Project Byzantium

Mesh networking for the Zombie Apocalypse

Disclaimer

We do not speak for our employers, past or present.

We don't speak for HacDC, either.

Project Byzantium is entirely separate from our day-, evening- and other jobs.

Who we are

Ben the Pyrate (@sitwon)

- Linux sysadmin and developer
- Experienced with live and embedded distros
- Concerned about disaster relief and network neutrality

Haxwithaxe

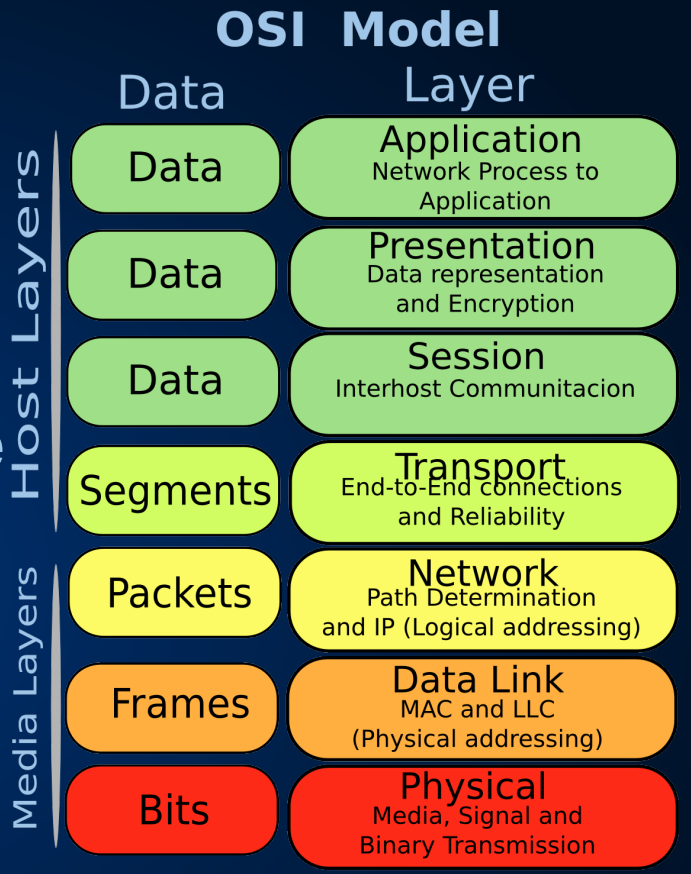
- Linux sysadmin and programmer
- Experience developing live distros and OpenWRT based firmware
- Net neutrality, freedom of speech, emergency communications

The Doctor (@virtadpt)

- BOFH/system architect/security consultant/social activist
- Experience with alternative communications technologies
- Concerned about censorship, emergency communications, freedom of speech

Basic Assumptions

- You're familiar with the OSI model
- You know what routing does (layer 3)
- You know how to use 802.11 (layers 1 & 2)
- You like being connected
- You need to communicate with people



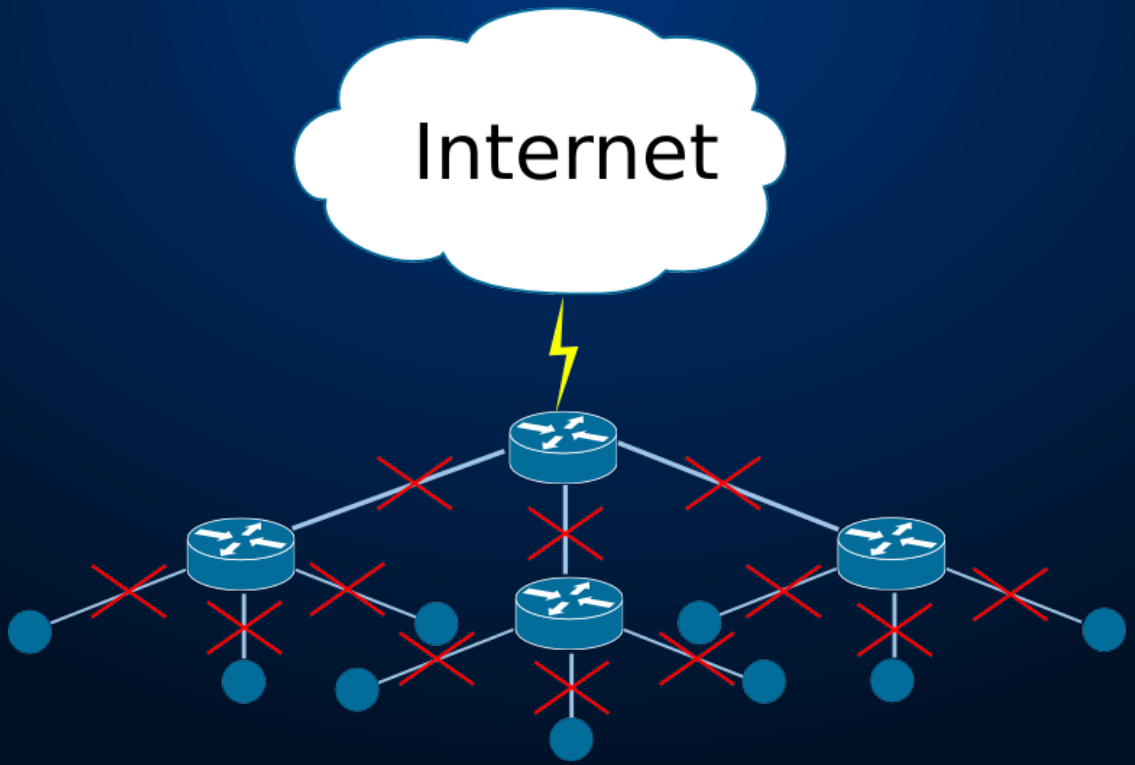
sources: JB Hewitt and Gonzalo Rivero
via http://commons.wikimedia.org/wiki/File:Osi-model-jb.svg
under GPL v1.2
Source code available upon request

The Internet is BROKEN.

It fails on many levels, but let's start from the bottom.

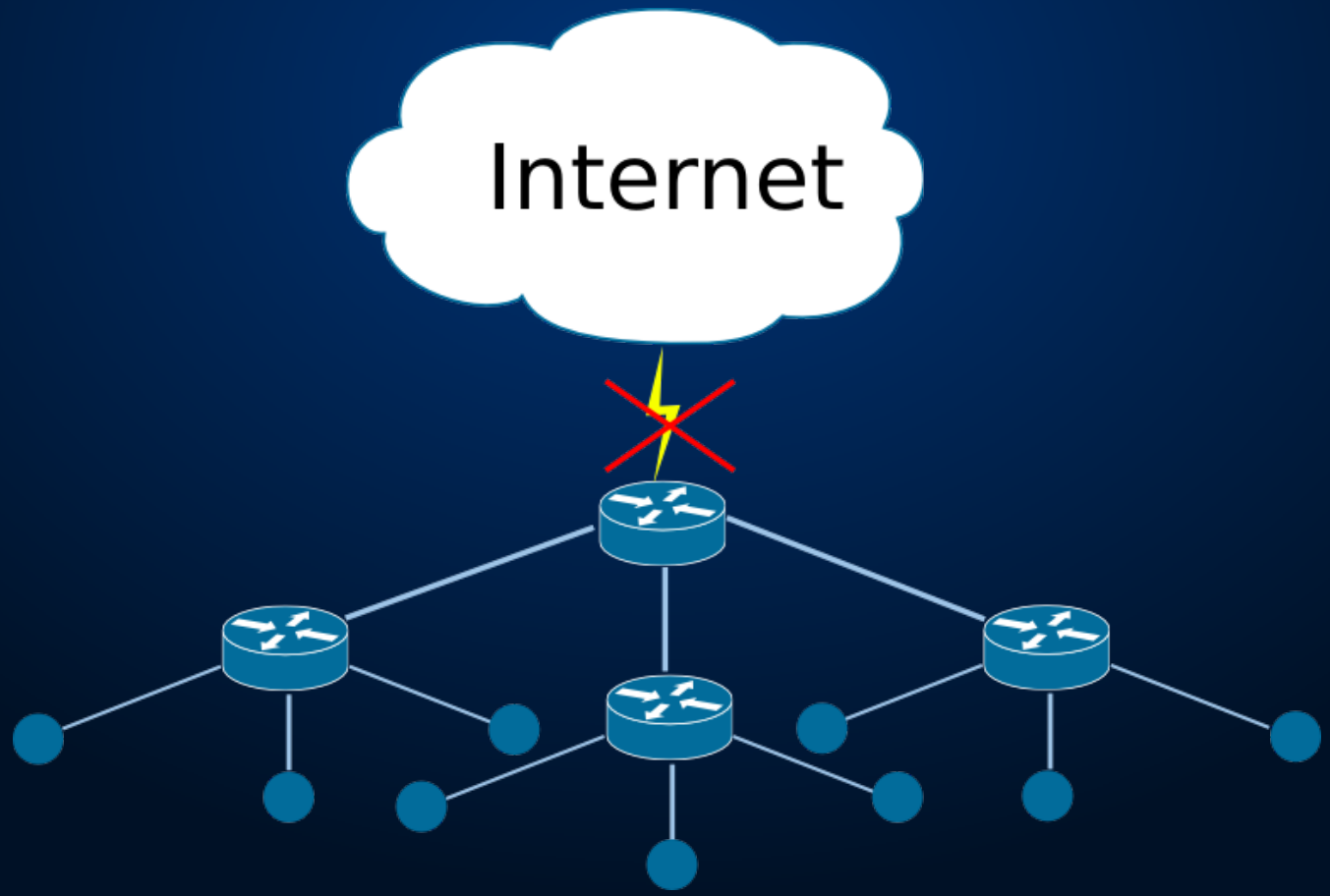
Use Case #1: The Katrina Problem

- Massive infrastructure failure
- Natural disaster
- Power grid failure
- Connectivity is patchy at best, likely unavailable
- What still works barely works
- Need to communicate (organize relief, call for help)



Use Case #2: The Egypt Problem

- Deliberate compromise of network infrastructure
- ISPs taken offline
- Need to collaborate with other people securely
- Need to contact the outside world
- Active adversary working against you!



Our Approach

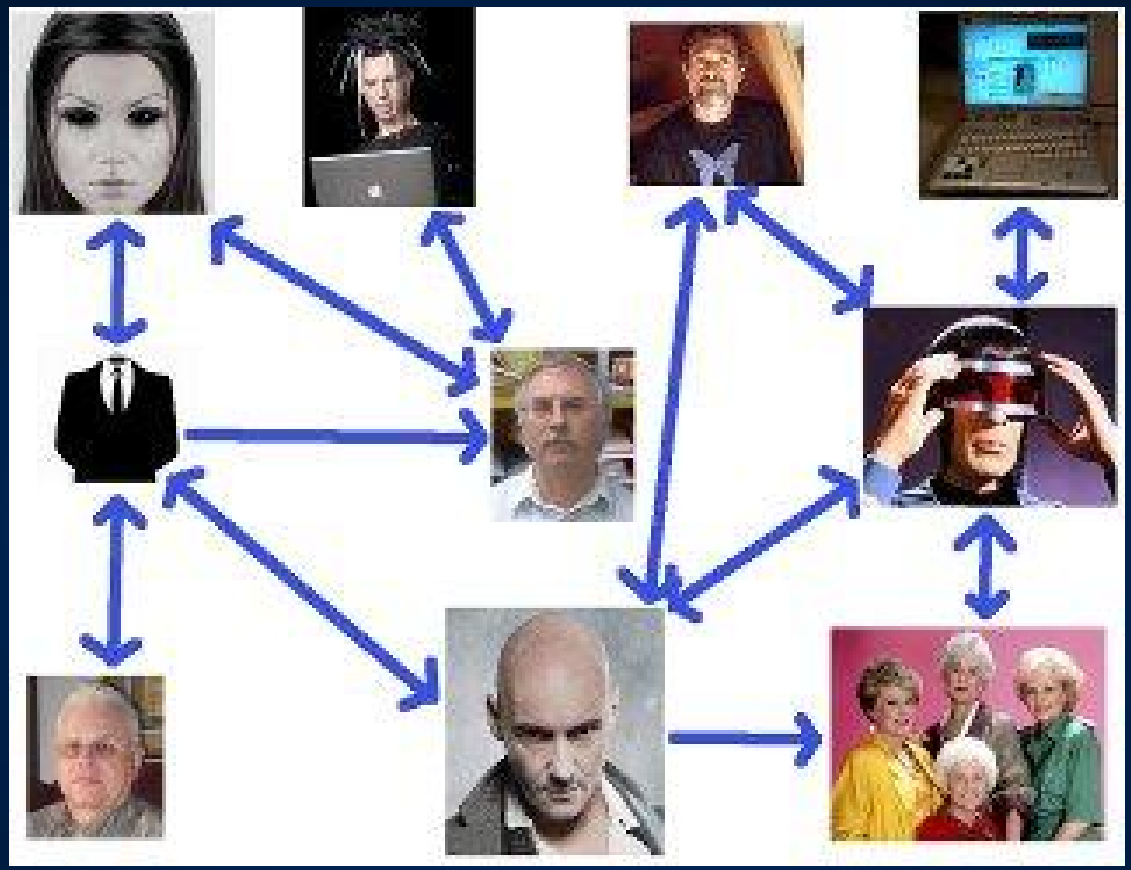


Image credits: Their respective creators.

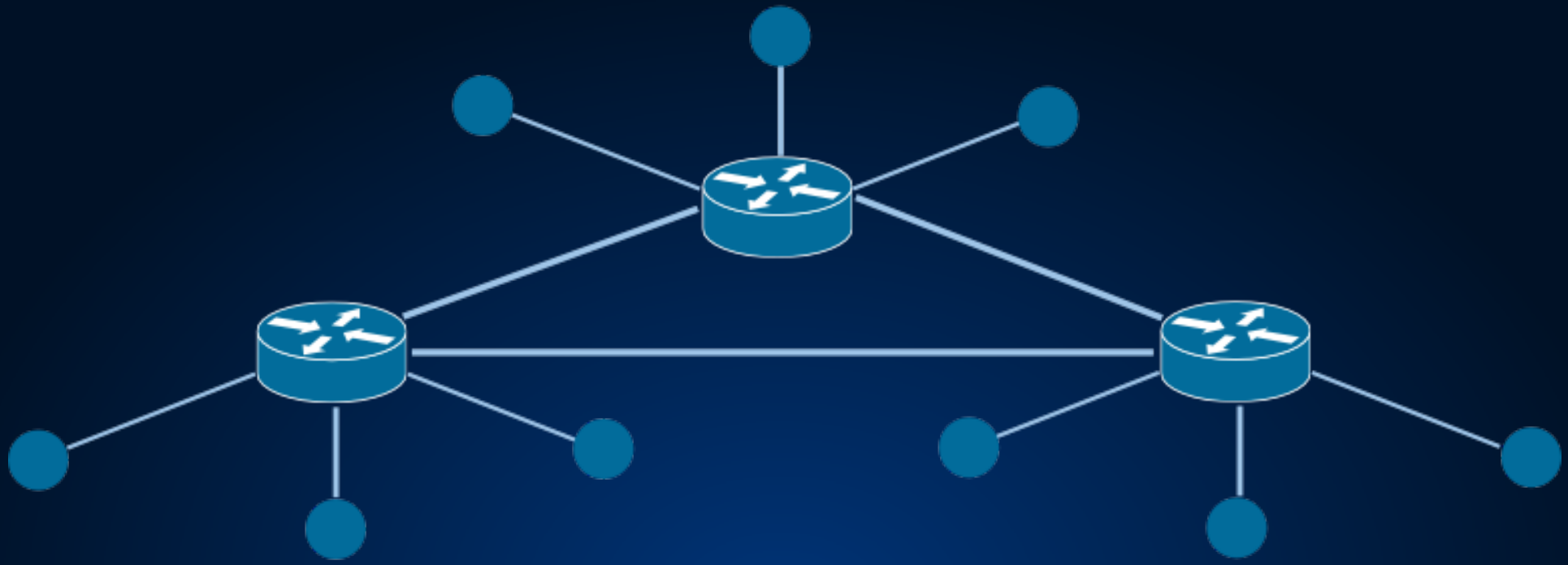
Mobile, ad-hoc wireless mesh network

But wait! Isn't the Internet a decentralized network?

Image credit: wiki.digitalmethods.net

Doesn't the Internet interpret censorship as damage and route around it?

Not really.

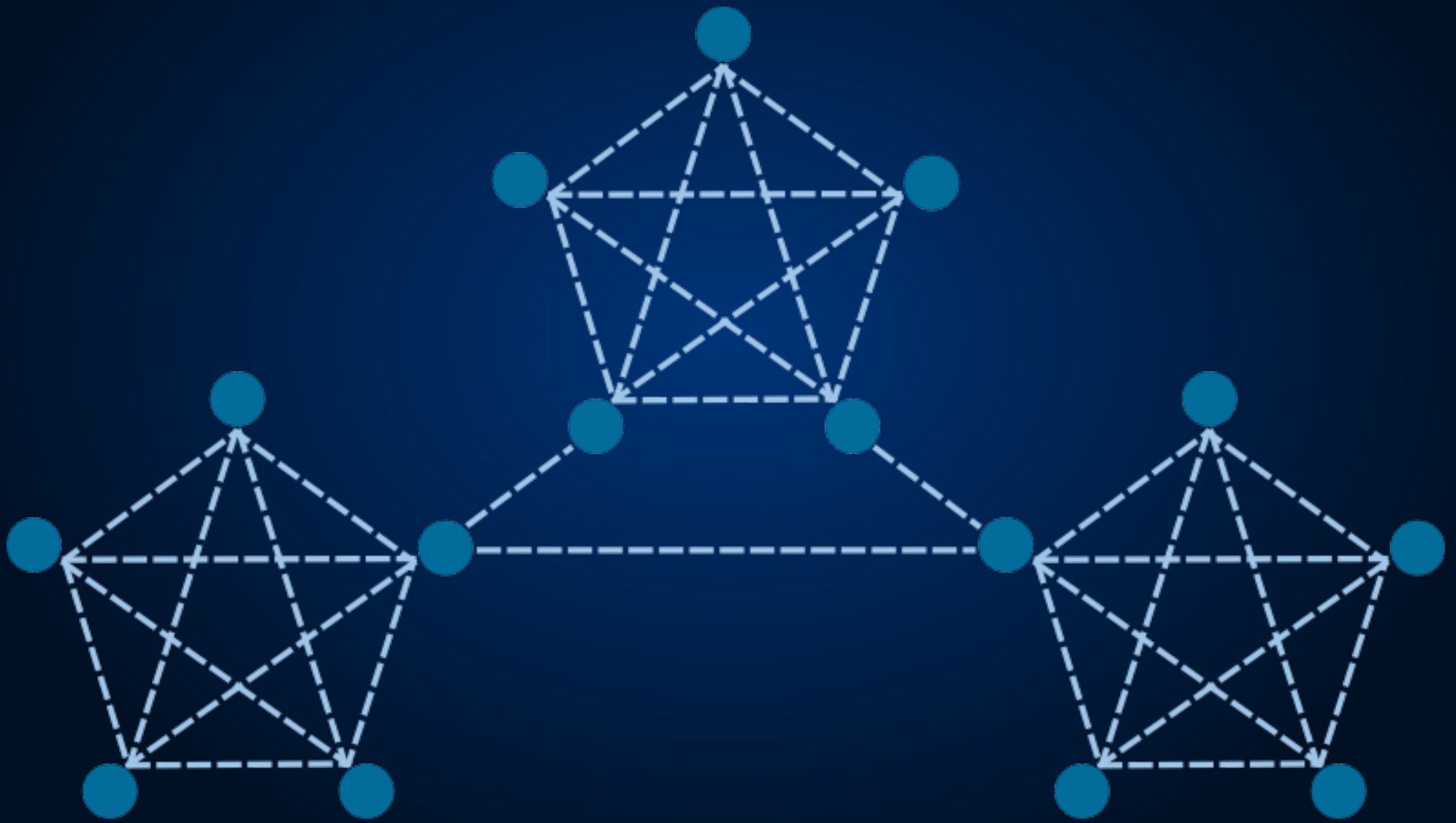


The Internet is a partial mesh. It's mostly hierarchical. Lots of networks have routers which are single points of failure.

Many networks don't have redundant links.

Just ask /San [Jose,Carlos]/ in March 2009. Also, ask any backhoe operator.

What we need is a true mesh network with multiple redundant routes between endpoints.



Ad-hoc wireless + mesh routing == Mobile ad-hoc mesh network

Image credit: freshpaint.deviantart.com
License: CC BY-NC-SA v3.0 Unported

We can already do this, but we need to make it easy.

Design Goals

- Cheap, readily available equipment (after SHTF)
- Rapidly deployable
- Extensible
- Robust and reliable
- Secure
- Low maintenance

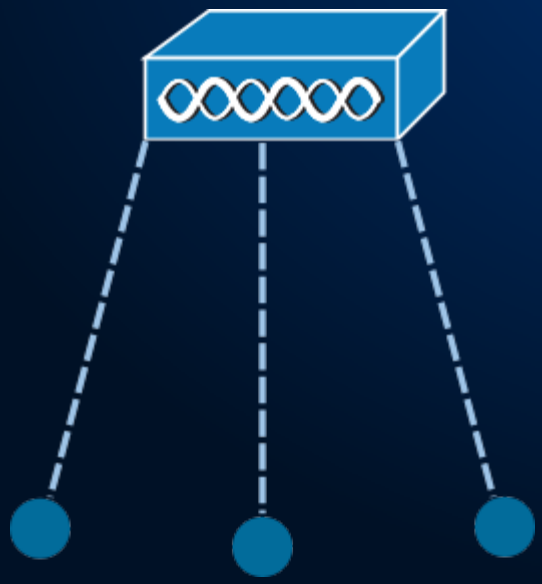
Design Constraints

- Solve Katrina first, Egypt second
- A small group of minimally skilled individuals should be able to deploy the solution
  - As easy to use as a home wireless router
- Needs to support a larger community of users
- Sufficient tools available to accomplish arbitrary tasks
- Minimal collusion required
- Not all devices on a network run mesh routing software
- Compatible with as much common* equipment as possible

* common here != common there

Ad-Hoc Networking

- Takes place at OSI layer 2
- Built into 802.11 standard
- Almost any WiFi enabled device can do it
- Requires minimal configuration
- No central AP required
- Clients communicate with one another in a peer-to-peer like fashion
- Does not implement multi-hop (aka no routing)



Mesh Routing

- Usually takes place at OSI layer 3
- Some nodes forward traffic to destination
- A number of protocols exist
  - By 'a number' we mean around 70
  - http://urlw.us/list_O_mesh_protocols
- Not all protocols
  - ...have the same features
  - ...solve the same problems
  - ...are equally efficient
- Some have serious flaws

Open 802.11s

- Software implementation of the IEEE mesh routing standard
- Built into the Linux, BSD kernels
- Meant to be implemented in wireless chipsets' firmware
- Does not require exotic userspace tools to configure
- Immature
- Not all implementations fully support the protocol
- Interoperability between soft- and hard- versions can be dodgy
- Not widely used

OLSR (Optimized Link State Routing)

- Link State Routing Protocol
- Layer 2 agnostic
- Predates 802.11
- No link-quality awareness in the standard
  - Some implementations have it
  - Experimental
- Loop detection is just now being implemented
- Very chatty - topology information flooding

BATMAN-Advanced

- Better Approach To Mobile Ad-hoc Networking
- Has link-quality awareness, loop avoidance
- Implemented as a kernel module since v2.6.38
- A result of the isolation of Egypt in February of 2011
- Provides a virtual layer 2 interface
- Very active community
- Challenging to troubleshoot
- batctl utility
  - required
  - steep learning curve
  - not packaged by many distros
- Doesn't lend itself to rapid deployment

Babel

- Distance vector routing protocol
- Uses link quality to help determine optimal routes
- Traffic density aware
- Converges rapidly
- Proactive loop avoidance (mathematically proven)
- Runs in userspace
- Manages the OS routing table
- Minimal configuration - config files are generally four lines at most

Why don't you use...

- Tor?
- CJDNS?
- I2P?
- TINC?
- Retroshare?
- Freenet?

They aren't low-level enough.

- All of those applications operate at the Transport Layer or above (OSI Layer 4).
- If you don't have the Network Layer (OSI Layer 3) or below you're still dead in the water.
- They can fail if your ISP...
  - Uses DPI to filter traffic
  - Filters ports
  - Stops routing
  - Shuts off their infrastructure
- Ad-hoc mesh networks set up an entirely separate system at the Network layer and below.

Announcing Byzantium Linux v0.2α

- LiveCD/USB distribution
- Based on Porteus Linux (http://porteus.org/)
- Utilities for live replication in the field
- Mesh routing software
- Software development/debugging tools
- Network troubleshooting/monitoring tools
- Resource hosting software - LAMP
- Web control panel for administering the node
- Proof-of-concept user services
  - IRC with web client
  - Collaborative text editor

Network configuration

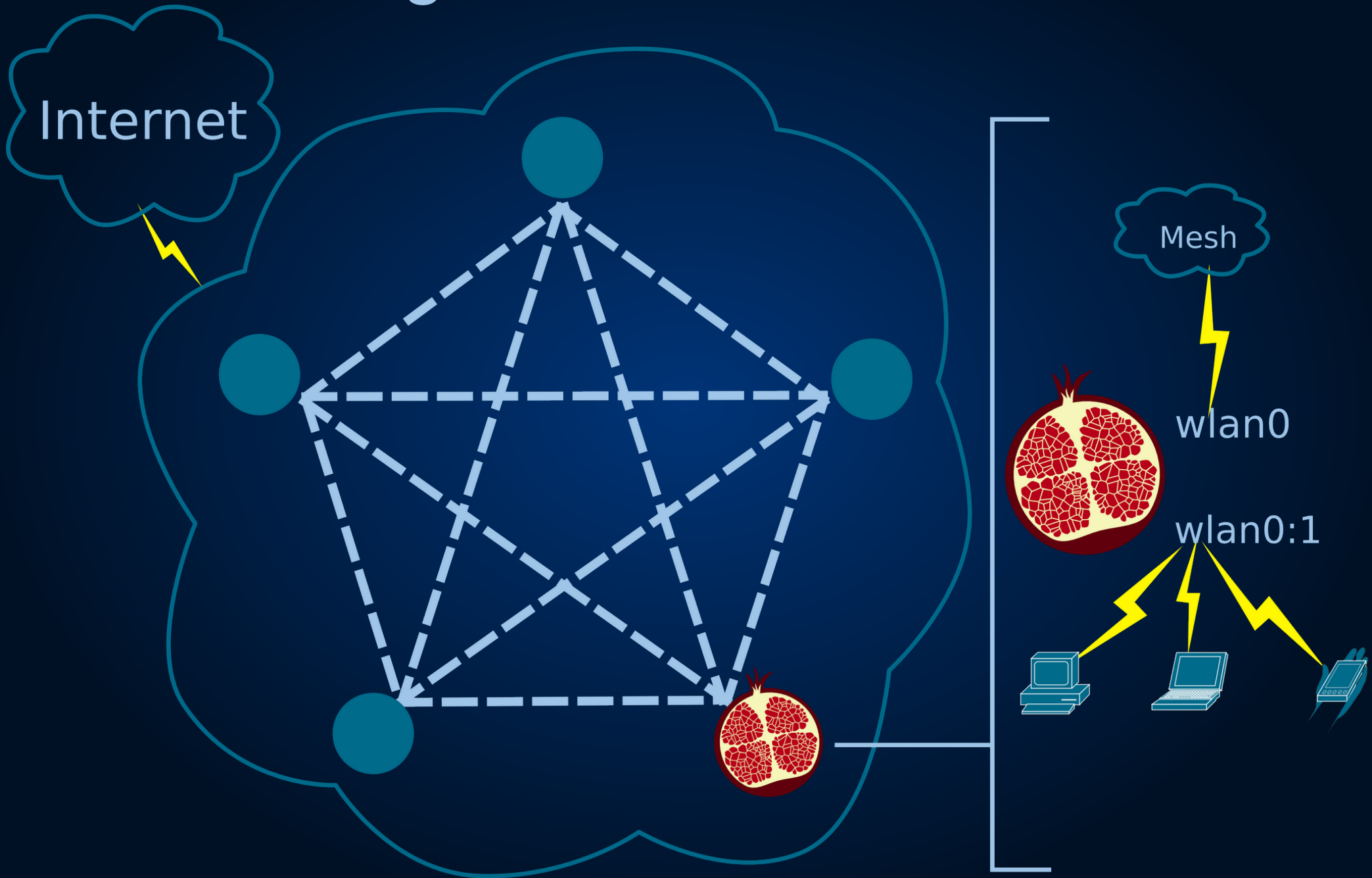
Node configuration

- Pseudo-random RFC-1918 address (192.168/16)
- arping used to detect duplicates
- Assigns address to mesh interface as a /32

Client configuration

- All clients placed in a 10/24
- DHCP and DNS with dnsmasq
- Config files generated by control panel
- Only one wi-fi interface? No problem!
  - IP alias interacts with clients – wlan0:1

Handling non-mesh client nodes



Zen of Inter-Mesh Links

- Why?
  - Connecting meshes farther apart than unaugmented Wi-Fi range (1/2 block?)
  - Can't assume consistent coverage of mesh nodes
- How?
  - Improvised parabolic or wave guide antenna
  - Tunnel through another network
    - Dialup
    - VPN
    - Packet radio
  - Sneakernet or IP over avian carrier
  - Combinations of any or all of the above
  - Solutions are likely specific to use case

Incidental use cases

- Classrooms/Conventions/Seminars
  - Captive portal
  - Host local content
  - Extend coverage
- Extending the range of a home network
  - Use a spare laptop instead of buying a second router
- Community/municipal wireless networks
  - Extend coverage at minimal cost
  - Host local content and services
  - No expensive special equipment or WISPs needed
- Guerilla wireless
  - Quick to set up and take down
  - Dynamically expandable
  - No central point of failure

Other Mesh Networking Projects

- Freifunk
  - Community wireless network in Germany
  - Uses OpenWRT routers as permanent infrastructure
- Athens Wireless Metropolitan Network
  - One of the largest active mesh networks in the world
  - Community owned infrastructure
  - Opt-in network, governed by consensus
- Commotion Wireless
  - Product of The New America Foundation's Open Technology Institute
  - Aimed at community/municipal wireless networks
  - Requires exotic routers which become permanent infrastructure
- FreedomBox
  - Focused on protecting privacy and federation of public services
  - Mesh networking as a way to avoid surveillance and censorship
- ReseauLibre
  - Community network inspired by Freifunk
  - Developed by Foulab in Montreal

Potential Threats

- No central authority means anyone can add nodes to the mesh
- Lots of distributed services don't encrypt federation traffic
  - Mitigated by opportunistic IPsec?
- Mesh routing protocols suffer from route injection attacks
  - Babel is implementing cryptographic authentication of routes
  - Non-advantageous routes probably won't be used
- Wireless jamming
  - Every wireless net is vulnerable to this
  - Nodes jump channel
  - BBRS

Middle Eastern Threats

- Egypt: No routing tables == no traffic
  - No ISP infrastructure == not a problem
- Syria: ISPs lose power (Homs)
  - Independent equipment, power supplies
- Syria: Military wardriving for open access points (Homs)
  - Ad-hoc nodes seem to slip under their radar
    - Might not in the future
  - Ad-hoc networks dependent on BSSID not ESSID
- Social engineering attacks to gather intel
  - Warn people to not give away sensitive info
  - OPSEC training (beforehand preferably)
- OSINT surveillance of public sites
  - Byzantium resources don't touch the public Net

Potential threats in other countries

- Social engineering attacks and infiltrators
  - OPSEC warning, training
- Passive surveillance
  - Encryption of traffic between nodes
  - Encryption of client traffic
- Active surveillance
  - OPSEC
  - Fluidity of network architecture
  - Avoids DPI equipment
- Seizure of nodes
  - No persistent storage by default
  - Support for encrypted storage
  - Relatively innocuous or even covert equipment
- Subpoena of service provider
  - No service provider to contact
  - Difficulty locating node(s) running services

What we need

- More developers
  - Python
    - Knowledge of i18n and DBus
  - Admin-type shell scripting
  - User interface design (HTML/CSS)
- People testing Byzantium
  - Stress- and otherwise
  - Bug reports
  - Patches!
- Translators/Editors
  - User interface
  - Documentation
    - System
    - Pre/Post-Emergency Literature
- Suggestions

Comments? Questions? Suggestions?

How to contact us:

Mailing list: byzantium+subscribe@hacdc.org
Freenode IRC network: #byzantium
Twitter: #projectbyzantium
Github: https://github.com/Byzantium