MTIN Consulting

# Mikrotik everyday

Justin Wilson

www.mtin.net

www.j2sw.com

www.midwest-ix.com

# Why you should care…sorta


- **Justin Wilson**
  CCNP – Comtrain – MTCNA – MTCRE – MTCWE
- Active in ISP industry since 1993
- COO MidWest-IX / CEO MTIN.NET
- Active Member of Brothers WISP
- Owned and operated several ISPs
- Huge Gi Joe Collector

www.mtin.net • j2sw.com • www.thebrotherswisp.com • www.midwest-ix.com

# Topics

- 1:1 Nat, 1:Many Nat, DMZ trick
- Carrier Grade Nat
- BGP notes
- Questions

# Who do we NAT?

- NAT isn't all bad, but needs managed
- IPv4 is scarce or expensive
- IPv6 is slowly being adopted
- "Security" by obscurity

# NAT

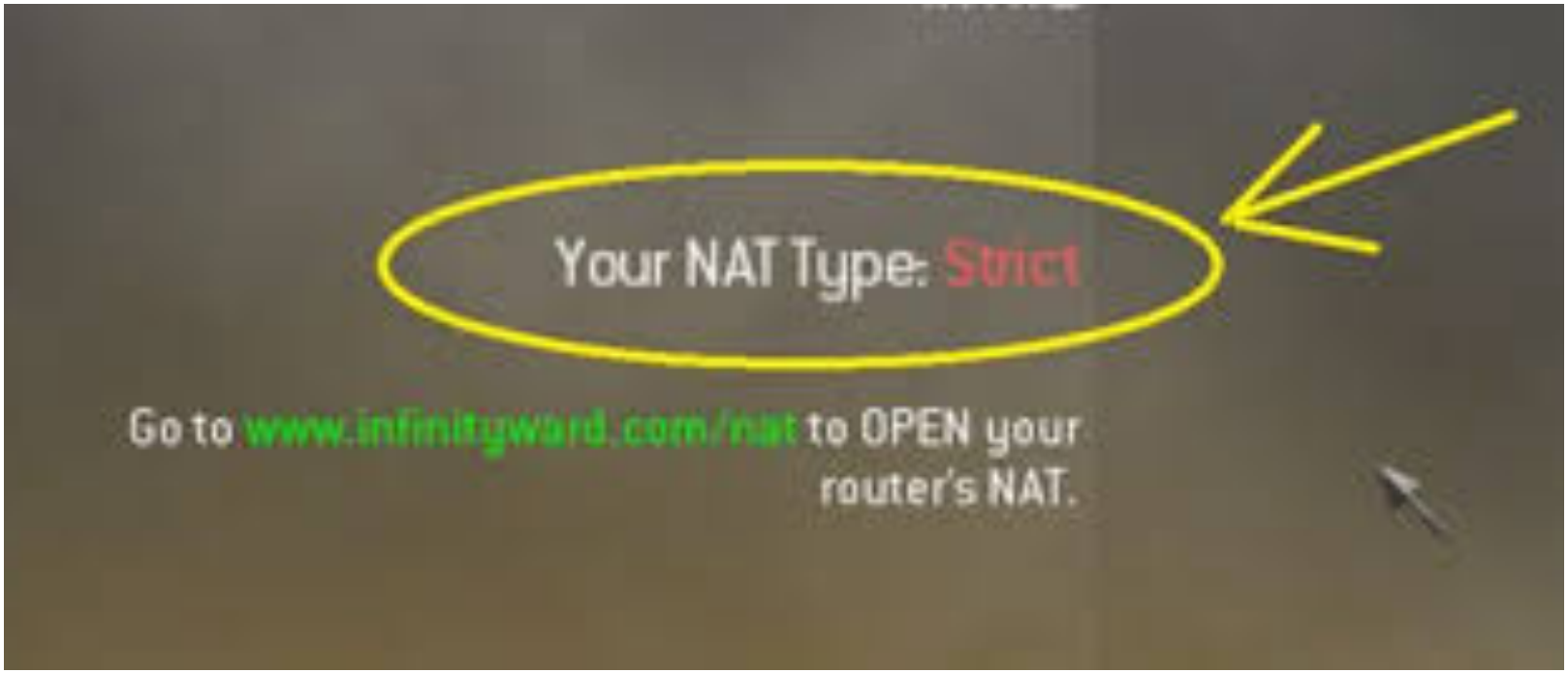
- The triple threat
  - Natted at edge
  - Natted at cpe
  - Natted at customer router

# NAT

- Most ISPs hate this guy

www.mtin.net • j2sw.com • www.thebrotherswisp.com • www.midwest-ix.com

# Why?




www.mtin.net • j2sw.com • www.thebrotherswisp.com • www.midwest-ix.com

=

www.mtin.net • j2sw.com • www.thebrotherswisp.com • www.midwest-ix.com

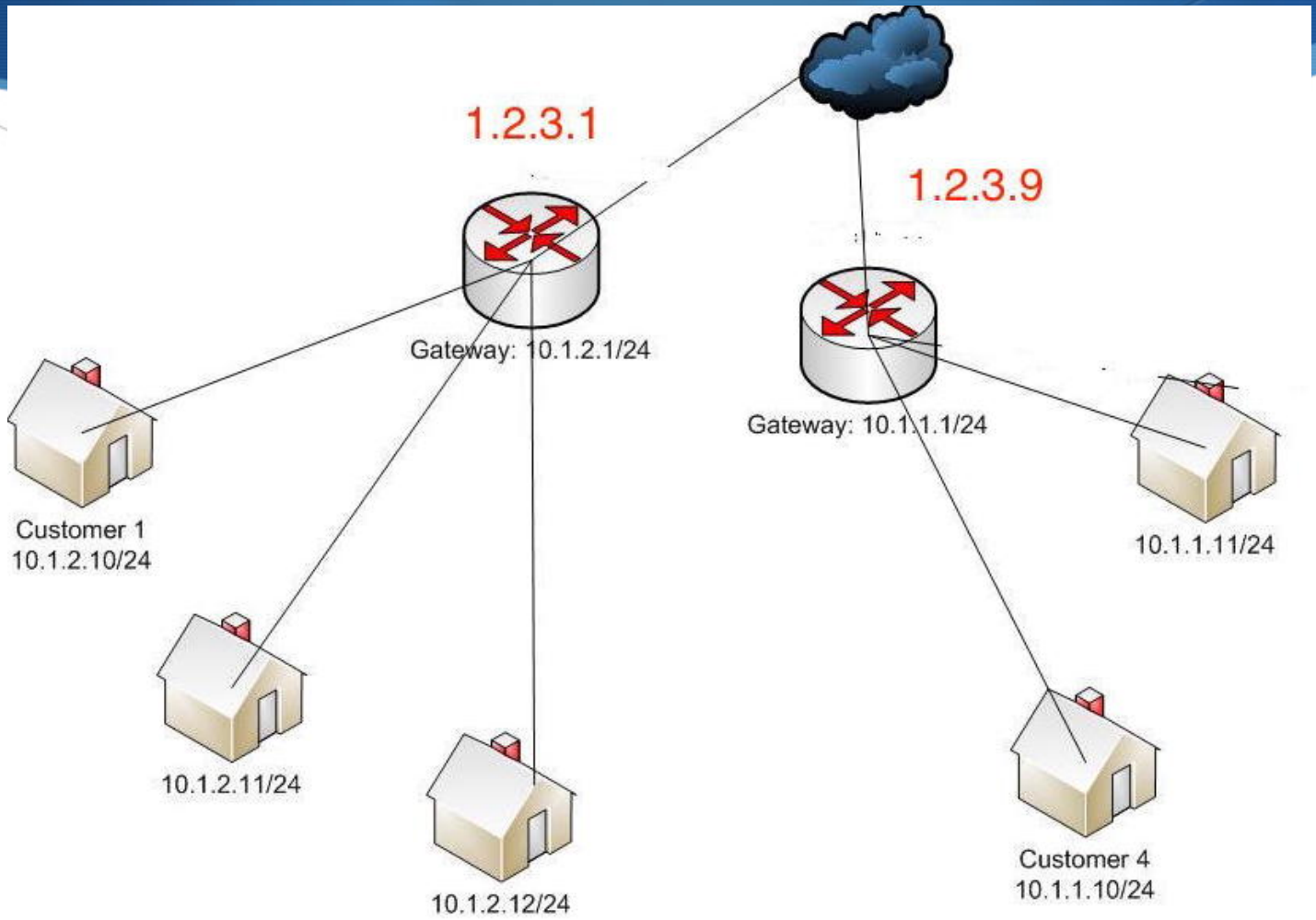
# DMZ Nat

- Forwards all ports to a single IP
- Setup DHCP to hand out that one IP
- Very hands off approach
- Can be used on a CPE in router mode or a wired router.

# 1:Many Nat

- Useful for mitigating some of the port issues
- Do on a per tower or per sector basis
- Can be dropped in anytime
- Splits up “nat domains”
- Balance between giving publics and natting

# 1:Many Nat




www.mtin.net • j2sw.com • www.thebrotherswisp.com • www.midwest-ix.com

# 1:Many Nat

- Use src-nat and dst-nat
- Do on a per tower or per sector basis
- Netmap can also be used
- ```
  /ip firewall nat
  add chain=srcnat src-address=10.1.2.0/24
  action=src-nat to-addresses=2.2.2.3
  ```
  ```

# 1:Many Nat scheme

- Route a /29 or appropriate block
  - 1.2.3.0/24 is our example
- 6 useable IP addresses 1.2.3.1-1.2.3.6
- IP breakdown
  - 1.2.3.1- Customer gateway
  - 1.2.3.2-1.2.3.5 – Static/business customers
  - 1.2.3.6 – 1:Many Nat IP

# Carrier Grade Nat

- How is it different?
- Nat444 vs Nat44
- Know your RFCS
  - RFC 6598
  - RFC 7422
  - RFC 6888

# Disadvantages

- CPU and Memory intensive
- Port forwarding no longer an option
- You end up deploying IPv6 anyway
- Still is Nat
  - Multiple ppl behind a single address causes issues for accounting and tracking
  - Still have issues with services “seeing” too many Ips

# Advantages

- Ummmm……..
- Seriously not many. Better usage of natting
- “Easier” than IPv6
- If you know nat you can configure CGN

# Better things than CGN

- Dual-Stack
- Nat64
- DS-Lite
- 6RD
- Kittens..cus it's the Internet

# UPnP can be your friend

- Universal Plug and Play get a bad rep
  - Mikrotik addresses the biggest issues with UPnP.
  - Allow-disable-external-interfaces
- Many UPnP vulnerabilities are a direct result of router code vulnerabilities (not Mikrotik)
- Most articles are more than 2 years old.
- If you provide managed Mikrotiks you can be a hero

# UPnP can be your friend

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| ;;; upnp 192.168.20.18: Teredo | | | | | | | | |
| 23 | D | dst-nat | dstnat | | 50.158.140.31 | 17 (... | | 3074 |
| ;;; upnp 192.168.20.18: DemonwarePortMapping | | | | | | | | |
| 24 | D | dst-nat | dstnat | | 50.158.140.31 | 17 (... | | 1200 |

# Let's talk about BGP baby..just you and me

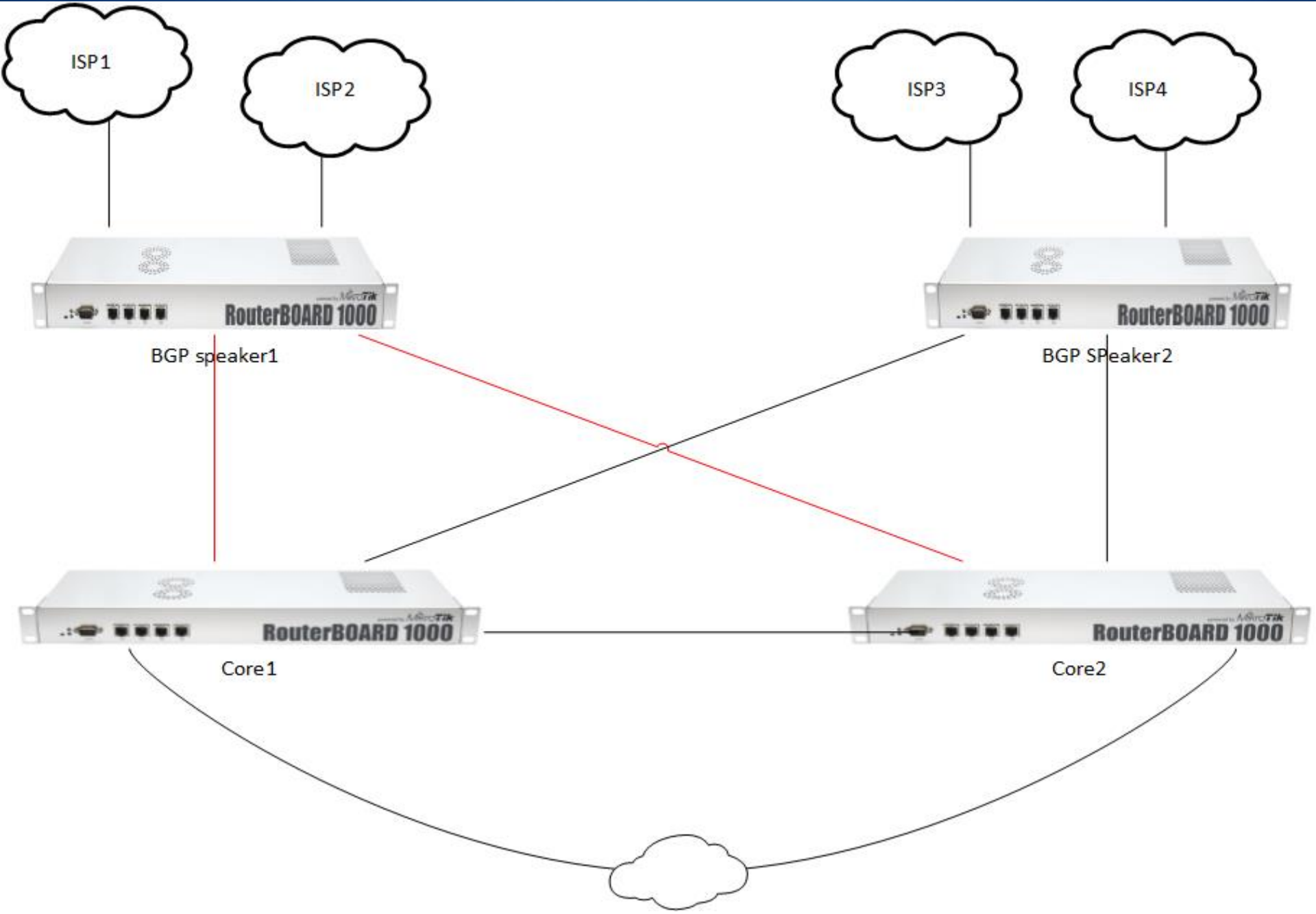

www.mtin.net • j2sw.com • www.thebrotherswisp.com • www.midwest-ix.com

# BGP considerations

- Design and Engineering
- Peer Setup
- Filters & Security
- Types of peering

# Design and Engineering

- Everything starts with a good foundation
- Modular approach
- Redundancy and serviceability
- 3 Tier design
  - Edge
  - Core
  - Access


ISP1
ISP2
ISP3
ISP4
RouterBOARD 1000
RouterBOARD 1000
BGP speaker1
BGP SPeaker2
RouterBOARD 1000
RouterBOARD 1000
Core1
Core2

# Design and Engineering

- Don't make your routers do everything – Modularize
- Sales will love you
- Redundancy
  - Greg Sowell's upcoming presentation
- Easier to upgrade
- Better performance

# BGP Tips

- Deny-ALL in & out filters for testing
- Global routing table is above 600,000 non aggreggated
- New methods of thinking
  - Some folks are filtering out the large netblocks
  - 38.0.0.0/8 is a good example (Cogent ASN 174)

# 38.0.0.0/8 example

| | | |
|---|---|---|
| 38.2.195.0/24 | PSINet, Inc. | 256 |
| 38.2.201.0/24 | PSINet, Inc. | 256 |
| 38.8.6.0/24 | PSINet, Inc. | 256 |
| 38.8.48.0/24 | PSINet, Inc. | 256 |
| 38.9.9.0/24 | PSINet, Inc. | 256 |
| 38.9.51.0/24 | PSINet, Inc. | 256 |
| 38.9.79.0/24 | PSINet, Inc. | 256 |
| 38.9.120.0/24 | PSINet, Inc. | 256 |
| 38.18.0.0/19 | PSINet, Inc. | 8,192 |
| 38.18.64.0/20 | PSINet, Inc. | 4,096 |
| 38.18.80.0/20 | PSINet, Inc. | 4,096 |
| 38.18.96.0/20 | PSINet, Inc. | 4,096 |

www.mtin.net • j2sw.com • www.thebrotherswisp.com • www.midwest-ix.com

# BGP Filters

- Tom Smyth's presentation
- In-Bound filter
  - Lots of Denies
  - Deny your own IP space
  - Deny non-routeable (ie. 192.168.0.0./16)
  - Don't accept smaller than a /24

# Types of peering

- Public Peering
  - Usually at an Internet Exchange (IX)
  - 50-80% of your traffic can be offloaded
  - Usually much cheaper (.27 per meg for Netflix?)
- Private peering
  - Usually between two individual parties
  - Settlement free and paid peering

www.mtin.net • j2sw.com • www.thebrotherswisp.com • www.midwest-ix.com

# Resources

- www.mtin.net/blog
- www.thebrotherswisp.com
- j2sw.com
- Ask questions.
- Facebook has very active groups

# Questions? Callouts