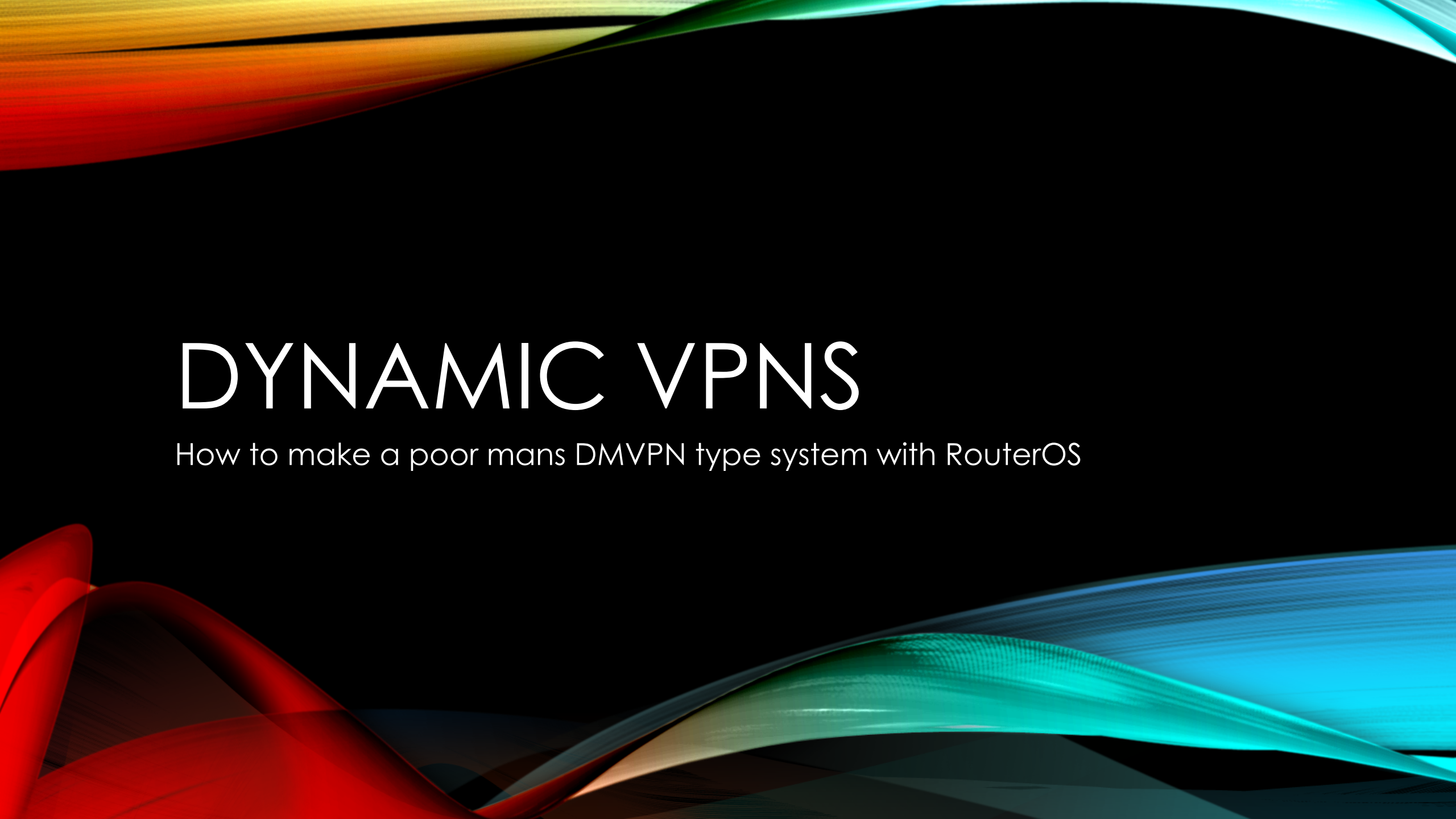




DYNAMIC VPNS

How to make a poor mans DMVPN type system with RouterOS

WHO AM I?

- Welby McRoberts
 - Twitter: @welbymcroberts
 - Email: welby+ros@thevpn.co.uk
 - LinkedIn: <https://uk.linkedin.com/in/welbymcroberts>
- Principal Engineer at Rackspace
- RouterOS user since early 2009
- Operating Systems & Applications focus with a bit of networking

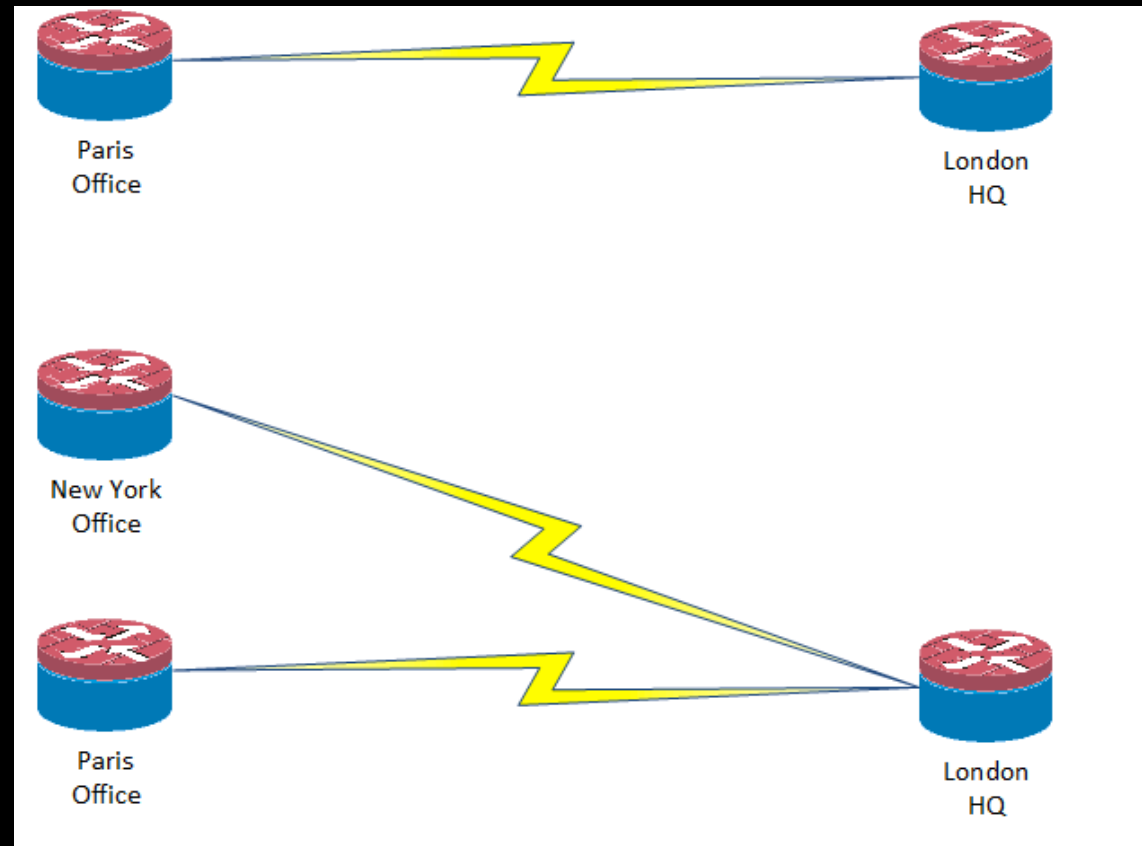
CRASH COURSE IN VPNS

- Private link between two systems
 - Site to Site
 - Client to Site
- Plethora of protocols
 - SSTP
 - L2TP
 - PPTP
 - GRE
 - IPSEC
 - EOIP
 - OVPN
- Do not require encryption

VPN DESIGN

- Simple Site to Site
 - HQ to Branch office
- Multiple Branch
 - Branches generally don't connect to each other
 - Star Topology

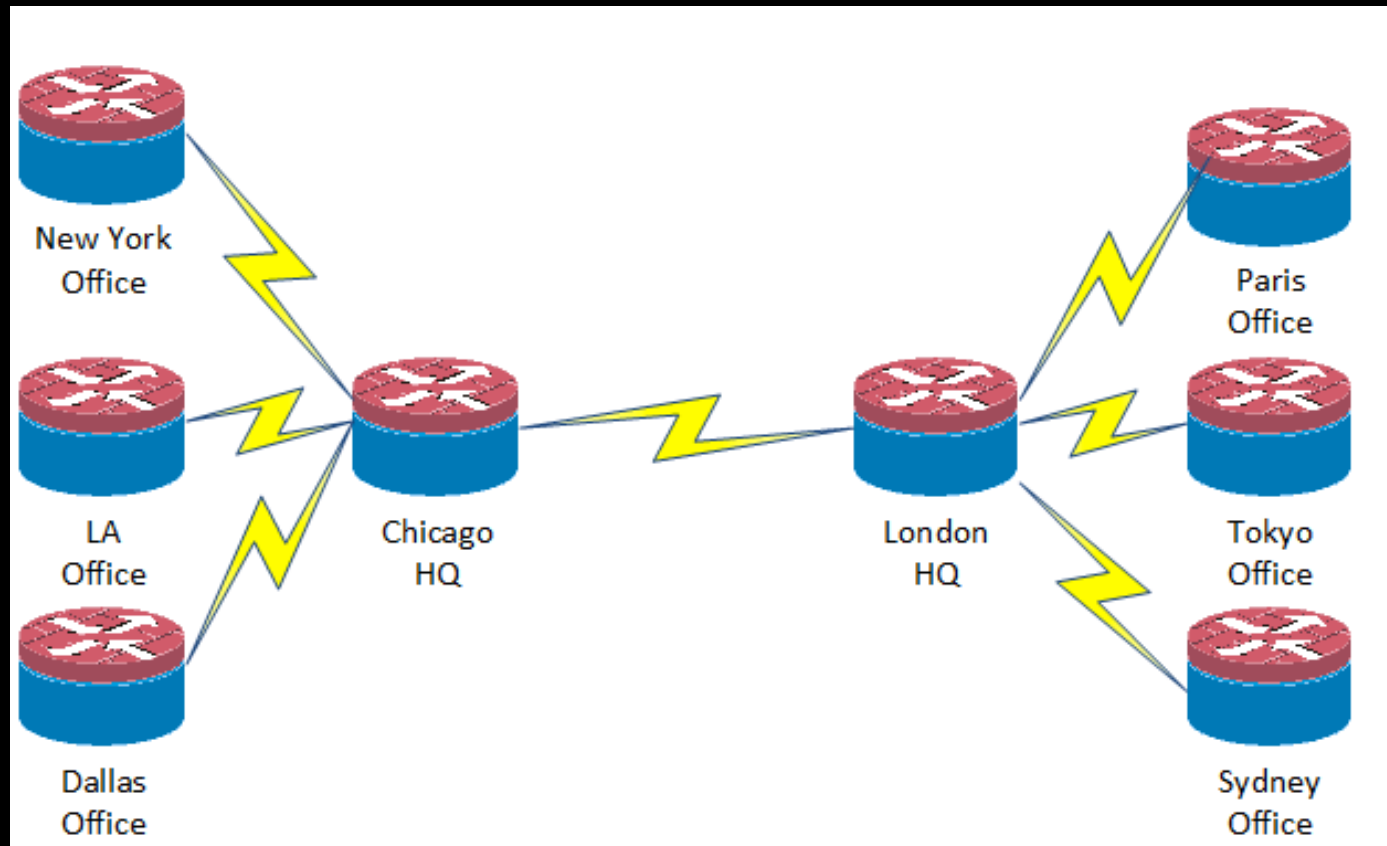
SIMPLE VPN EXAMPLES



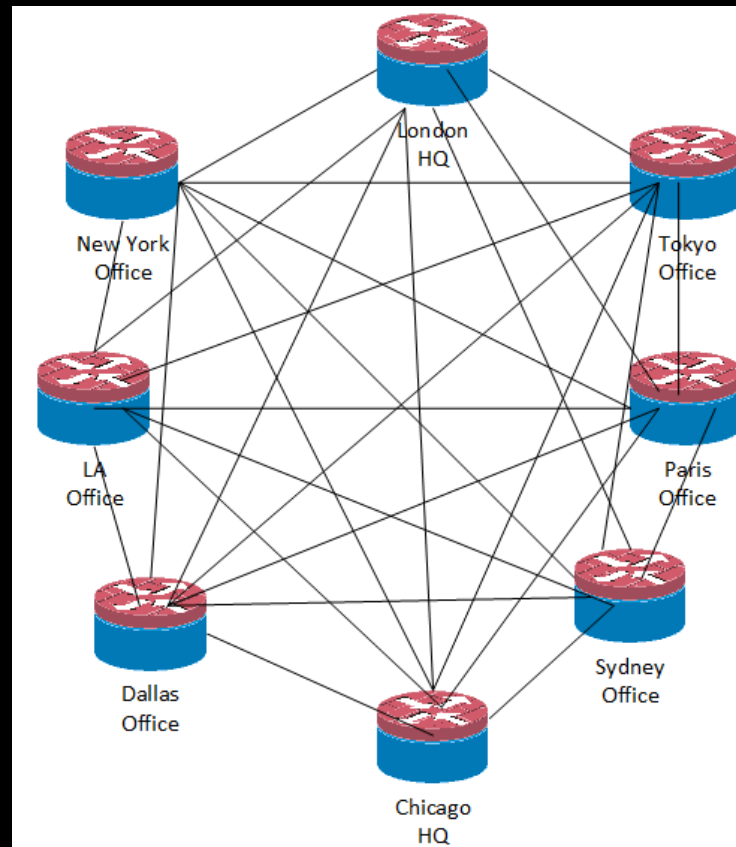
COMPLEX VPN DESIGN

- Multiple HQ or Branches
 - Major management overhead
 - One change at HQ can mean a change at each branch
 - Bandwidth limitations at HQ can cause issues
- Partial / Full Mesh VPN
 - Plain IPSec becomes a nightmare to manage
 - BW Issues are mitigated
 - Sanity can be lost

MULTIPLE-HUB & SPOKE



MESH VPN



SOLUTIONS FOR MESH VPN

- Different vendors have implemented their own
- Cisco
 - DMVPN
 - Multipoint GRE Tunnel
 - 'Easy' Config
 - Single tunnel interface created on Hub and Spokes
 - Uses proprietary protocol for identifying correct GRE endpoint
 - OSPF (or other Dynamic Routing Protocol) can be used to distribute routes
- Juniper
 - GET-VPN
 - Also supported by Cisco – ish

ROUTEROS

- No support for DMVPN (no NHRP)
- No GET-VPN support
- We do however have the prerequisites for a system
 - GRE
 - Works on a number of platforms
 - IPSec
 - Works on most platforms
 - PSK or CA
 - Dynamic Routing
 - Pick a protocol!

HOW DO WE ACHIEVE THIS

- The feather in the hat for RouterOS

Scripting!

- Leaves our options open
- Not perfect however
 - When coming from a full OS perspective, it can be quite a shock.
- Would be interested in a more "common" language being used
 - Python/Perl/Ruby etc – Obviously some security concerns
 - Lua – What happened?
 - Even TCL - If it's good enough for F5 in their TMOS, I'm sure it's fine for RouterOS!

WHY IS SOME OS GUY SPEAKING ABOUT THIS?

- As a general rule, Operating systems folk shy away from networking
- As the lines between networking and systems are blurring thanks to 'SDNs' both sides need to learn parts of the others craft
- Labs are 'boring'
 - Participation from Home
 - Large numbers of peers
 - 'Complex' network
 - Overlapping Network ranges
 - Reduces anxiety around the subject
- Increases knowledge of OS as well as networking

HOW HAVE WE DONE IT?

- Group of about 10-15 friends / colleagues
- Mostly RouterOS
 - Most folks have started with RB(7 | 9)51's
- Some Linux & FreeBSD
 - Some people just aren't ready to give up that control
- "TheVPN"
 - CA
 - Ipsec
 - GRE
 - BGP
 - RouterOS Script

HOW DOES IT WORK

- Central Server(s)
 - Python Web App running on Cloud
- User signs up for account
 - Approval by existing member
- User adds router
 - Provides: DNS, Router Type
 - Is provided: API Key, Router's AS Number, CA Cert, Router Cert + Key
- User can request a number of IP ranges
 - Assigned to a Router (and in turn an AS)

ROTUEROS SCRIPT

- Ensures Global config is in place
 - BGP Instance
 - Route Filters
 - Interface List
- Gets peers from the Web App
 - String manipulation on RouterOS is a PITA
NAME | DNS | PROTO | PORT | BGPIP | BGPAS | LOCIP | REMIP
welby | welbys.dns.for.home | GREIPSEC | 0 | 1.2.3.4 | 65500 | 4.3.2.1 | 1.2.3.4,
 - Creates Tunnel for each Peer
 - GRE Interface
 - IPSec Peer & Policy

ROTUEROS SCRIPT

- Removes old Tunnels
 - GRE
 - IPSec Peer & Policy
- Puts all tunnels in interface list
- Create BGP Peers for missing peers
- Remove unneeded BGP Peers

ISSUES?

- Misconfiguration
 - If you don't control it. Don't trust it
 - Without the route filters in place, someone injected a default route.
- Dynamic DNS
 - Home ISPs generally don't give any static Ips
 - Script resolves the DNS on each run.
- Bandwidth
 - UK & US generally have awful upstream
- Latency
 - Some people use Virgin Media – The Roller coaster of latency

FUTURE IMPROVEMENTS

- Multiple Uplinks
 - Currently no support for multiple addresses.
- Manipulating AS-Path on latency
 - The Script could potentially do a latency check to a remote and change the AS-Path length
- Queues
 - We're toying with the idea of using queues to limit BW
- Other protocols
- Scripts for other devices
- FW Rules & Route Filters
- Looking Glass
- Your Suggestions are welcome!

CAN I USE THIS

- All code is Open Source
- MIT License
- <https://github.com/welbymcroberts/thevpn.co.uk/>
- Web App is being re-developed
- Commercial Use is allowed by License
 - It is however asked that if you are to use it in a commercial setting that a donation is made to a charity listed on the GitHub page, or an equivalent charity of your companies choice.
 - Individuals can also donate to their charity of choice😊
- Contribute changes / feature requests / improvements!

QUESTIONS?

