

Ad-Hoc IP Networking

A Case Study using the Dirty 30 Race

Willem Schreüder, AC0KQ

Chris Hamilton, AE5IT

John Maxwell, W0VG

RMHAM University

November 17, 2018

Outline

Why IP?

The history of the Dirty 30

Available IP technologies

Designing and Planning

Deployment and Execution

Summary

Why IP?

IP is a disruptive technology

Served agencies like IP transparency

- Email

- VoIP and Cell phone

- Video

We like IP transparency

- Linking repeaters

- Data transfer

- Control

Challenges

Practical use require speed (bandwidth)

Bandwidth implies UHF-SHF frequencies

UHF-SHF means line of sight

Mountainous terrain means no line of sight

No plug-and-play operation

Need to plan, deploy and test beforehand

Solutions

IP supports flexible networking

- Redundancy

- Configurability

Point-to-point microwave has high throughput

- Light weight

- Low power

- High gain

- Reasonable cost

Case Study: Dirty30

Ultra-marathon (30 miles/50 km)

7250 feet elevation change

Most trails not vehicle accessible

400+ runners

Golden Gate State Park

Mountainous 7,500' to 10,500'

Considerations

Tracking hundreds of runners is critical

- Accurately recording bibs

- May have dozens of runners per minute

- Finding lost runners is difficult

- Consequences of a lost runner are serious

Communications are difficult

- No cell service

- VHF radio works well

- Aid stations are in valleys

- Mountains everywhere



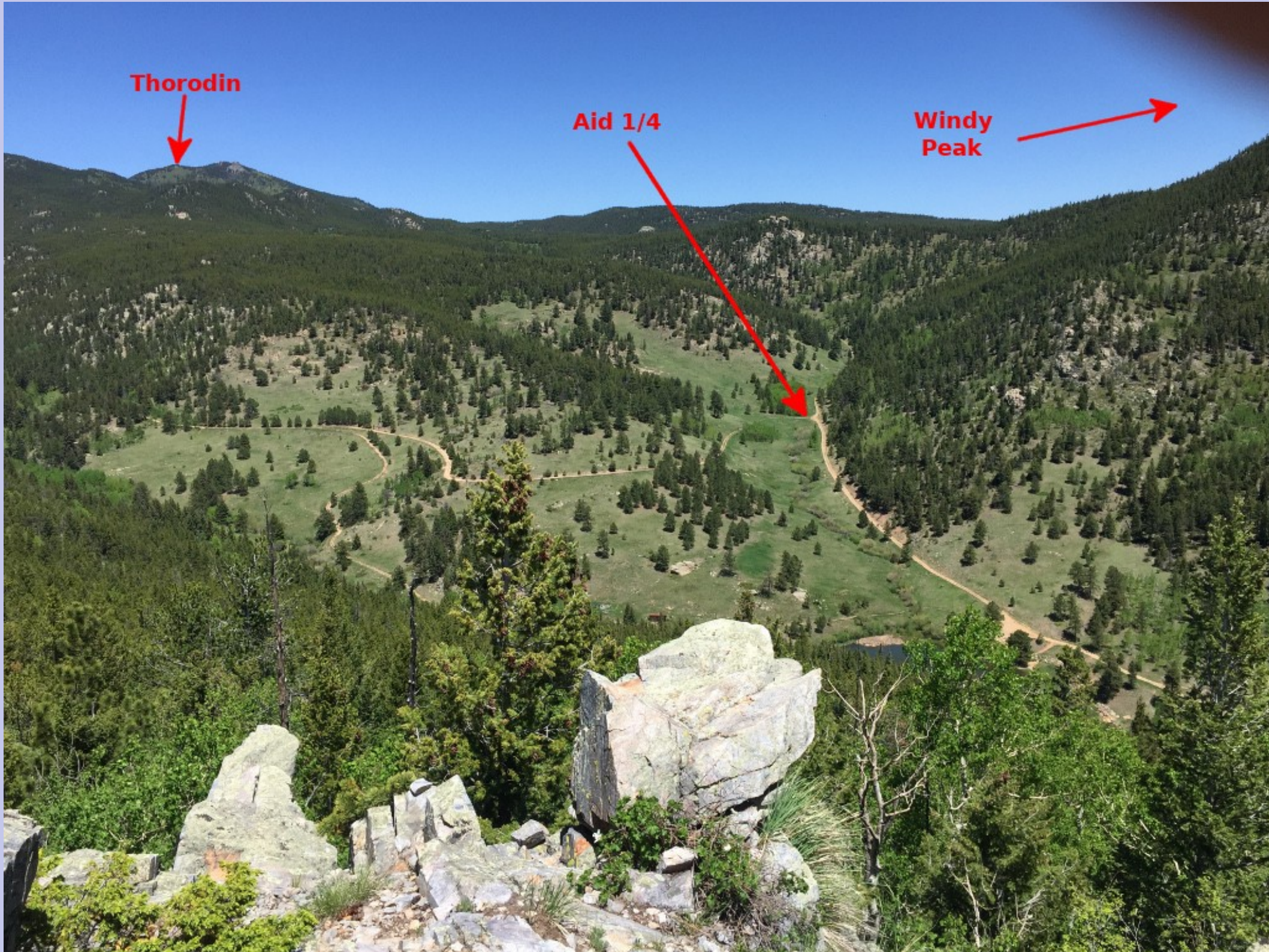
Thorodin



Aid 1/4



**Windy
Peak**



Dirty30 2014

100 runners

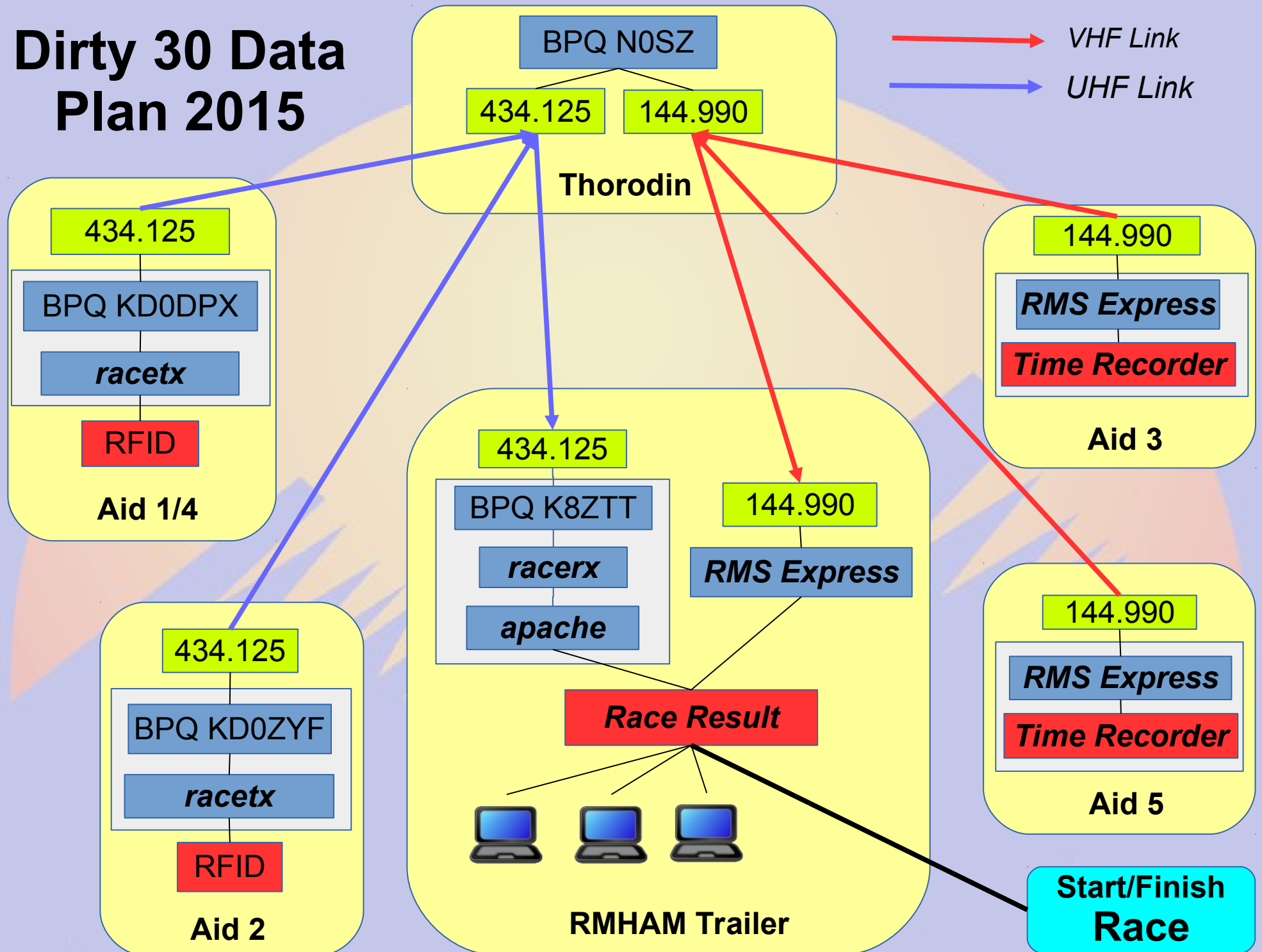
Record bibs by hand

Packet from aid stations to start/finish

Aid 1/4 BPQ relay

6 hams

Dirty 30 Data Plan 2015



Dirty30 2016

Self contained data radios

300 runners

RFID at Aid 1/4, 2, 3 and Windy

Problems

Encrypted bibs

Data radio failures

Insufficient training

Dirty30 2017

First use of microwave

350 runners

RFID at Aid 1/4, 2, 3 and Windy

Problems

Wind blowing antennas out of alignment

Lack of coordination

Windy Peak



Dirty30 2018

Success with microwave

- 400 runners

- RFID at all aid stations and Windy

- Redundant satellite and microwave

- WiFi at Start/Finish

Problems

- Two day event

City Lights

High Gain
Tremont Peak

Sector Antenna
Aid 1/4
Aid 5
Windy Peak
Start/Finish



Secrets to Success

Planning

Months of mapping

Weeks of configuration

Days of deployment

Hours of enjoyment

Lots of help

Training session



What never works

Expecting plug-and-play

People showing up unprepared

Hardware not tested

Unfamiliar with software

Unclear objectives

Remember the seven Ps

RFID for Tracking

Reliably reads bibs

Hand entry approximately 1% error

Can read clumps of runners

Must still be visually checked

Folded bibs, water bottles

Keeps people occupied, fail safe

Still the best available technology

Crucial due to size and difficulty of event

RaceRite

Well built

Self contained

Battery

AC power

DC power

Web interface

Reliable



Surprises

Mountain top noise in ISM band

Effect of wind on tree mounts

Difficulty in locating peaks/sites

Time it takes to deploy

Overall complexity

Other things considered

BBHN/AREDN mesh

Balloon/drone mounted microwave

900MHz data radios

DMR Data

VHF APRS with custom data protocol

Satellite modems

Available Technology

Our weapon of choice is Mikrotik product due to configurability and flexibility. Each device has its use.



LHG
Light Head
Grid 0-10 mi



Dish &
Netmetal
10-50mi



MANTbox
0-20 miles



QRT Panel
0-15 miles

Available Technology

Our weapon of choice is Mikrotik product due to configurability and flexibility. Each device has its use.



The LHG “Light Head Grid” is used for medium distance shots, has dual chain “MIMO” radios. They are very light and transport well where weight is a concern.

International versions will do 5650-5925 out of the box with Superchannel selection.

Cost is about \$50.00 each.

Available Technology

Our weapon of choice is Mikrotik product due to configurability and flexibility. Each device has its use.



For longer distance shots we use MIMO radios called “Netmetal 5” 2W International radios with 2’ 30dBi dishes.

The distances achieved with this is easily 50 miles with a -68 signal.

Dishes are \$150-250

Netmetal 5 2xMiMo International \$130

Available Technology

Our weapon of choice is Mikrotik product due to configurability and flexibility. Each device has its use.



For point-to-multipoint applications, we use the International version of the MantBox. They make these units in 15dBi and 19dBi versions. This unit is the 15dBi.

Can do 10 miles with an LHG and a MantBox in point to multipoint configurations.

Cost is about \$115.00 for the international version.

Available Technology

Our weapon of choice is Mikrotik product due to configurability and flexibility. Each device has its use.



The QRT Panel is used for shorter distance than the LHG, LHG-XL or Dish. It can be used like all Mikrotik product for Point-To-Point or Point-To-Multipoint to provide flexibility. Nice looking, and robust.

Panel can be used out to 8-10 miles on a point to multipoint or 10-15 miles point to point.

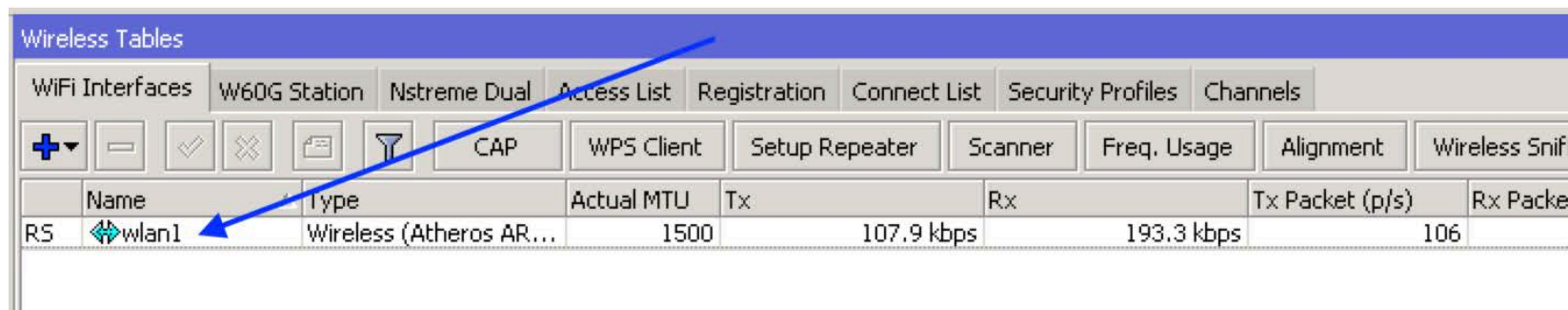
\$120.00-160.00

Configuration

- ◆ Superchannel configuration is used to allow the radio transmitter to work outside of the normal frequencies.
- ◆ These radios can be set up to operate from 5650-5925 which is the ham band.
- ◆ Ultimate flexibility paves the road to futility. Be careful! Remember your band edges and channel width. 20MHz channel at 5650MHz would put your low skirt at 5640!

Configuration

Under Wireless, Double Click the line that shows wlan1 which will bring you to the actual configuration screen.



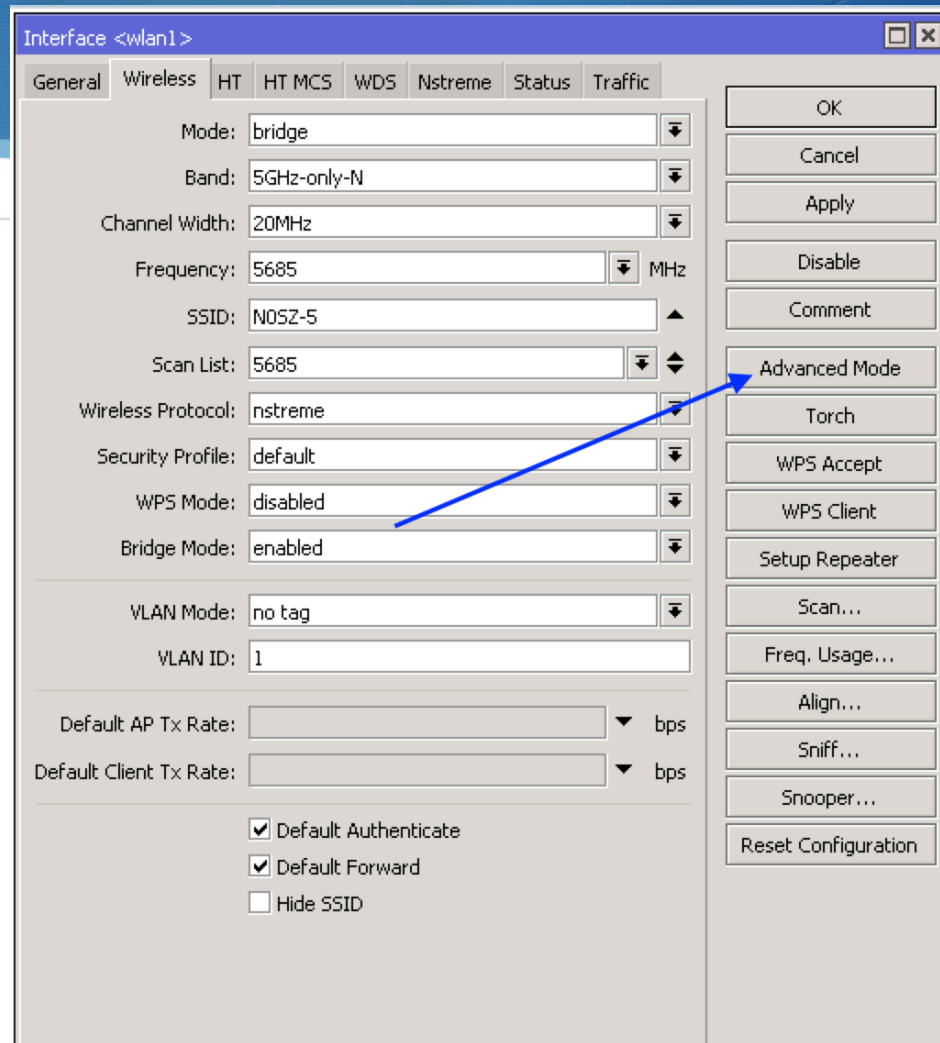
The screenshot shows a window titled "Wireless Tables" with a tabbed interface. The "WiFi Interfaces" tab is selected. Below the tabs is a toolbar with various icons. A table displays the following data:

| | Name | Type | Actual MTU | Tx | Rx | Tx Packet (p/s) | Rx Packe |
|----|-------|-------------------------|------------|------------|------------|-----------------|----------|
| RS | wlan1 | Wireless (Atheros AR... | 1500 | 107.9 kbps | 193.3 kbps | 106 | |

Configuration

Click on Advanced Mode to be able to access the “Superchannel” option

This does require an international radio in order to get this option!



Interface <wlan1>

General Wireless HT HT MCS WDS Nstreme Status Traffic

Mode: bridge

Band: 5GHz-only-N

Channel Width: 20MHz

Frequency: 5685 MHz

SSID: N0SZ-5

Scan List: 5685

Wireless Protocol: nstreme

Security Profile: default

WPS Mode: disabled

Bridge Mode: enabled

VLAN Mode: no tag

VLAN ID: 1

Default AP Tx Rate: bps

Default Client Tx Rate: bps

☒ Default Authenticate

☒ Default Forward

☐ Hide SSID

OK

Cancel

Apply

Disable

Comment

Advanced Mode

Torch

WPS Accept

WPS Client

Setup Repeater

Scan...

Freq. Usage...

Align...

Sniff...

Snooper...

Reset Configuration

Basic Wireless Configuration

Interface <wlan1>

General Wireless Data Rates Advanced HT HT MCS WDS ...

Mode: bridge

Band: 5GHz-only-N

Channel Width: 20MHz

Frequency: 5685 MHz

SSID: N05Z-5

Radio Name: 000C42942621

Scan List: 5685

Wireless Protocol: nstreme

Security Profile: default

WPS Mode: disabled

Frequency Mode: superchannel

Country: no_country_set

Antenna Gain: 0

Bridge Mode: enabled

VLAN Mode: no tag

VLAN ID: 1

Default AP Tx Rate: bps

Default Client Tx Rate: bps

☒ Default Authenticate

☒ Default Forward

☐ Hide SSID

Multicast Helper: default

☒ Multicast Buffering

☒ Keepalive Frames

OK Cancel Apply Disable Comment Simple Mode Torch WPS Reset WPS Client Setup Repeater Scan... Freq. Usage... Align... Sniff... Snooper... Reset Configuration

enabled running slave running ap

Mode changes depending on function

Band is freq and modulation type

Channel width generally is 20mhz

Frequency is "center" of channel

SSID Required to match each end! Use
callsign on ham.

Scan List is required for station!

Wireless Protocol nstreme best for distance

Security profile is encryp. (NOT ON HAM)

Freq Mode "Superchannel" allow out of band.
This function is not available in NON-INTL
radios. You must use international radios in
order to get out of band functions!

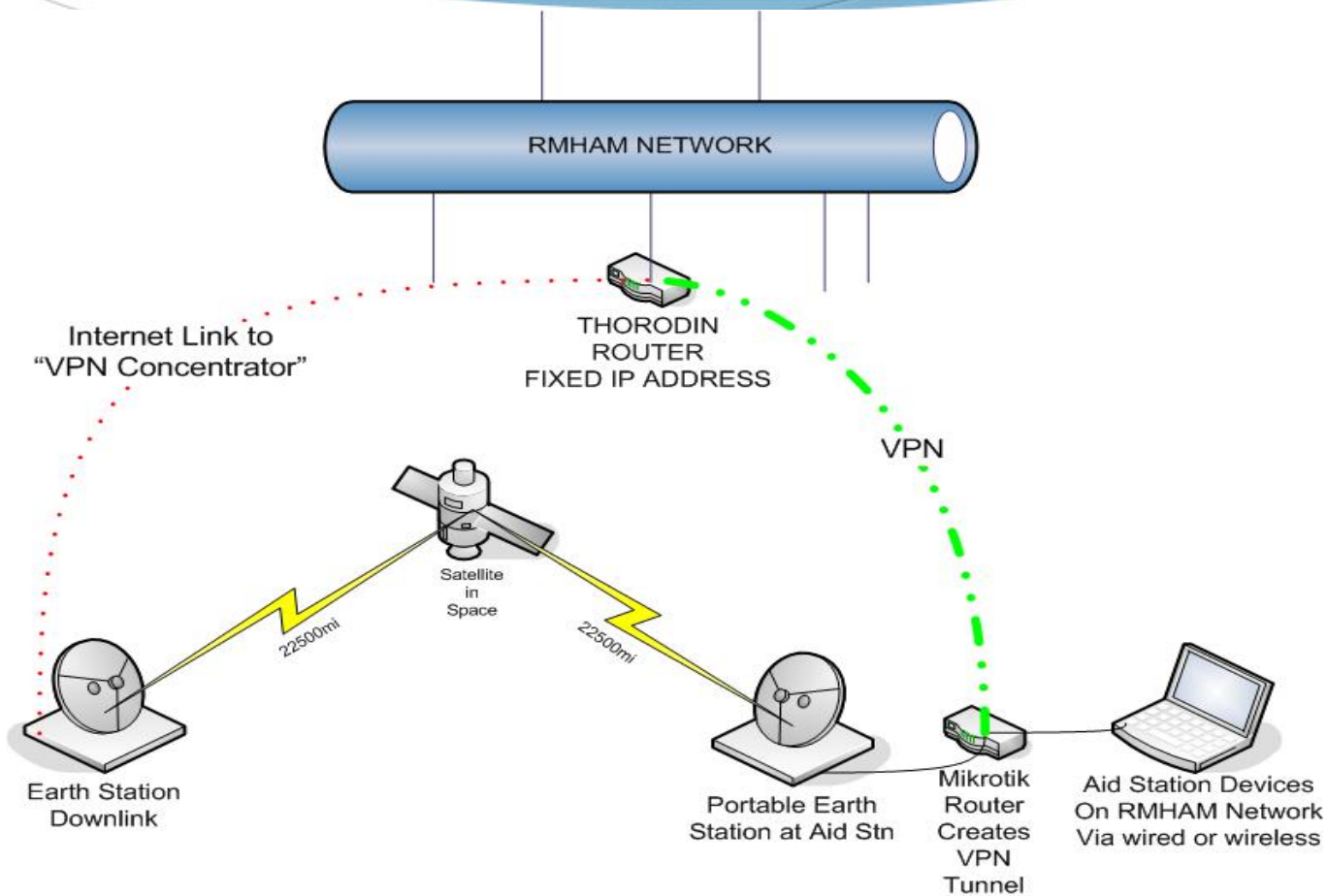
Satellite Integration

- ◆ There are some places that you CANNOT use line of sight devices and higher bandwidth is not available.
- ◆ Geosynchronous satellites may be needed. Ping times of 600-700ms. If you need low latency, don't use satellite!
- ◆ Satellite service will get you 15+mbps down and 2-4mbps up
- ◆ VPN would be required to connect you to a terrestrial network like the RMHAM network.

VPN

- 💧 VPN is a protocol to extend a remote IP network securely through certain protocols over an IP tunnel.
- 💧 PPTP, SSTP, L2TP, OpenVPN
- 💧 Mikrotik supports all of these protocols out-of-the-box and more.
- 💧 Static IP address is required for at least one endpoint connectivity or tears and brain damage will be involved!

VPN



Commercial Cellular Options

- ◆ Cradlepoint/Pepwave units are good for areas that have cellular/LTE service to create a solid network link. 10-50ms
Price is anywhere from \$150-\$600 depending on models.
There are options for any carrier.

Click to close image, click and drag to move. Use arrow keys for next and previous.



Click to close image, click and drag to move

Wireless ISP Options

- 💧 Wireless ISPs provide a good service that will give you reliable internet and may likely be in your area. They use 5.8GHz and 2.4GHz wireless service to provide internet to many locations.
- 💧 They use “point to multipoint” hardware from manufacturers like Mikrotik or Ubiquiti hardware to create a network.
- 💧 We use Mountain Broadband in the Golden Gate Canyon area to feed the network and create our internet tunnel at Aid 2 and backfeed commercial internet to the aid stations via Tremont.
- 💧 Most terrestrial ping times are from 1ms-30ms.
- 💧 This is a prime example of “Learn Your Course!”

Freewave 900mhz NLOS

Freewave is a 900MHz Near-Line-Of-Sight option for ethernet and serial connectivity at 128kbps. Many ethernet and serial radios are available on Ebay CHEAP.

Requires high gain antennas

Requires 12v external power

Only 128kbps. VERY SLOW.

Don't allow browsing and turn off automatic updates!!



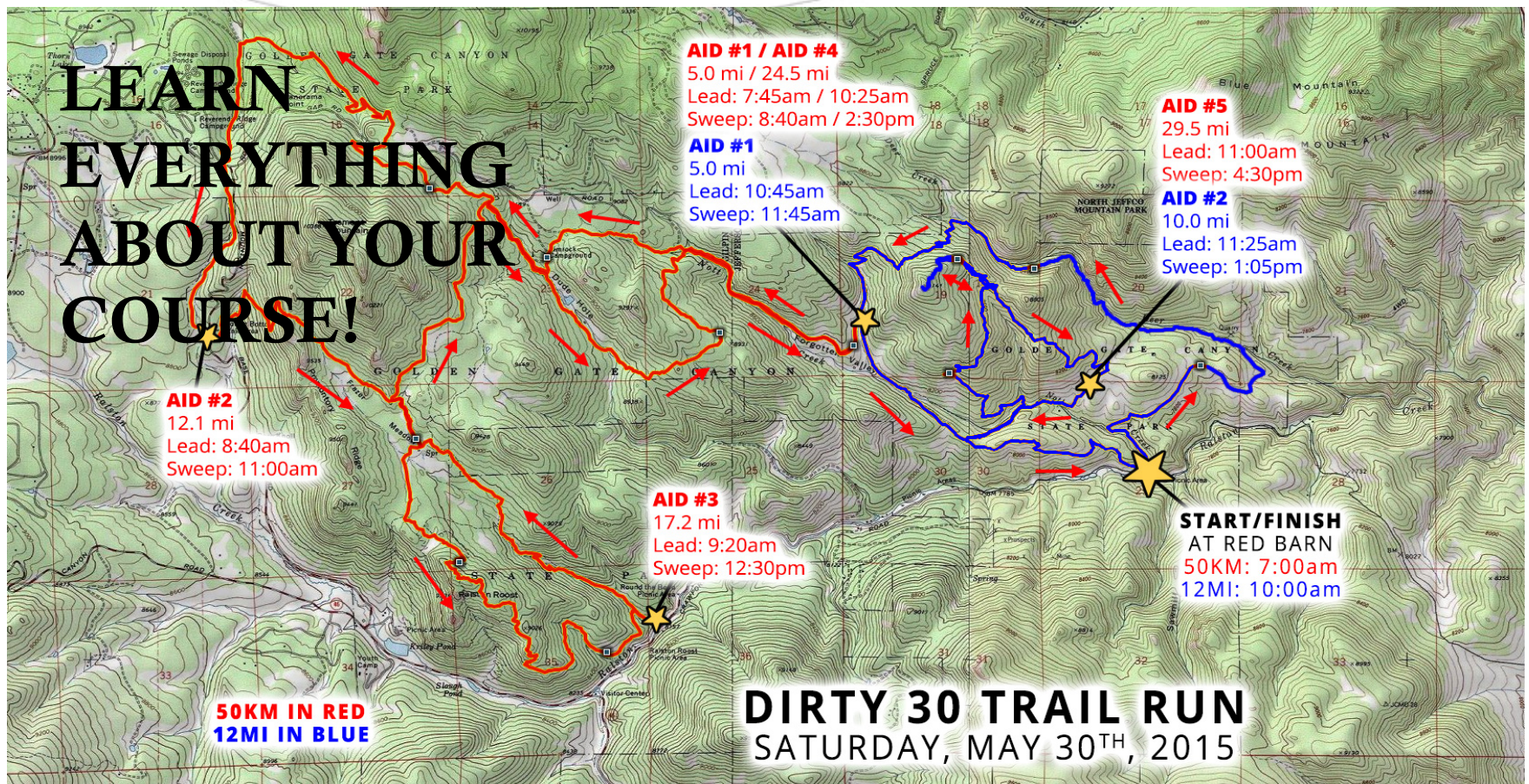
Power Budget and Weight

- Remote locations have a finite lifetime
- Each Mikrotik draws 60mA at 24V and 120mA at 12V
- Two devices is 240mA at 24V
- Event lasts two full days, plus time to get the devices in place. 240ma over 60 hours is 14400mAh or 14.4 amp hours at 24V or two 10AH 12V batteries in series. HEAVY.
- Your pack is going to be miserable to hike with.

Power Budget and Weight

- 💧 Mikrotik has a wide power input. 8-36 volt DC input allows many options for powering your devices.
- 💧 Two batteries in parallel put out 12V at double the amperage
- 💧 Two batteries in series put out 24V at the same amperage but the efficiency of the devices is a bit better and will run a bit longer.
- 💧 Some thought needs to be there about what power is required.

Design and Planning

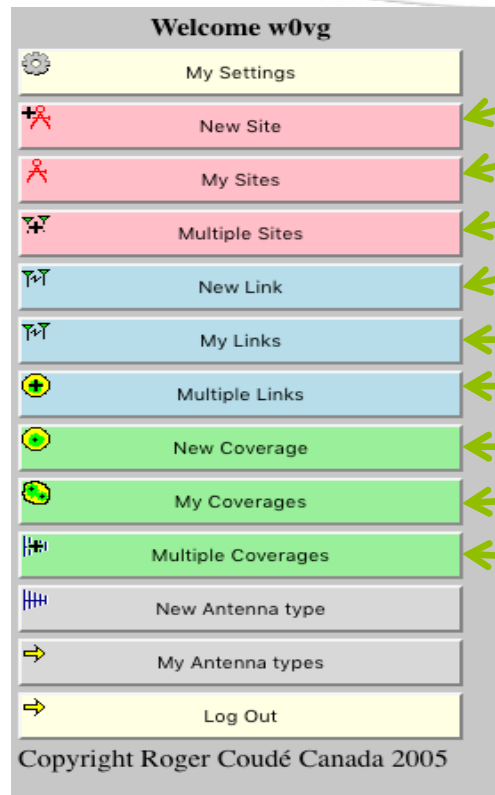


Design and Planning

The tool we use:

- ◆ Radio Mobile Online by VE2DBE
- ◆ <http://www.ve2dbe.com/rmonline.html>
- ◆ Great path design, propagation design and handles multiple sites! Works only on Ham Band frequencies as they sell a commercial package to ISPs.

Design and Planning



- ← Add site FIRST here
- ← Edit your sites here
- ← See multiple sites on map
- ← Add a new link here (requires two sites!)
- ← Edit your existing links
- ← View Multiple Links
- ← Add new coverage (add site first!)
- ← View and edit coverages
- ← Show multiple coverages at the same time

Design and Planning



The screenshot shows the 'Radio Mobile' application window with a 'New Site' dialog box open. The dialog box contains the following fields and controls:

- Locate**: A button at the top of the dialog.
- Latitude**: A text input field containing '39.90973623'.
- Longitude**: A text input field containing '-105.46875000'.
- Zoom**: A text input field containing '2'.
- Name**: A text input field containing 'Test Site'.
- Elevation (m)**: A text input field containing '2608.0'.
- Description**: An empty text input field.
- Group**: An empty text input field.
- Add to My Sites**: A button at the bottom of the dialog.
- Cancel**: A button at the bottom left of the dialog.

We use Radio Mobile Online to do our point-to-point calculations. This will be a quick-step-through as to how to add a site, and create a point-to-point calculation.

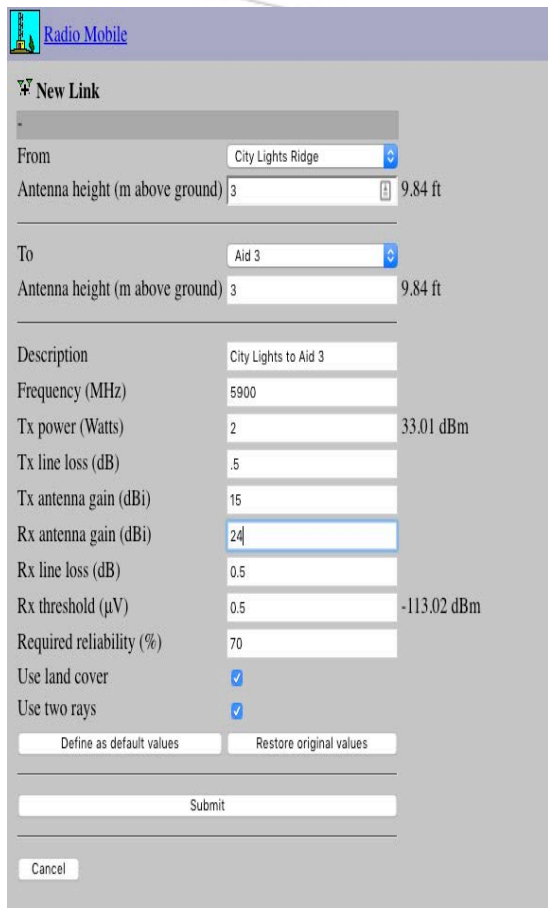
Click New Site, then drag the map pointer close to where it needs to be. Submit.

This window will pop up. You may change Lat/Lon at this point, and then you **MUST** name it.

Then click to “Add to My Sites”

This will create a usable endpoint. Create a separate second site to do point-to-point.

Design and Planning



Radio Mobile

New Link

From: City Lights Ridge

Antenna height (m above ground): 3 9.84 ft

To: Aid 3

Antenna height (m above ground): 3 9.84 ft

Description: City Lights to Aid 3

Frequency (MHz): 5900

Tx power (Watts): 2 33.01 dBm

Tx line loss (dB): .5

Tx antenna gain (dBi): 15

Rx antenna gain (dBi): 24

Rx line loss (dB): 0.5

Rx threshold (µV): 0.5 -113.02 dBm

Required reliability (%): 70

Use land cover: ☒

Use two rays: ☒

Define as default values Restore original values

Submit

Cancel

In the list, now click on New Link. This menu will come up.

Choose the first site in From and tell the program antenna height in METERS!!!

Choose the second site in To and tell the program the receive site antenna height in METERS.

Name the site under Description

Design and Planning

Radio Mobile

New Link

From: City Lights Ridge

Antenna height (m above ground): 3 (9.84 ft)

To: Aid 3

Antenna height (m above ground): 3 (9.84 ft)

Description: City Lights to Aid 3

Frequency (MHz): 5900

Tx power (Watts): 2 (33.01 dBm)

Tx line loss (dB): .5

Tx antenna gain (dBi): 15

Rx antenna gain (dBi): 24

Rx line loss (dB): 0.5

Rx threshold (uV): 0.5 (-113.02 dBm)

Required reliability (%): 70

Use land cover: ☒

Use two rays: ☒

Define as default values | Restore original values

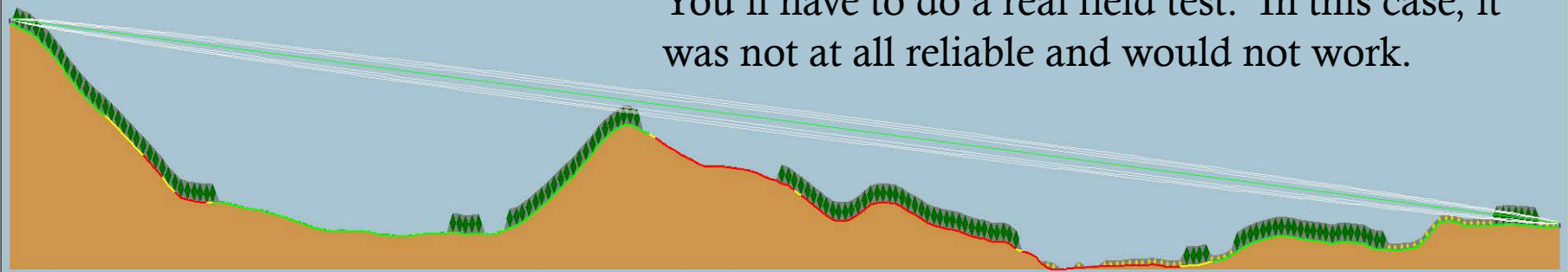
Submit

Cancel

- In Frequency, you should put a ham-band frequency in this box in MHz. 5900 is 5.9GHz.
- TX Power in Watts 30dBm=1W
- TX Line Loss in dB (actual line loss on TX side)
- TX Antenna Gain (actual antenna gain of TX Site)
- RX Antenna Gain (actual antenna gain of RX Site)
- RX Line Loss in dB (actual line loss on the RX side)
- Receiver threshold in uV can be found on the specific radio cut sheet. Most radios are -90ish in this realm
- Choose use land cover (trees) and Use two rays.
- Click Submit and the program will whirl and spin for a while.

Design and Planning

This is a grazing path and may or may not work. You'll have to do a real field test. In this case, it was not at all reliable and would not work.



City Lights to Aid 3

[City Lights Ridge \(1\)](#)

| | |
|------------------|-------------------------|
| Latitude | 39.851891 ° |
| Longitude | -105.385301 ° |
| Ground elevation | 2647.9 m |
| Antenna height | 3.0 m |
| Azimuth | 223.78 TN 215.72 MG ° |
| Tilt | -3.74 ° |

(2) [Aid 3](#)

| | |
|------------------|-----------------------|
| Latitude | 39.835984 ° |
| Longitude | -105.405151 ° |
| Ground elevation | 2488.3 m |
| Antenna height | 3.0 m |
| Azimuth | 43.77 TN 35.70 MG ° |
| Tilt | 3.72 ° |

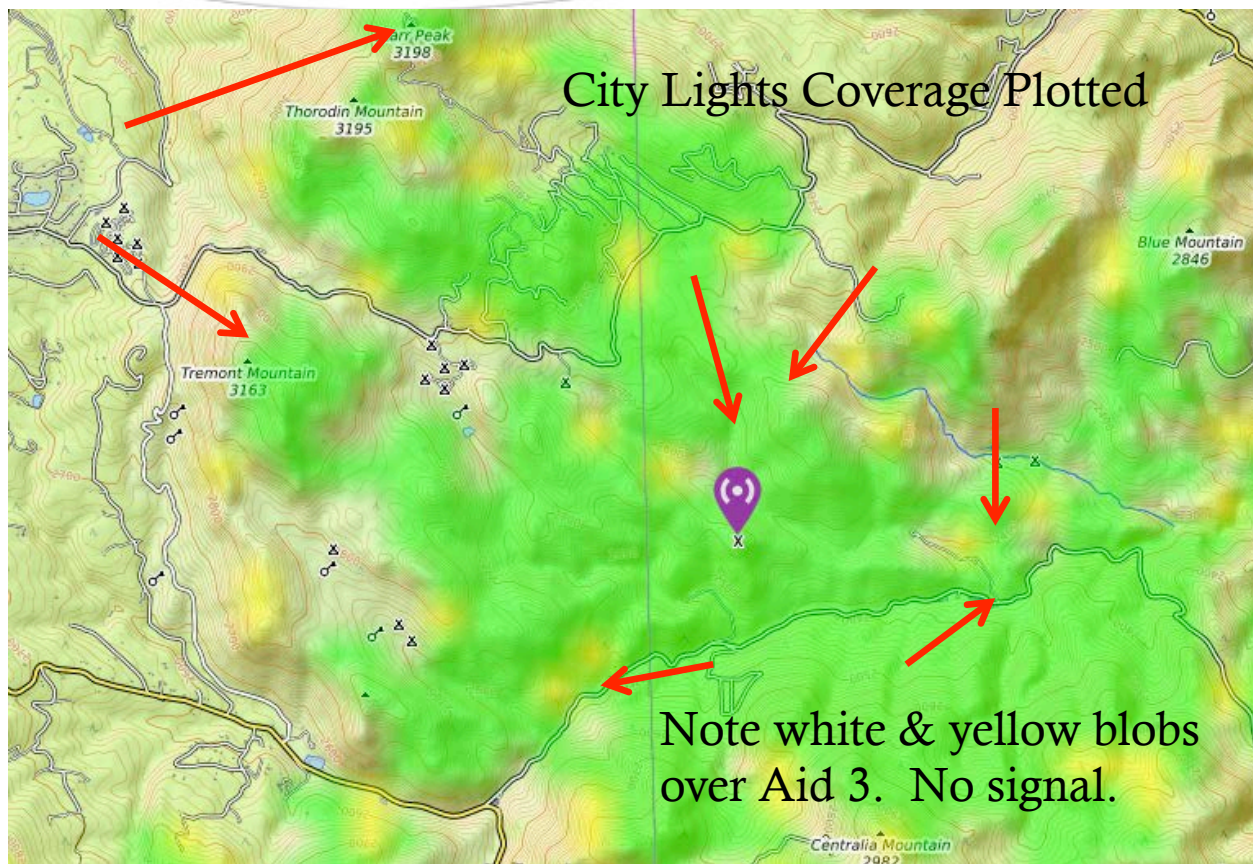
Radio system

| | |
|-----------------|-------------|
| TX power | 33.01 dBm |
| TX line loss | 0.50 dB |
| TX antenna gain | 15.00 dBi |
| RX antenna gain | 24.00 dBi |
| RX line loss | 0.50 dB |
| RX sensitivity | -113.02 dBm |

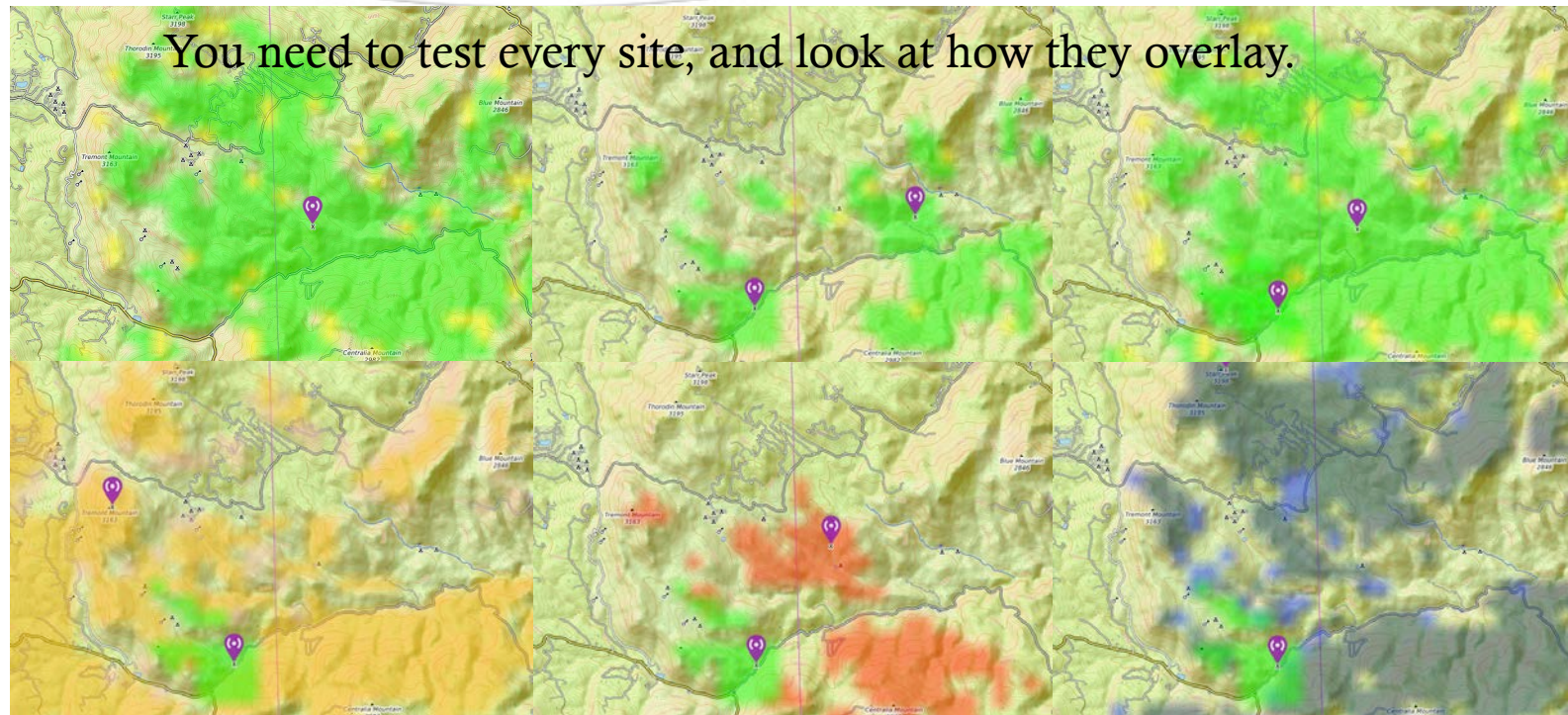
Propagation

| | |
|------------------|-----------|
| Free space loss | 115.62 dB |
| Obstruction loss | 9.86 dB |
| Forest loss | 4.06 dB |
| Urban loss | 0.00 dB |
| Statistical loss | 6.69 dB |
| Total path loss | 136.23 dB |

Design and Planning



Lather, Rinse and Repeat

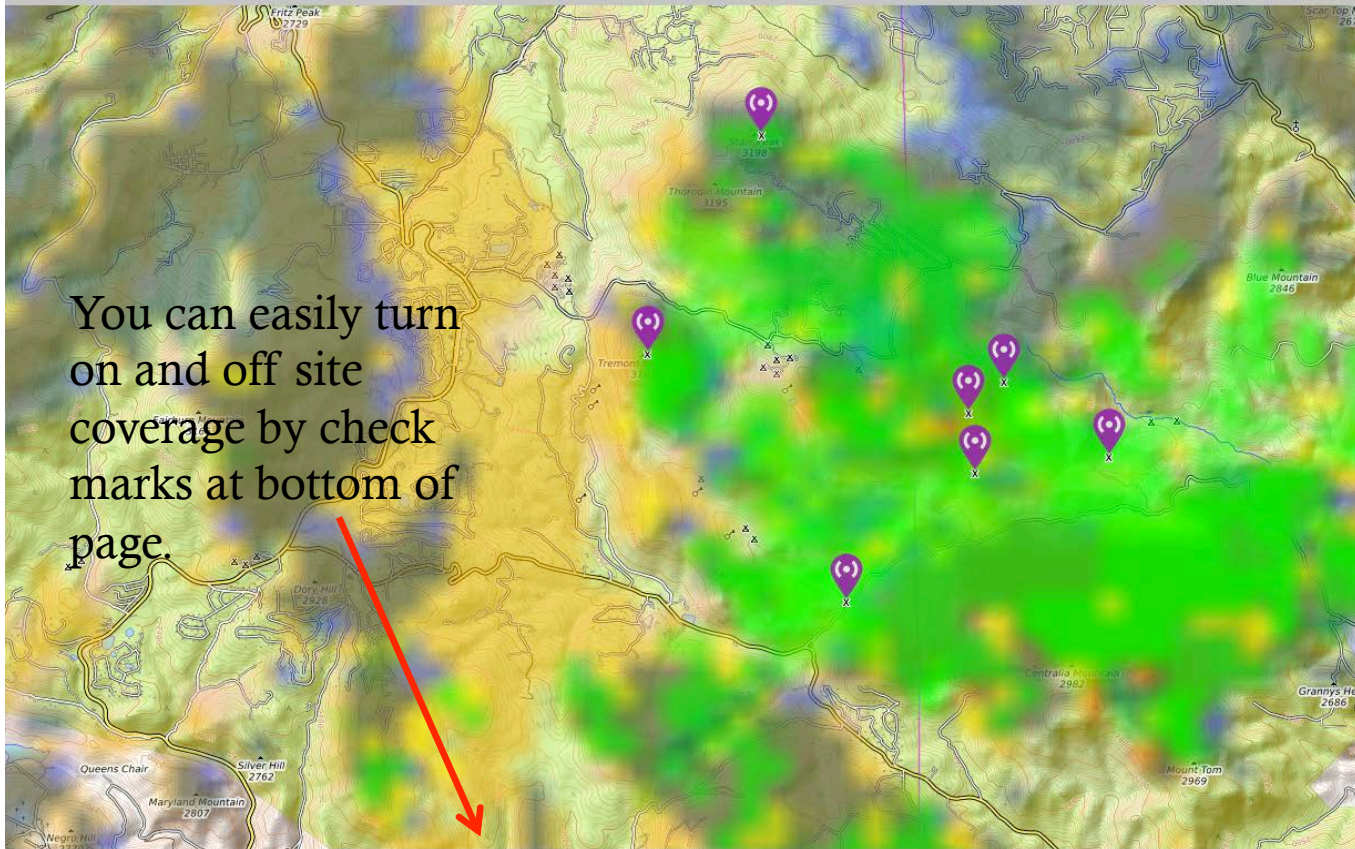


Editing Coverage Map Content

Radio Mobile

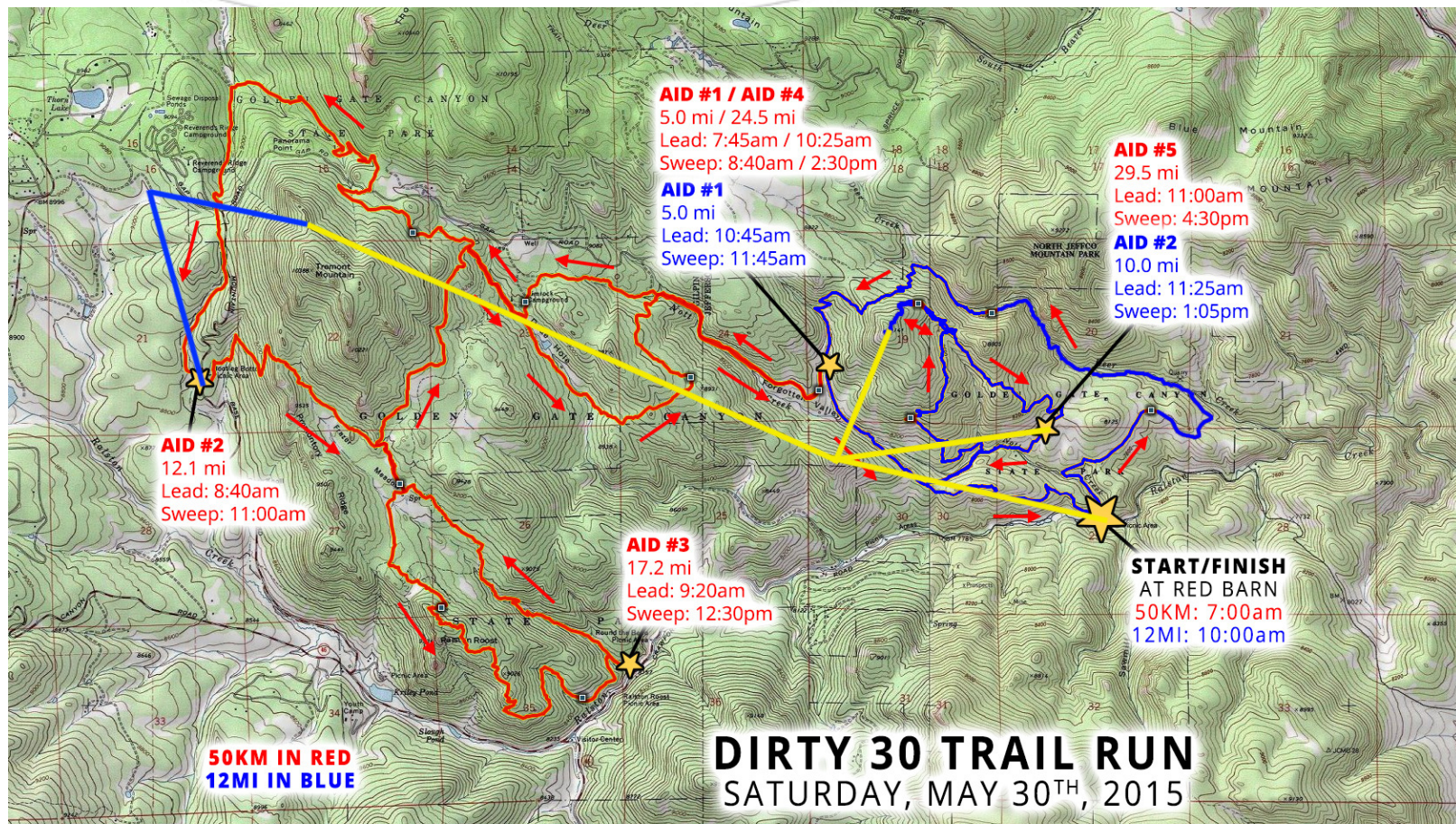
Par/By Roger Coudé VE2DBE

You can easily turn on and off site coverage by check marks at bottom of page.



to Multiple Coverages OpenTopoMap ☒ Windy Peak ☒ Aid 1/4** ☒ Tremont Mountain* ☒ Thorodin 900 1W ☒ City Lights ☒ AID5 ☒ AID3 5900 MHz

Here's what you get...



The Moral of the Story...

- ◆ When designing an event, know your territory and everything in the territory.
- ◆ Find new and improved ways of connecting the remote locations.
- ◆ Amateur Radio is not your only tool in the toolbox.
- ◆ Plot and check every permutation. Think about the results of each of the options.
- ◆ Test everything in real-world conditions!

Quick Show and Tell



Quick Show and Tell



Quick Show and Tell

Have plenty of photos from your intended area!



Quick Show and Tell



Practical Considerations

You're building a physical thing

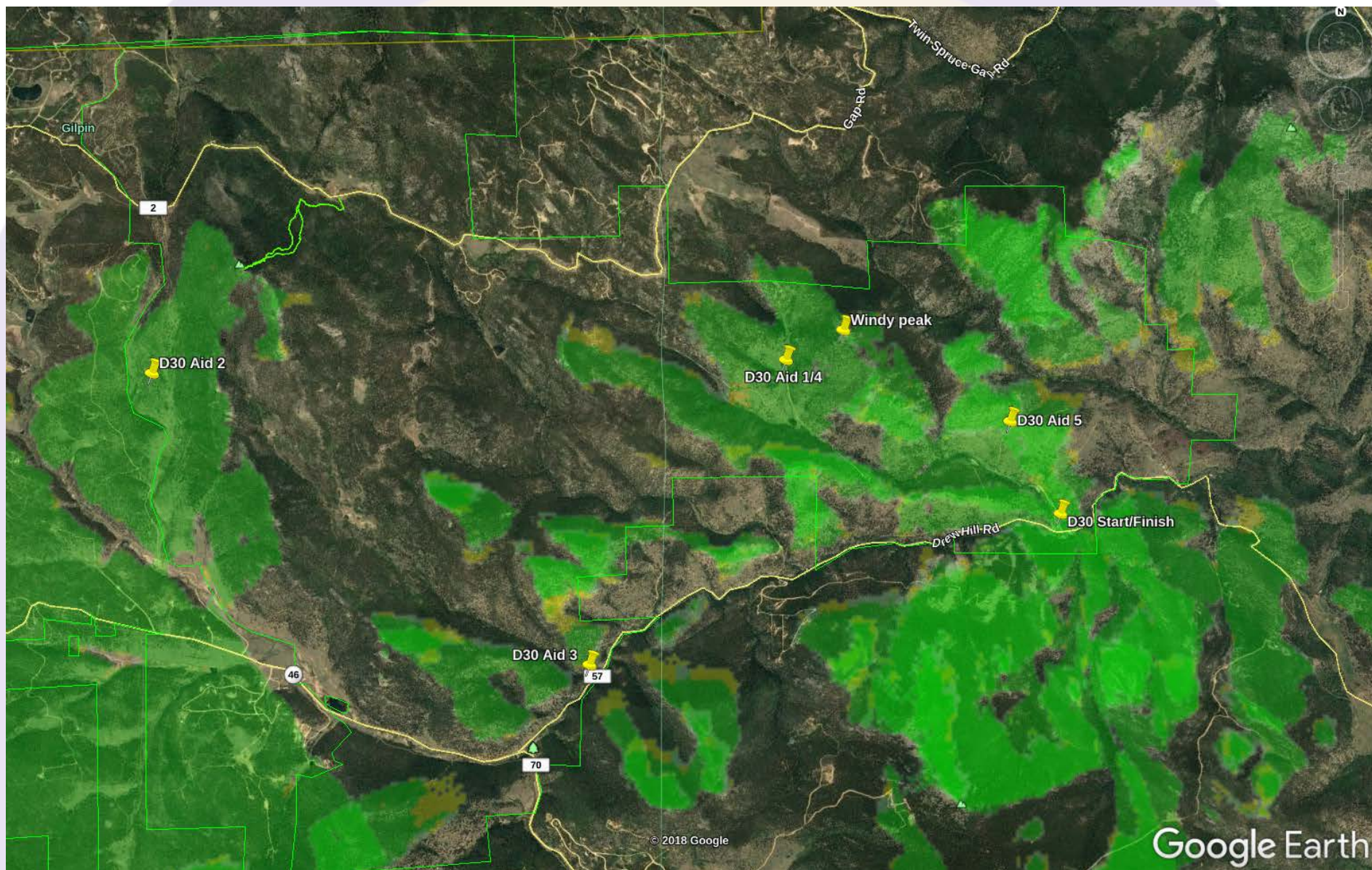
A lot of physical things

17 microwave radios in 2018

Plus mounts, power, cables, etc

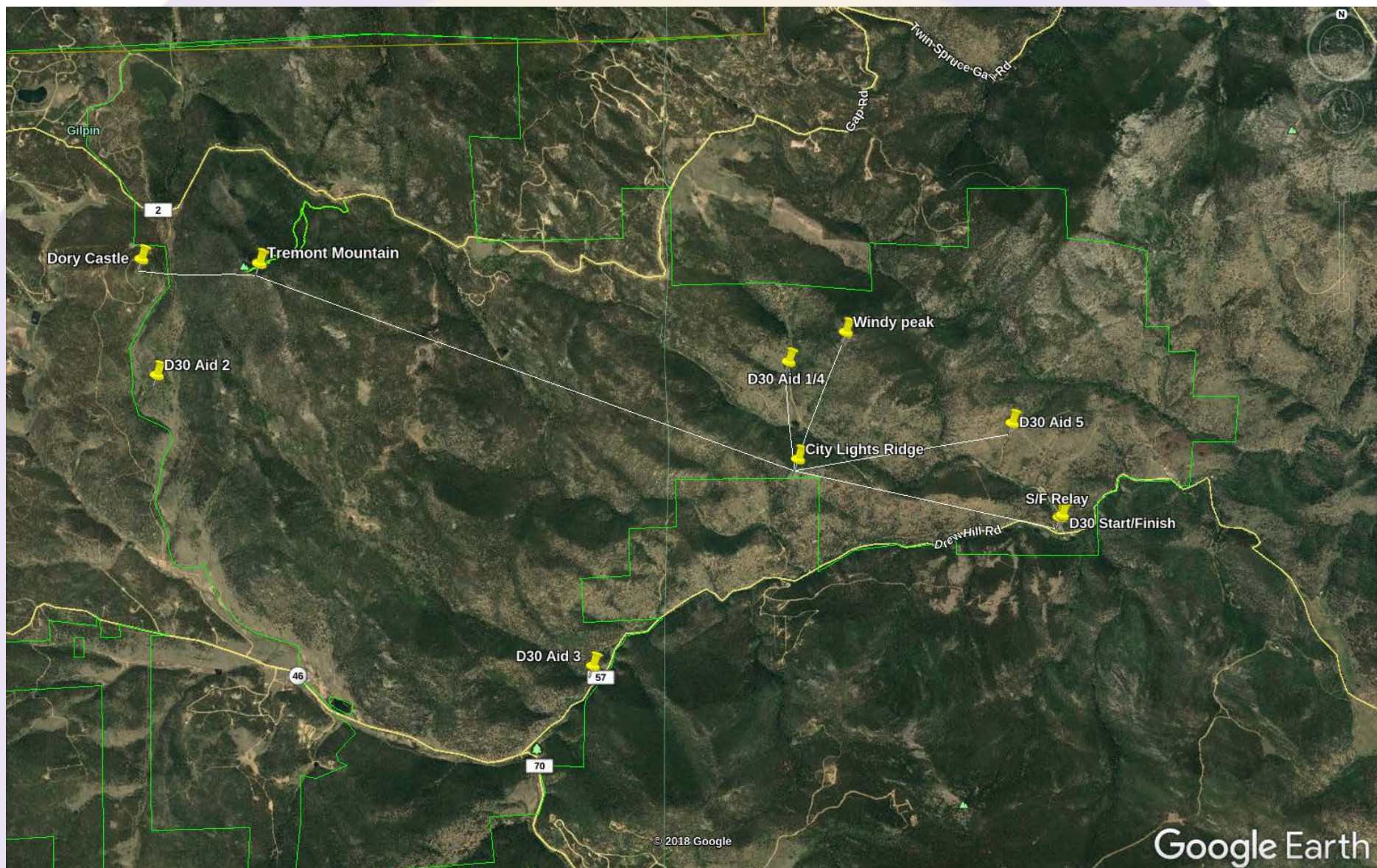
Weather, terrain, time

**Rocky Mountain
Ham Radio**



Coverage overlays

Identify likely areas all or most sites can see



Starting point for physical network layout

Practical Considerations

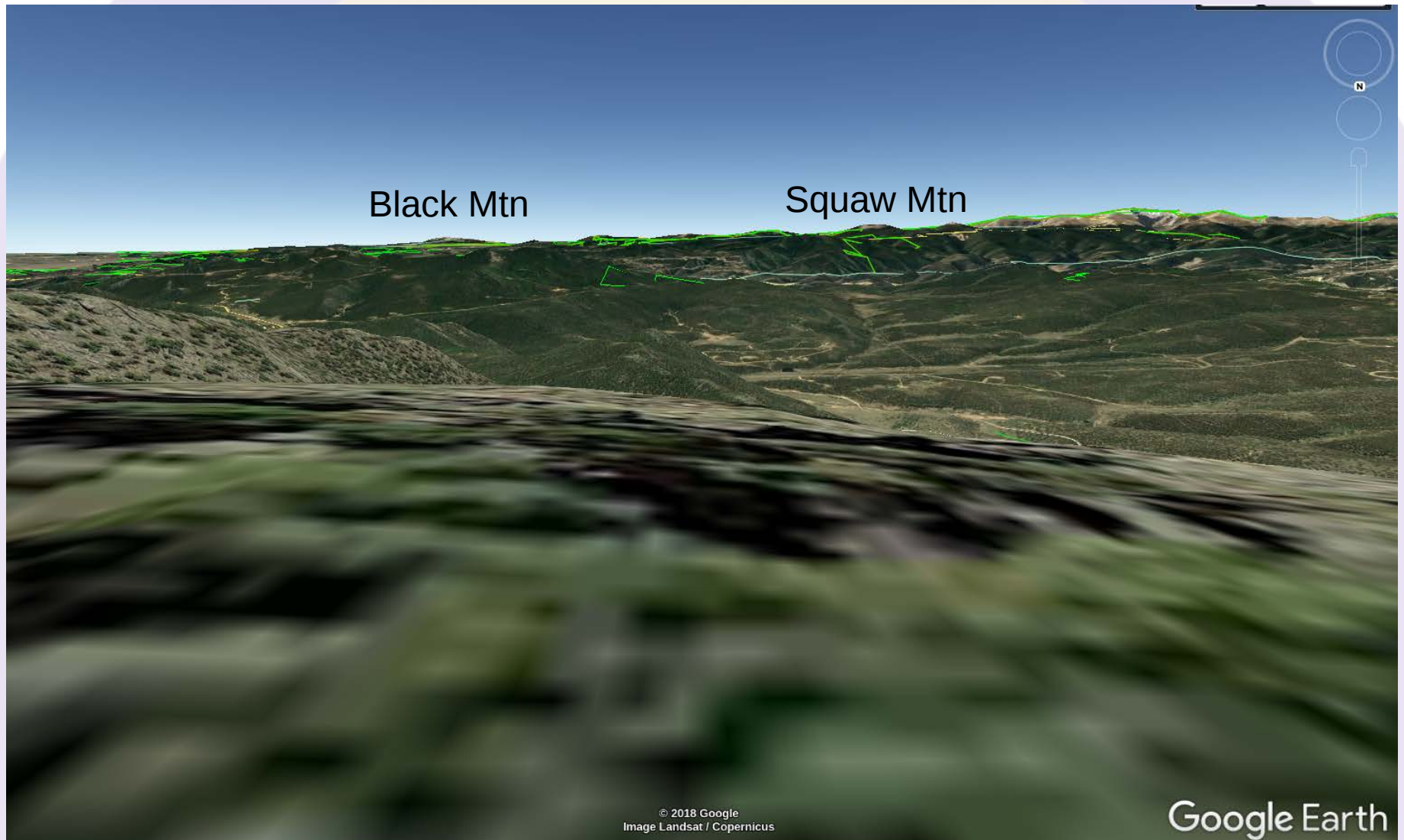
Predictions and models are fantastic tools for initial planning

Reality will surprise you – trees, hills, outcrops, boulders

Groundtruth! Hike, climb, glass, build, repeat

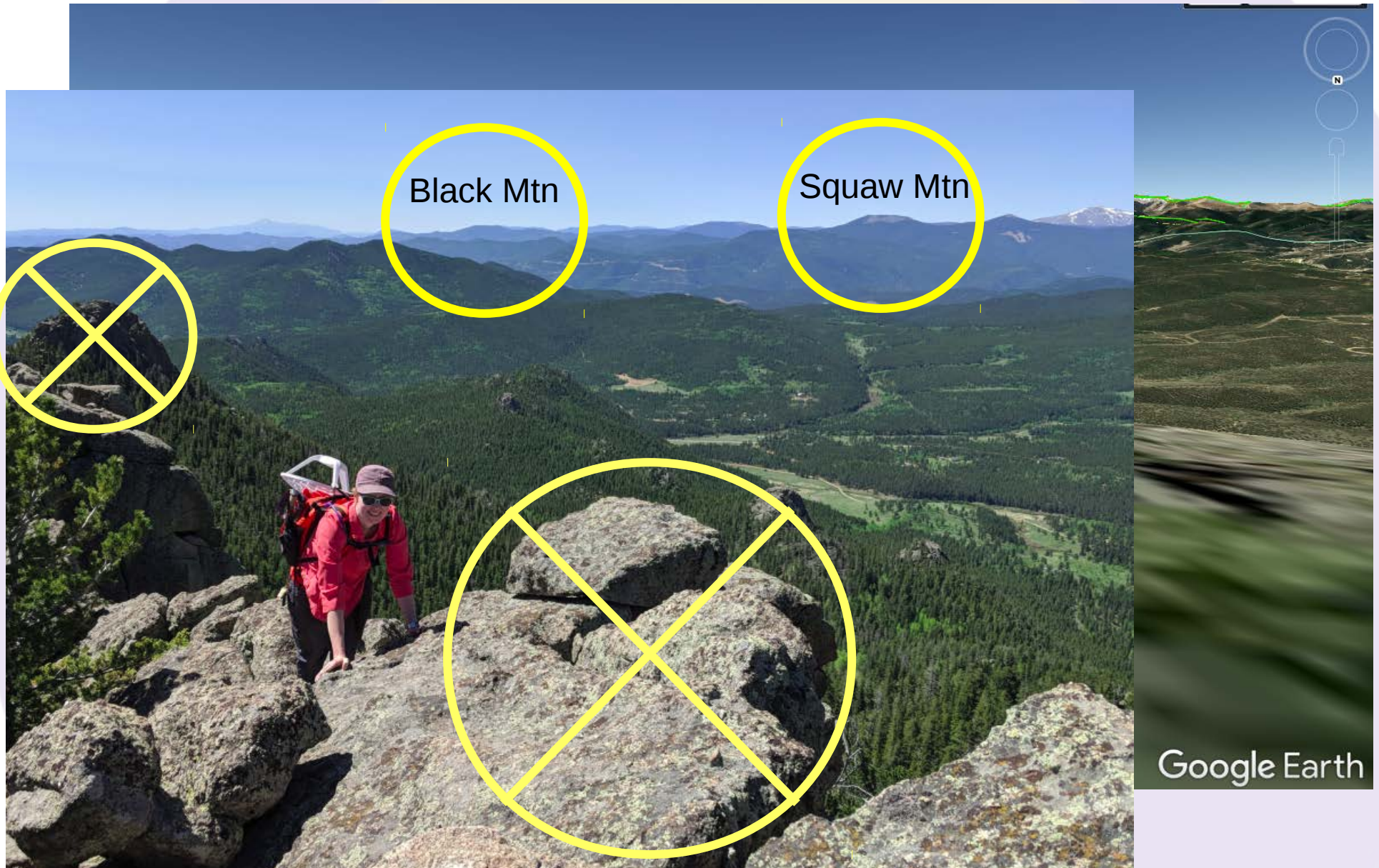
2017 five separate test deployments

Total overhaul two weeks before event



Radio Mobile, Google Earth, PeakFinder all based on USGS terrain data

Objects smaller than about 40 ft will be missing

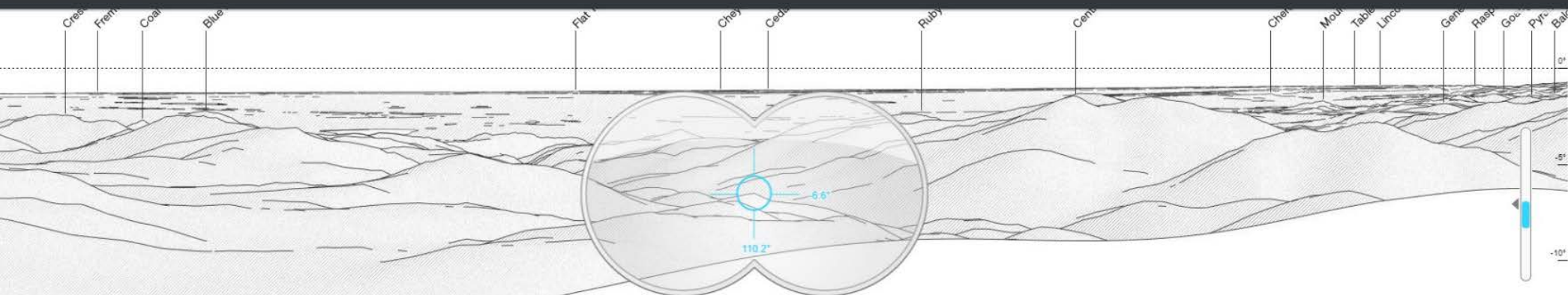


Entire hills wiped out of existence!



Ham Radio

And there are trees!



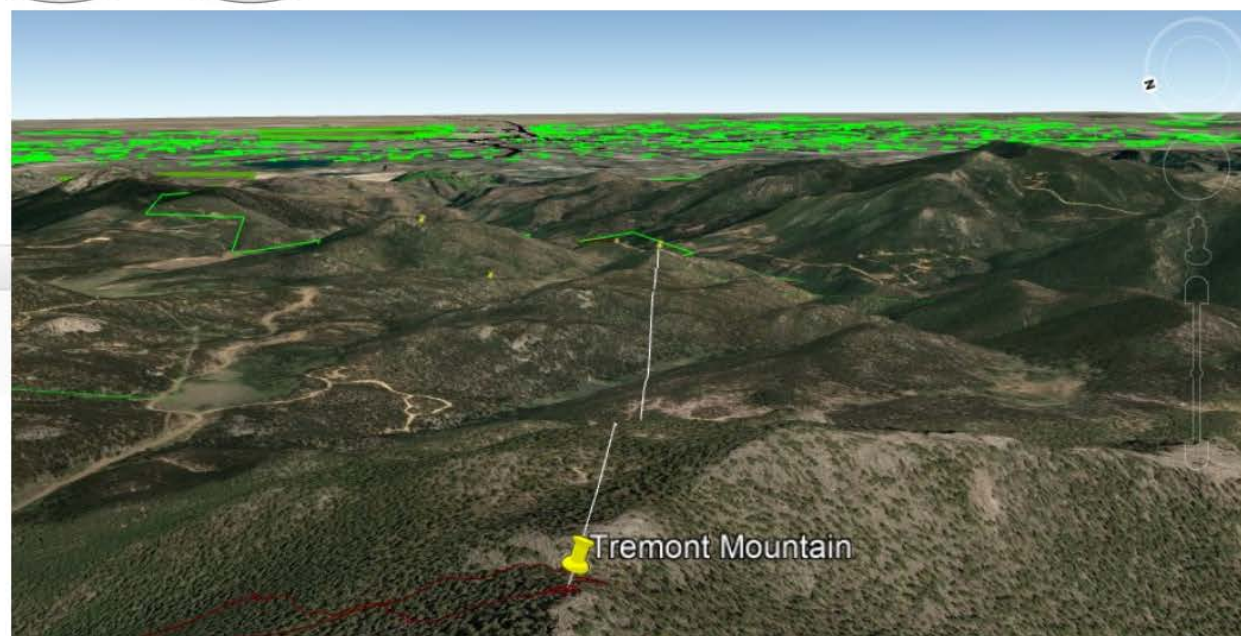
| 80° | 80° | 100°

nk | Twitter

ictured:

Tremont to Dory Castle:

miles @ 274 - 18 degrees



With directional antennas it helps to know where you're aiming.

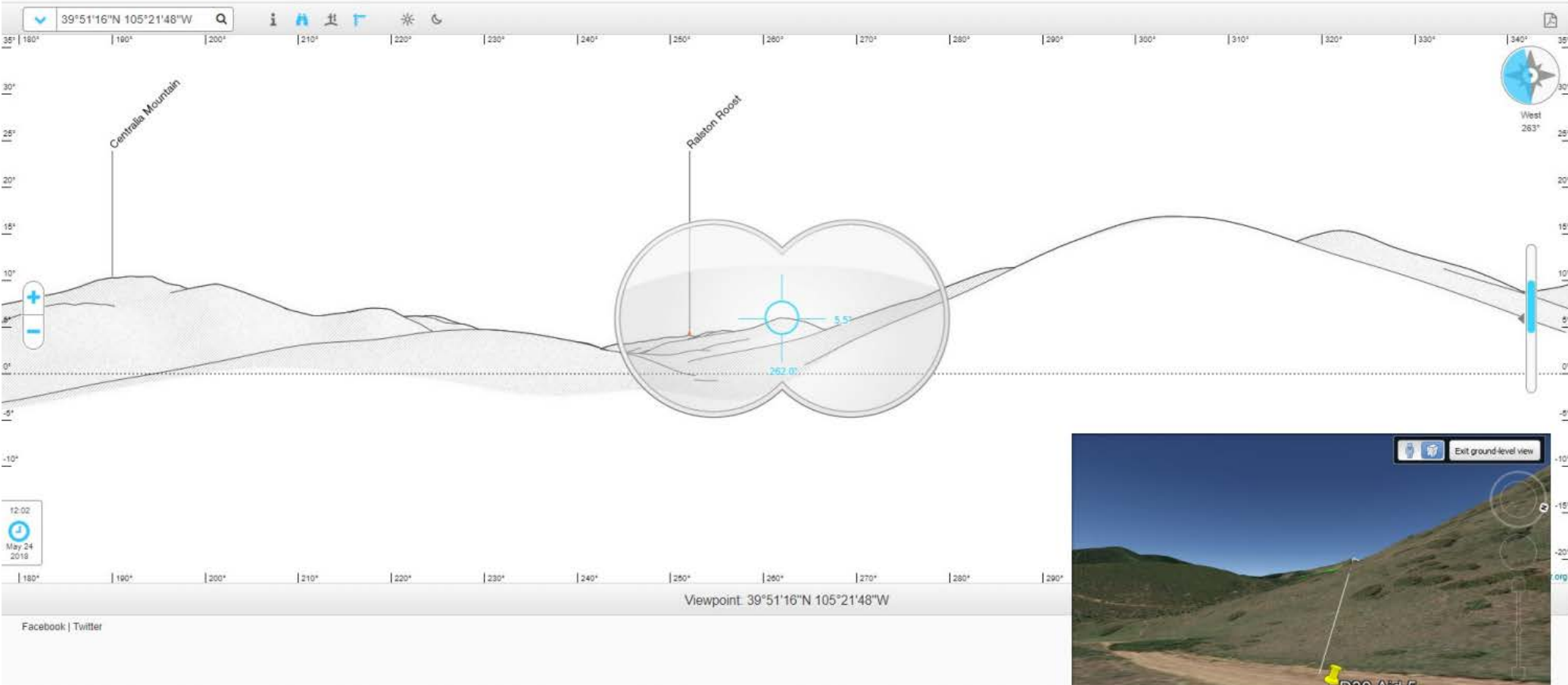
Peakfinder gives high-contrast terrain diagrams

Google Earth overlays satellite imagery over terrain

Compass headings and elevation angles

True or magnetic north? ~ 10 degree difference near Denver

Cut sheets provided for every site and target



Forecast is centered 120 feet southwest (downhill) from the service road intersection. You may relocate your gear along the route as needed in order to ensure reception, exact location is not critical.

Some sites are easier!
At least when it's sunny.

Build with the
masts you
have...



...not necessarily
the masts you
want!



It's always winter in the mountains

Practical Considerations

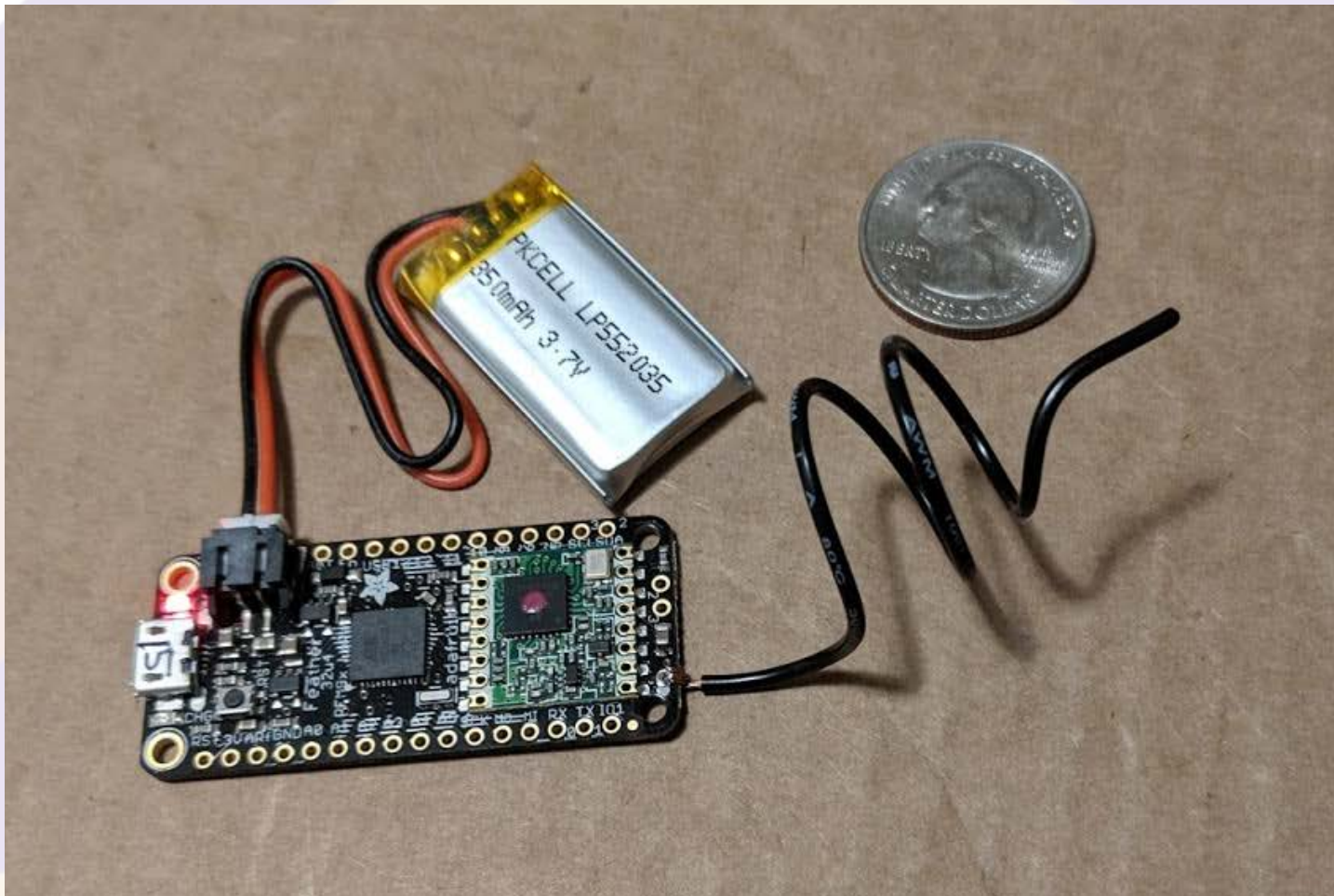
You'll have a lot of work to do

Deploy as early as you can

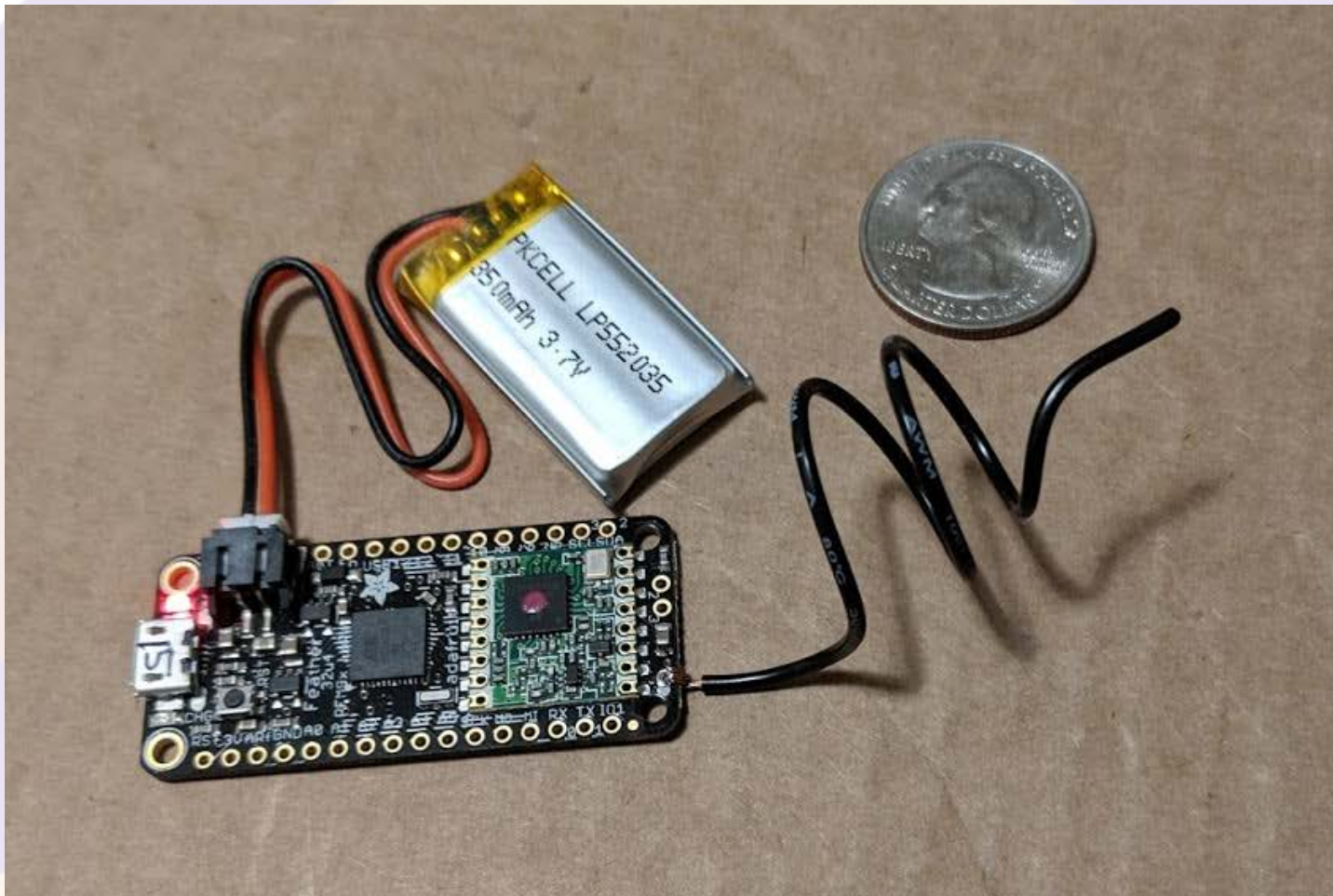
***...But no earlier!* Early setup vs. power budget**

Remote sites on timers, or remotely activated?

**Rocky Mountain
Ham Radio**



LoRA Feather power switch
Hourly check for activation signal
Latching relay to control high-current equipment
...but every useful tool is also another thing to break



LoRA - “Low-power long-range”
Proprietary packet network
Low data rate, noise-tolerant
3 - 100 mW, 70cm and 33cm bands
~2.5 mile range on simple dipole
Adafruit Feather microcontroller line ~ \$35

Adapted for Ham use by Travis Goodspeed KK4VCZ

Practical Considerations

Speaking of things breaking...

Multiple technology stacks to support

Have generalists at every site and mobile

Have specialists reachable on demand

Dedicated voice channel for technical support

Laptops, tools

Field Power

Cables

**Rocky Mountain
Ham Radio**

Rovers clearly
identifiable to
course
marshals



...but no need
to be (or invite)
this guy

Event Headquarters

Computers, LAN, file sharing, collaborative docs

Microwave network tie-in

Commercial satellite

Packet

Field power

Cables

**Rocky Mountain
Ham Radio**

Aid stations

Packet

RFID readers

Configuration correct?

Are they turned on?

Field power

Cables

**Rocky Mountain
Ham Radio**

Microwave network

Physical build – wind, masts

IP routing, DHCP, VPN

Unit configuration (freq, modulation, etc)

Field power

Cables

**Rocky Mountain
Ham Radio**

Common Theme:

Cables cause 80% of your problems

Power issues cause the other 80%

**Rocky Mountain
Ham Radio**

Toolboxes

Wirecutters

Crimpers

Connectors

Butane soldering iron

Adapters

**Rocky Mountain
Ham Radio**

IP Networking

- Bridged
 - No configuration, traffic broadcast everywhere
- Static Routed
 - Configured to route traffic as needed
- Dynamic Routed (OSPF)
 - Configured to route automatically as needed
- Mesh Routing (OLSR, WDS, UniFi)
 - Little configuration, automatic routing

Ubiquiti UniFi Mesh

- Pros
 - Works out of the box with minimal configuration
 - Weather proof
 - Device is both Mesh Relay and Access Point
 - Excellent bandwidth
- Cons
 - Limited to ISM bands
 - Limited range
- Applications
 - Start/finish and vendor area

Mikrotik WDS Mesh

- Pros
 - Works out of the box, more difficult to configure
 - Weather proof (OmniTik)
 - Can be tuned to ham band (Superchannel)
- Cons
 - Needs separate access point
 - Limited range
- Applications
 - Relays over obstructions

WDS Mesh 1

Session Settings Dashboard

Safe Mode Session: 6C:3B:6B:5E:E0:A6

Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal

Mesh

Mesh Ports FDB

+ - ✓ ✗ Mesh Traceroute Find

| | Name | Type | Actual MTU | L2 MTU |
|---|-------|------|------------|--------|
| R | mesh1 | Mesh | 1500 | |

1 item out of 8

WDS Mesh 2

admin@6C:3B:6B:5E:E0:A6 (RedBarn) - WinBox v6.39.1 on OmniTIK 5 PoE (mipsbe)

Session Settings Dashboard

Safe Mode Session: 6C:3B:6B:5E:E0:A6

Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal

Mesh

Mesh Ports FDB

Find

| Interface | Mesh |
|-----------|-------|
| ether1 | mesh1 |
| I ether2 | mesh1 |
| I ether3 | mesh1 |
| I ether4 | mesh1 |
| I ether5 | mesh1 |
| wds2 | mesh1 |

6 items

WDS Mesh 3

Interface <wlan1>

General Wireless HT HT MCS WDS Nstreme NV2 Status ...

Mode ap bridge

Band 5GHz-A/N

Channel Width 20MHz

Frequency 5180 MHz

SSID: WDS-MESH

Scan List: default

Wireless Protocol any

Security Profile default

WPS Mode push button

Bridge Mode enabled

VLAN Mode no tag

VLAN ID: 1

Default AP Tx Rate bps

Default Client Tx Rate bps

☒ Default Authenticate

☒ Default Forward

☐ Hide SSID

OK

Cancel

Apply

Disable

Comment

Advanced Mode

Torch

WPS Accept

WPS Client

Setup Repeater

Scan...

Freq. Usage...

Align...

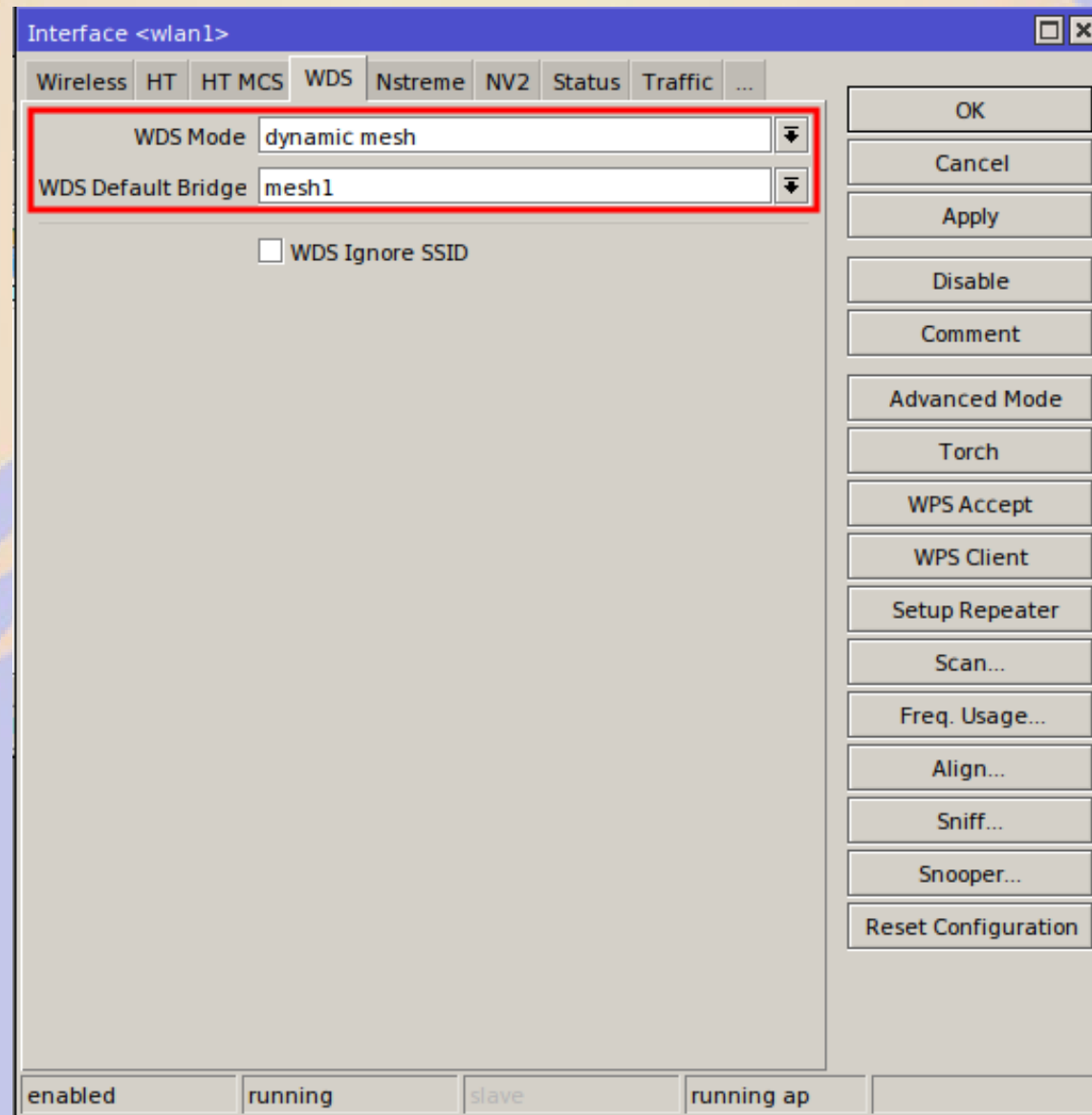
Sniff...

Snooper...

Reset Configuration

enabled running slave running ap

WDS Mesh 4



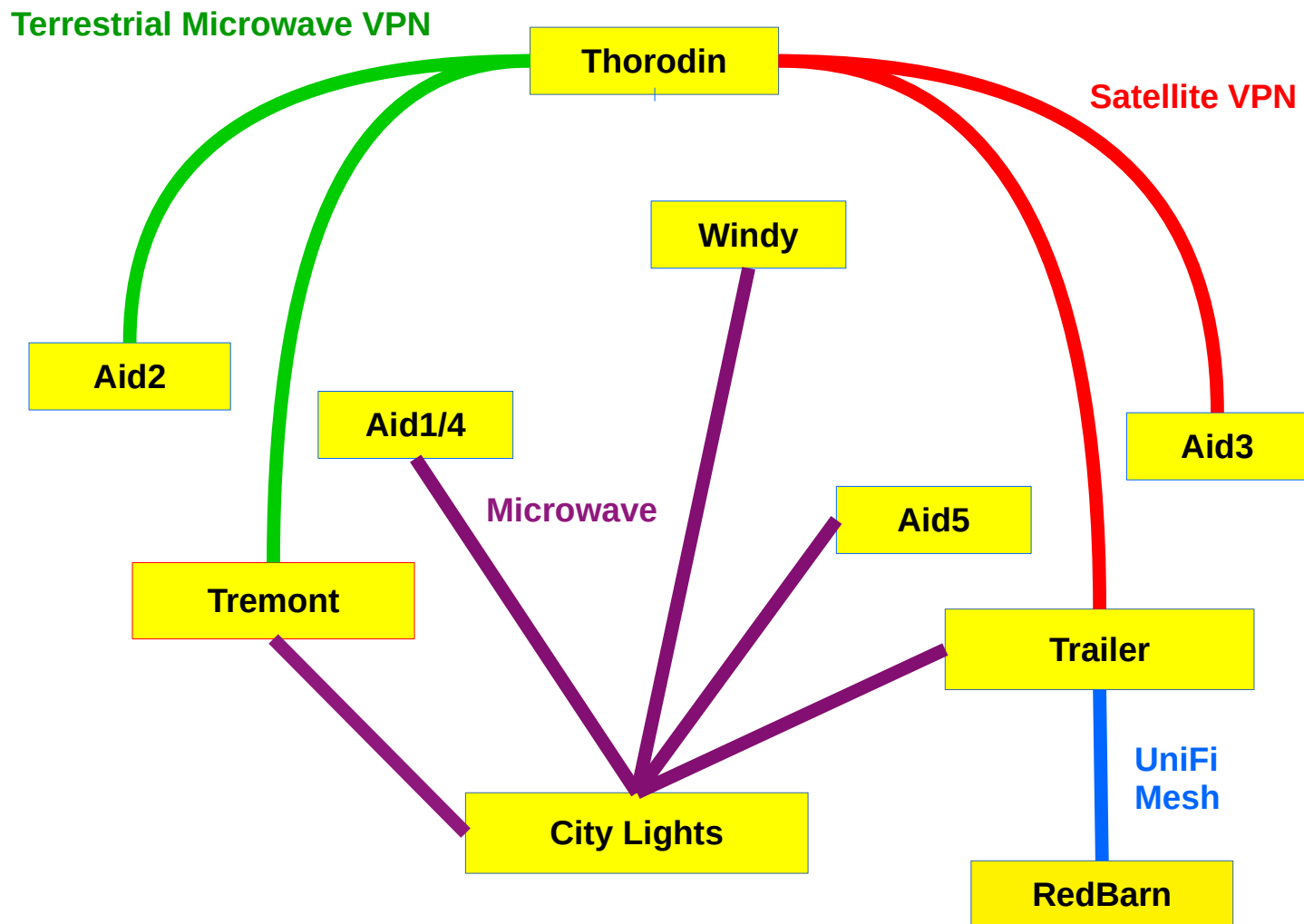
BBHN/AREDN Mesh

- Pros
 - Works on different hardware (mostly Ubiquiti)
 - Can be tuned to ham bands
- Cons
 - Needs custom firmware
 - Limited range
 - Does not handle topology changes well
 - Inflexible on addressing and routing

Point to Point & Point to Multi-Point

- Bridged
 - Packets are repeated everywhere
 - Cannot contain loops
- Static routes with failover
 - Configure primary and secondary routes
- Dynamic routes (OSPF)
 - Assign cost to each link
 - OSPF finds lowest cost route
 - Loops provide redundancy

Dirty30 Network Design



Dirty30 Network

- OSPF for general routing
- Static routes for spokes
- VPN to cross external networks
- Redundant paths
- City Lights remains single point of failure

VPN Server 1

Session Settings Dashboard

Safe Mode Session: 10.30.31.1

PPP

Interface PPPoE Servers Secrets Profiles Active Connections L2TP Secrets

PPP Scanner PPTP Server **SSTP Server** L2TP Server OVPN Server PPPoE Scan

| Name | Type | Actual MTU | L2 MTU | Tx | Rx | Tx Packet (p/s) |
|-------------------|------|------------|--------|----|----|-----------------|
| 0 items out of 12 | | | | | | |

SSTP Server

☒ Enabled

Port: 443

Max MTU: 1500

Max MRU: 1500

MRRU: [dropdown]

Keepalive Timeout: 60

Default Profile default-encryption [dropdown]

Authentication ☒ mschap2 ☒ mschap1
☒ chap ☒ pap

Certificate: none [dropdown]

TLS Version: any [dropdown]

☐ Verify Client Certificate
☐ Force AES
☐ PFS

OK Cancel Apply

terOS WinBox

VPN Server 2

Session Settings Dashboard

Session 10.30.31.1

Safe Mode

Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
LCD
MetaROUTER
Partition
Make Snapshot

PPP

Interface PPPoE Servers **Secrets** Profiles Active Connections L2TP Secrets

PPP Authentication&Accounting

Name Password Service Caller ID Profile Local Address Remote Address Last Logged

New PPP Secret

Name aid3

Password *****

Service any

Caller ID

Profile default-encryption

Local Address 172.16.88.1

Remote Address 172.16.88.37

Routes

Limit Bytes In

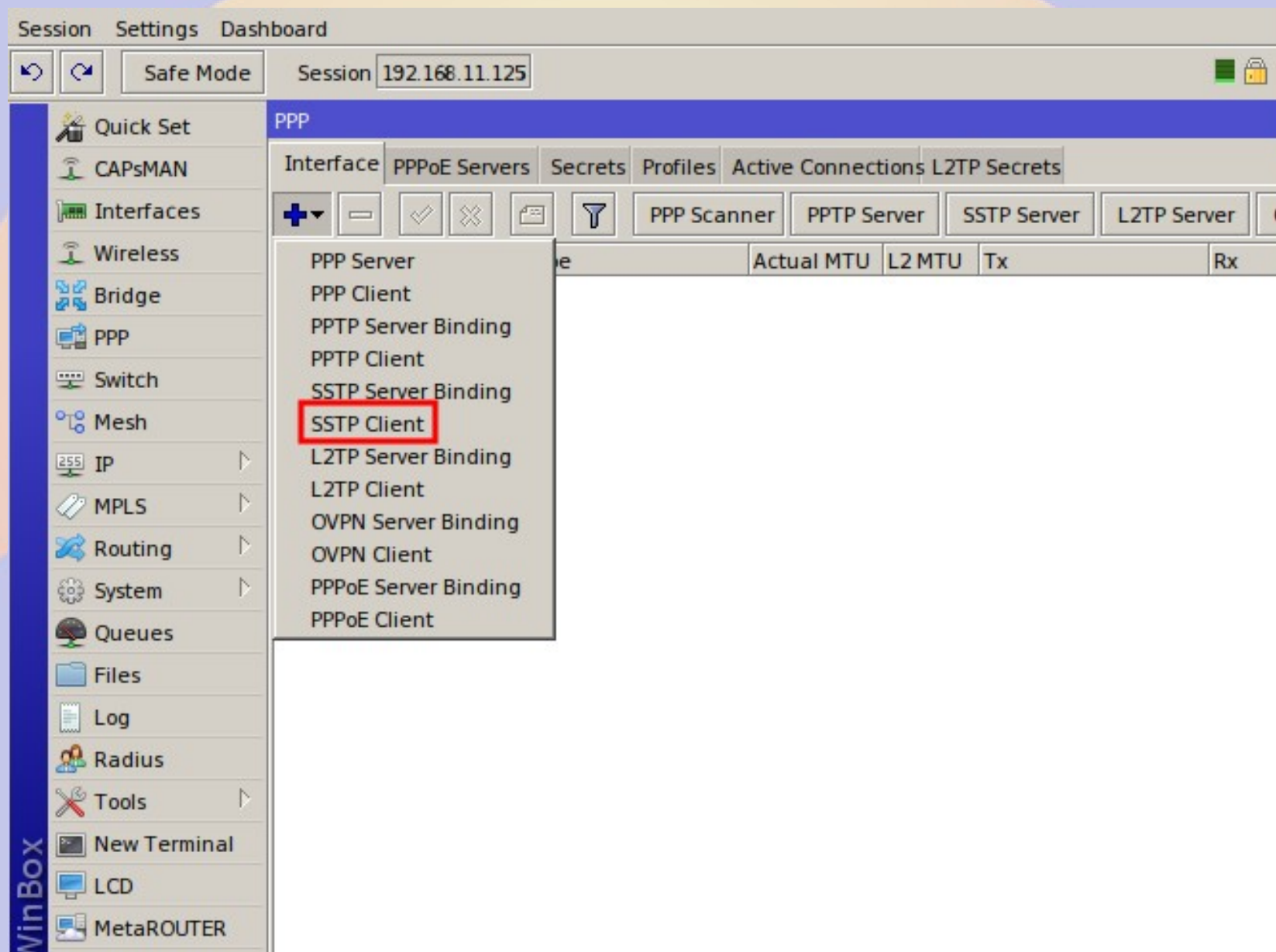
Limit Bytes Out

Last Logged On

enabled

OS WinBox

VPN Client 1



VPN Client 2

- Select a name that describes the VPN type and destination

New Interface

General | Dial Out | Status | Traffic

Name: sstp-thor

Type: SSTP Client

Actual MTU:

Max MTU: 1500

MRRU:

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Torch

enabled running slave Status:

VPN Client 3

- Set IP of server
- DO NOT verify cert
 - (unless you set one)
- Set username, password and profile
- DO NOT select
 - Dial on Demand
 - Add Default Route

Interface <sstp-thor>

General **Dial Out** Status Traffic

Connect To: 8.32.228.14

Port: 443

Proxy:

Proxy Port: 443

Certificate: none

TLS Version: any

☐ Verify Server Certificate

☒ Verify Server Address From Certificate

☐ PFS

User: aid3

Password: *****

Profile: default-encryption

Keepalive Timeout: 60

☐ Dial On Demand

☐ Add Default Route

Default Route Distance: 1

Allow ☒ mschap2 ☒ mschap1

☒ chap ☒ pap

OK Cancel Apply Disable Comment Copy Remove Torch

enabled running slave Status: connected

VPN Client 3

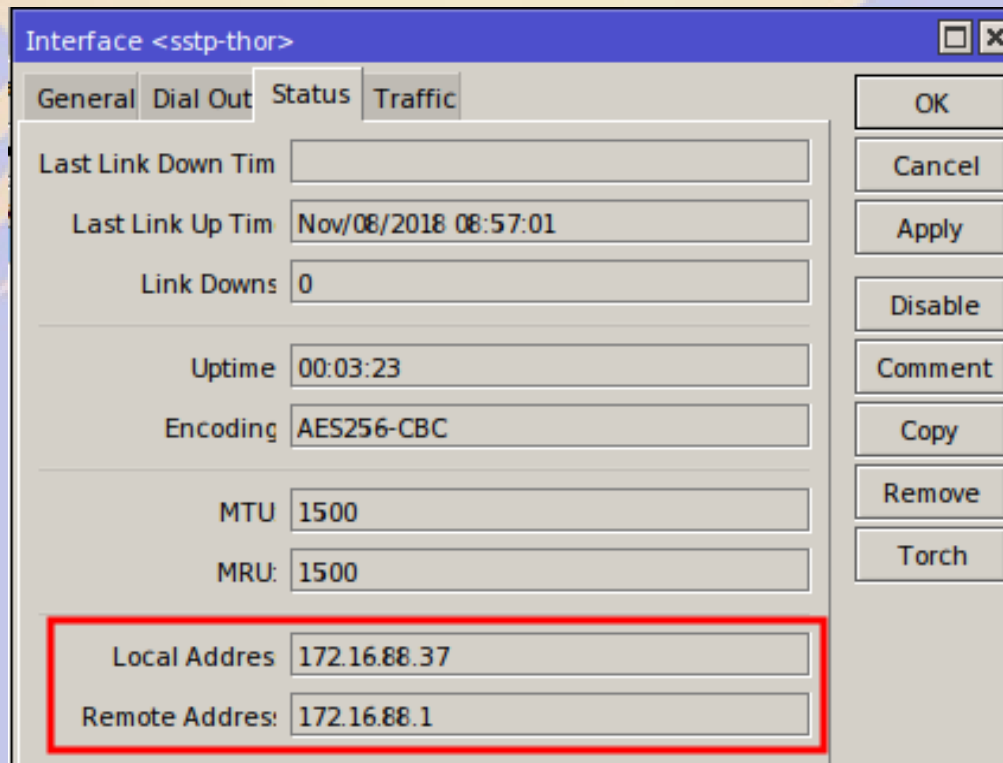
- Connection activates immediately
- MTU, Rx and Tx shows activity

The screenshot displays the Mikrotik WinBox interface. The top menu bar includes 'Session', 'Settings', and 'Dashboard'. Below this, there are navigation icons, a 'Safe Mode' button, and a 'Session' dropdown set to '192.168.11.125'. The left sidebar contains a tree view with categories like 'Quick Set', 'CAPsMAN', 'Interfaces', 'Wireless', 'Bridge', 'PPP', 'Switch', 'Mesh', 'IP', and 'MPLS'. The main panel is titled 'PPP' and has several tabs: 'Interface', 'PPPoE Servers', 'Secrets', 'Profiles', 'Active Connections', and 'L2TP Secrets'. The 'Active Connections' tab is selected, showing a table of active connections. A red rectangle highlights the first row of the table, which represents an active SSTP Client connection.

| | Name | Type | Actual MTU | L2 MTU | Tx | Rx | Tx Packet (|
|---|------------|-------------|------------|--------|----|-------|-------------|
| R | ❖sstp-thor | SSTP Client | 1500 | | | 0 bps | 0 bps |

VPN Client 4

- VPN addresses obtained from server
- Note traffic is encrypted over public internet



The screenshot shows a window titled "Interface <sstp-thor>". It has four tabs: "General", "Dial Out", "Status", and "Traffic". The "Status" tab is selected. The window displays various status fields and a list of buttons on the right.

| Field | Value |
|--------------------|----------------------|
| Last Link Down Tim | |
| Last Link Up Tim | Nov/08/2018 08:57:01 |
| Link Downs | 0 |
| Uptime | 00:03:23 |
| Encoding | AES256-CBC |
| MTU | 1500 |
| MRU | 1500 |
| Local Address | 172.16.88.37 |
| Remote Address | 172.16.88.1 |

Buttons on the right: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Torch.

VPN server 3

- Client connection <service-username>
- <> means dynamically created
 - Copy to make static (see OSPF discussion)

Session Settings Dashboard

Safe Mode Session 10.30.31.1

PPP

Interface PPPoE Servers Secrets Profiles Active Connections L2TP Secrets

PPP Scanner PPTP Server SSTP Server L2TP Server OVPN Server

| Name | Type | Actual MTU | L2 MTU | Tx | Rx |
|-----------------|---------------------|------------|--------|-------|-------|
| DR <<sstp-aid3> | SSTP Server Binding | 1500 | | 0 bps | 0 bps |

1 item out of 13

VPN Static Client Side Route

Session Settings Dashboard

Safe Mode Session 192.168.11.125

RouterOS WinBox

Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
LCD
MetaROUTER
Partition
Make Supout.rif
Manual
New WinBox
Exit

Route List

Routes Nexthops Rules VRF

Find all

| | Dst. Address | Gateway | Distance | Routing Mark | Pref. Source |
|-----|-----------------|--------------------------------|----------|--------------|-----------------|
| DAS | 0.0.0.0/0 | 192.168.11.1 reachable bridge1 | 1 | | |
| DAC | 172.16.88.1 | sstp-thor reachable | 0 | | 172.16.88.37 |
| DAC | 192.168.11.0/24 | bridge1 reachable | 0 | | 192.168.11.1... |

3 items

New Route

General Attributes

Dst. Address 10.0.0.0/8

Gateway 172.16.88.1

Check Gateway ping

Type: unicast

Distance

Scope 30

Target Scope 10

Routing Mark

Pref. Source

OK
Cancel
Apply
Disable
Comment
Copy
Remove

enabled active

VPN Routing Observations

- Route only 10.0.0.0/8 across VPN
 - All other traffic goes to default gateway
- Static route also required on server side
 - Server only knows link (172.16.X.X) address
 - Server probably OSPF - informs rest of network
- OSPF on client side will automatically route
 - Could use multiple VPNs to different end points
 - Add ospf-out filter to avoid flapping

OSPF Tips and Tricks

- Use bridge IP as router ID
- Set network type to PtP or PtMP
 - Changes propagate faster
- Make sure link costs are symmetric
- Do not export default routes
- Static routes should appear ONCE
- OSPF does not cure a bad network design

Configuring an OSPF Router

- Reset Configuration – No Default
- Add bridge and set ports
- Configure IP
 - address/subnet for bridge, etherX
 - set default route
 - set DNS
 - configure DHCP
- Configure OSPF
 - set Router ID, export connected and static as type 1
 - set OSPF network(s)
 - add OSPF filter(s) if you have a VPN WAN
- Customize rest to taste

Configuring OSPF Step 1

Session Setting Dashboard

Safe Mode Session 10.30.50.1

OSPF Instance <default>

General Metrics MPLS Status

Name default

Router ID 10.30.50.1

Redistribute Default Route never

Redistribute Connected Route as type 1

Redistribute Static Route as type 1

Redistribute RIP Route no

Redistribute BGP Route no

Redistribute Other OSPF Route no

In Filter ospf-in

Out Filter ospf-out

OK

Cancel

Apply

Disable

Comment

Copy

Remove

inBox

Quick Set

CAPsMAN

Interfaces

Wireless

Bridge

PPP

Switch

Mesh

IP

MPLS

Routing

System

Queues

Files

Log

Radius

Tools

New Terminal

LCD

MetaROUTER

Configuring OSPF Step 2

Session Setting Dashboard

Safe Mode Session 10.30.5...

OSPF

Instances Networks Areas Area Ranges Virtual Links Neighbors NBMA Neighbors Sham Links LSA Routes ...

+ - ✓ ✗ [Icon] [Icon] Find

| Network | Area |
|----------------|----------|
| 10.0.0.0/8 | backbone |
| 172.16.0.0/16 | backbone |
| 192.168.0.0/16 | backbone |

Session Setting Dashboard

Safe Mode Session 10.30.5...

OSPF

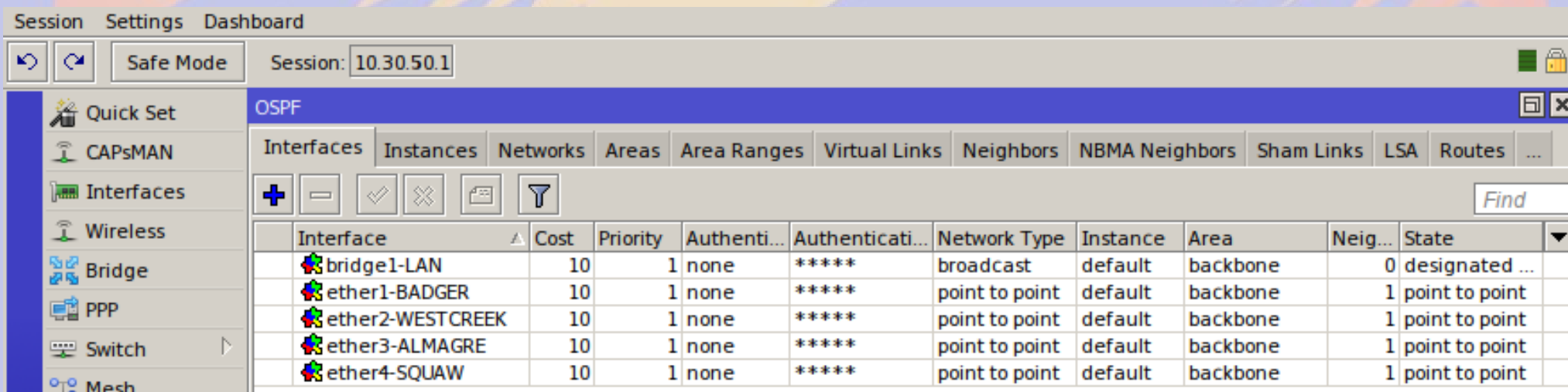
Networks Areas Area Ranges Virtual Links Neighbors NBMA Neighbors Sham Links LSA Routes ...

+ - ✓ ✗ [Icon] [Icon] Find

| Area Name | Instance | Area ID | Type | Default Cost | Interfaces | Active Interfaces | Neighbors |
|------------|----------|---------|---------|--------------|------------|-------------------|-----------|
| * backbone | default | 0.0.0.0 | default | | 5 | 5 | 4 |

Configuring OSPF Step 3

- All interfaces are automatically added
- Different weights needed for failover or setting a preferred route
- Default ethernet network type is broadcast
 - Change this to point-to-point



Session Settings Dashboard

Safe Mode Session: 10.30.50.1

OSPF

Interfaces Instances Networks Areas Area Ranges Virtual Links Neighbors NBMA Neighbors Sham Links LSA Routes ...

+ - [check] [x] [info] [filter] Find

| Interface | Cost | Priority | Authenti... | Authenticati... | Network Type | Instance | Area | Neig... | State |
|------------------|------|----------|-------------|-----------------|----------------|----------|----------|---------|----------------|
| bridge1-LAN | 10 | 1 | none | ***** | broadcast | default | backbone | 0 | designated ... |
| ether1-BADGER | 10 | 1 | none | ***** | point to point | default | backbone | 1 | point to point |
| ether2-WESTCREEK | 10 | 1 | none | ***** | point to point | default | backbone | 1 | point to point |
| ether3-ALMAGRE | 10 | 1 | none | ***** | point to point | default | backbone | 1 | point to point |
| ether4-SQUAW | 10 | 1 | none | ***** | point to point | default | backbone | 1 | point to point |

Configuring OSPF Step 4

- Only add static routes you absolutely must
 - A default static route
 - VPNs and routers NOT running OSPF

The screenshot shows the MikroTik WinBox interface. The top bar includes 'Session', 'Setting', and 'Dashboard' tabs. Below this is a 'Safe Mode' button and a 'Session' dropdown set to '10.30.5...'. The left sidebar contains a menu with icons for 'Quick Set', 'CAPsMAN', 'Interfaces', 'Wireless', 'Bridge', 'PPP', 'Switch', and 'Mesh'. The main window is titled 'Route List' and has tabs for 'Routes', 'Nexthops', 'Rules', and 'VRF'. The 'Routes' tab is active, showing a table of routes. A red box highlights the first row, which is the default static route for AS: 0.0.0.0/0 with gateway 10.20.6.2 reachable ether3-ALMAGRE. Below this row, there is a comment ';; westcreek DO NOT DELETE' and another route for XS: 10.30.115.0/24 with gateway 10.20.16.2.

| | Dst. Address | Gateway | Distance | Routing Mark | Pref. Source |
|----------------------------|----------------|------------------------------------|----------|--------------|--------------|
| AS | 0.0.0.0/0 | 10.20.6.2 reachable ether3-ALMAGRE | 1 | | |
| ;; westcreek DO NOT DELETE | | | | | |
| XS | 10.30.115.0/24 | 10.20.16.2 | 1 | | |

OSPF discovers its neighbors

Session Setting Dashboard

Safe Mode Session 10.30.5...

OSPF

Interfaces Instances Networks Areas Area Ranges Virtual Link Neighbors NBMA Neighbors Sham Links LSA Routes AS Border Routers Area Border

Y F

| Instance | Router ID | Address | Interface | State Change |
|----------|-------------|------------|------------------|--------------|
| default | 10.30.60.1 | 10.20.14.2 | ether1-BADGER | 5 |
| default | 10.30.120.1 | 10.20.6.2 | ether3-ALMAGRE | 6 |
| default | 10.30.30.1 | 10.20.5.1 | ether4-SQUAW | 9 |
| default | 10.30.115.1 | 10.20.16.2 | ether2-WESTCREEK | 8 |

OSPF distributes link database

LSA = Link State Advertisement

Session Setting Dashboard

Safe Mode Session 10.30.5...

RouterOS WinBox

OSPF

Interfaces Instances Networks Areas Area Ranges Virtual Links Neighbors NBMA Neighbors Sham Link LSA Routes AS Border Routers Area Border Routers

Find

| Instance | Area | Type | ID | Originator | Sequence Number | Age (s) |
|----------|----------|------------|---------------|--------------|-----------------|---------|
| default | | as externa | 10.30.28.0 | 10.30.20.1 | 80000012 | 194 |
| default | backbone | router | 10.0.8.1 | 10.0.8.1 | 80002f7f | 183 |
| default | | as externa | 10.120.125.0 | 10.0.11.1 | 80000ebb | 1386 |
| default | | as externa | 192.168.94.0 | 10.30.20.1 | 80000075 | 301 |
| default | | as externa | 192.168.227.0 | 10.30.20.1 | 80000054 | 1066 |
| default | | as externa | 192.168.110.0 | 192.168.11.1 | 80000004 | 1305 |
| default | | as externa | 10.30.110.0 | 10.30.20.1 | 80000453 | 904 |
| default | backbone | router | 10.30.160.1 | 10.30.160.1 | 80002a70 | 874 |
| default | backbone | network | 10.20.32.1 | 10.30.150.1 | 8000006d | 1240 |
| default | backbone | network | 10.20.2.1 | 10.30.20.1 | 800003fe | 246 |
| default | backbone | router | 10.30.20.1 | 10.30.20.1 | 8000a4c6 | 694 |
| default | backbone | network | 10.5.5.2 | 10.0.2.1 | 8000002c | 1290 |
| default | backbone | router | 10.0.13.1 | 10.0.13.1 | 800002e2 | 1279 |
| default | | as externa | 10.30.254.0 | 10.30.20.1 | 800002b3 | 542 |
| default | | as externa | 192.168.226.0 | 10.30.20.1 | 8000074b | 904 |
| default | | as externa | 10.30.106.0 | 10.30.32.1 | 8000024f | 803 |
| default | | as externa | 10.15.0.0 | 10.30.20.1 | 800001cc | 869 |
| default | | as externa | 10.16.0.0 | 10.30.20.1 | 800001cc | 869 |
| default | | as externa | 10.17.0.0 | 10.30.20.1 | 800001cc | 869 |
| default | | as externa | 10.18.0.0 | 10.30.20.1 | 800001cc | 869 |
| default | backbone | router | 10.0.11.1 | 10.0.11.1 | 80001250 | 594 |
| default | | as externa | 10.30.116.0 | 10.30.115.1 | 80000870 | 1485 |
| default | | as externa | 10.30.132.0 | 10.30.20.1 | 80000147 | 871 |
| default | backbone | network | 10.5.1.1 | 10.0.11.1 | 80000021 | 594 |
| default | | as externa | 10.0.1.0 | 10.0.11.1 | 80000ebe | 1356 |
| default | | as externa | 10.30.40.0 | 10.30.20.1 | 800001cc | 869 |
| default | | as externa | 192.168.80.0 | 10.30.20.1 | 80000093 | 933 |
| default | | as externa | 10.30.90.0 | 10.30.20.1 | 80000681 | 1033 |
| default | | as externa | 10.101.0.0 | 10.0.11.1 | 80000ebb | 1386 |
| default | backbone | router | 10.30.115.1 | 10.30.115.1 | 80000984 | 606 |
| default | | as externa | 10.30.81.0 | 10.30.80.1 | 80000220 | 1349 |
| default | | as externa | 10.30.24.0 | 10.30.20.1 | 80000022 | 922 |

126 items

Each instance finds shortest path

Session Setting Dashboard

Safe Mode Session 10.30.5...

RouterOS WinBox

OSPF

Interfaces Instances Networks Areas Area Ranges Virtual Links Neighbors NBMA Neighbors Sham Links LSA Routes AS Border Routers Area Border Routers

Find all

| Instance | Area | Dst. Address | Gateway | Interface | Cost | State |
|----------|----------|------------------|------------|--------------|------|------------|
| default | backbone | 172.16.120.5 | 10.20.6.2 | ether3-AL... | 110 | intra area |
| default | backbone | 172.16.101.12 | 10.20.6.2 | ether3-AL... | 40 | intra area |
| default | backbone | 10.20.6.0/24 | 0.0.0.0 | ether3-AL... | 10 | intra area |
| default | backbone | 10.20.14.0/24 | 0.0.0.0 | ether1-BA... | 10 | intra area |
| default | backbone | 192.168.111.0/24 | 10.20.5.1 | ether4-SQ... | 60 | ext 1 |
| default | backbone | 10.0.9.0/24 | 10.20.6.2 | ether3-AL... | 40 | intra area |
| default | backbone | 10.5.7.0/24 | 10.20.6.2 | ether3-AL... | 40 | intra area |
| default | backbone | 172.16.101.20 | 10.20.6.2 | ether3-AL... | 40 | intra area |
| default | backbone | 192.168.106.0/24 | 10.20.5.1 | ether4-SQ... | 60 | ext 1 |
| default | backbone | 10.20.26.0/24 | 10.20.16.2 | ether2-WE... | 220 | intra area |
| default | backbone | 172.16.101.1 | 10.20.6.2 | ether3-AL... | 50 | intra area |
| default | backbone | 10.30.211.0/24 | 10.20.5.1 | ether4-SQ... | 60 | ext 1 |
| default | backbone | 172.16.20.1 | 10.20.5.1 | ether4-SQ... | 50 | intra area |
| default | backbone | 192.168.0.0/24 | 10.20.6.2 | ether3-AL... | 40 | intra area |
| default | backbone | 10.0.8.0/24 | 10.20.14.2 | ether1-BA... | 21 | intra area |
| default | backbone | 10.20.22.0/24 | 10.20.5.1 | ether4-SQ... | 30 | intra area |
| default | backbone | 192.168.11.0/24 | 10.20.5.1 | ether4-SQ... | 40 | intra area |
| default | backbone | 10.5.1.0/24 | 10.20.6.2 | ether3-AL... | 40 | intra area |
| default | backbone | 10.0.11.0/24 | 10.20.6.2 | ether3-AL... | 40 | intra area |
| default | backbone | 172.16.120.1 | 10.20.6.2 | ether3-AL... | 130 | intra area |
| default | backbone | 10.0.13.0/24 | 10.20.6.2 | ether3-AL... | 50 | intra area |
| default | backbone | 10.1.1.0/24 | 10.20.6.2 | ether3-AL... | 150 | ext 1 |
| default | backbone | 10.5.10.0/24 | 10.20.6.2 | ether3-AL... | 40 | intra area |
| default | backbone | 172.16.20.35 | 10.20.5.1 | ether4-SQ... | 40 | intra area |
| default | backbone | 10.30.116.0/24 | 10.20.16.2 | ether2-WE... | 40 | ext 1 |
| default | backbone | 172.16.20.22 | 10.20.5.1 | ether4-SQ... | 180 | intra area |
| default | backbone | 172.16.20.108 | 10.20.5.1 | ether4-SQ... | 40 | intra area |
| default | backbone | 10.1.2.0/24 | 10.20.6.2 | ether3-AL... | 40 | intra area |
| default | backbone | 10.20.1.0/24 | 10.20.5.1 | ether4-SQ... | 50 | intra area |
| default | backbone | 10.20.29.0/24 | 10.20.5.1 | ether4-SQ... | 60 | ext 1 |
| default | backbone | 172.16.20.76 | 10.20.5.1 | ether4-SQ... | 40 | intra area |
| default | backbone | 172.16.101.4 | 10.20.6.2 | ether3-AL... | 40 | intra area |

204 items

Border routers are the edge of the OSPF Autonomous System

Session Setting Dashboard

Safe Mode Session 10.30.5...

OSPF

Interfaces Instances Networks Areas Area Ranges Virtual Links Neighbors NBMA Neighbors Sham Links LSA Routes AS Border Routers Area Border Routers

Find

| Instance | Router ID | Gateway | Interface | Cost | State | |
|----------|--------------|------------|------------------|------|------------|--|
| default | 10.30.20.1 | 10.20.5.1 | ether4-SQUAW | 30 | intra area | |
| default | 10.30.32.1 | 10.20.5.1 | ether4-SQUAW | 20 | intra area | |
| default | 192.168.73.1 | 10.20.5.1 | ether4-SQUAW | 40 | intra area | |
| default | 10.30.80.1 | 10.20.5.1 | ether4-SQUAW | 40 | intra area | |
| default | 10.30.115.1 | 10.20.16.2 | ether2-WESTCREEK | 10 | intra area | |
| default | 10.0.11.1 | 10.20.6.2 | ether3-ALMAGRE | 30 | intra area | |
| default | 10.30.120.1 | 10.20.6.2 | ether3-ALMAGRE | 10 | intra area | |
| default | 10.1.2.1 | 10.20.6.2 | ether3-ALMAGRE | 30 | intra area | |
| default | 192.168.11.1 | 10.20.5.1 | ether4-SQUAW | 30 | intra area | |

OSPF adds routes (DAo)

Session Setting Dashboard

Safe Mode Session 10.30.5...

RouterOS WinBox

Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
LCD
MetaROUTER
Partition
Make Supout.rif
Manual
New WinBox
Exit

Route List

Routes Nexthops Rules VRF

Find all

Filter

| | Dst. Address | Gateway | Distance | Routing Mark | Pref. Source |
|-----|--------------|---------------------------------------|----------|--------------|--------------|
| AS | 0.0.0.0/0 | 10.20.6.2 reachable ether3-ALMAGRE | 1 | | |
| DAo | 10.0.0.0/24 | 10.20.6.2 reachable ether3-ALMAGRE | 110 | | |
| DAo | 10.0.1.0/24 | 10.20.6.2 reachable ether3-ALMAGRE | 110 | | |
| DAo | 10.0.2.0/24 | 10.20.6.2 reachable ether3-ALMAGRE | 110 | | |
| DAo | 10.0.3.0/24 | 10.20.6.2 reachable ether3-ALMAGRE | 110 | | |
| DAo | 10.0.4.0/24 | 10.20.6.2 reachable ether3-ALMAGRE | 110 | | |
| DAo | 10.0.5.0/24 | 10.20.6.2 reachable ether3-ALMAGRE | 110 | | |
| DAo | 10.0.8.0/24 | 10.20.14.2 reachable ether1-BADGER | 110 | | |
| DAo | 10.0.9.0/24 | 10.20.6.2 reachable ether3-ALMAGRE | 110 | | |
| DAo | 10.0.10.0/24 | 10.20.16.2 reachable ether2-WESTCREEK | 110 | | |
| DAo | 10.0.11.0/24 | 10.20.6.2 reachable ether3-ALMAGRE | 110 | | |
| DAo | 10.0.12.0/24 | 10.20.6.2 reachable ether3-ALMAGRE | 110 | | |
| DAo | 10.0.13.0/24 | 10.20.6.2 reachable ether3-ALMAGRE | 110 | | |
| DAo | 10.1.1.0/24 | 10.20.6.2 reachable ether3-ALMAGRE | 110 | | |
| DAo | 10.1.2.0/24 | 10.20.6.2 reachable ether3-ALMAGRE | 110 | | |
| DAo | 10.5.1.0/24 | 10.20.6.2 reachable ether3-ALMAGRE | 110 | | |
| DAo | 10.5.2.0/24 | 10.20.6.2 reachable ether3-ALMAGRE | 110 | | |
| DAo | 10.5.3.0/24 | 10.20.6.2 reachable ether3-ALMAGRE | 110 | | |
| DAo | 10.5.4.0/24 | 10.20.14.2 reachable ether1-BADGER | 110 | | |
| DAo | 10.5.5.0/24 | 10.20.6.2 reachable ether3-ALMAGRE | 110 | | |
| DAo | 10.5.7.0/24 | 10.20.6.2 reachable ether3-ALMAGRE | 110 | | |
| DAo | 10.5.10.0/24 | 10.20.6.2 reachable ether3-ALMAGRE | 110 | | |
| DAo | 10.11.0.0/24 | 10.20.5.1 reachable ether4-SQUAW | 110 | | |
| DAo | 10.11.3.0/24 | 10.20.5.1 reachable ether4-SQUAW | 110 | | |
| DAo | 10.11.8.0/24 | 10.20.5.1 reachable ether4-SQUAW | 110 | | |
| DAo | 10.15.0.0/16 | 10.20.5.1 reachable ether4-SQUAW | 110 | | |
| DAo | 10.16.0.0/16 | 10.20.5.1 reachable ether4-SQUAW | 110 | | |
| DAo | 10.16.0.250 | 10.20.5.1 reachable ether4-SQUAW | 110 | | |
| DAo | 10.17.0.0/16 | 10.20.5.1 reachable ether4-SQUAW | 110 | | |
| DAo | 10.18.0.0/16 | 10.20.5.1 reachable ether4-SQUAW | 110 | | |
| DAo | 10.20.0.0/24 | 10.20.5.1 reachable ether4-SQUAW | 110 | | |
| DAo | 10.20.1.0/24 | 10.20.5.1 reachable ether4-SQUAW | 110 | | |

207 items

VPN Problems

- When the VPN drops, the dynamically created interface on the **server** is deleted and properties assigned to it is lost
 - Solution: Create a permanent instance by copying the dynamic interface after it connects.
- When OSPF discovers the WAN address of the VPN endpoint can be reached via RF, it will try to run the VPN over RF
 - Solution: Filter the WAN address so that other routers do not discover it

OSPF VPN Setup Procedure

- Add VPN as shown above
 - Enable server
 - Add secret and IP info on server
 - Add VPN on client
- On the **server** right click and copy the dynamic interface
 - Create a permanent interface name
 - Delete the dynamic interface
- On the OSPF>Interfaces tab set the cost
- Add an ospf-out filter to prevent WAN export

OSPF Filters

- ospf-in
 - causes the local router to ignore these routes
 - routes are still shared with other routers
- ospf-out
 - prevents the router from exporting the route
 - works only for external routes
 - directly connected routes are still exported if set

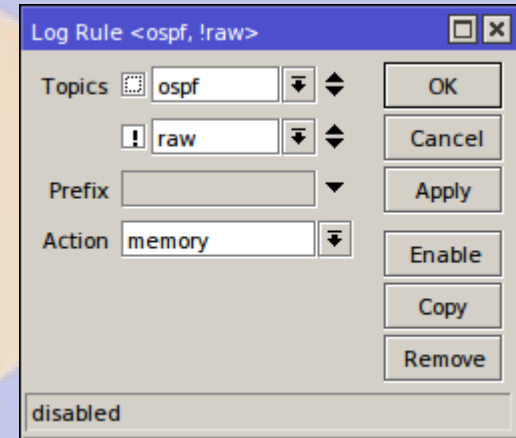
ospf-out

- Match the ***subnet***, not WAN address
- prefix-length
 - omit if just one
 - wildcard for multiple
 - 24-32 wildcards /24
- Actions=discard

The screenshot shows the 'Route Filter <72.19.163.96/29>' dialog box. The 'Chain' dropdown is set to 'ospf-out' and the 'Prefix' field contains '72.19.163.96/29'. These two fields are highlighted with a red rectangle. Below these fields are various configuration options: 'Prefix Length', 'Match Chain', 'Protocol', 'Distance', 'Scope', 'Target Scope', 'Pref. Source', 'Routing Mark', 'Route Comment', 'Route Tag', 'Route Targets' (with an 'Invert Route Targets' checkbox), 'Site Of Origin' (with an 'Invert Site Of Origin' checkbox), 'Address Family', 'OSPF Type', and an 'Invert Match' checkbox. On the right side of the dialog are buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', and 'Remove'. At the bottom left, the status 'enabled' is shown.

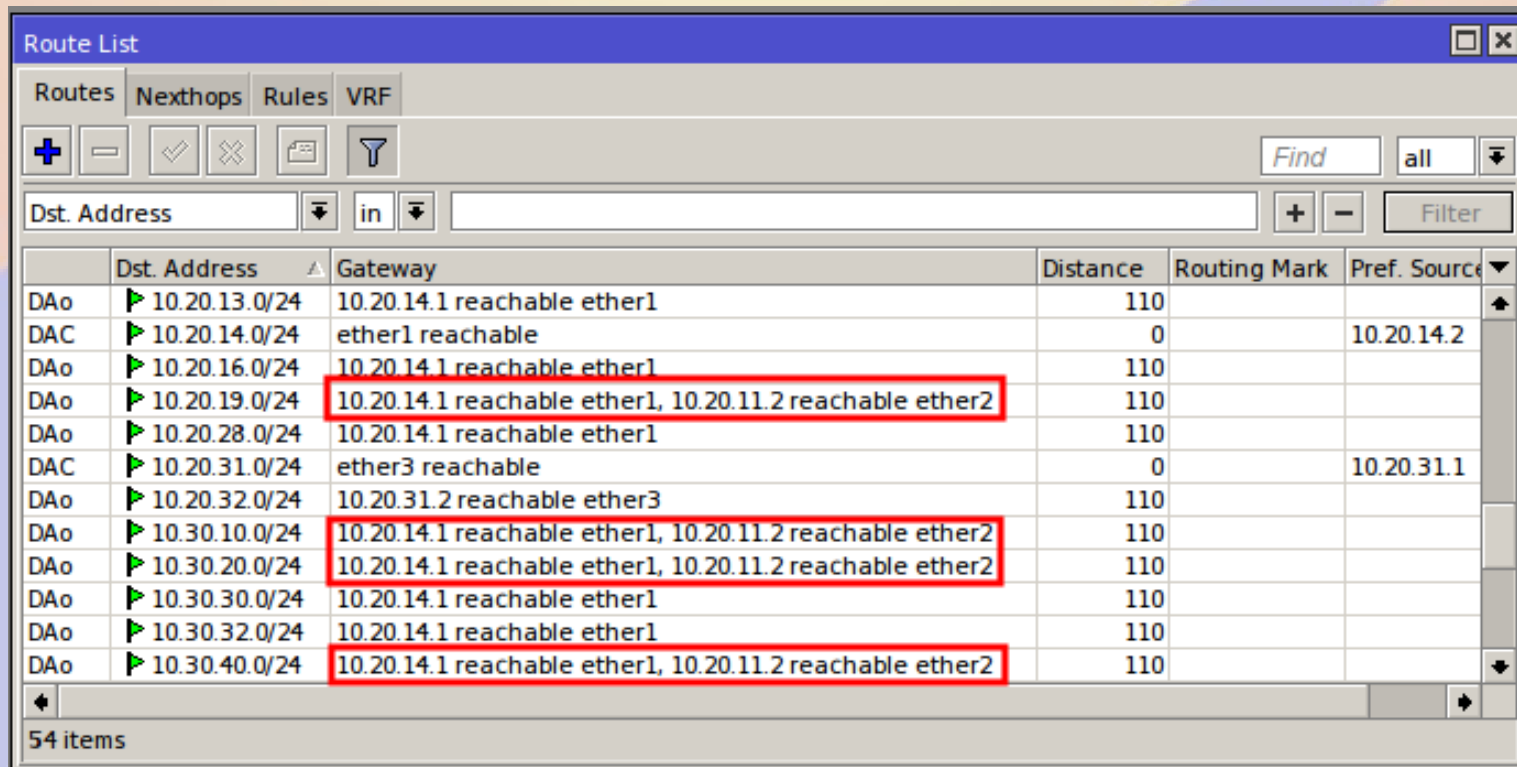
Debugging OSPF

- Add log rule for OSPF
 - /system logging add topics=ospf,!raw
- Weird log entries may require a reboot of the router
 - database out of date



Avoid split routes

- Make sure weights are symmetric
- Weight your preferred path lower
- **DO NOT ADD STATIC ROUTES**



The screenshot shows a 'Route List' window with a table of routes. The table has columns for 'Dst. Address', 'Gateway', 'Distance', 'Routing Mark', and 'Pref. Source'. Several routes are highlighted with red boxes, indicating split routes where multiple gateways are listed for the same destination address.

| | Dst. Address | Gateway | Distance | Routing Mark | Pref. Source |
|-----|---------------|--|----------|--------------|--------------|
| DAo | 10.20.13.0/24 | 10.20.14.1 reachable ether1 | 110 | | |
| DAC | 10.20.14.0/24 | ether1 reachable | 0 | | 10.20.14.2 |
| DAo | 10.20.16.0/24 | 10.20.14.1 reachable ether1 | 110 | | |
| DAo | 10.20.19.0/24 | 10.20.14.1 reachable ether1, 10.20.11.2 reachable ether2 | 110 | | |
| DAo | 10.20.28.0/24 | 10.20.14.1 reachable ether1 | 110 | | |
| DAC | 10.20.31.0/24 | ether3 reachable | 0 | | 10.20.31.1 |
| DAo | 10.20.32.0/24 | 10.20.31.2 reachable ether3 | 110 | | |
| DAo | 10.30.10.0/24 | 10.20.14.1 reachable ether1, 10.20.11.2 reachable ether2 | 110 | | |
| DAo | 10.30.20.0/24 | 10.20.14.1 reachable ether1, 10.20.11.2 reachable ether2 | 110 | | |
| DAo | 10.30.30.0/24 | 10.20.14.1 reachable ether1 | 110 | | |
| DAo | 10.30.32.0/24 | 10.20.14.1 reachable ether1 | 110 | | |
| DAo | 10.30.40.0/24 | 10.20.14.1 reachable ether1, 10.20.11.2 reachable ether2 | 110 | | |

54 items

OSPF Gochas

- VPN in PPP>Secrets
 - Only set local and remote address
 - Routes must be blank
- OSPF>Interfaces + adds a default ***all*** interface
 - Do not add any interfaces manually
- Link weight must be set on both ends
 - Different weights for a link may cause split routes

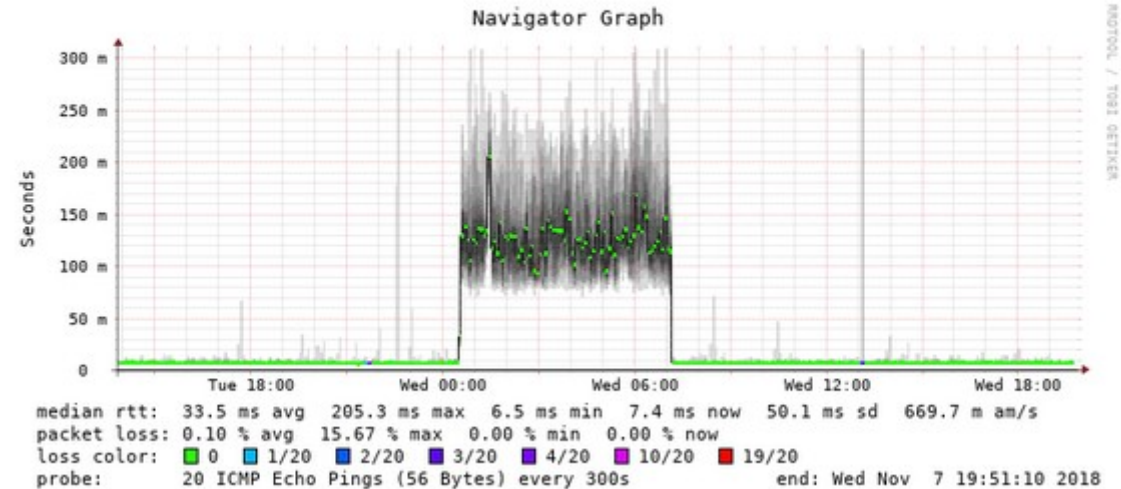
This is too complicated

- It is worth it because you retain control
 - Weights determine a preferred route
 - Keep commercial traffic off the ham bands
 - Link states are on/off, you evaluate bandwidth/latency
 - Failover is fast and reliable
 - You can monitor what is going on
- If links are flaky revert to static routes
 - PtP/PtMP tolerates errors better than broadcast

Monitor your Network

- Smokeping shows VPN failover
 - RF 9ms
 - VPN 150ms
- Netwatch shows target status
 - Use shorter interval for real time monitoring

Mosquito Pass Router (10.30.150.1)



| Netwatch | | | | |
|---------------|----------|-----------|--------|----------------------|
| Host | Interval | Timeou... | Status | Since |
| Fremont | | | | |
| 10.0.2.1 | 00:01:00 | 1000 | up | Nov/06/2018 19:50:00 |
| Cripple Creek | | | | |
| 10.0.8.1 | 00:01:00 | 1000 | up | Sep/18/2018 12:50:00 |
| Cedarwood | | | | |
| 10.0.11.1 | 00:01:00 | 1000 | up | Nov/07/2018 09:57:00 |
| K0JSC | | | | |
| 10.1.2.1 | 00:01:00 | 1000 | up | Nov/06/2018 19:50:00 |
| Lee Hill | | | | |
| 10.30.10.1 | 00:01:00 | 1000 | up | Nov/07/2018 00:05:00 |
| Thorodin | | | | |
| 10.30.20.1 | 00:01:00 | 1000 | up | Oct/16/2018 17:50:00 |
| Squaw | | | | |
| 10.30.30.1 | 00:01:00 | 1000 | up | Sep/22/2018 09:18:00 |

15 items

Aid Station Design

- How will runners pass by?
 - MUST read all runners
 - Multiple reads are inconvenient
 - Networked RFID
- Checking the reader
 - Make sure every runner is read
 - Folded bibs
 - Water bottles
 - Watch for false reads
 - Library cards
 - Toll passes

Backing up the Automated System

- Record bibs by hand
 - Compare with RFID
 - Download all readings
- Be ready to send data to the trailer
 - Forward via packet
- Use voice for drops and special cases
 - Cut armband as positive confirmation
 - Bibs that do no read
 - Medical issues

Manage the Wifi

- Password protect hotspots
- Do not share it with the aid station volunteers
 - Everybody has a phone wanting WiFi
 - Could violate Part 97
- Manage your own devices
 - Turn off Windows/iOS updates
 - Don't surf the web
- Bandwidth is at a premium
 - We have enough but it is a shared resource

Legal Issues

- We do not support commercial races
 - Must have a substantial charitable component
- We only do times for runner safety
 - We do ***tracking*** not ***timing***
- We satisfy Part 97 requirements
 - No encryption, plain text traffic
 - Nothing commercial on ham bands
 - Vendor are on commercial satellite only
 - Traffic marshals on commercial DMR

Summary

- IP is a disruptive technology
- Doing IP well requires UHF-SHF
- In mountainous terrain this is hard
 - Plan using RadioMobile, Google Earth, etc.
 - Test in the field to validate
 - Use OSPF to make it robust
- This is hard, but the payoff is huge
 - Our served agencies really want this