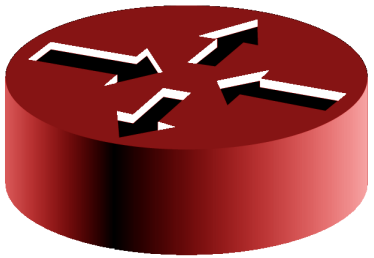
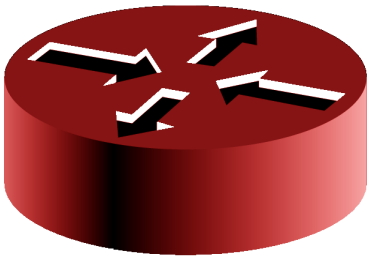
Wireless Connect

Ogma Connect

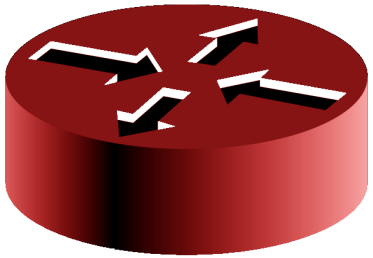
MikroTik

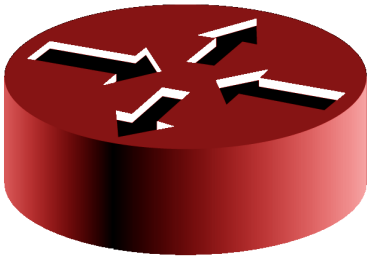
MikroTik Router OS BGP RTBH and DDOS Mitigation





Prague Czech Republic 27th of March





Why am I here

- Inspired by others who lead the charge in pursuit of excellence and who share knowledge
  - Wardner Maia of MD Brazil and his great presentations
  - Patrick Schaub of FMS Germany his presentations and year round collaboration
  - Martin Krug of RF Elements
  - Tomas Kirnak of RF Elements
  - Lorenzo and his legendary Demos vrrp redundant routers for under 100 euros :)
  - Greg Sowel of MikroTik University :)
  - Steve Discher of ISP supplies... Great book by the way... :)
  - The Brothers Wisp.
    - JJ Boyd Justin Wilson Mike Hammet Justin Miller Andrew Cox and Andrew Thrift

Wireless Connect Ltd.

- Irish Company Incorporated in 2006
- Operate an ISP in the centre of Ireland.
- Extensive Infrastructure Expertise.
- Certified MikroTik Partners
  - Training
  - Certified OEM Integrators
  - Consultants
  - Value Added Resellers

Speakers Profile:

- Technical Director Wireless Connect
- MikroTik Trainer since June 2007
- Trainer number 22
- Passionate about
  - MikroTik Router OS
  - Internet Security (prudent)
  - Finding elegant solutions to technical problems (pedantic)
- Love interacting and exchanging ideas and knowledge :)
- That is why I love the US and EU MUMs :)

Wireless Connect & MikroTlk

- Partners since June 2006
- Regular contributor of feedback to MikroTik on RouterOS
- We offer Extensive Training and Consultancy Services for services providers and enterprises that require advanced network services
- Presented 11 MUM Presentations since 2008

Our Favourite Routing Product

- When you absolutely positively need to route as many packets per second as possible
- X86 Based Routers Running ROS 6.x
  - Intel Servers with premium Hardware redundancy features High Bandwidth PCI-e expansion slots
  - Intel 2600 Xeon CPUs
  - Hot LAVA 10GE / 1GE multi port adapters
- Highest Performance per Core
- Highest Performance overall

Presentation Objectives

- Discuss Denial of Service methods
- Discuss Denial of Service mitigation concepts and strategies
- Discuss BGP Remote Triggered Black Holes

Why this Topic

- On my usual Security Theme :)
- People are better of when they are communicating with each other.
- I believe strongly in the right to free expression and
- ISPs have a duty to have an open efficient platform on which our customers can communicate with who ever they want, whenever they want
- Denial of Service attacks and their organizers pose a persistent threat to our ability to communicate freely

Wireless Connect BGP Setup

- 2 Paid Transit Providers
  - Cogent AS174 10GbE
  - Attrato / Hibernia Networks 10GbE
- 60 Peers on INEX internet Exchange 1GbE
  - Google (via Exchange Route servers)
  - Microsoft (Direct)
  - Akami (Direct)
  - Amazon EU (Direct)
  - Netflix (Direct)
  - Hurricane Electric (Direct)
- 2 Transit clients
- 2 Private peering relationships

Wireless Connect BGP Infrastructure

- Extensively use Mikrotik for Trafficking infrastructure
- OpenBGPD for Looking Glass system
- 2x X86 Ogma Connect BGP Routers for eBGP peering sessions
  - Serve eBGP for all our external Peering sessions (running 6.22 ROS)
  - Serve as Redundant Route Reflectors for iBGP
- 5x iBGP Routers in a Redundant setup
  - 3x X86 iBGP Routers
    - 1x Firewall
    - 1x BGP Signaled VPLS Concentrator
    - 1x Dedicated VPN Concentrator for International Clients
  - 2x CCR 1016 iBGP Routers
    - 1x Firewall
    - 1x BGP Signaled VPLS Concentrator

BGP Brief

- It is a first and foremost a reliable, scalable signaling protocol
- Exchanges NLRI (network layer reach-ability information).
- NLRI --- Not just Routes... contains the following information
  - Prefix 5.134.88.0
  - Prefix Length (cidr subnet mask) /21
  - BGP Attributes such as
    - AS Paths one can trace the origins of prefixes
    - Origin
    - Communities... used to advertise policies between peers (and a whole lot more)
- Perhaps we can manipulate signals between routers, and use it to send additional information.

Under the bonnet of BGP

- Uses TCP as the transport protocol (port 179)
  - (reliable transport)
- Initial full routing table exchange between peers
- Incremental updates after initial exchange
  - Withdrawals
  - Updates

Denial Of Service Attacks

- Manifest as spikes in usage of resources
  - CPU
  - Bandwidth
  - Disk I/O
- Attackers Objective
  - Consume all available Resources on your network so that legitimate users requests cant be served.
  - Damage reputation ---> Ruin your business
  - Could open an opportunity for your adversary and take over your business

Types of DOS

- Single source Denial of Service Attacks
  - Can be Potent
  - Straightforward to identify the source of the attack
  - Straightforward to mitigate
- Distributed Denial of Service Attacks
  - Quite Potent
  - Difficult to identify source of attack
  - Difficult to mitigate
- Reflected Amplification attacks
  - Most potent
  - Difficult to identify source of attack
  - Difficult to mitigate
  - Generally catastrophic

What is so difficult about DDOS

- DDOS mitigation requires out of the box thinking.
- If a DDOS packet arrives at your device it has been successful
- Remember fundamental rule of QoS
  - You can only control traffic that leaves your system (from the router)
  - You cannot reduce traffic coming towards your system (from the providers router)

Out of the Box thinking

- You need to think of protection outside your own systems to mitigate the attack.
- By the time a DDOS packet has arrived at your Router Interface it is too late
  - Bandwidth has already been consumed

DDOS Traffic Sources

- Infected / compromised systems that become zombies under the control of a malicious organization who controls the “zombie army” using a collection of Command and Control servers (A BotNET)
- These pose a persistent and serious threat to your network. An attack can last from 5 minutes to a number of days / weeks

DDOS Traffic Facilitators

- Misconfigured CPES in ISPs
- Misconfigured internet facing Servers or Services
- ISPs who don’t implement BCP 38 Anti Spoofing Filters on their upstream links

DDOS Using CPEs / Computers

- Any Device that responds to UDP with a larger message than the requester can and will facilitate an Amplification attack
- Mikrotik CPEs are No Exception
  - DNS
  - NTP (with NTP Package Enabled)
  - SNMP

DDOS Using CPEs / Computers

- Any Device that responds to UDP with a larger message than the requester can and will facilitate an Amplification attack
- Mikrotik CPEs are No Exception
  - DNS
  - NTP (with NTP Package Enabled)
  - SNMP

DDOS using mis-configured Servers

- Servers that are in locations of High bandwidth such as data centers are very attractive for people wishing to mount an attack
- The Following Services are particularly vulnerable
  - DNS
  - NTP
  - SNMP
  - Chargen

What Services are at Most Risk

- Attackers love using DNS, NTP and SNMP for reflection attacks
- Why ?
- UDP cant verify source
- AMPLIFICATION
  - Because if you send a small message to these services they can respond with a much larger message
  - If I can generate 1Gb of traffic on an attack device, I can amplifiy the affect by a factor of:

$$\frac{\text{Request Size (Bytes)}}{\text{Response Size (Bytes)}}$$

Amplification

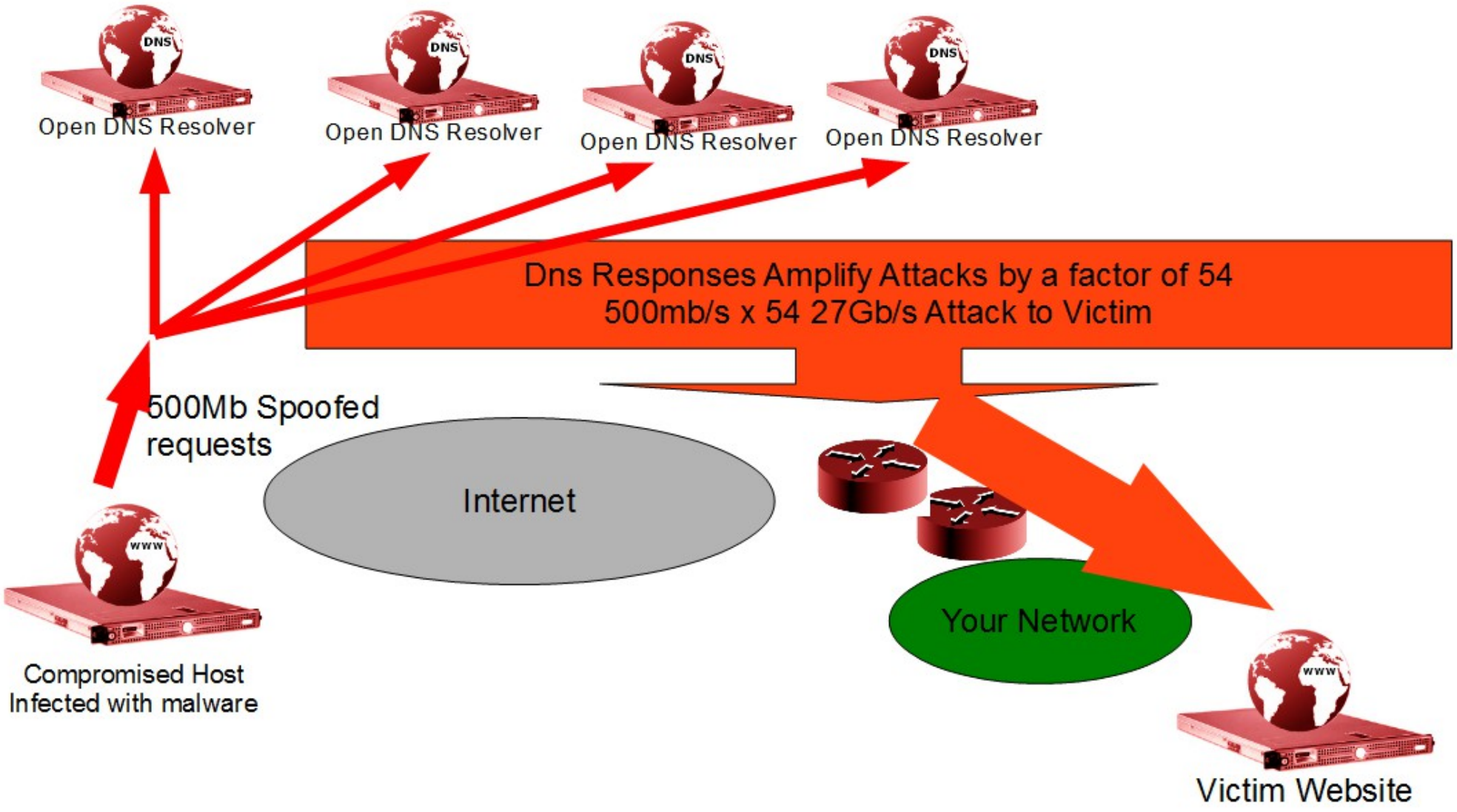
- DNS
  - MX Records
  - Dns Extensions
- SNMP
  - GetBulk Request
  - GetNext Request
  - (SNMP query of Routes on a BGP Router with Full routing table (Oh.....***#)
- NTP
  - Query list of Clients that queried server
  - ntpdc –c monlist ntpserver.com

Amplification Factors (Typical)

Protocol	Bandwidth Amplification Factor	Vulnerable Command
DNS	**28 to 54**	see: TA13-088A [1]
NTP	**556.9**	see: TA14-013A [2]
SNMPv2	**6.3**	GetBulk request
NetBIOS	**3.8**	Name resolution
SSDP	**30.8**	SEARCH request
CharGEN	358.8	Character generation request
QOTD	140.3	Quote request
BitTorrent	3.8	File search
Kad	16.3	Peer list exchange
Quake Network Protocol	63.9	Server info exchange
Steam Protocol	5.5	Server info exchange

Based on US CERT Research and Publications

Reflected Amplification Illustrated



Amplification Example

- Botnet generates 500mb of Spoofed DNS Requests towards open resolvers
- 27Gb/s Attack to a victim
- Nasty
- Attacks have
  - Perpetrators (deliberate)
  - Facilitators (through error or (on purpose (compromised hosts)))
  - Transit Service providers
  - Victim

What can you Do?

- Filter (using Input) chain all Inbound traffic to your Public facing Routers. Deny New or invalid UDP packets
- Disable any service and prevent it from listening on the public interface.

What can MikroTik Do to Help

- 1) implement a “CPE mode” where an interface that dials out DHCP or PPPoE and gets a default route, that the vulnerable services are not bound to that interface
- 2) Allow for firewall Classification of Interface groups.
- 3) Prevent binding on interfaces that have an active default route associated with them.
- 4)Perhaps merge DNS Resolver with DHCP Server.. and only bind to an interface IP that has DHCP Server running

What ISPS Should Do to Help Others

- BCP 38 – Best Current Practice 38
- Create a Filter on your Outermost Routers and Block traffic **leaving** your network that does **NOT** meet any of the following Criteria
  - Has a Source IP that is on Your network
  - Has a Source IP that is on your Transit Clients Network
  - Has a Source IP that is on your peers Network

ISP BCP 38 Rules

#		Action	Chain	Src. Address	Dst. Address	Proto...	Dst. Port	In. Inter...	Out. Int...	Src. Address List	Bytes	Packets
;;; Accept Our IP Address Ranges to Cogent												
7		acc...	forward						ether1	WC_ISP_andTransitCustomerRanges	522.1 GiB	2863 506...
;;; Drop Traffic inbound to our network from our own Ip ranges spoofed												
8		drop	forward					ether1		WC_ISP_andTransitCustomerRanges	6.5 MiB	193 079
;;; Drop Traffic inbound to our network from our own Ip ranges spoofed												
9		drop	forward					ether3		WC_ISP_andTransitCustomerRanges	0 B	0
;;; Drop Spoofed IPS to Cogent												
10		drop	forward						ether1	!WC_ISP_andTransitCustomerRanges	36.8 MiB	383 378
;;; Drop IP Directed Broadcast onto INEX LAN												
11		drop	forward						ether2		0 B	0
;;; Accept Our IP Ranges to Inex LAN 1												
12		acc...	forward						ether2	WC_ISP_andTransitCustomerRanges	0 B	0
;;; Drop Spoofed Packets to Inex LAN 1												
13		drop	forward						ether2	!WC_ISP_andTransitCustomerRanges	0 B	0
;;; Drop IP Directed Broadcast onto INEX LAN												
14		drop	forward						ether3		0 B	0
;;; Accept Our IP Ranges to Inex LAN 2												
15		acc...	forward						ether3	WC_ISP_andTransitCustomerRanges	0 B	0
;;; Drop Spoofed Packets to INEX LAN 2												
16		drop	forward						ether3	!WC_ISP_andTransitCustomerRanges	0 B	0

What ISPs should do to Protect them selves ?

- Filter traffic coming into your network
- Subscribe to Team Cymru Bogon Route Servers (automatically filter private, special or reserved addresses, and un allocated IP ranges (ie non internet addresses)
- Filter RFC 1918 private addresses
  - 10.0.0.0/8
  - 192.168.0.0/16
  - 172.16.0.0/12

ISPs Protecting themselves

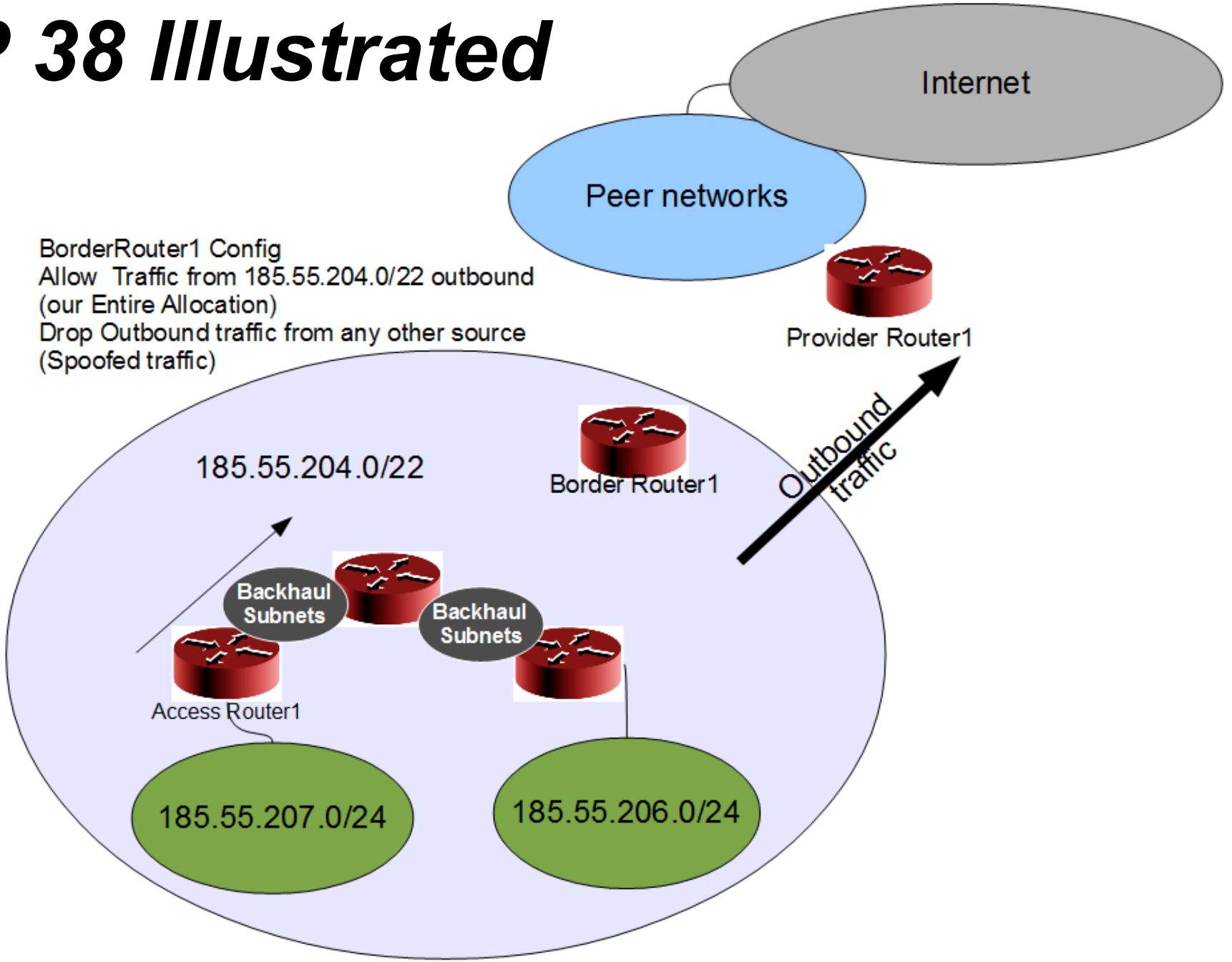
- Filter traffic allegedly sourced from inside your network
  - Prevent accidental routing of internal traffic over internet
  - Reduce security impact of prefix hijacking
  - Prevent DDOS of UDP services serving to your own customers
    - DNS
    - NTP
    - SNMP
    - Chargen

#		Action	Chain	Src. Address	Dst. Address	Proto...	Dst. Port	In. Inter...	Out. Int...	Src. Address List	Bytes	Packets
;;; Drop Traffic inbound to our network from our own Ip ranges spoofed												
8		drop	forward					ether1		WC_ISP_andTransitCustomerRanges	6.5 MiB	193 035
;;; Drop Traffic inbound to our network from our own Ip ranges spoofed												
9		drop	forward					ether3		WC_ISP_andTransitCustomerRanges	0 B	0

BCP 38 benefits

- Maintaining BCP 38 Filters will will not be used as a vector for attacking someone elses network
- Implementing this rule combined with logging can be an early warning of issues on your network
  - Botnets
  - Malware
  - Viruses

BCP 38 Illustrated



BCP 38

- If Every ISP applied BCP 38 then Spoofed traffic on the internet would almost be completely eliminated.
- Anti Spoofing measures globally would eliminate “global Reflected amplification attacks”

The Problem with BCP 38

- It is classic “Pay it forward” by implementing BCP 38 you will protect other peoples networks from malware on your network…
  - Everyone else will do the same for me …
  - they will have my back...
- A few large ISPs not implementing BCP 38 would severely limit the usefulness of everyone elses BCP 38 implementation
- Kind of like Vaccination if you want to eradicate a disease you need to vaccinate the entire population against it.

BCP 38 Benefits

- As BCP 38 becomes more widely implemented.
  - Botnet generated spoofed attack traffic will be restricted at the borders of the ISP.
  - Reflected amplification attacks potency will be severely reduced.

Widespread BCP38 adoption

- Malware / botnets likely reaction to prolific BCP 38 deployment
- Reduce reliance on reflected amplification attacks,
- Increase reliance on direct spoofed attacks
  - Limit spoofing to what is “allowed within an ISP”
    - What is the Zombie PC real ip address ?
    - OK lets do a Whois and Find out what AS number is announcing the prefix that the IP is part of
    - OK lets spoof random IPs within the /21 IP allocation
    - e.g. my IP is 5.134.89.134
    - Who is 5.134.89.134, 5.134.88.0/21 (so I can possibly spoof traffic with the following IP addresses 5.134.88.1-5.134.95.254

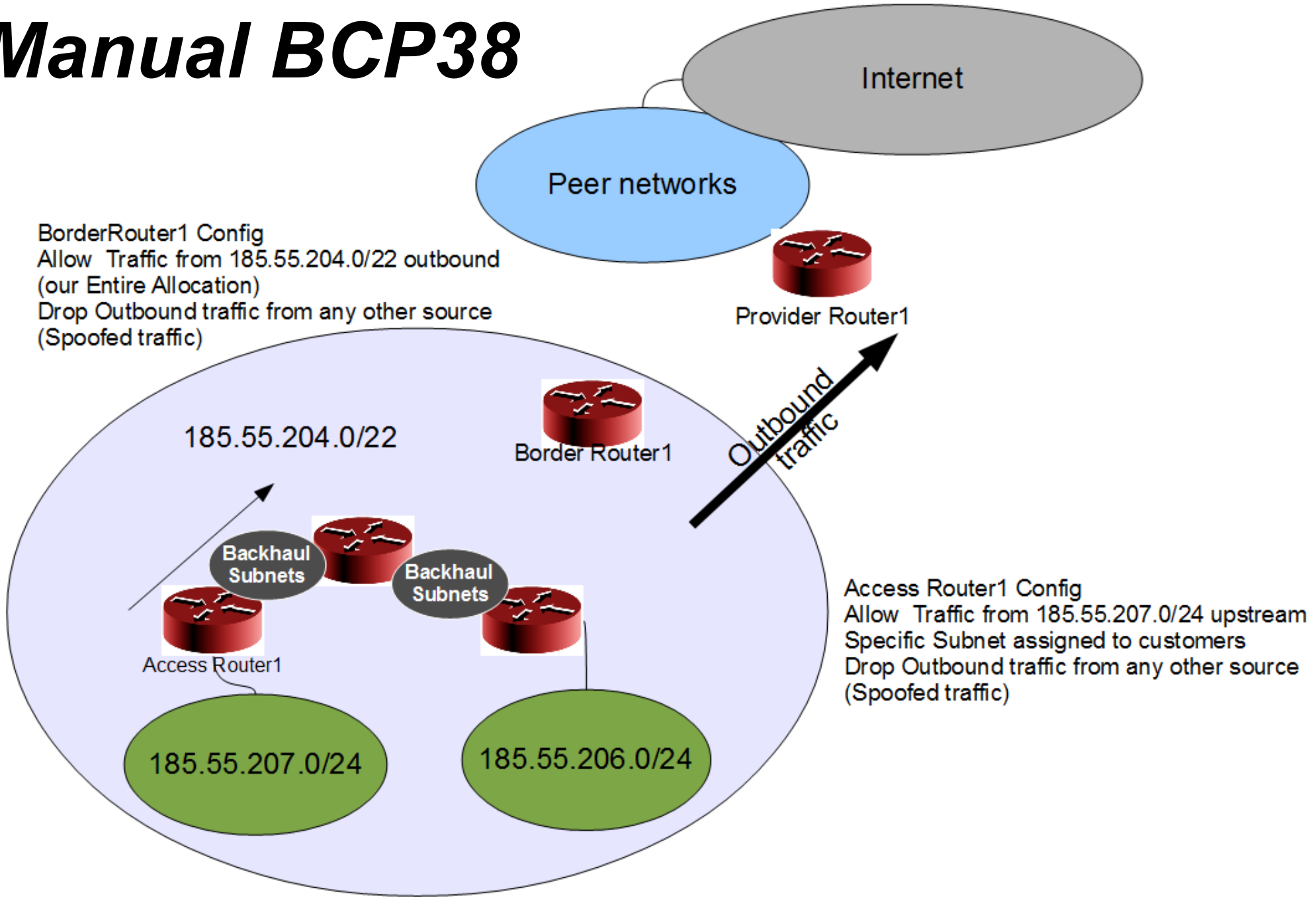
BCP 38 Limitations

- Implementation of BCP 38 at the only at border would still allow
- Spoofing from addresses witin the AS still possible
- Must apply BCP on specific Customer Subnets (hard to manage Manual)
- Malware will evolve

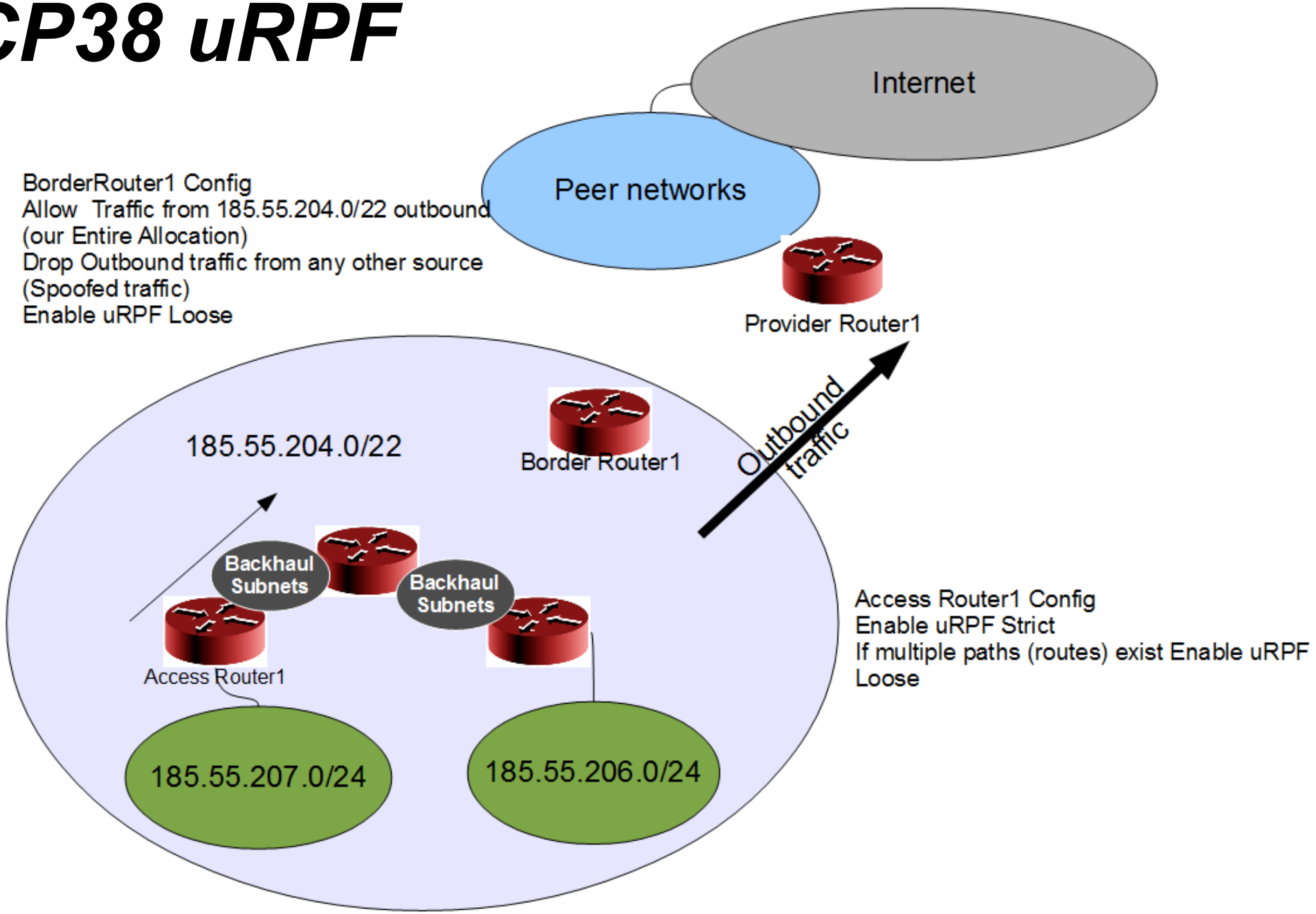
Responding to Malware evolution

- Spoofed Traffic within an ISP cannot be dealt with by BCP38 alone
- However this threat can be more easily be identified and managed by victims
  - Because spoofed traffic will obviously come from the same IP range
    - Why am I getting all this traffic from the ip range 5.134.88.0/21 ?
- BCP 38 can be implemented in a granular level, ISP subnet by Subnet by using strict uRPF (Unicast Reverse Path Forwarding)
  - URPF allows easy to manage granular and accurate mitigation of spoofed traffic.

Manual BCP38

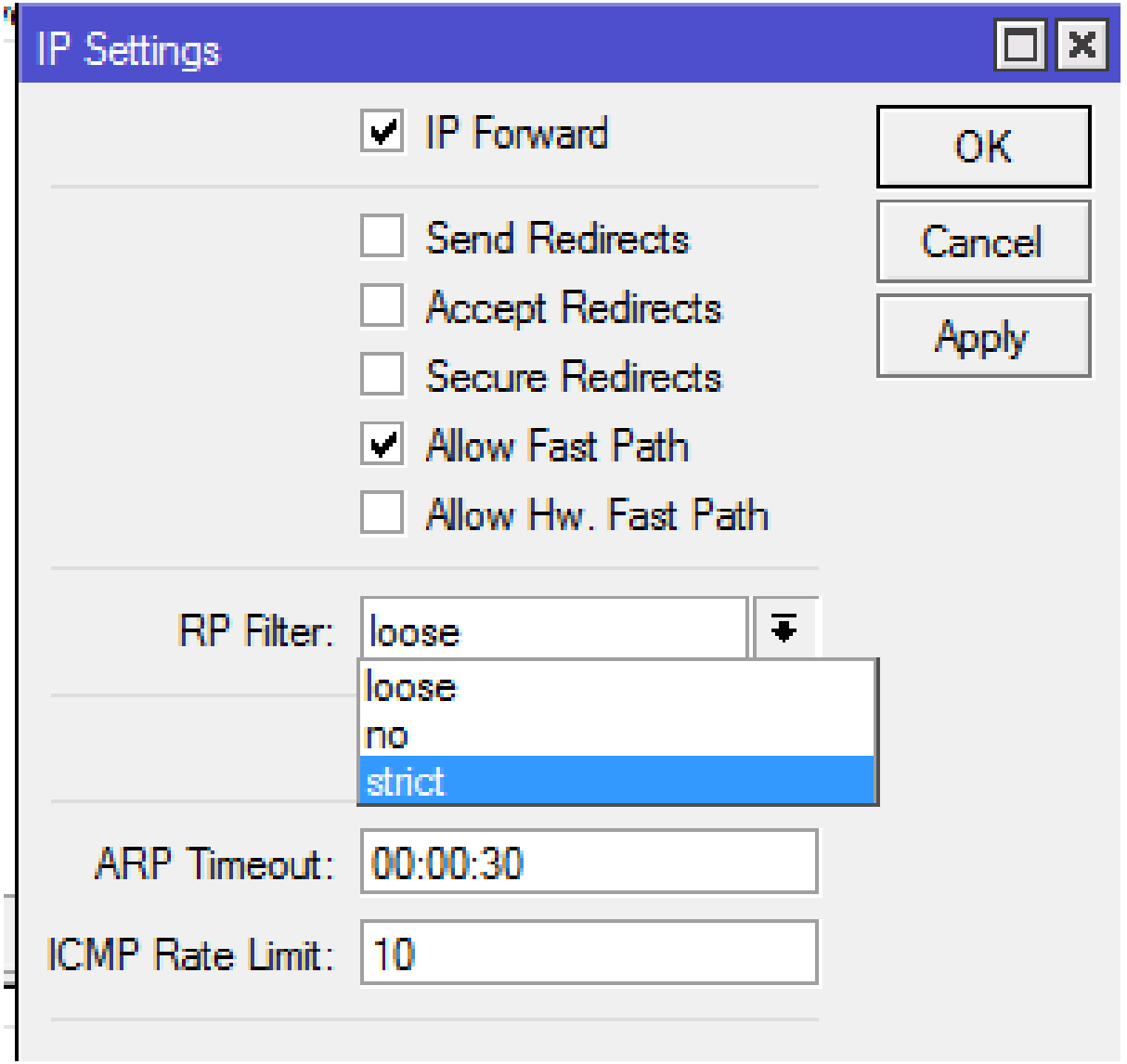


BCP38 uRPF



Turn on uRPF on Mikrotik

IP / IP Setttings



uRPF

- Route Traffic if the packets arrived on an interface on which you have a valid route in your FIB to the Src of the Traffic
- Strict uRPF Forward packets if ingress interface matches best possible Route in route table for traffic Source
- Loose uRPF Forward packets if ingress interface route exists in the
- If Route points at a Black-hole.. Don’t forward the traffic
- Faster than blocking with firewall Forward rule

Full Internet Route Tables & uRPF

- Pros
  - Have full visibility
  - Automatically Identify Upstream Faults on your own router
  - Provides automatic granular fail over of traffic to backup carriers
  - URPF provides some level of Source validation on traffic coming in... non internet addresses dropped.

- Make sure to remove default route (no need as you have the entire internet routing table)

What are the symptoms of a DDOS

- Massive Packet Loss
- At first it looks like a possible routing issue (but routing tables look ok)
- Links are Fully utilized (Inbound)
- Lots of UDP Traffic to one or more addresses on your network
- Your Link will Flat line / Saturate at full capacity and your providers network graphing systems will show a significant spike in traffic destined for you network

How Do I protect my network

- Do your Best.... and hope that your best will allow you prevail over the adversary
- Plan for the eventuality work out what you can and cant do.

How do I defend against attack?

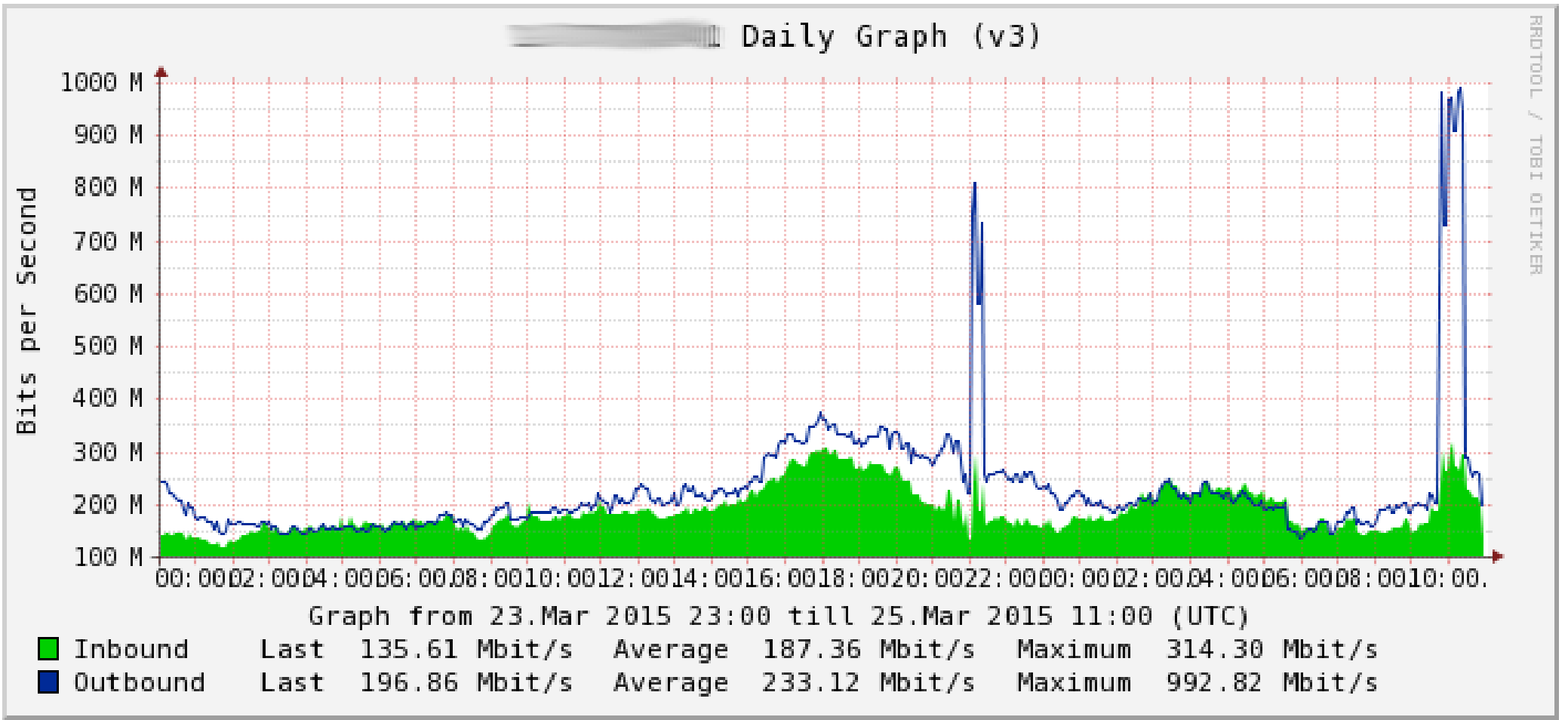
- Keep Calm
- Work through it … you will be backup soon...

Planning your Response

- Work out what your Upstream ISP capabilities are in dealing with a DDOS
- Work out what capabilities your network hardware has.
- What your links can handle
- Prepare an Incident response plan
  - Who is in control of the situation
  - What is acceptable to change with out Change control
    - Emergency Change Aproval Boards (Quorum rules etc)
- Identify weak points of your system and mitigate them
  - Purchase Hardware and software for management of the situation

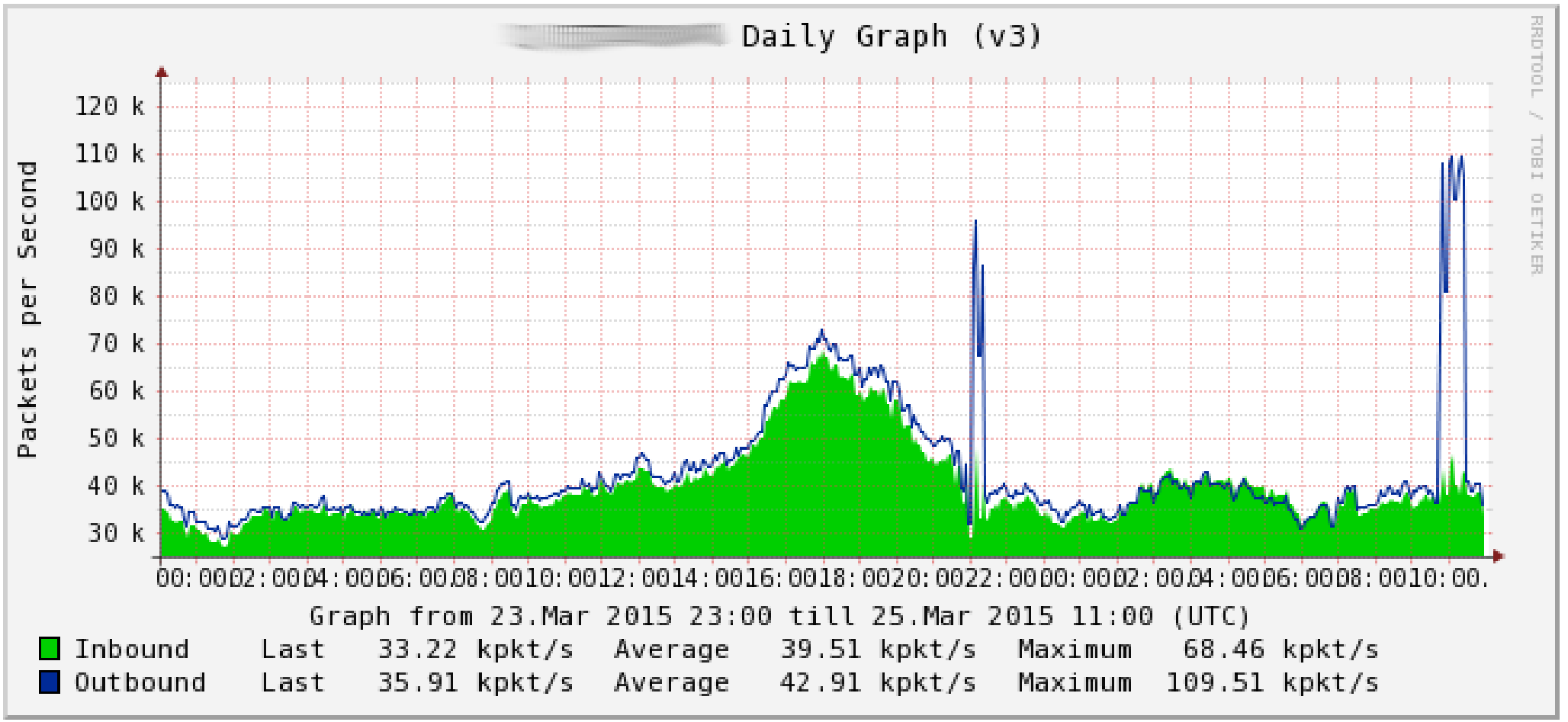
Detect a DOS attack- Bandwidth

- Check inbound interface Graphs for sudden spikes either on your router (Inbound Traffic)
- Or from your Service Providers monitored port (Outbound traffic)



Detect a DOS attack Packets per sec

- Check inbound interface Graphs for sudden spikes either on your router (Inbound Traffic)
- Or from your Service Providers monitored port (Outbound traffic)

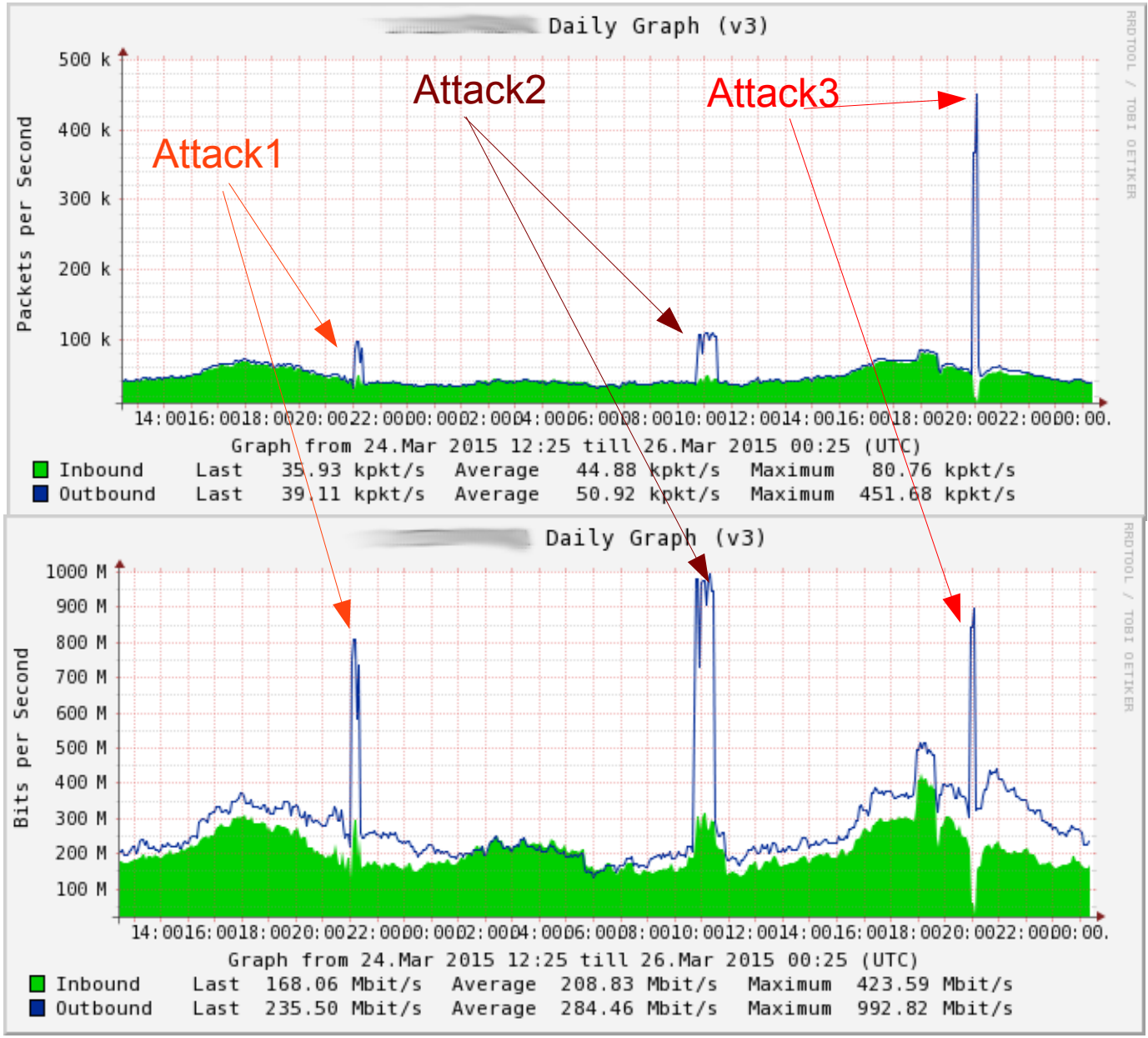


Monitoring tools for Networks

- Open NMS (lots of guys like this one)
- Observium (easy setup, lovely Graphs not hugely customizable)
- DUDE
- Netxms Tomas Kirnak worships this product (it is impressive)
- MRTG Mulit Router Traffic Grapher.. Thanks Tobias Oetkier (what all monitoring systems are based on
- PRTG
- Set Bandwidth Alert Thresholds, consider out of band Alerting (SMS etc) if your Email infrastructure is deep within your network.
- Cacti / Munin if you can get them working Greg Sowell does a great article on setting up Cacti … (I still hate Cacti)

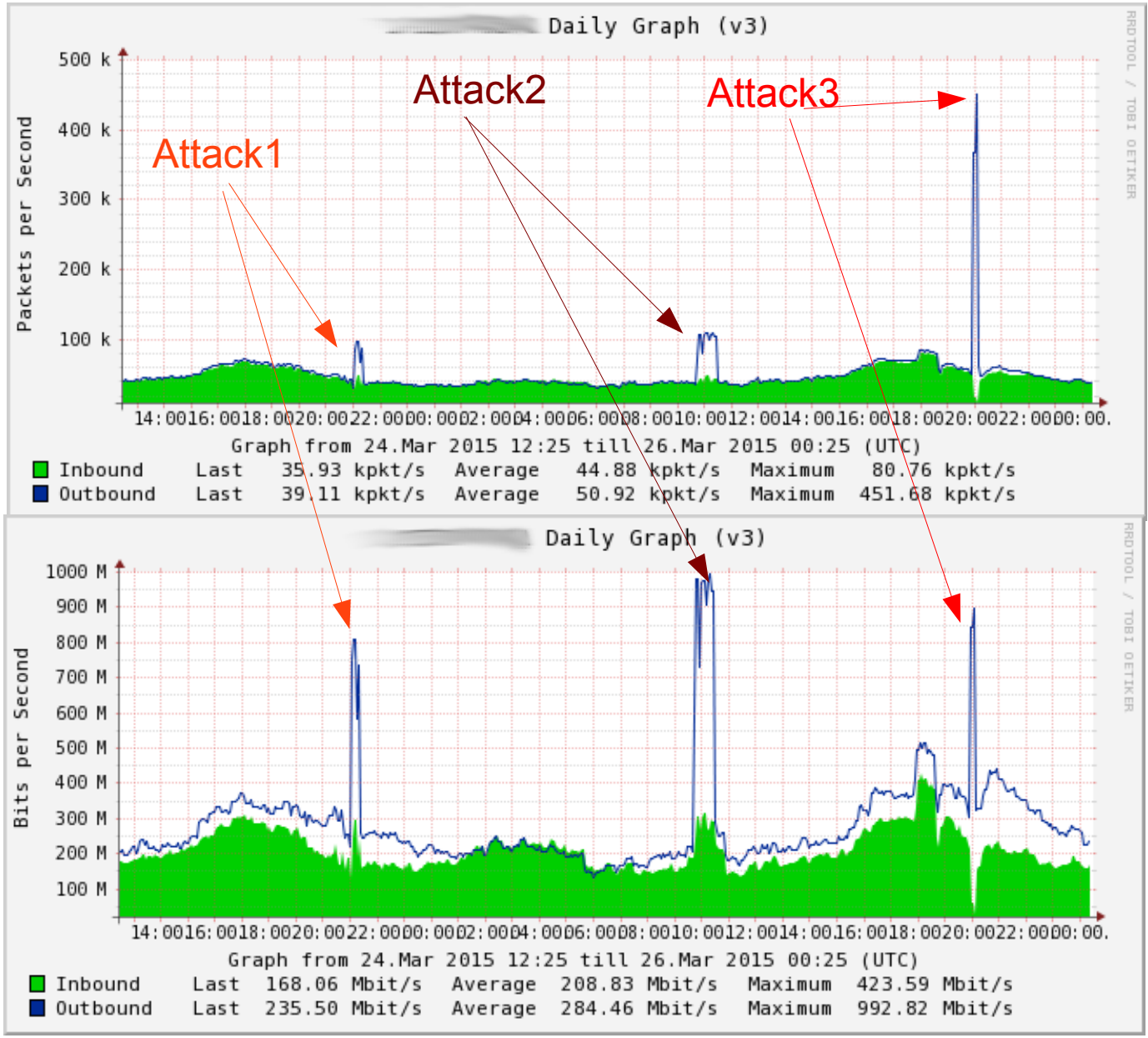
Analysing DOS traffic PPS vs bPS

- 3 attacks 1 day,
- Attack1
  - Peak bps 800mb/s (legitimate link demand 300mb/s)
  - Peak pps 100K packets per second (legitimate link demand about 40K packets per second
- Attack2
  - Peak bps 992mb/s (legitimate link demand 250mb/s)
  - Peak pps 110K packets per second (legitimate link demand about 30K packets per second
- Attack 3
  - Peak bps 900mb/s (legitimate link demand 350mb/s)
  - Peak pps 460K packets per second (legitimate link demand about 60K packets per second



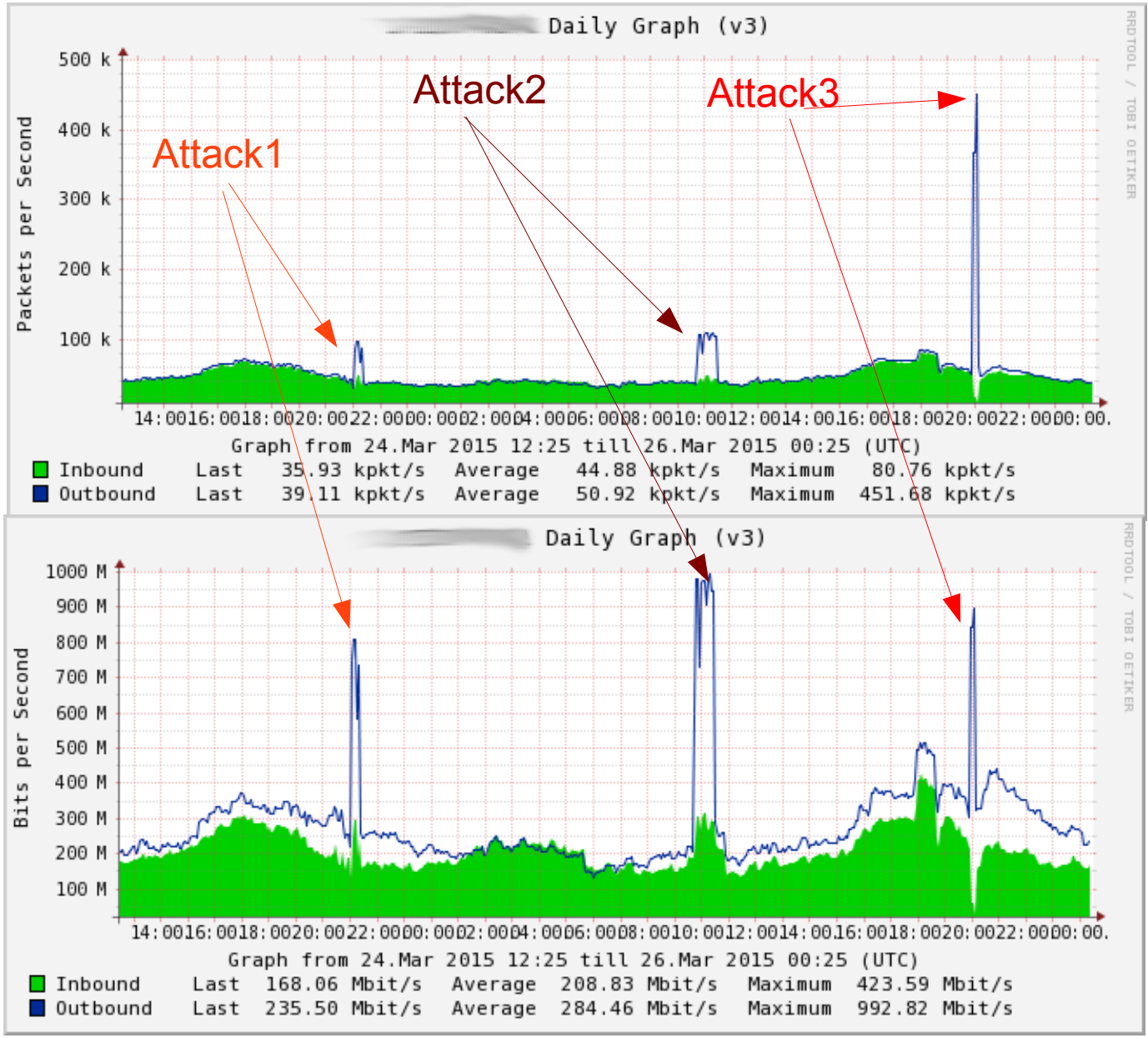
Analysing DOS traffic PPS vs bPS

- 3 attacks 1 day,
- Attack1
  - Detected bad traffic 500mb/s
  - 60k per second bad traffic
  - 1041bytes per bad packet (approx)
- Attack2
  - Detected bad traffic 700mb/s
  - 80k per second bad traffic
  - 1093 bytes per bad packet (approx)
- Attack 3
  - Detected bad traffic 550Mb/s
  - 410K packets per second bad traffic
  - 162 bytes per bad packet (approx)



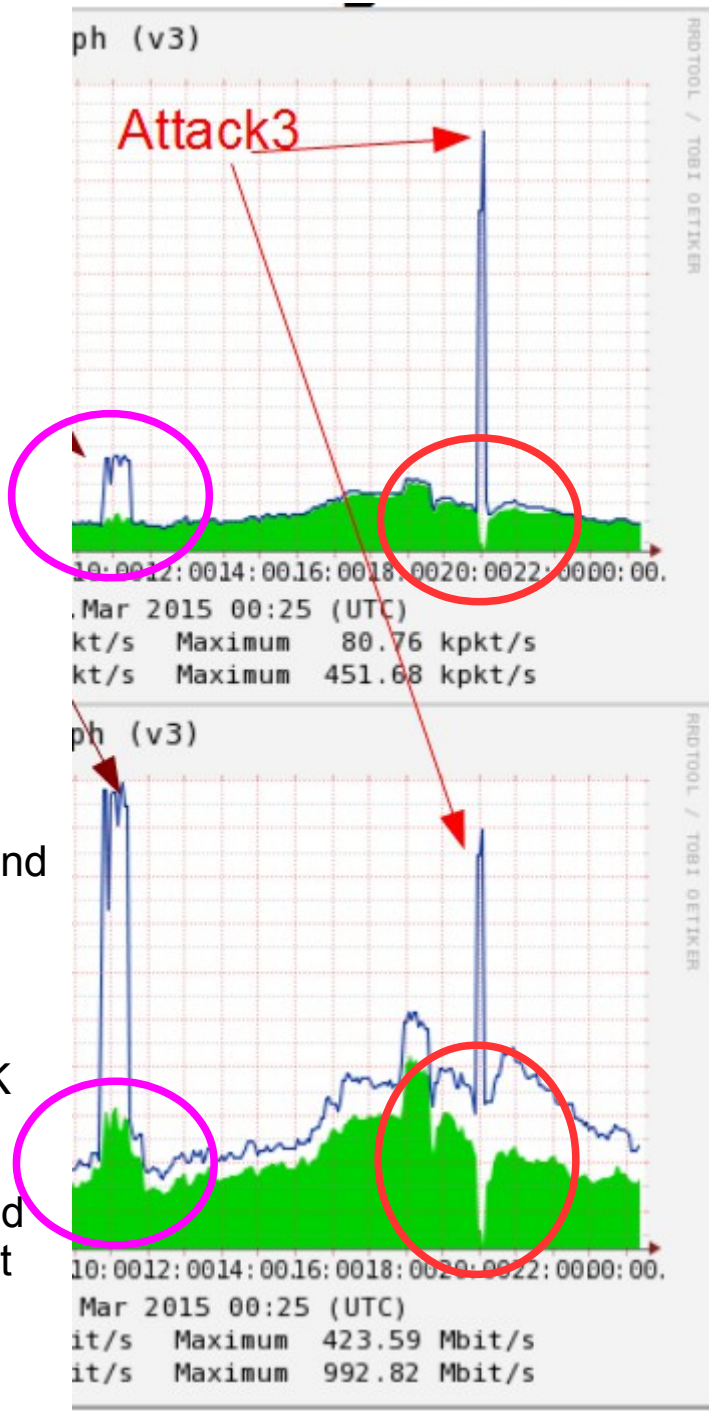
Analysing DOS traffic PPS vs bPS

- 3 attacks 1 day,
- Attack1
  - Detected bad traffic 500mb/s
  - 60k per second bad traffic
  - 1041bytes per bad packet (approx)
- Attack2
  - Very similar signature to attack1
  - Affecting same victim IP as attack1
  - Similar packet profile(approx)
- Attack 3
  - Detected bad traffic 550Mb/s
  - 410K packets per second bad traffic
  - 162 bytes per bad packet (approx)



DDOS measurement Uncertainty

- Key aspect of Measurement is that there is no significant disturbance in the system..(just enough to make a measurement and no more)
- Problem with DDOS is there is a massive Distrurbance, and different results each time,
- Compare Attack 2 and Attack 3 on the right
- Attack 2 had much higher peak Traffic bit rate compared with Attack 2
- However one can also see a significant decrease in legitimate traffic in Attack 3
- It would be very fair to assert that the DDOS in Traffic 3 displaced legitimate traffic Successfully this is show by the reduction in outbound traffic
- Notable Exception
- TCP Syn attacks will lead to a consequential increase in TCP SYN ACK return traffic (servers responding to the spoofed connection reuests
- In this case the increase in outbound traffic in attack 2 is actually caused by the attack being a SYN flood (and could well have displaced a lot of legitimate traffic



Removing Uncertainty

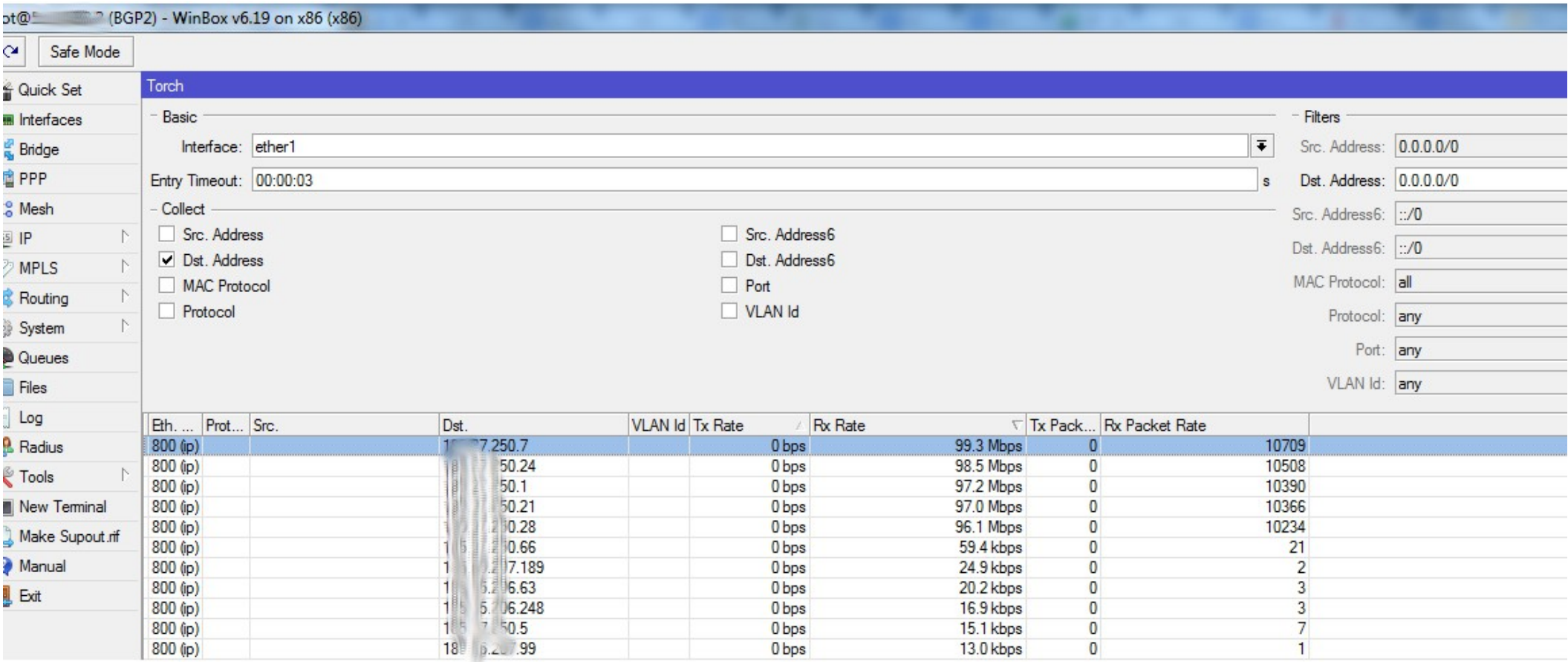
- Enter Netflow / Sflow :)
- Mikrotik supports Netflow
- Sflow is Sampled 1 in 1000 or 1 in 10000 packets sampled rather than every packet (lower resources required)
- Real effect of DDOS can be measured (before during and after)
- Requires effort and resources to setup preparing for an attack (not so much in response to an attack)
-

But I didn't Setup Netflow :(

- Dont worry … Happens everyone Including me :)
- That is why the tool Torch exists...
- It allows you to shine a light in a very dark place...

Torch and net-flow

- It is kind of like a torch when you are out camping...
- Netflow is more like the floodlight system in your national stadium



What if I'm attacked

- Implement the Plan
- Try to identify the target of the attack (where is all the traffic heading towards)
- Work with all interested parties,
  - The Victim (could be an ordinary customer)
  - Your Peers / Upstream ISPs
- Use Torch /Netflow to identify which servers / services are being targeted ...is it a single ip or an entire sub-net

Victim Profiles

- Gamers
- Gamers
- Trolls
- Trolls
- Trolls
- Gamers
- Government Organizations subject to dispute
- Commercial Organizations subject to dispute

Working with Victim of the DDOS

- Inform them.... tell them the nature of the problem ...
  - They are under attack
  - You are working to mitigate the attack
  - To get them back up you will have to change their public IP range
  - That the attack may follow their new IP and that this will have to be repeated for the duration of the attack

Working with Victim of the DDOS

- Prepare to migrate them to a new IP range
  - assist them with DNS moves if necessary (short TTL)
- Prepare the IP Migration in a manner that makes it as simple for the client as possible
- Repeat the migration from one IP to another

Working with Your ISP Transit Providers

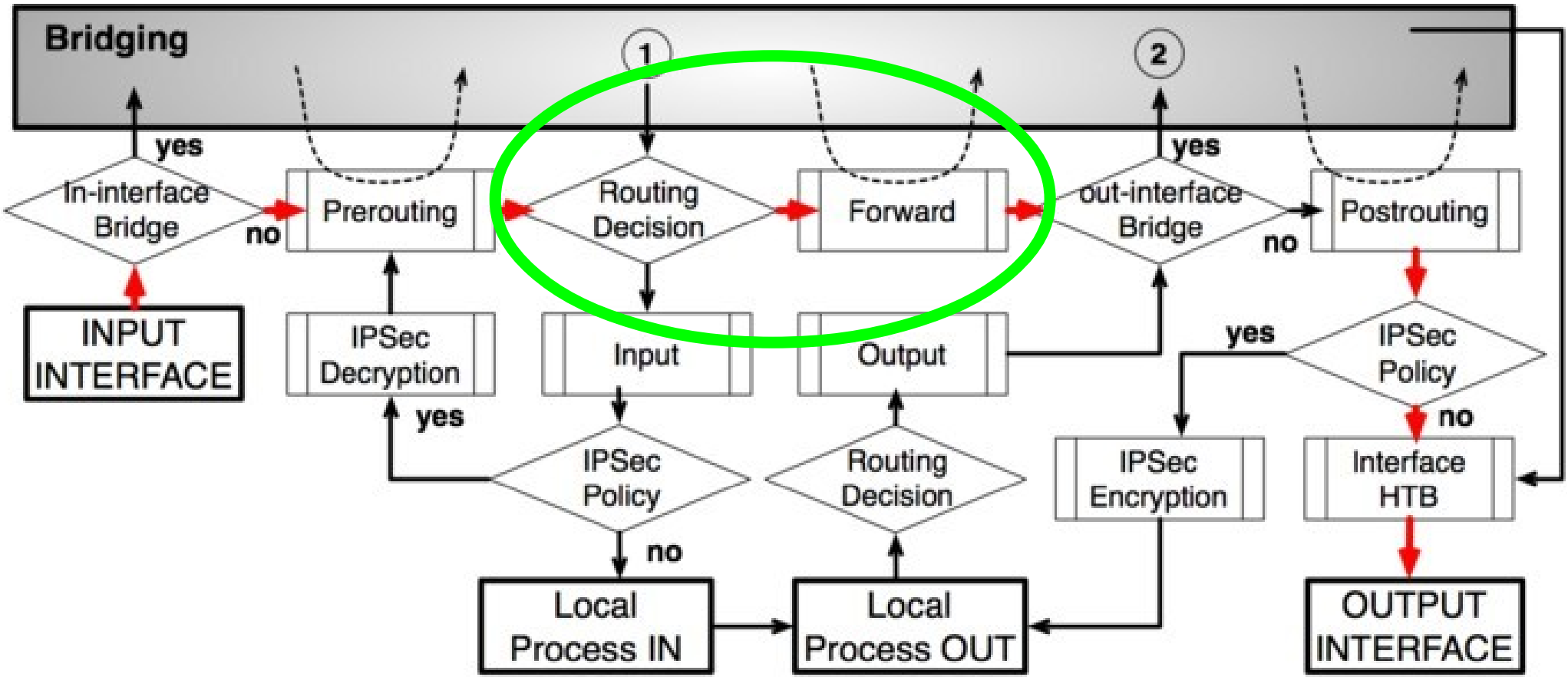
- Contact them by phone and let them know the situation.
- Let them know the Ips on your network that are being attacked
- Your provider has much more capable Routers and they should be able to “blackhole the IP address under attack across their network”

What are Black hole routes ?

- Using the routing process to filter packets

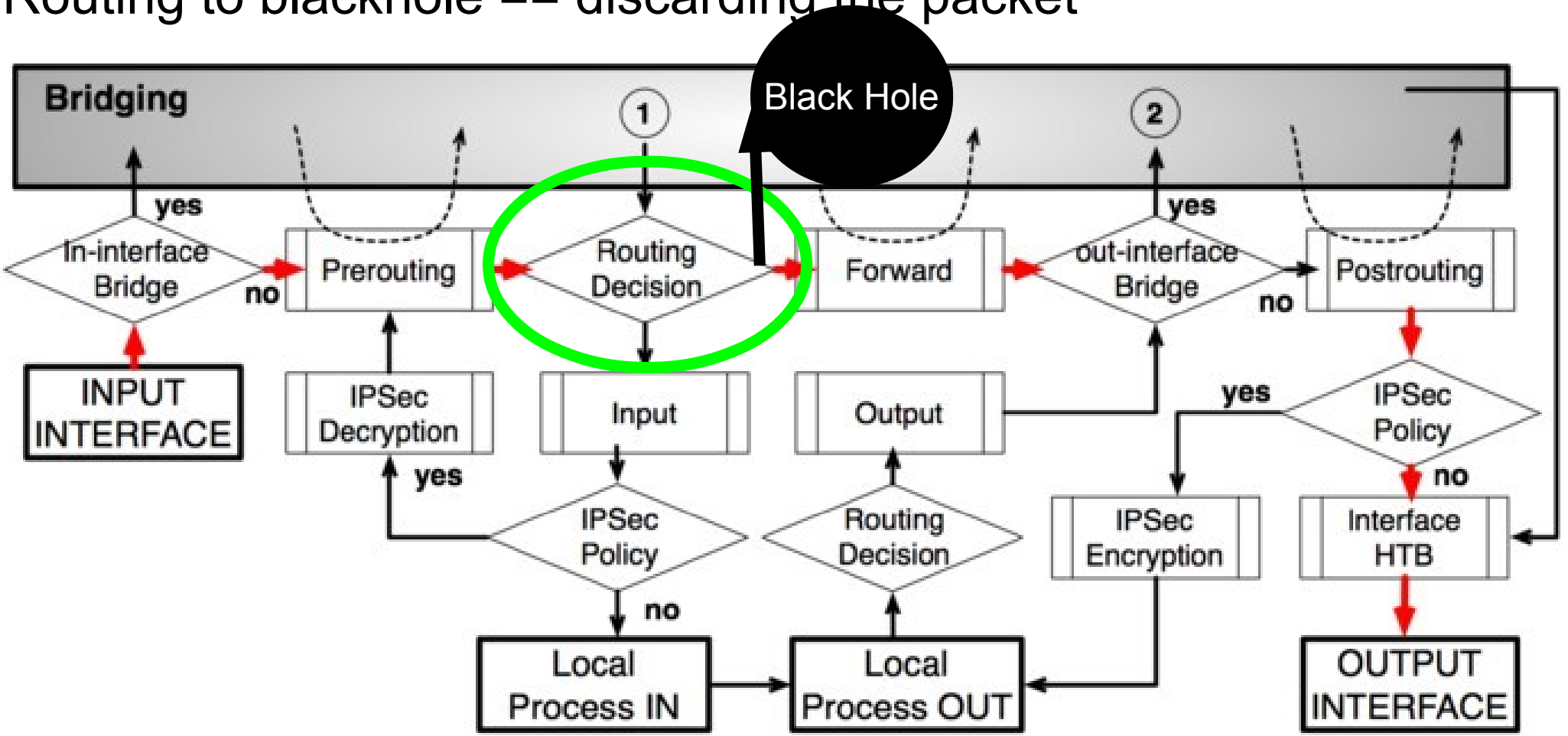
Standard Firewall Filtering

- Filtering with the Firewall Forward Chain
- 3 processes: Pre-routing(Mangle), Routing, Forward (filter)



Black hole

- Filtering with the Routing Process
- Forward or not made early (at routing process)
- Routing to blackhole == discarding the packet

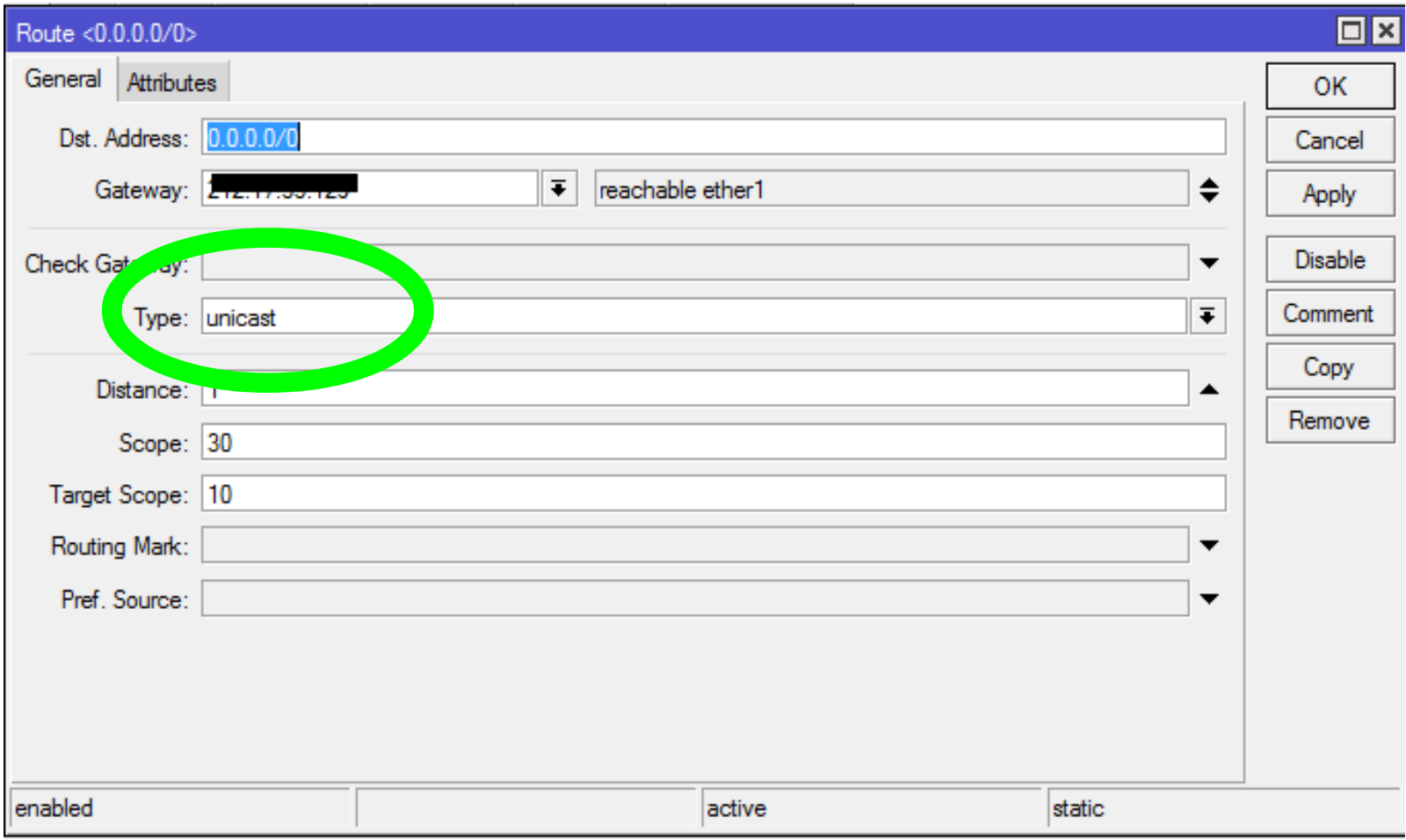


Efficient

- Checking and dropping in the
  - Routing process
- As opposed to
  - Routing process
  - +
  - Forward Filter Process
- When running close to CPU capacity of a router
- CPU cycles saved during the processing of each packet can make a real difference

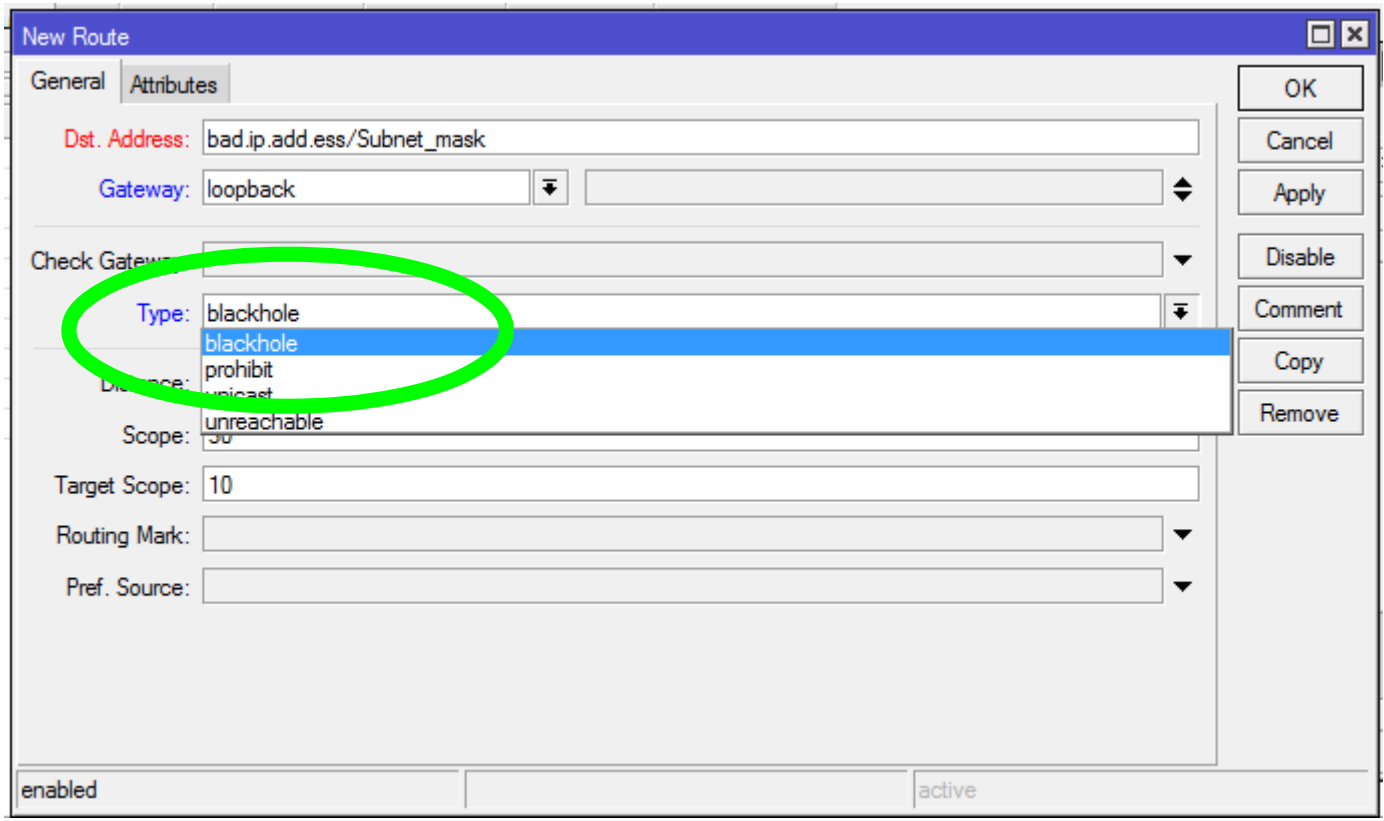
Filtering Using Routes

- Most people are familiar with Routing as a tool to help traffic reach its destination
- These “Normal” routes are called Uni cast routes



Adding a Black Hole route

- Black Hole – the name from the astronomical phenomena where any object placed into the Black Hole will never leave due to the force of gravity!
- Black Hole Route – Discard the Packet (and end processing of it)



Black hole

- Once this step is completed
  - Traffic Levels will Decrease to your network
  - All Legitimate traffic destined for the black holed Ips will be dropped
  - All Attack traffic destined for the black holed Ips will be dropped also

Faster Response for DDOS issues

- Is there a way to automate that DDOS Remediation process outlined previously?

Faster Response for DDOS issues

- Is there a way to automate that DDOS Remediation process outlined previously?

Faster Response for DDOS issues

- Is there a way to automate that DDOS Remediation process outlined previously?
- YES!

Remote Triggered Black Holes

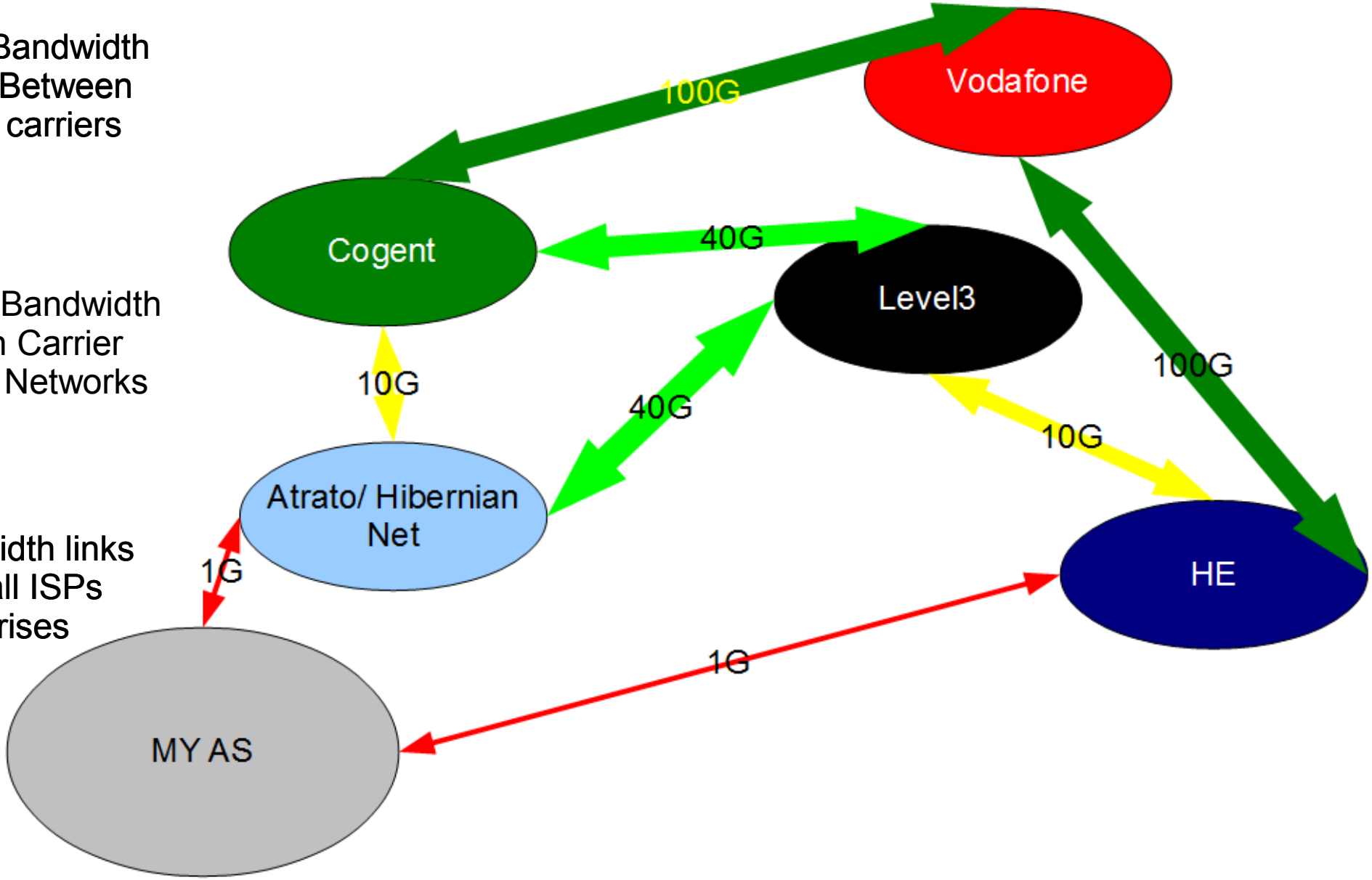
- A way to automate the process of Blocking traffic destined for Ips in your network On your Peers / Providers Network
- Stops Traffic Before it is too late...
- Too Late (when the traffic has swamped your NIC on your Router)
- You have maximum control over the process
  - No Implementation lag
  - Allows a more responsive approach to changes in attack dynamics

Internet (simplified)

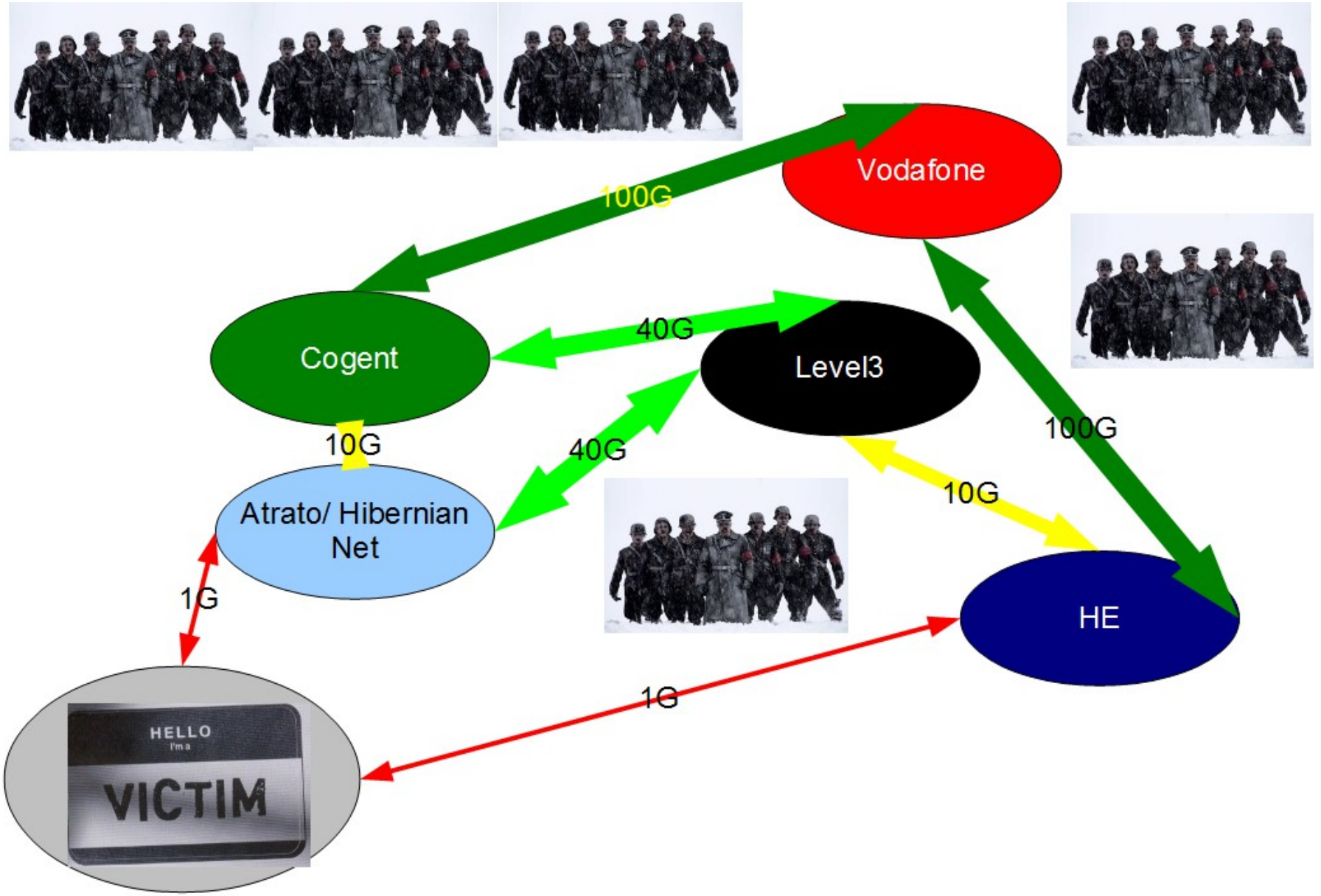
High Bandwidth Links Between Large carriers

High Bandwidth within Carrier Core Networks

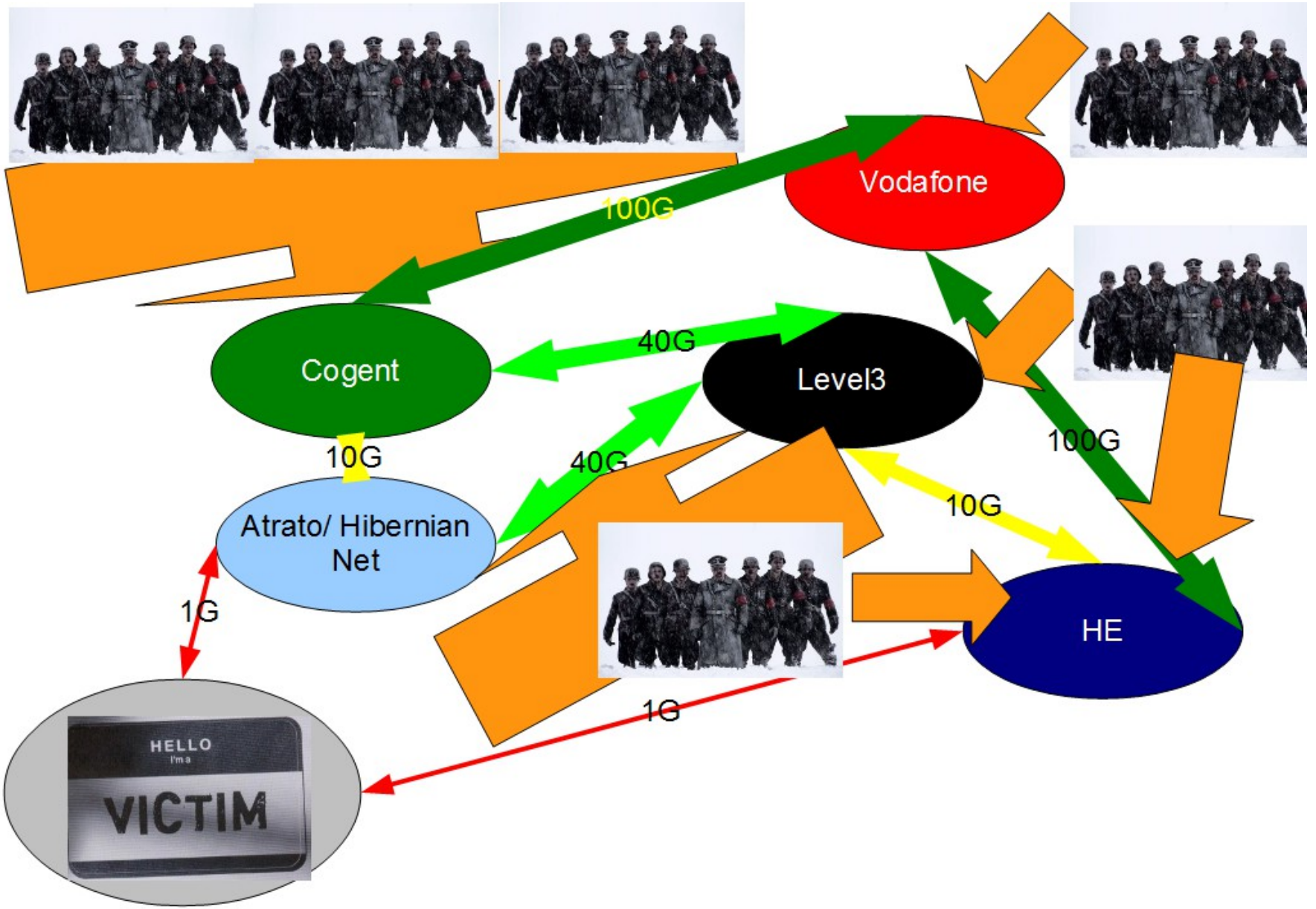
Small Bandwidth links to Small ISPs Enterprises



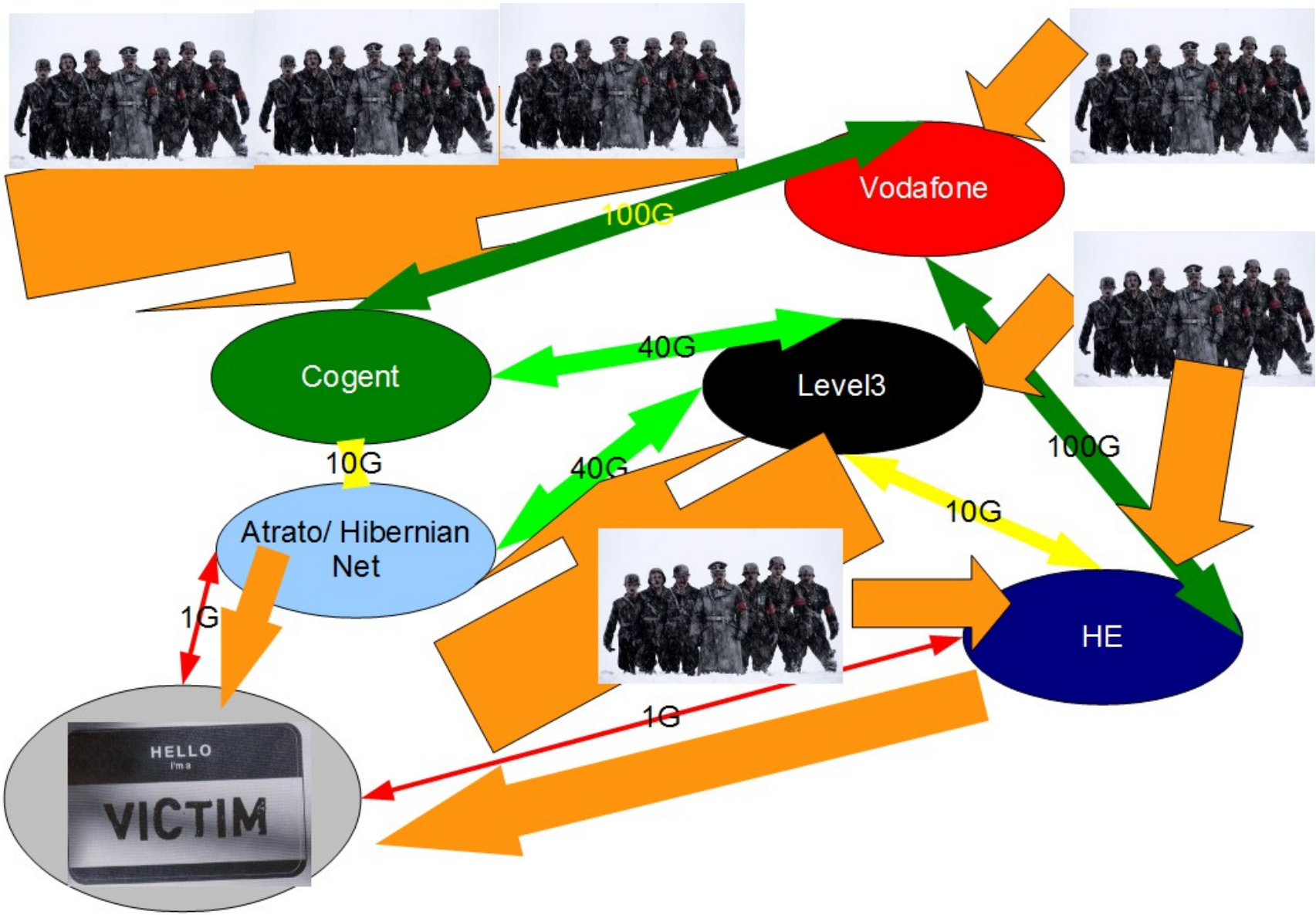
Enter Zombie Armies / Bot Nets



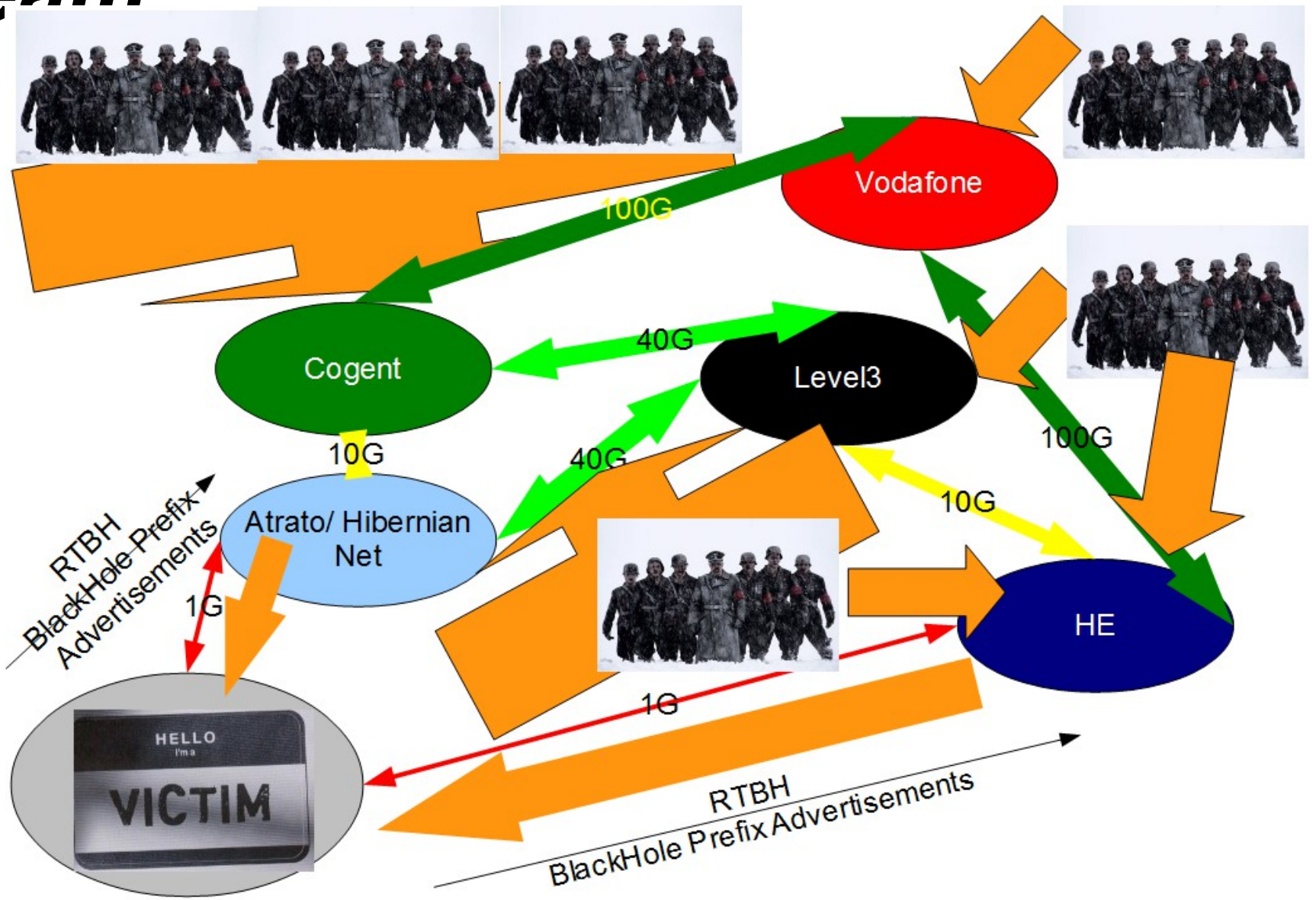
Attack Begins Flooding UDP traffic



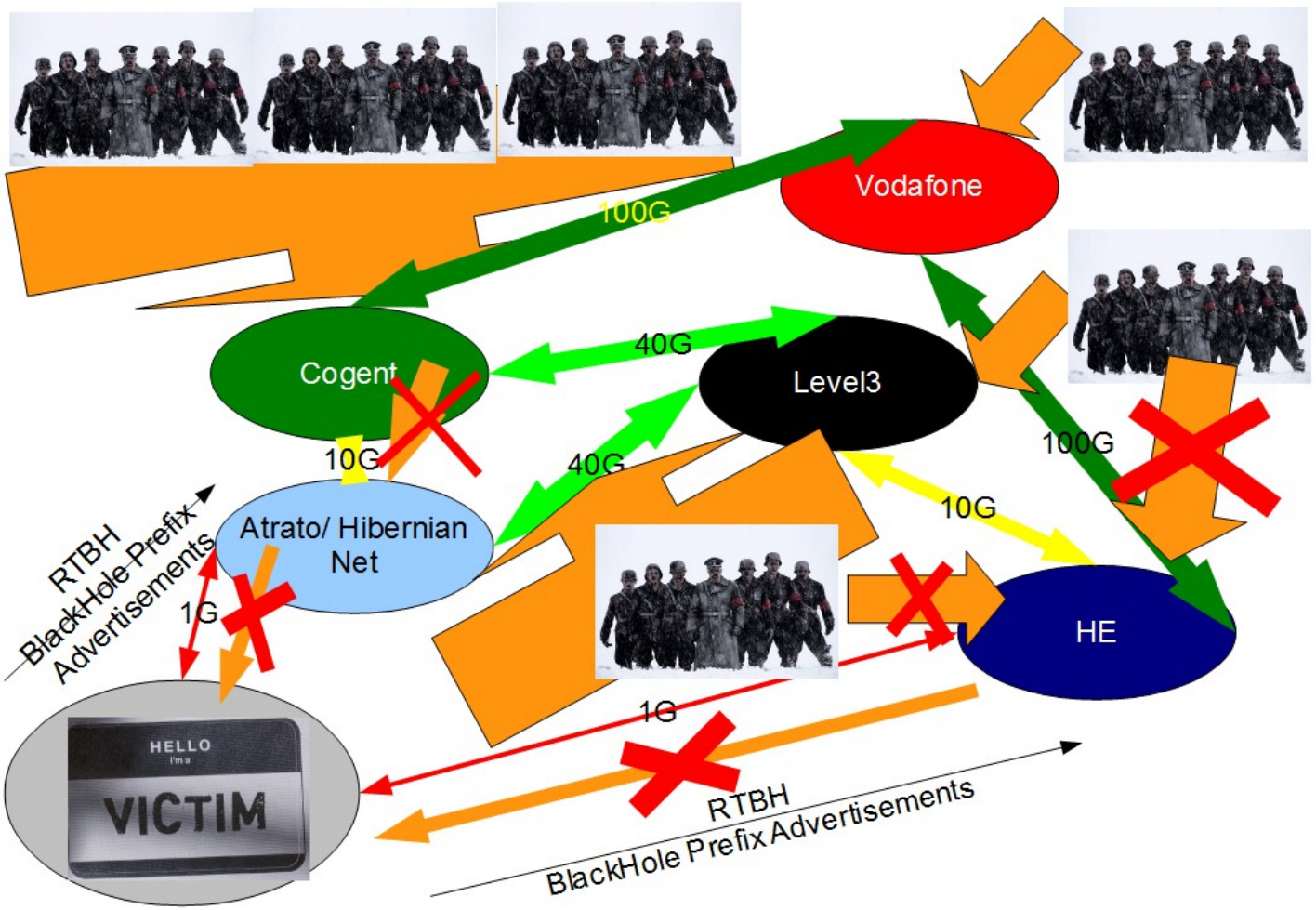
Flood Converges on your Transit Links



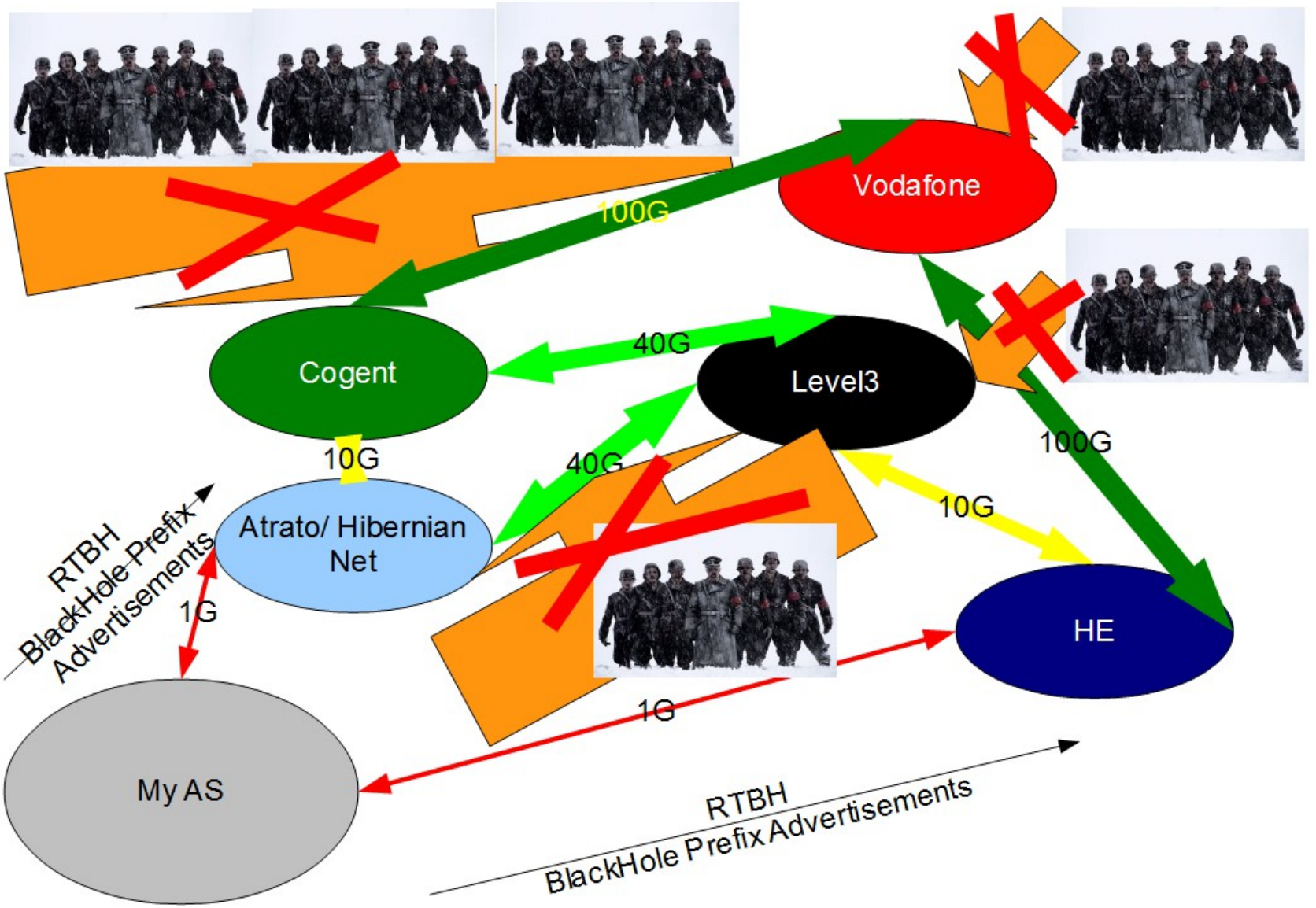
Advertise Black hole prefixes upstream



Upstream ISPs cut the traffic Before it is too late Before your Links Saturate



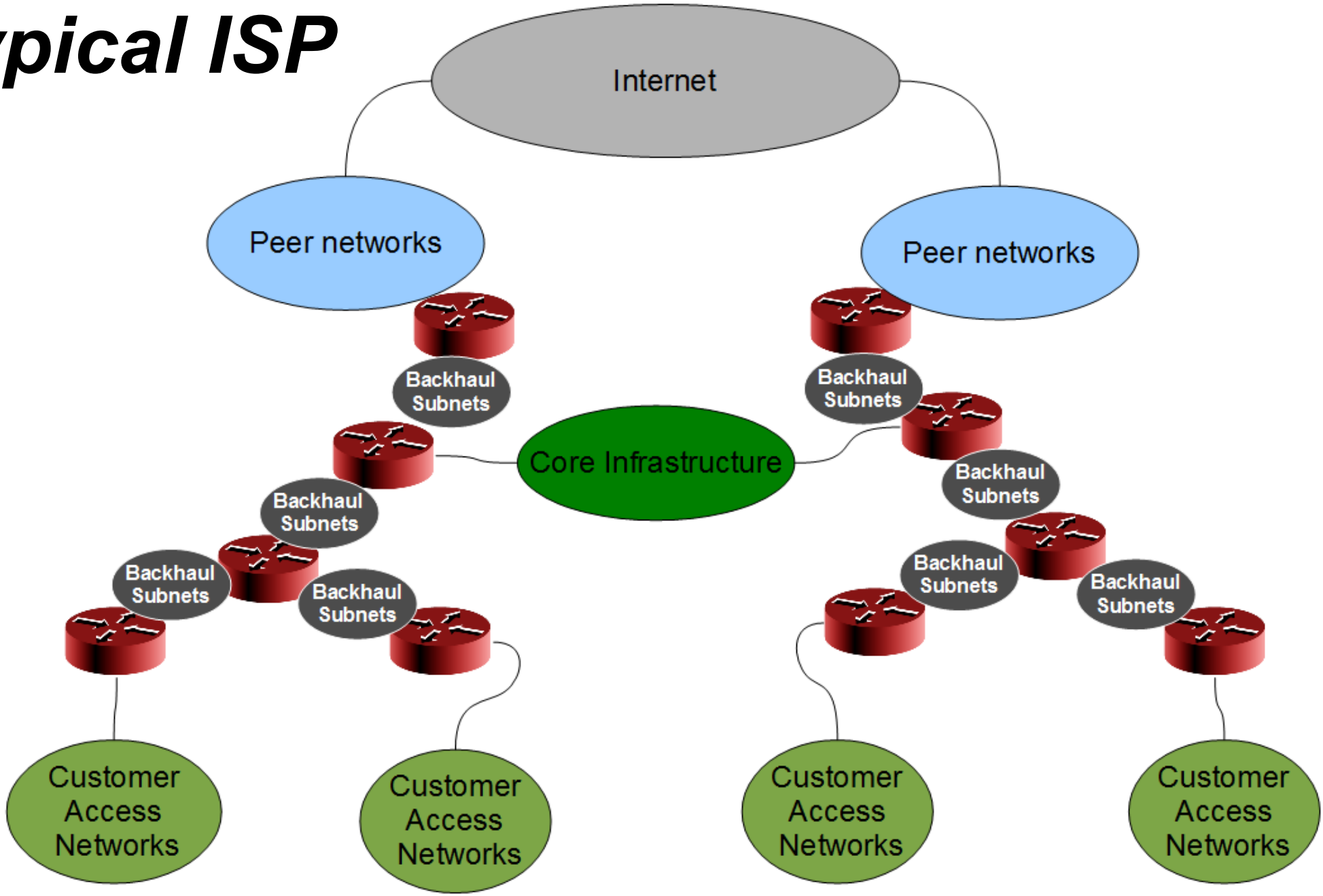
Upstream ISPs Pass on details of attack to their peers



Reducing the incoming Attack

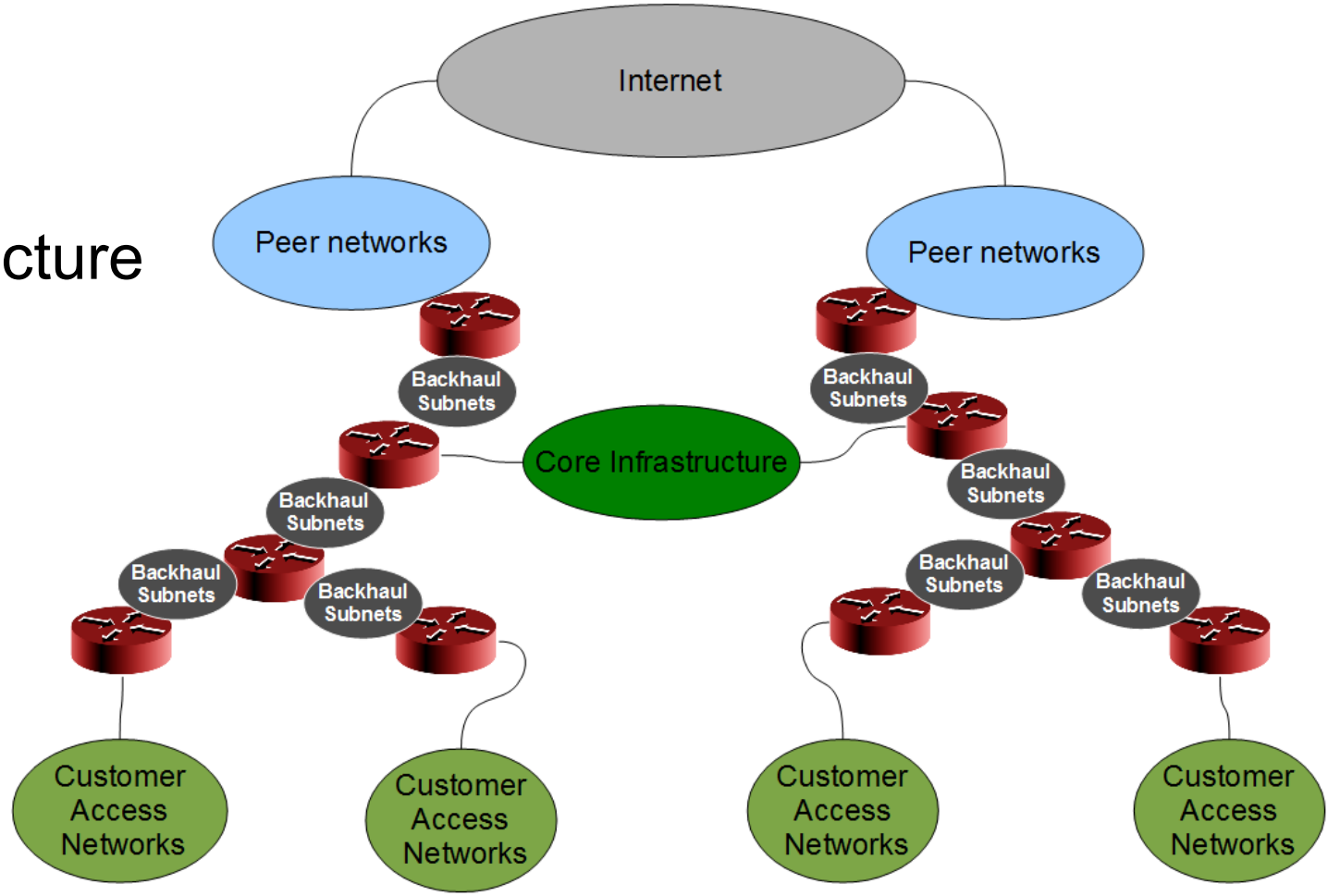
- Allow traffic to your customers
- Block everything else

Typical ISP



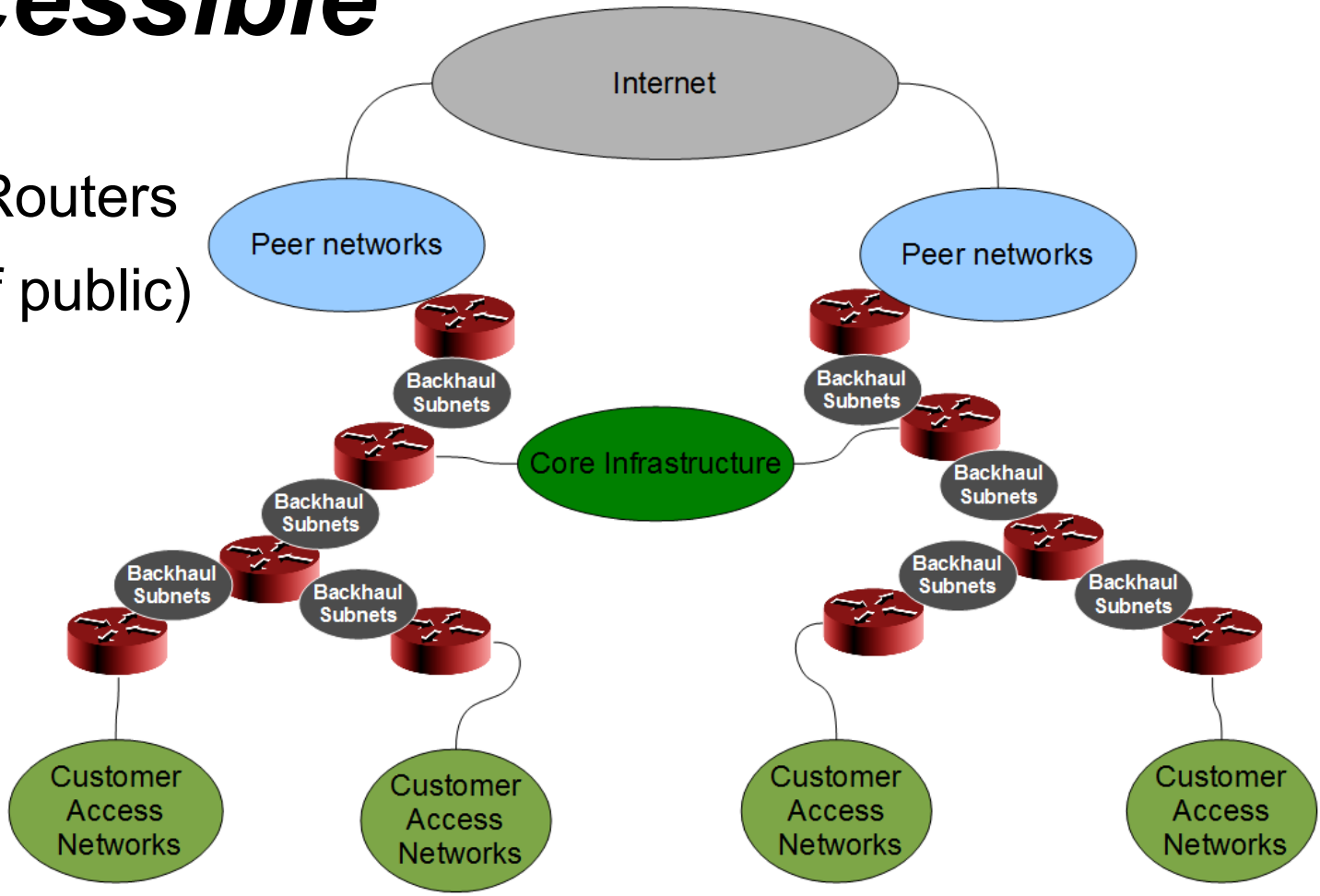
What really needs to be Internet Accessible

- Customer VIPs
- Some Core Infrastructure Ips
- Not Much else...



What Ips that don't have to be internet accessible

- Back haul subnets
  - Subnets between Routers
  - Management ips (if public)
- Un Allocated VIPs
- Un Used VIPs



If an IP doesn't need to be internet accessible can we simply black-hole it ?

If an IP doesn't need to be internet accessible can we simply black-hole it ?

- Cant argue with that logic...

Client Subnet Analysis - /30

Subnet Mask CIDR	Network Address	Your Router IP CPE Default GW	Customer CPE IP	Subnet Broadcast
/30 255.255.255.252	0	1	2	3

- What IP addresses need to be accessed from the internet ?

What needs to be routable ?

- Client IP addresses.

What can we obviously blackhole?

Client Subnet Analysis - /30

Subnet Mask CIDR	Network Address	Your Router IP CPE Default GW	Customer CPE IP	Subnet Broadcast
/30 255.255.255.252	0	1	2	3

- Easy we can block Network Address and Subnet Broadcast Addresses!
- For example we can create the following black hole routes
  - 192.168.0.0/32
  - 192.168.0.3/32

Can we Lock this down further?

We can Black hole our Router IP

Subnet Mask CIDR	Network Address	Your Router IP CPE Default GW	Customer CPE IP	Subnet Broadcast
/30 255.255.255.252	0	1	2	3

- Our Router does not need to be reachable from the Internet
- For example we can create the following black hole routes
  - 192.168.0.1/32

Black Hole Network and Broadcast

Subnet Mask CIDR	Network Address	Your Router IP CPE Default GW	Customer CPE IP	Subnet Broadcast
/30 255.255.255.252	0	1	2	3

- Blocking 3 of the 4 IPs in the Subnet
- We reduce our attack surface by 75%
- Customer IP is un-affected by change

Downside?

- Traceroutes from outside your network to clients may have gaps in it
- BOOO HOOOO HOOOOO

Who Cares ?

Its worth it! :)

- Will Increase the Sizes of your Routers Routing Tables
  - Buy Bigger Routers Bitches :)
  - CCRs 16GbRam (not a problem)
  - 64bit Router OS ... on x86... ----- Wont be a problem

What about /29s?

What about /29s?

I'm glad you asked !

What about /29s ?

Subnet Mask CIDR	Network Address	Your Router IP CPE Default GW	CPE IP?	CPE IP?	CPE IP?	CPE IP?	CPE IP	Subnet Broadcast
/29 255.255.255.248	0	1	2	3	4	5	6	7

- Well lets apply the same logic as before...

What about /29s ?

Subnet Mask CIDR	Network Address	Your Router IP CPE Default GW	CPE IP?	CPE IP?	CPE IP?	CPE IP?	CPE IP	Subnet Broadcast
/29 255.255.255.248	0	1	2	3	4	5	6	7

- Well lets apply the same logic as before...

What about /29s ?

Subnet Mask CIDR	Network Address	Your Router IP CPE Default GW	CPE IP?	CPE IP?	CPE IP?	CPE IP?	CPE IP	Subnet Broadcast
/29 255.255.255.248	0	1	2	3	4	5	6	7

- 3 of 8 Ips have been Blackholed
- 37.5% reduction in attack surface

Any more improvements ?

Potentially ....

- How many IPs are active on client side?

3 used IPs (VRRP/ Loadbalancer)

Subnet Mask CIDR	Network Address	Your Router IP CPE Default GW	x	x	CPE IP RIP	CPE IP RIP	CPE IP VIP	Subnet Broadcast
/29 255.255.255.248	0	1	2	3	4	5	6	7

- 5 of 8 Ips have been Blackholed
- 62.5% reduction in attack surface
-

2 used IP addresses

Subnet Mask CIDR	Network Address	Your Router IP CPE Default GW	x	x	x	CPE IP	CPE IP	Subnet Broadcast
/29 255.255.255.248	0	1	2	3	4	5	6	7

- 6 of 8 Ips have been Blackholed
- 75% reduction in attack surface

1 used IP addresses

Subnet Mask CIDR	Network Address	Your Router IP CPE Default GW	x	x	x	x	CPE IP	Subnet Broadcast
/29 255.255.255.248	0	1	2	3	4	5	6	7

- 7 of 8 Ips have been Blackholed
- 87.5% reduction in attack surface

So If my entire Network is under attack...

- If your entire network is being attacked (all IP adresses s in your Allocation)
- You Can reduce the traffic inbound to your network
- Traffic Reduction by the order of

$$\frac{\textit{No. of Blackholed IP Addresses}}{\textit{No. of IP Addresses in Prefixes Advertised in eBGP}}$$

So Start planning your Defense

- Map out your network IP Plan
  - http://iptrack.sourceforge.net/
- Introduce a Standard for Subnet provisioning to clients
  - Our Router will have the First / Last IP in the subnet
  - Client Router will be the Last / First IP in the subnet
- Reserve an allocation of Ips for Transmission / Back haul networks
  - Block a summary supernet of Back haul Subnets

If things get Really Scary

- Do Arp Scanning of Client Subnets ..
  - to identify if more un-used IPS can be Blackholed...
- If you can reduce exposed Ips by 90%...
- You can reduce the attack traffic by 90% also :)

Filtering based on Source

- Deployed generally only on internal Networks (where you trust the advertiser)
- Transit Peering Oh my God --- 8.8.8.8 is attacking us .... Can you please black hole them .... Whoops
- If you Identify a source of attack you can blackhole with RPF on your Network
- You can contact NOC of up-streams and explain what you are seeing .... they will help...
- Spoofed UDP traffic ... harder to deal with ... 8.8.8.8 may not be Screwing your Network

Automatic RTBH between ISPs

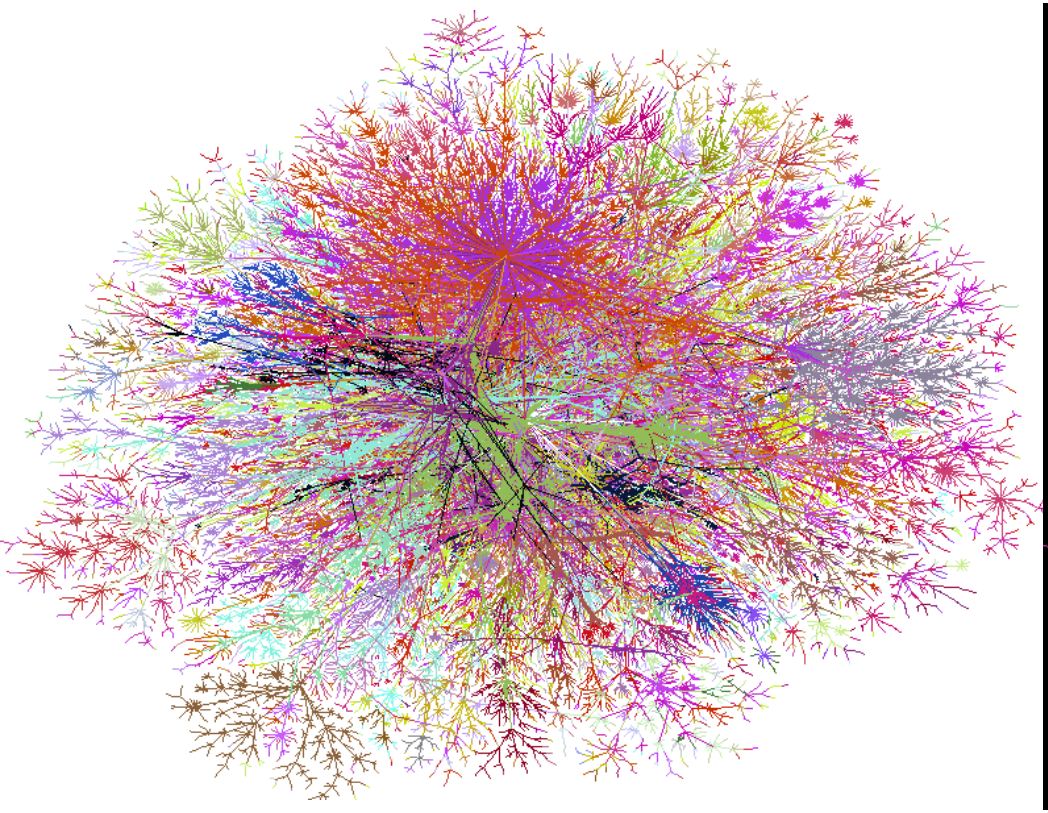
- Automatically accept Black hole announcements (with appropriate community from your customer if
  - They only announce prefixes within their own IP assignments (check RIPE RPSL
  - They only announce /32 routes
  - Limit the number of prefixes they can announce
  - Trust based on the fact they can only block their own IP ranges

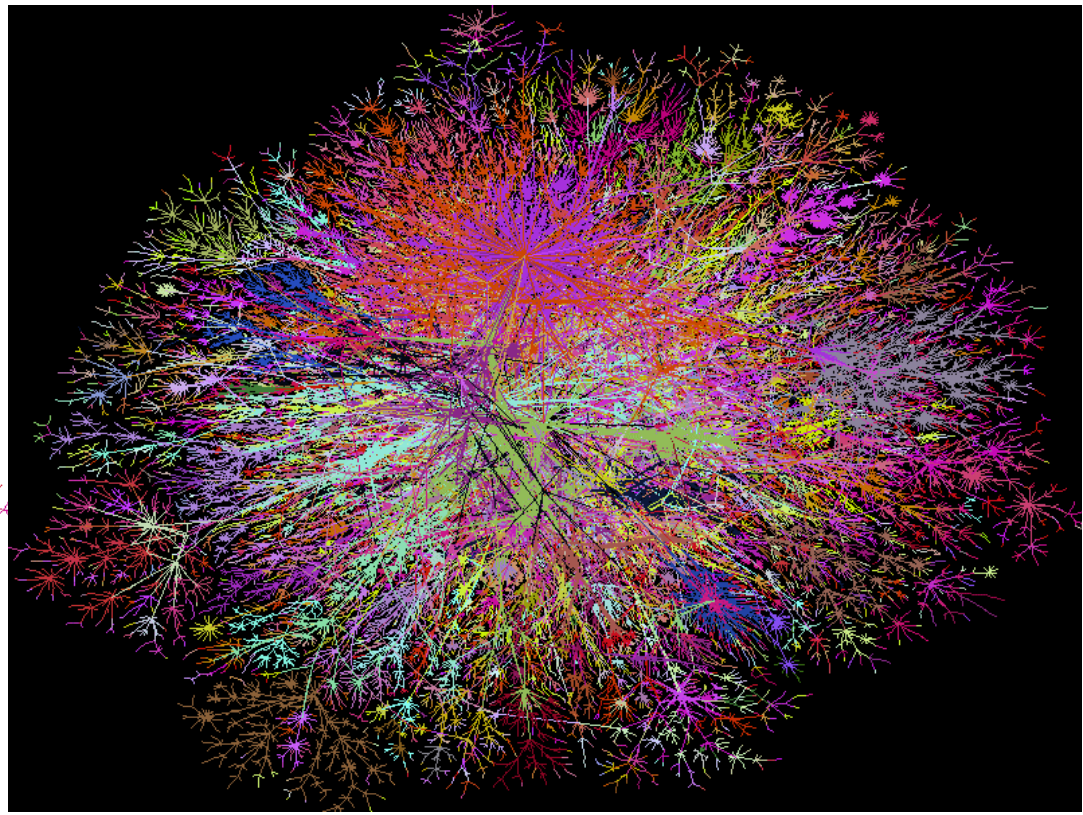
RTBH -Preventing Collateral Damage

- If Customer A suffers a Large scale DDOS attack
- Then all your other customers will suffer
- Better off to
  - Black hole customer A
  - Contact them and give them alternate IP address
  - Advertise your Black hole route to your upstream Black Hole Route servers (if you own the IP under attack)
  - Providers are only too happy to help dropping DDOS traffic Across their Network

BGP-- Bogon filtering illustrated

- All unallocated areas of IPv4 spaces are masked off with blackhole Routes
- Communication with illegally advertised addresses will not be possible





RTBF Guidelines

- Ask your transit provider for a peering session with their black hole route server (insist on this)
- Set up your own Black hole route server(iBGP Route Reflector Setup)
- Configure your own Black hole Route Servers and Core routers to do Black hole Filtering based on Src and Destination

RTBF Guidelines

- Do Setup Peering with downstream providers blackhole route servers
- Do Filter your Route Advertisements and use BGP communities to signal policy changes
- Do Filter on your core routers to accept only /32s from your BH RS
- Do Filter peering sessions with third parties.(their Prefixes only)

Further Reading on RTBH

- Presentation by INEX CTO at RIPE
  - https://ripe65.ripe.net/presentations/285-inex-ripe-routingwg-amsterdam-2012-09-27.pdf
- Sample Configurations for RTBH Servers and Clients (IOS and JUNOS
  - https://www.inex.ie/rtbh
- Cisco white paper on RTBH and Uni cast Reverse Path Forwarding
  - http://www.cisco.com/c/dam/en/us/products/collateral/security/ios-network-foundation-protection-nfp/prod_white_paper0900aecd80313fac.pdf

Thanks For your Attention