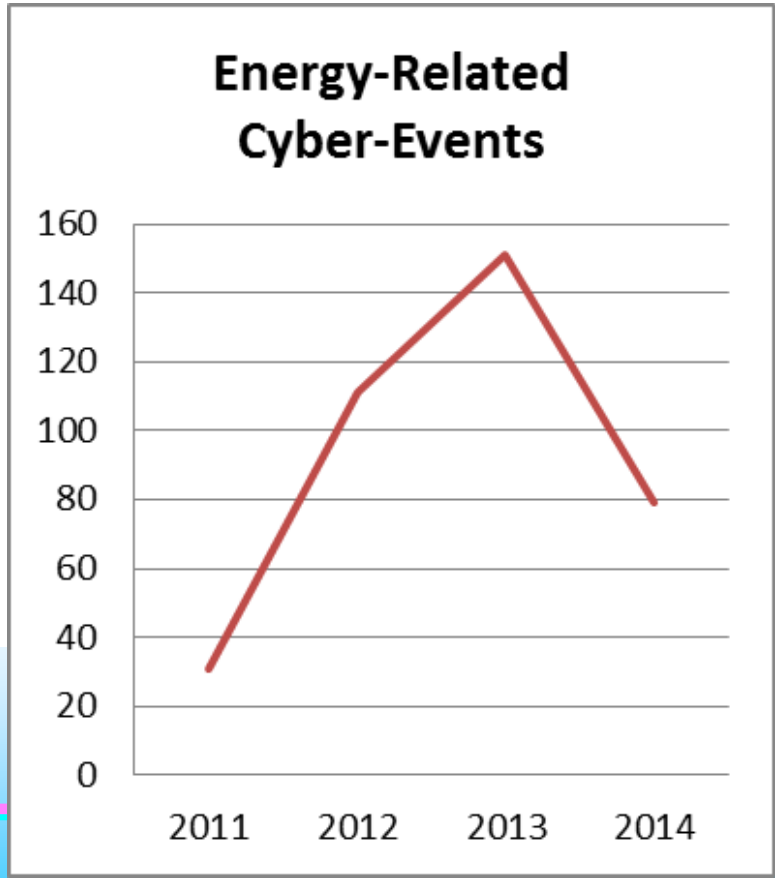
Loss of Power

Intentional – Other Reports

- Parts of the U.S. power grid are attacked online or in person every four days (per an analysis of federal energy records).
- From 2011 to 2014: the U.S. Department of Energy received 362 reports from electric utilities of physical or cyber attacks that interrupted power services.
- Department of Homeland Security was alerted to energy-related “cyber incidents”…

  2014: 79
  2013: 151
  2012: 111
  2011: 31

  The lower 2014 number is attributed to attacks being more difficult to detect.



Is this scenario likely?

What has caused communications outages?

Loss of Connectivity

Accidental – in the news

- ***March 2015, Arizona.*** Several thousand people lost Internet and phone service for 12 hours when an electric company crew accidentally cut a fiber-optic line in northern New Mexico.
- ***2013, Washington.*** Underwater fiber-optic cable snapped leaving residents on the San Juan Islands without Internet and telephone for 10 days.
- ***March 2012, Morgan Hill.*** Most Verizon phone and Internet connections were down for the day because a major fiber-optic cable was accidentally cut.

What has caused communications outages?

Loss of Connectivity

Intentional – in the news

- ***April 2009, San Jose.*** underground fiber-optic cables were cut knocking out landlines, cell, and Internet for 10,000's in Santa Clara, Santa Cruz and San Benito Counties.

What has caused communications outages?

Loss of Connectivity

Intentional – in the news

- ***February 2015, Arizona.*** Vandals cut through an underground bundle of fiber-optic cables; ATMs were down, stores couldn't process credit cards, and 9-1-1 emergency service was unavailable. ~15 hour outage.
- ***June 30, 2015, Sacramento.*** three major fiber cables connecting the region were cut; disrupts service to Sacramento, Rocklin; ~15 hour outage
- ***July 1, 2015, San Jose.*** Break-in to an underground vault and vandals cut three fiber-optic cables belonging to Level 3 and Zayo.
- **July 15, 2015, San Joaquin County.** Fiber optic line intentionally cut causing 9-1-1 outages; 10 hour outage.
- **September 3, 2015, CA North Coast.** Vandals cut AT&T fiber cable in Hopland disrupting Internet, landline and cellphone service.

What has caused communications outages?

Loss of Connectivity

Intentional – and then there is the FBI report-out…

…even more cable cuts throughout the Bay Area

- July 6, 2014, 9:44 p.m., Berkley. Near 7th St. and Grayson St.
- July 6, 2014, 11:39 p.m., Fremont. Niles Canyon Blvd and Mission Blvd.
- July 7, 2014, 12:24 a.m., Walnut Creek. Jones Road and Iron Horse Trail.
- July 7, 2014, 12:51 a.m., Fremont. Niles Canyon Blvd. and Alameda Creek.
- July 7, 2014, 2:13 a.m., San Jose. Stockton Ave. and University Ave.
- Feb 24, 2015, 11:30 p.m., Fremont. Niles Canyon Blvd. and Mission Blvd.
- Feb 24, 2015 11:30 p.m., Fremont. Niles Canyon Blvd. and Alameda Creek.
- June 8, 2015, 11:00 p.m., Alamo. Danville Blvd. and Rudgear Road.
- June 8, 2015, 11:40 p.m., Fremont. Overacker Ave. and Mowry Ave.
- June 9, 2015, 1:38 p.m., Walnut Creek. Jones Road and Parkside Dr.

What has caused communications outages?

Loss of Connectivity

Other Notes

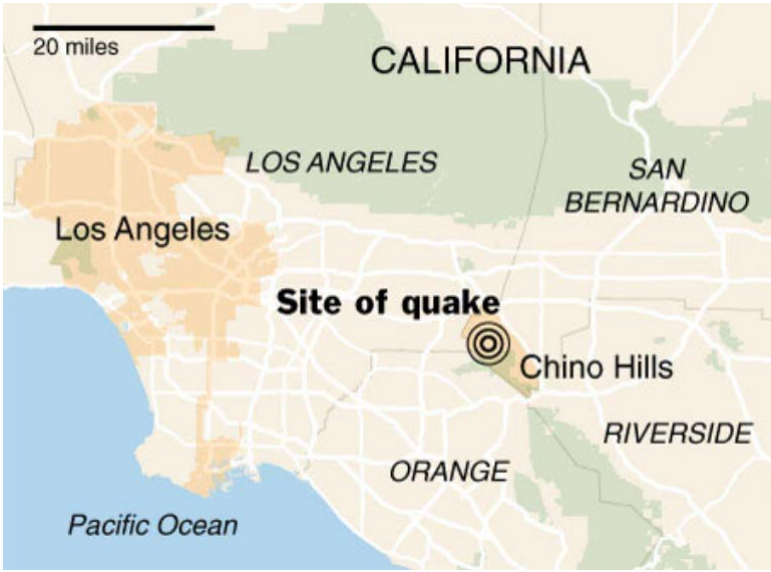
- In 1995, U.S. Commerce Dept's NIST warned that the "power of optical fiber technology is **diminishing the number of geographic transmission routes**," concentrating the flow of information and "resulting in an **increase in network vulnerability**."
- Companies deploy more than **10 million miles of fiber annually** in the U.S., **increase the risk** of damage from backhoes, trench-diggers and shovels.
- The FCC reported that outages on high-capacity fiber lines in the U.S. more than doubled from **221 in 2010 to 487 in 2014**.
- And… are these intentional cable cuts a *Test*?

What could cause communications outages?

System Overload

Natural *(2 examples)*

- July 30, 2008, Los Angeles. Magnitude 5.4 earthquake, San Bernardino County. **Cell phone lines were jammed** as people frantically made calls immediately after the jolt. CA OES urged Californians to free up the lines for emergency use. No damage was reported to the network infrastructure.
- August 23, 2011, Washington DC. Magnitude 5.8 earthquake struck central Virginia. **Cell phone networks were jammed** in Manhattan, Washington D.C., and other areas. SMS could get through. Major carriers reported no major problems with their network infrastructure.



What could cause communications outages?

Solar Storms, Solar Flares

Date	Event	Duration	Impact
September 1859	Solar Storm (Carrington)	Unknown	Unknown
August 1972	Solar Flare, Illinois	Unknown	Unknown
March 1989	Solar Flare, Quebec	9 hours	6,000,000

- In 2012, NASA said the sun unleashed two massive plasma clouds that ***barely missed*** a catastrophic encounter with Earth.
  - "A direct strike could've caused widespread power outages and other damaging effects."
  - "If it had hit, we would still be picking up the pieces 2 years later."
  - NASA also cited research suggesting that there is a 12% chance of something like this happening in the next decade.

Takeaways

- Fewer fiber optic cable paths means wider impact when a cable break occurs.
- Intentional cable cuts are up.
- Cyber attacks on the power grid are also increasing.
- POTS will be gone within 5-10 years.
- Communications is growing more dependent on local rather than central power sources.

Managing Communications Risks

What can we control?

- City backup generators
- City 2-way radio systems
- AM TIS Station
- Ham Radio
- Local staff and volunteers

What can't we control?

- Power generation and distribution
- Landline (POTS) phone
- Cell telephone network
- Digital network

This implies that we should…

apply **Mitigations** here

apply **Contingencies** here

Assessing the Risks

Class 1: Unacceptable

- …in any circumstance.
- **7 Risks** related to City Hall Access, Loss of Power

Class 2: Undesirable

- Tolerable if the risk reduction is impracticable or costs are grossly disproportionate to the improvement gained.
- **9 Risks related to loss of residents' ability to dial 911**

Class 3: Tolerable

- …if the cost of risk reduction would exceed the improvement.
- **27 Risks** identified

Class 4: Acceptable

- …as it stands, though it may need to be monitored.
- None identified

Friday afternoon, 4:00pm

Bay Area power outage

39 hours into the blackout.

The Cupertino City Manager requested ARES and CERT teams to activate Saturday *if they wake up to no telephone service at home*. The request is to do the following:

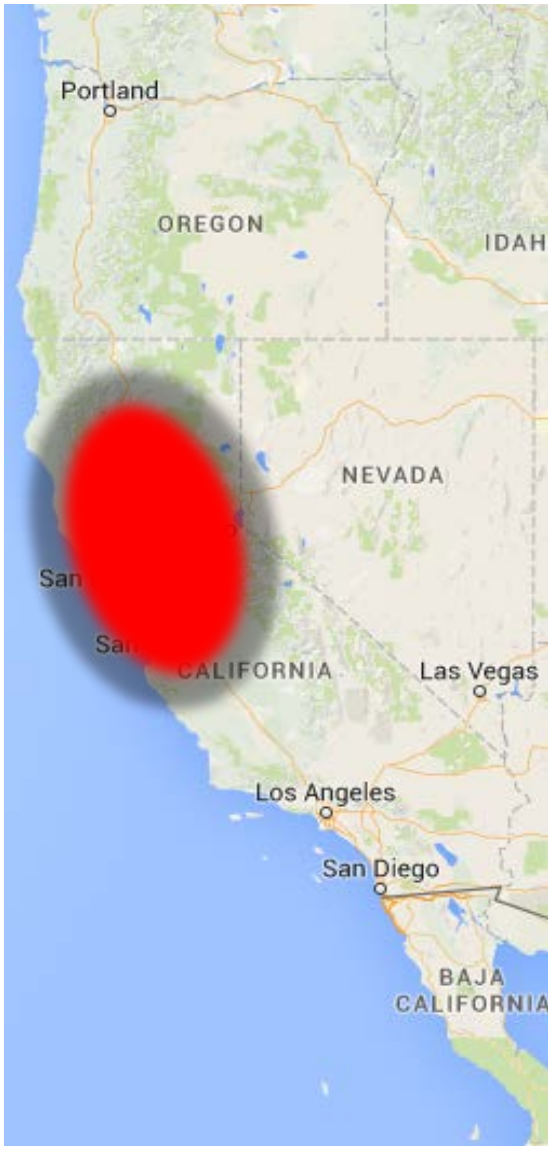
- Set up communications outreach locations throughout the City to pass on information and relay resident requests for help.
- Support the EOC.

Saturday early morning, 1:30am

Bay Area power outage

Almost 48 hours into the blackout.

- Wireline and cell phone communications fail throughout all of Santa Clara County.
- No dial tones were heard on picking up the telephone handset.
- Placing 911 calls is no longer possible.



Saturday morning, 8:00am

Bay Area power outage

55 hours into the blackout.

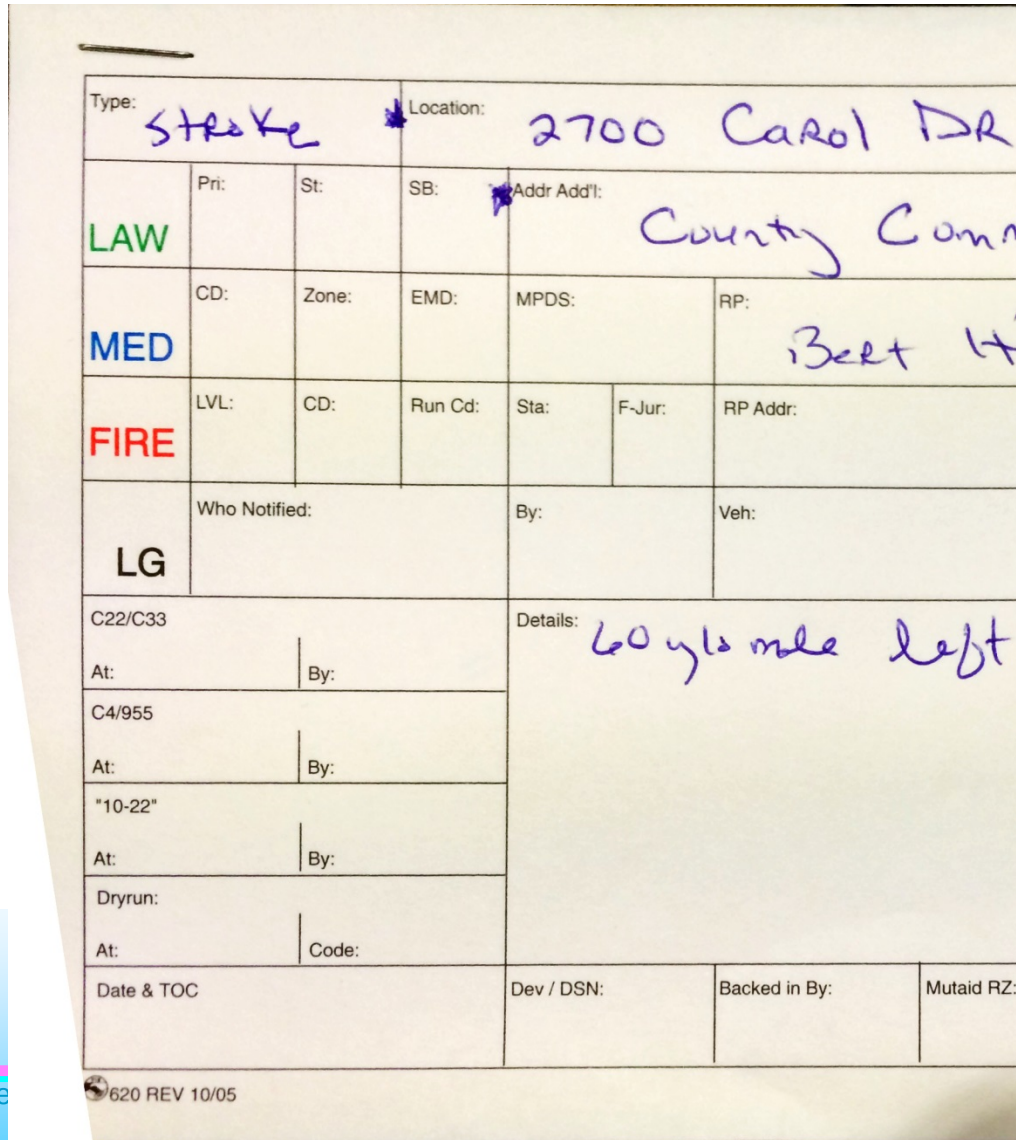
- Activated CARES Emergency Net.
- Simulated an operator at County Comm; activated the “911” net.
- Deployed 10 CARES+CERT teams to staff field community emergency request stations.
- Used scripted event injects.
- Passed 52 messages over 2 hours; 26 to the EOC, 26 on the “911” net.

Debrief

Bay Area power outage

After Action Report Highlights

- Refine the deployment details and information handoffs with County Comm; involve other impacted cities.
- Re-do the Comm Outage Drill in May, this time by Packet.



www.cupertinoares.org

Welcome to Cupertino ARES/RACES

This site is operated by and for Cupertino Amateur Radio Emergency Service (CARES) members interested in emergency preparedness and amateur radio communication. Visitors are welcome to check us out.

What's News!

Cupertino survives simulated Communications Outage

Posted by Jim KN6PE, 21 Nov 2015

Cupertino Citizen Corps held a Communications Outage exercise where we simulated a total loss of landline and cell phone communications throughout the Bay Area. Ten teams, each consisting of a CARES and CERT member, were deployed into the field to establish Community Emergency Assistance Request stations to help distribute information from the City as well as take in and pass simulated 911 requests for help. With the teams handling a total of 52 messages over 2 hours, we confirmed that integrating CCC members is a great way to leverage our resources. We learned a lot and plan to refine our processes based on the feedback we received. Thanks to all who participated for your help! More Details...

Upcoming Activities

7 Apr 2016, General Meeting
Packet Overview, 7:30pm to 9:00pm, EOC, City Hall

16 Apr 2016, Hands-on Packet Training
Excellent prep for the May drill, 9:00am - 12:00pm, EOC, City Hall

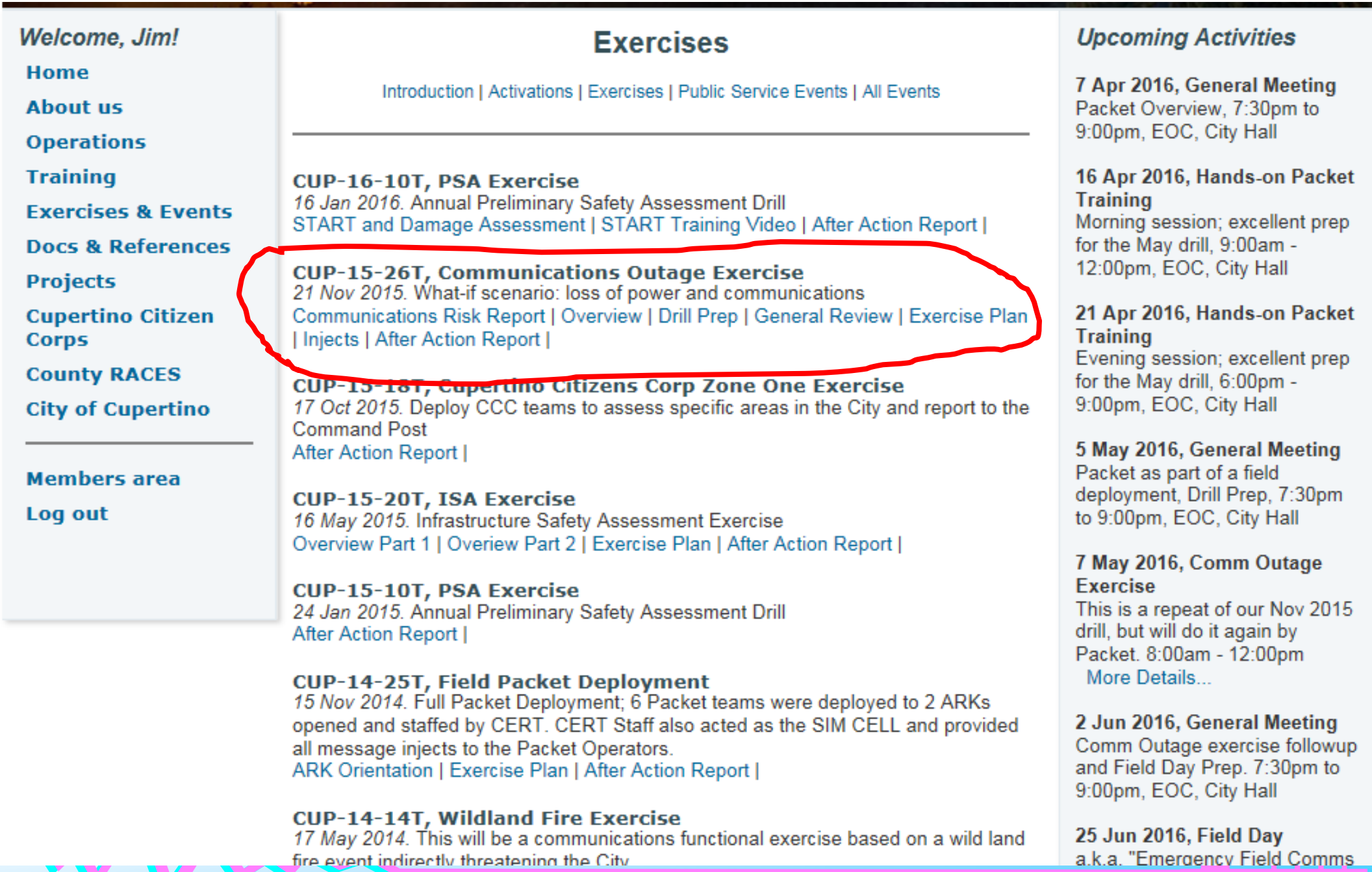
21 Apr 2016, Hands-on Packet Training
Excellent prep for the May drill, 6:00pm - 9:00pm, EOC, City Hall

5 May 2016, General Meeting
Packet as part of a field deployment, Drill Prep, 7:30pm to 9:00pm, EOC, City Hall

7 May 2016, Comm Outage Exercise
This is a repeat of our Nov 2015 drill, but will do it again by Packet. 8:00am - 12:00pm
More Details...

2 Jun 2016, General Meeting
Comm Outage exercise followup and Field Day Prep. 7:30pm to 9:00pm, EOC, City Hall

www.cupertinoares.org



Welcome, Jim!

- Home
- About us
- Operations
- Training
- Exercises & Events
- Docs & References
- Projects
- Cupertino Citizen Corps
- County RACES
- City of Cupertino

- Members area
- Log out

Exercises

Introduction | Activations | Exercises | Public Service Events | All Events

---

CUP-16-10T, PSA Exercise
16 Jan 2016. Annual Preliminary Safety Assessment Drill
START and Damage Assessment | START Training Video | After Action Report |

CUP-15-26T, Communications Outage Exercise
21 Nov 2015. What-if scenario: loss of power and communications
Communications Risk Report | Overview | Drill Prep | General Review | Exercise Plan | Injects | After Action Report |

CUP-15-18T, Cupertino Citizens Corp Zone One Exercise
17 Oct 2015. Deploy CCC teams to assess specific areas in the City and report to the Command Post
After Action Report |

CUP-15-20T, ISA Exercise
16 May 2015. Infrastructure Safety Assessment Exercise
Overview Part 1 | Overiew Part 2 | Exercise Plan | After Action Report |

CUP-15-10T, PSA Exercise
24 Jan 2015. Annual Preliminary Safety Assessment Drill
After Action Report |

CUP-14-25T, Field Packet Deployment
15 Nov 2014. Full Packet Deployment; 6 Packet teams were deployed to 2 ARKs opened and staffed by CERT. CERT Staff also acted as the SIM CELL and provided all message injects to the Packet Operators.
ARK Orientation | Exercise Plan | After Action Report |

CUP-14-14T, Wildland Fire Exercise
17 May 2014. This will be a communications functional exercise based on a wild land fire event indirectly threatening the City

Upcoming Activities

7 Apr 2016, General Meeting
Packet Overview, 7:30pm to 9:00pm, EOC, City Hall

16 Apr 2016, Hands-on Packet Training
Morning session; excellent prep for the May drill, 9:00am - 12:00pm, EOC, City Hall

21 Apr 2016, Hands-on Packet Training
Evening session; excellent prep for the May drill, 6:00pm - 9:00pm, EOC, City Hall

5 May 2016, General Meeting
Packet as part of a field deployment, Drill Prep, 7:30pm to 9:00pm, EOC, City Hall

7 May 2016, Comm Outage Exercise
This is a repeat of our Nov 2015 drill, but will do it again by Packet. 8:00am - 12:00pm
More Details...

2 Jun 2016, General Meeting
Comm Outage exercise followup and Field Day Prep. 7:30pm to 9:00pm, EOC, City Hall

25 Jun 2016, Field Day
a.k.a. "Emergency Field Comms

Thank you!... Questions?

Anatomy of a Communications Outage