

The Biggest MUM in the World



MikroTik BGP Security

Jogjakarta, Indonesia

MikroTik

Rofiq Fauzi



About Rofiq Fauzi

- Using MikroTik (v.2.97) since 2005, as Network Engineer at WISP.
- 2007, Network & Wireless Engineer at INDOSAT Central Java Area
- 2008, IT Network & Telco Procurement at INDOSAT HQ
- 2012-Now, MikroTik Consultant & Certified Trainer (MTCNA, MTCRE, MTCTCE, MTCWE, MTCUME, MTCINE) at **ID-Networkers** (PT Integrasi Data Nusantara).
- 2013-Now, Network Manager at WISP Indomedianet, Indonesia
- 2013-Now, Network Consulting Engineer at Connexin Limited, Hull, UK

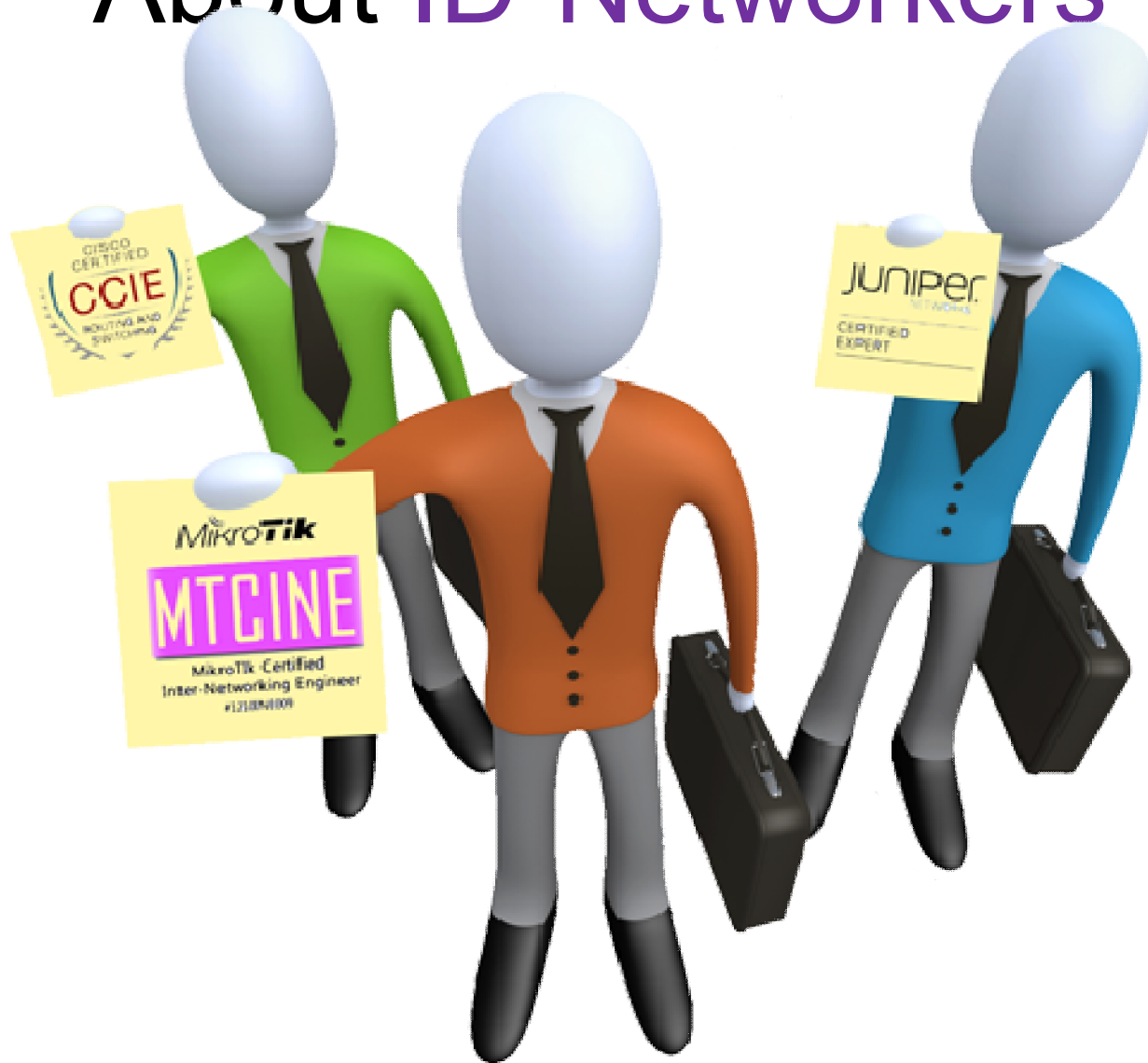
CONSULTANT

<http://www.mikrotik.com/consultants/asia/indonesia>

CERTIFIED TRAINER

<http://www.mikrotik.com/training/partners/asia/indonesia>

About ID-Networkers



EXPERT LEVEL TRAINERS & CONSULTANS

In the Most Prestigious Networking Certification

OVERVIEW

We are young entrepreneurs, we are only one training partner & consultant who has expert level trainers in the most prestigious networking certification, CCIE Guru , JNCIE Guru and MTCINE guru, which very limited number in Indonesia even Asia. Proven that hundred of our students pass the certification exam every year. We are the biggest certification factory in Indonesia.

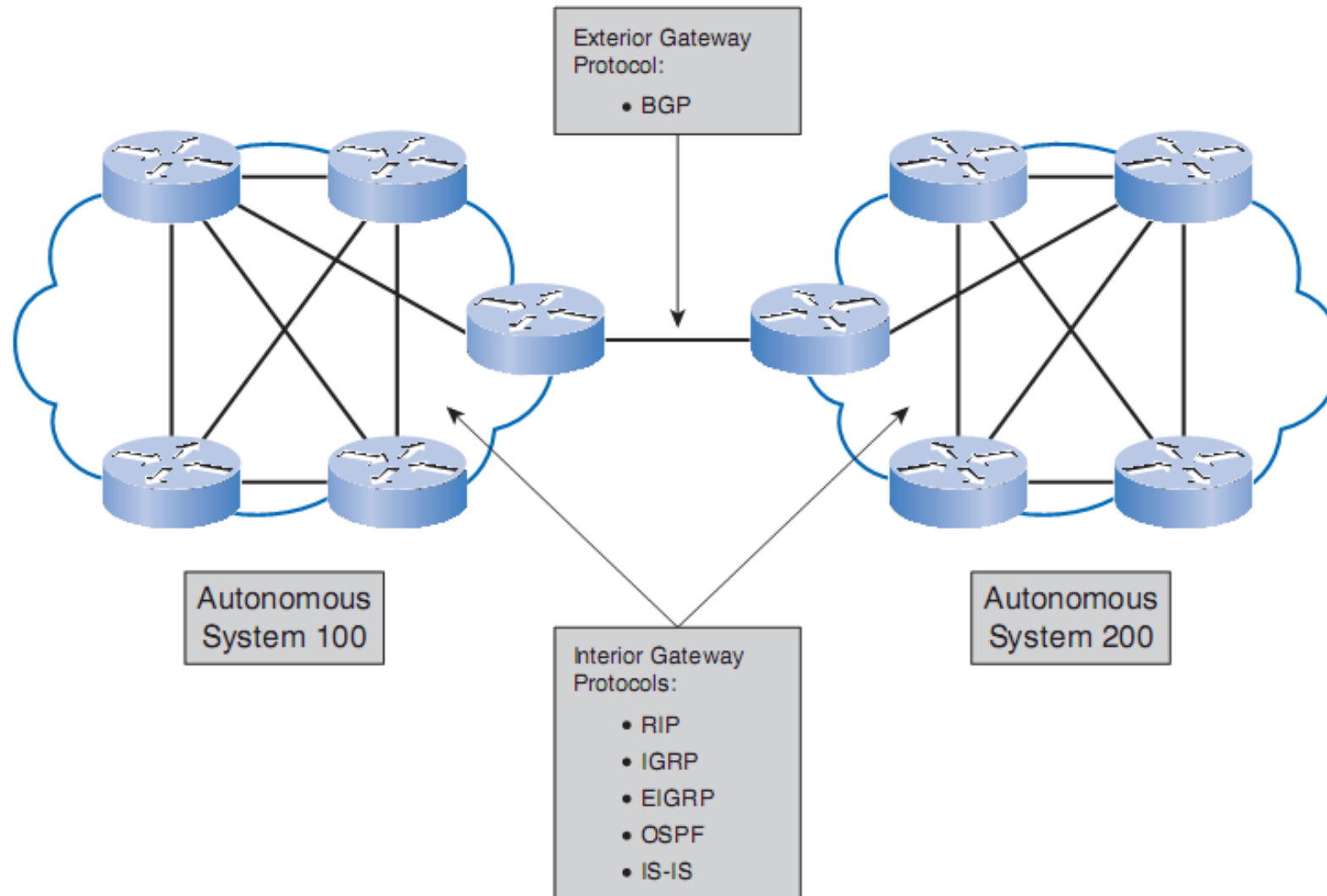
WEBSITE

www.id-networkers.com

About BGP

- BGP is one of many dynamic routing protocols
- Internet formed by BGP routing
- Designed to exchange routing and reachability information between **autonomous systems (AS)** on the Internet
- BGP also has capability to carrying information about diverse routed protocols (ipv4, ipv6, l2vpn, vpnv4)

Interior and Exterior Gateway Protocol



Interior and Exterior Gateway Protocol

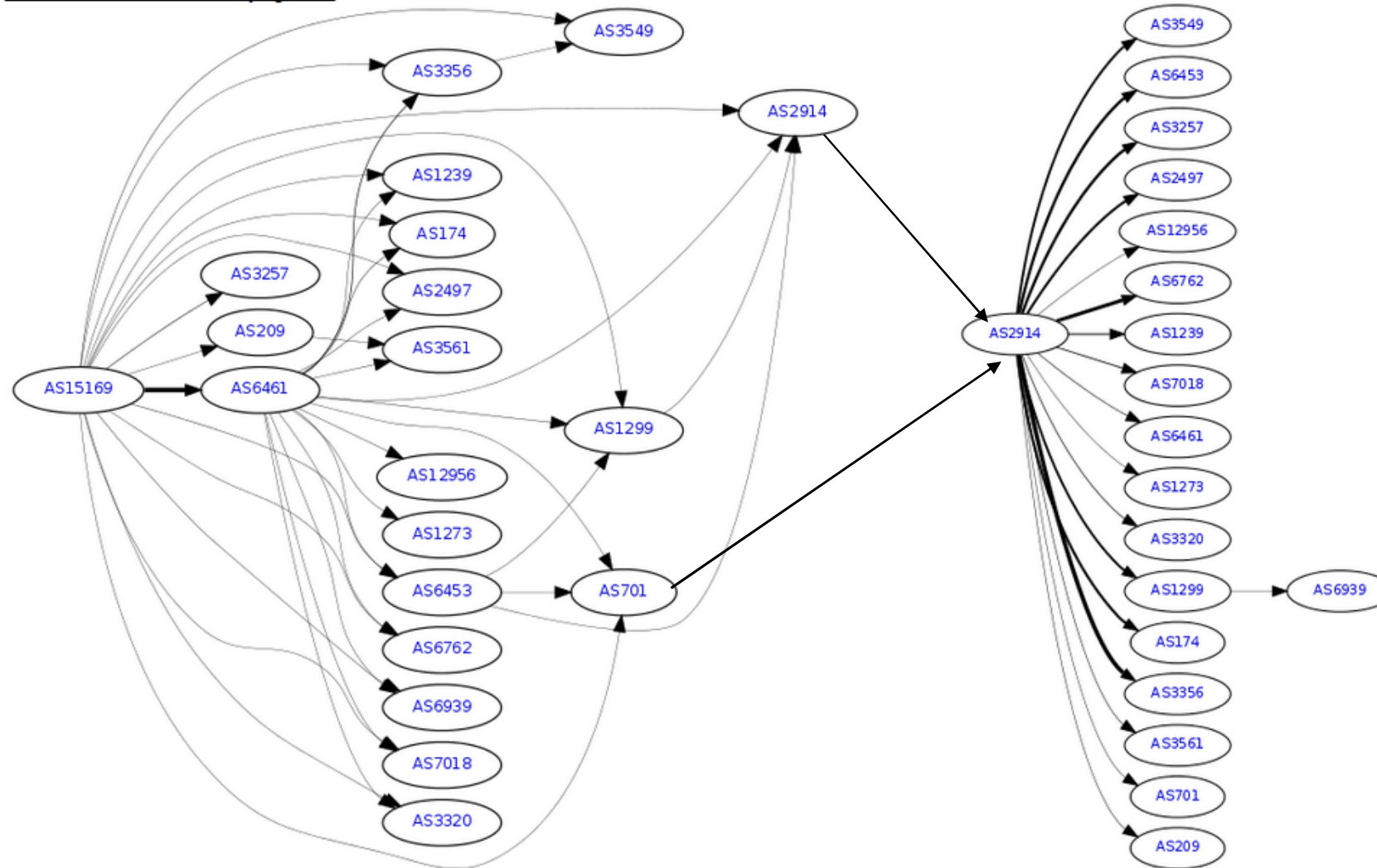
- Interior Gateway Protocol (IGP)
Handle routing within an Autonomous System (one routing domain). Can be said that the IGP is a routing that works on our proprietary network, or all routers are belong to us.
- Exterior Gateway Protocol (EGP)
Handles the routing between Autonomous Systems (inter-domain routing). Can be said that the EGP is working or routing between our networks with not our networks.

Autonomous **Systems (AS)**

- AS is a combination of networks and routers are usually in one ownership or control that has a similar routing protocol.
- AS 16 bit, or use decimal (0 - 65535)
 - Range 1 - 64511 used for Internet
 - Range 64512 - 65535 used for private
- With 16-bit AS Numbers, only around 65,000 unique numbers are possible.
- The introduction of 32-bit ASNs increases the supply of AS Numbers to four billion.
- AS Number allocation is managed by IANA

BGP between AS in the Internet

AS15169 IPv4 Route Propagation



IN BGP WE TRUST

Full trust between BGP peers is one of the weaknesses of the protocol.



Mr Leak give wrong information to Mr X



Mr X give right information but coming from wrong source



Wrong information will spread to all

The Internet's **Vulnerable Backbone**

YouTube Hijacking: A RIPE NCC RIS case study

Publication date: 17 Mar 2008 — [news](#), [ris](#), [internet governance](#)

Introduction

How an Indonesian ISP took down the mighty Google for 30 minutes

Internet's web of trust let a company you never heard of block your Gmail.

by Sean Gallagher - Nov 6 2012, 11:07pm SEAST



Google's services went offline for many users for nearly a half-hour on the evening of Nov 6 2012.

Syria shuts down the Internet

Posted by Andree Toonk - November 29, 2012 - [BCP instability](#) - 9 Comments

As of 10:27 UTC this morning the majority of the Internet in Syria is no longer accessible to the rest of the world and can be considered as offline. Syria has only one major provider, The Syrian Telecommunications Establishment. This provider is government owned and originates 56 out of 62 Syrian prefixes.

Turkey Hijacking IP addresses for popular Global DNS providers

Posted by Andree Toonk - March 29, 2014 - [Hijack](#), [News and Updates](#) - 26 Comments

At BGPmon we see numerous BGP hijacks every single day, some are interesting because of the size and scope. It all starts with a single IP address. This starts with a single IP address.

BGP Hijacker Steals Bitcoins

Researchers at Dell's Secureworks have discovered [multiple BGP incidents used to steal bitcoins](#). According to Secureworks, the attacker used a compromised administrator account at a yet undisclosed provider ISP.



Indonesia Hijacks the World

03 APR, 2014 | 3:09 PM | BY EARL ZMIJEWSKI

Yesterday, Indosat, one of Indonesia's largest telecommunications providers, leaked large portions of the global routing table multiple times over a two-hour period. This means that, in effect, Indosat claimed that it "owned" many of the world's networks. Once someone makes such an assertion, typically via an honest mistake in their routing policy, the only question remaining is how much of the world ends up believing them and hence, what will be the scale of the damage they inflict? Events of this nature, while relatively rare, are certainly not unheard of and can have geopolitical implications, such as when China was involved in a similar incident in 2010.

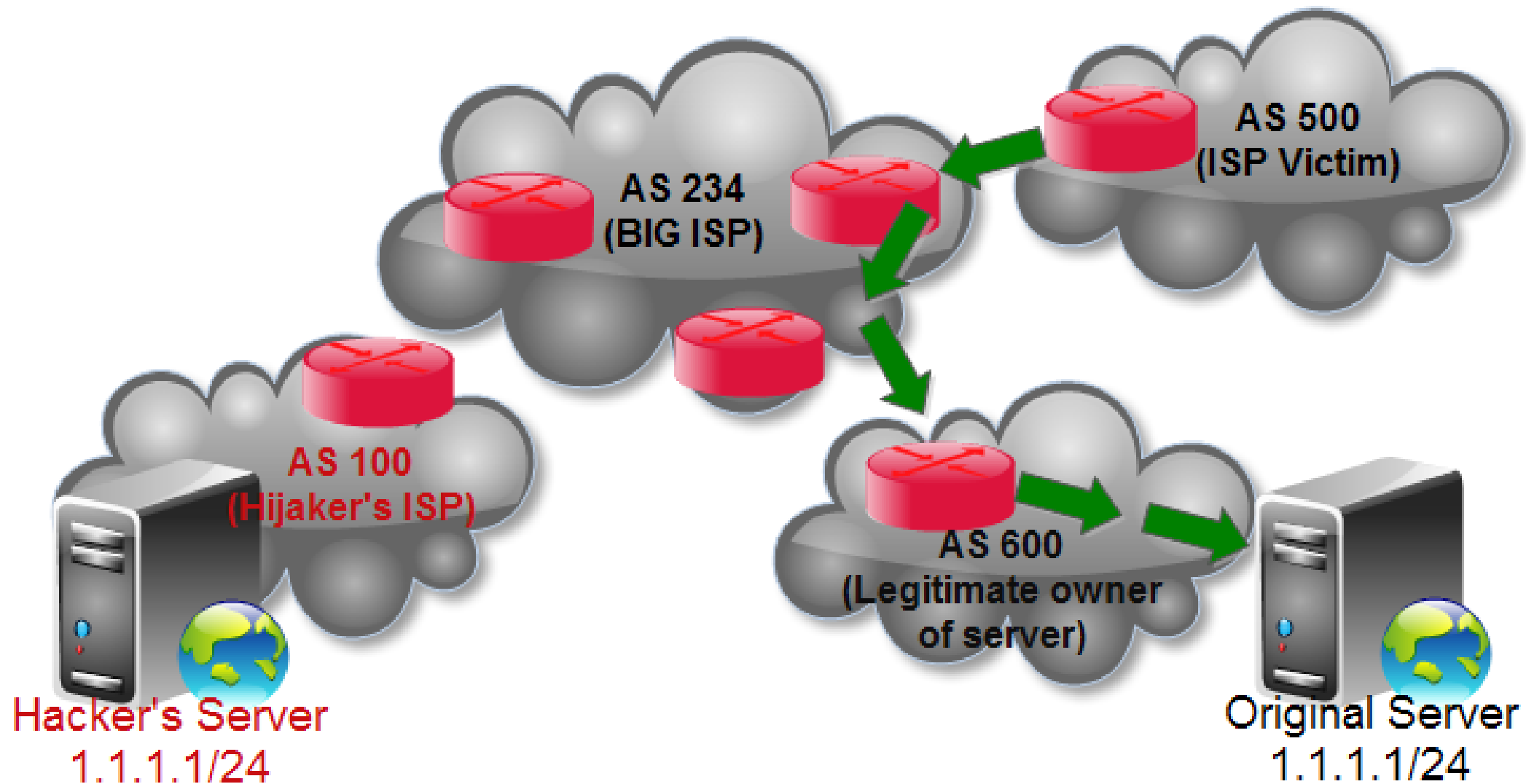
General Types of BGP Attacks

- Prefix Hijack
- Denial of service
- Creation of route instabilities (flapping)

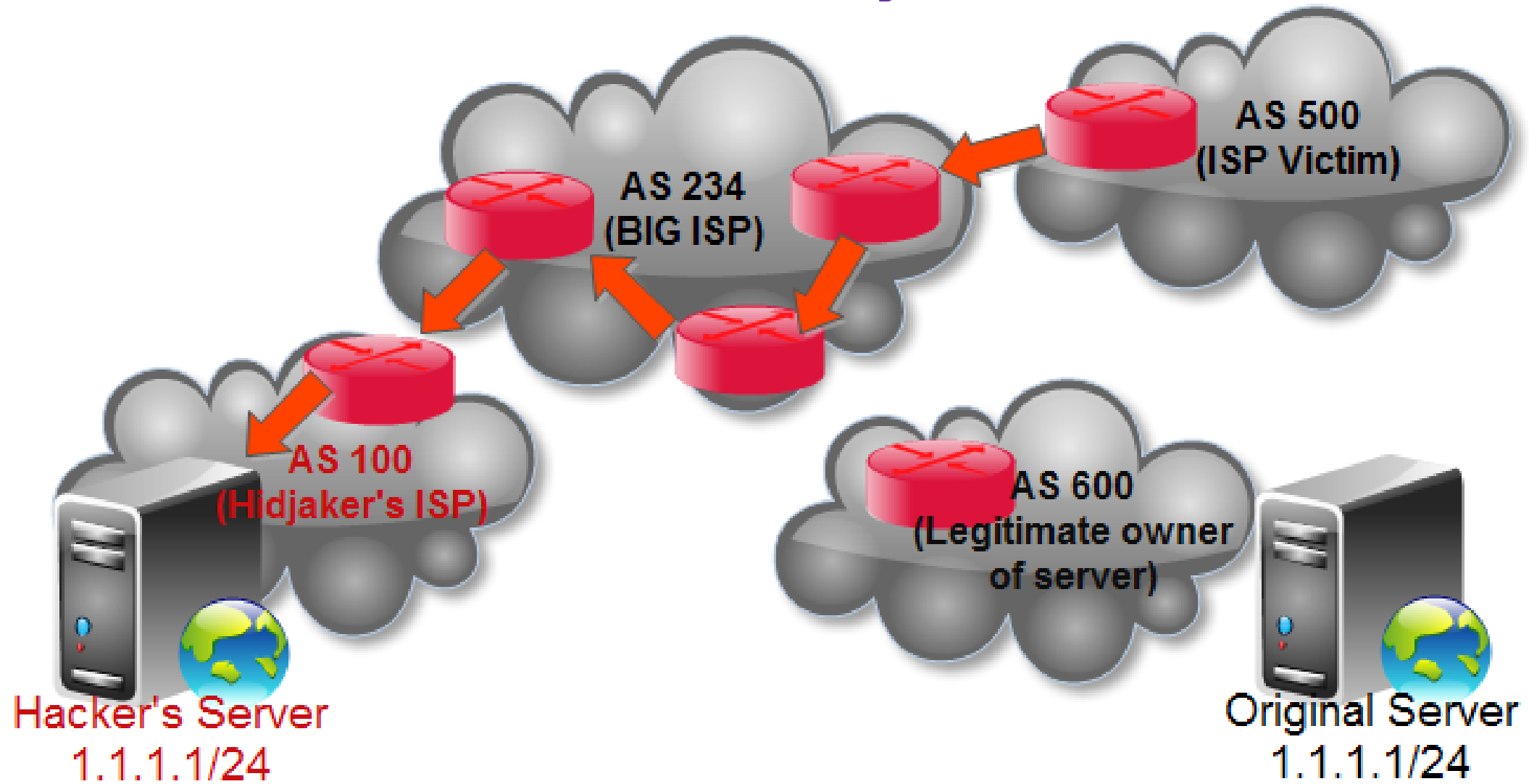
Prefix Hijack

- Prefix hijacking, a misbehavior in which a misconfigured or malicious BGP router originates a route to an IP prefix it does not own,
- Its is becoming an increasingly serious security problem in the Internet

How Attackers Can Hijack BGP

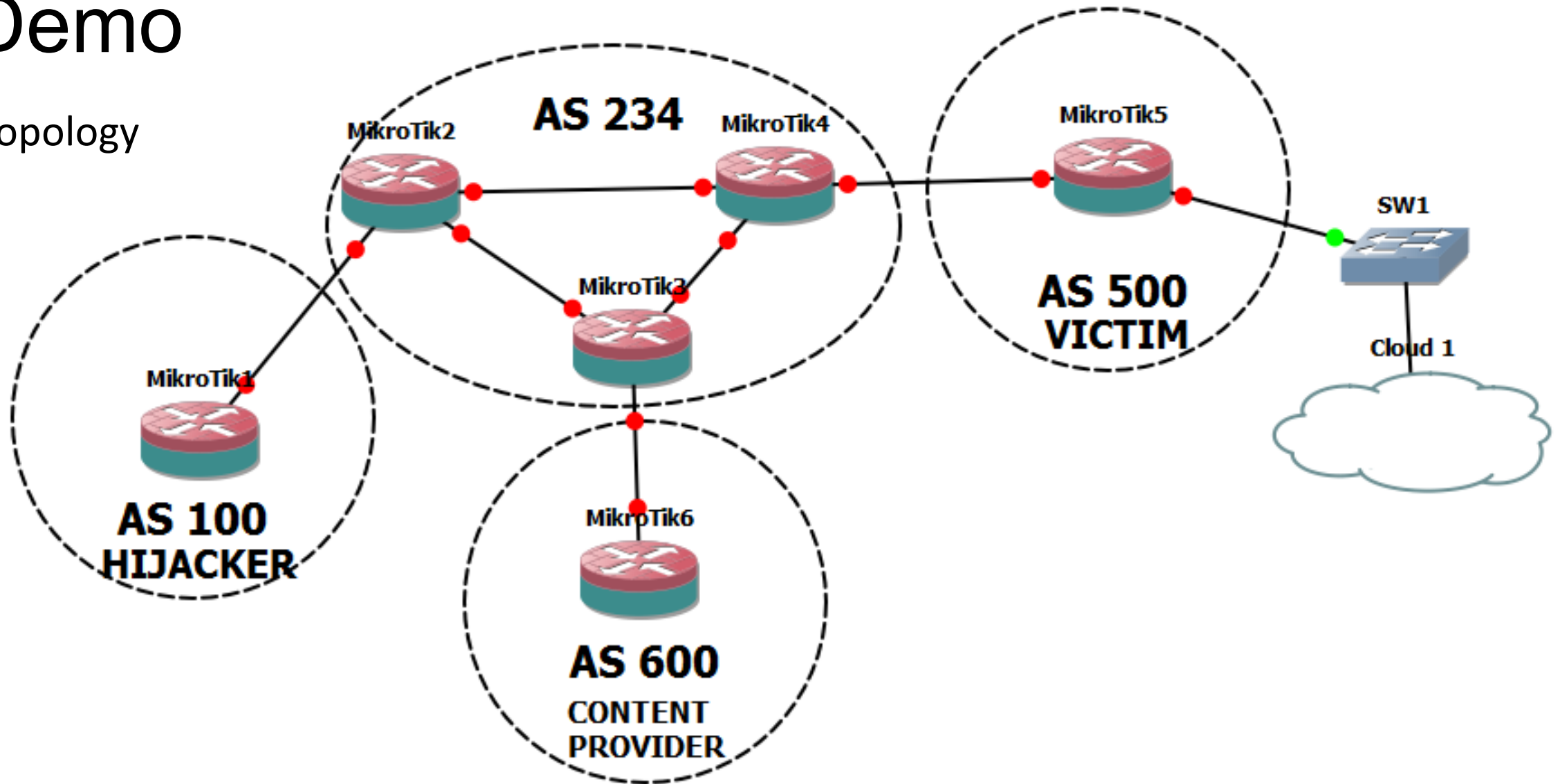


How Attackers Can Hijack BGP



Demo

Topology



Demo

- Install GNS3, if you didn't know how to install mikrotik on GNS3, follow our previous MUM presentation slide at: www.mikrotik.com/presentations/ID13/rofiq.pdf
- Create topology (slide 15)
- Configure BGP peering between all AS, don't forget for AS 234 its using iBGP peer (mesh peering or router refelctor)
- Create loopback interface (bridge interface) in Router1 and Router6, and put ip 1.1.1.1/32 on the both bridge interfaces.
- On Router6, in routing BGP network, advertise network 1.1.1.1/32
- Check in Router1, we can see in IP route, prefix 1.1.1.1 with as path 234,600 that's mean prefix 1.1.1.1/32 originated from 600
- On Router1, in routing BGP network advertise network 1.1.1.1/32 too
- Check in Router1, we can see in IP route, prefix 1.1.1.1 will change as path to 234,100

DDOS Attack

- One of the denial of service (DDOS), happens on mikrotik router's winbox service when the attacker is requesting continuously a part of a .dll/plugin file
- It raises router's CPU 100% and other actions. The "other actions" depends on the routers version and the hardware.
- For example on Mikrotik Router v3.30 there was a LAN corruption, **BGP fail**, whole router failure
 - Mikrotik Router v2.9.6 there was a **BGP failure**
 - Mikrotik Router v4.13 unstable wifi links
 - Mikrotik Router v5.14/5.15 rarely stacking
- Behaviour may vary most times, but ALL will have CPU 100% . Most routers **loose BGP** after long time attack

Ref: <http://www.133tsec.com/2012/04/30/0day-ddos-mikrotik-server-side-ddos-attack/>

Demo **Attack**

- Download testing script from <http://www.133tsec.com/wp-content/uploads/2012/04/mkDI.zip>
- Extract it in your C folder
- Run in your windows command prompt
C:\> mkDI.py <RouterIPAddress> * 1
- Watch your router CPU usage

Warning! This content and tool are for education proposed only, I am not responsible for anything that might happen to you or your routers if you use it to DDOS your router, and or causing any damage or error.

Defend **BGP Attacks**

- Good BGP Router Configuration
- Detect False Route Announcements
- RPKI

Good Router Configuration

Use routing filter to control prefix exchange between BGP peering

In Filters

- Don't accept your own prefixes
- Don't accept RFC 1918 (private IP address) and other reserved ones (RFC 5735)
- Don't accept default route (unless you need it)
- Don't accept prefixes longer than /24
- Don't accept BOGONS prefixes
- Limit your Max Prefix
- Limit AS_Path

Out Filters

- Announce only owned prefixes (in case you do not provide transit to other AS's)

Credit to Wardner Maia, ref: http://mdbrasil.com.br/en/downloads/1_Maia.pdf

MikroTik Routing Filter

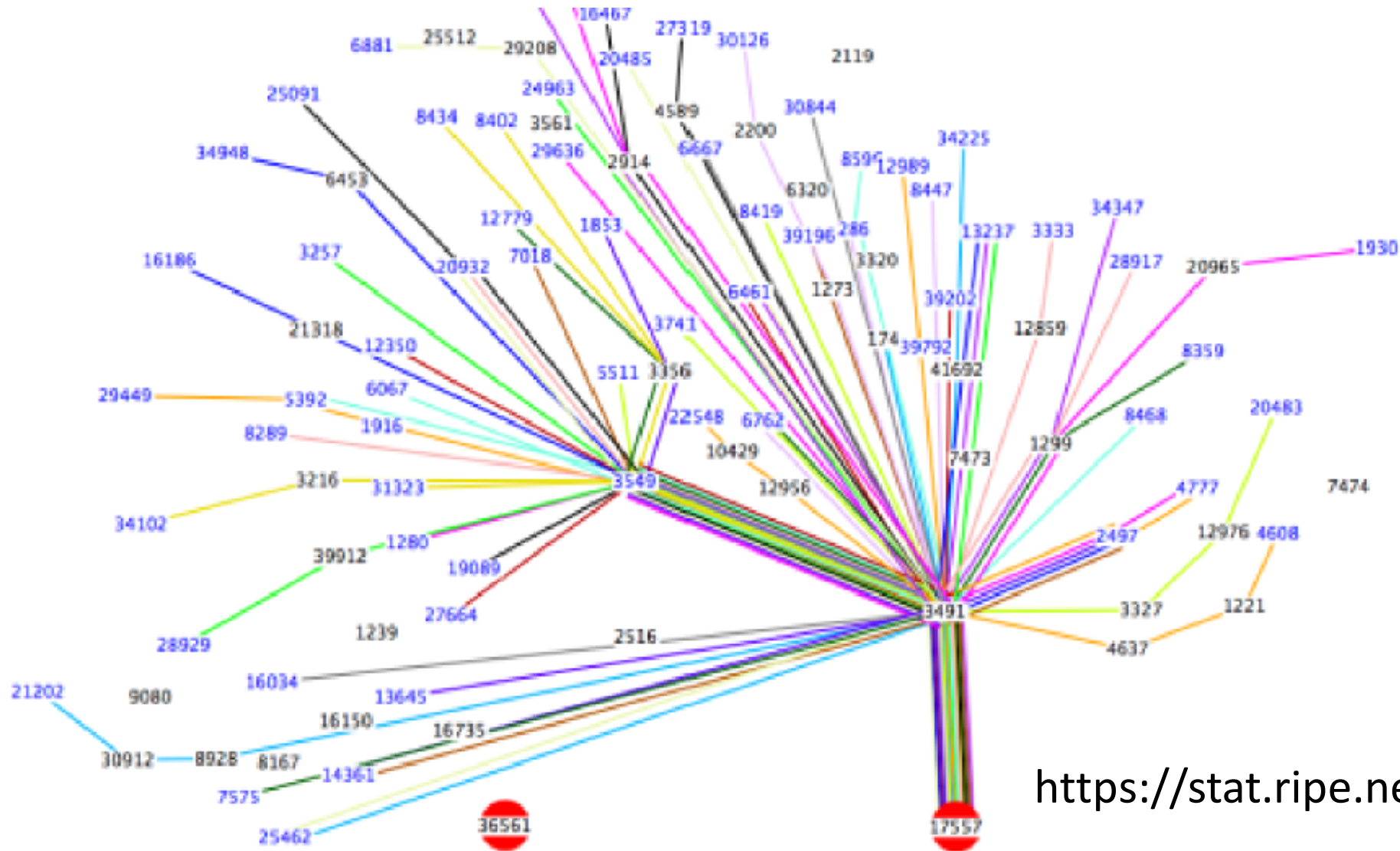
- http://wiki.mikrotik.com/wiki/Manual:Routing/Routing_filters
- Easy way to manage and filter receiving and propagating prefix in MikroTik RouterOS.
- Easy way to set any routing parameters
- Using ip firewall filter algorithm (if-then condition)
- Can be assign in BGP instance (out-filter only) and BGP peering (in and out filter)

MikroTik Routing Filter

The screenshot shows the MikroTik WinBox interface. On the left is a sidebar with navigation options like 'Quick Set', 'Interfaces', 'Bridge', 'PPP', 'Mesh', 'IP', 'MPLS', 'Routing', 'System', 'Queues', 'Files', 'Log', 'Radius', 'Tools', 'New Terminal', 'LCD', 'Partition', 'Make Supout.rif', 'Manual', and 'Exit'. The main window displays a table of 'Route Filters' with columns for '#', 'Chain', and 'Prefix'. A 'New Route Filter' dialog box is open in the foreground, showing configuration options for a new filter. The 'Chain' field is set to 'GGC-in'. Other fields include Prefix, Prefix Length, Match Chain, Protocol, Distance, Scope, Target Scope, Pref. Source, Routing Mark, Route Comment, Route Tag, Route Targets, Site Of Origin, and checkboxes for 'Invert Route Targets' and 'Invert Site Of Origin'. Buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', and 'Remove' are visible on the right side of the dialog.

#	Chain	Prefix
0	ix-out	103.
1	ix-out	103.
2	ix-out	103.
3	ix-out	103.
4	ix-out	
5	ix-in	
6	diamond-...	103.
7	diamond-...	103.
8	diamond-...	103.
9	diamond-...	103.
10	diamond-...	
11	diamond-in	
12	mpls-out	103.
13	mpls-out	103.
14	mpls-out	103.
15	mpls-out	103.
16	mpls-out	
17	mpls-ix-out	103.
18	mpls-ix-out	103.
19	mpls-ix-out	103.
20	mpls-ix-out	103.
21	mpls-ix-out	103.
22	mpls-ix-out	
23	mpls-in	
24	GGC-out	103.
25	GGC-out	103.
26	GGC-out	103.
27	GGC-out	103.
28	GGC-out	

Detect False Route Announcements



<https://stat.ripe.net/widget/bgplay>

Detect Route Flapping

Detect Routing table size:

```
/system scheduler
```

```
add interval=5m name=schedule1 on-event=detect-route start-time=startup
```

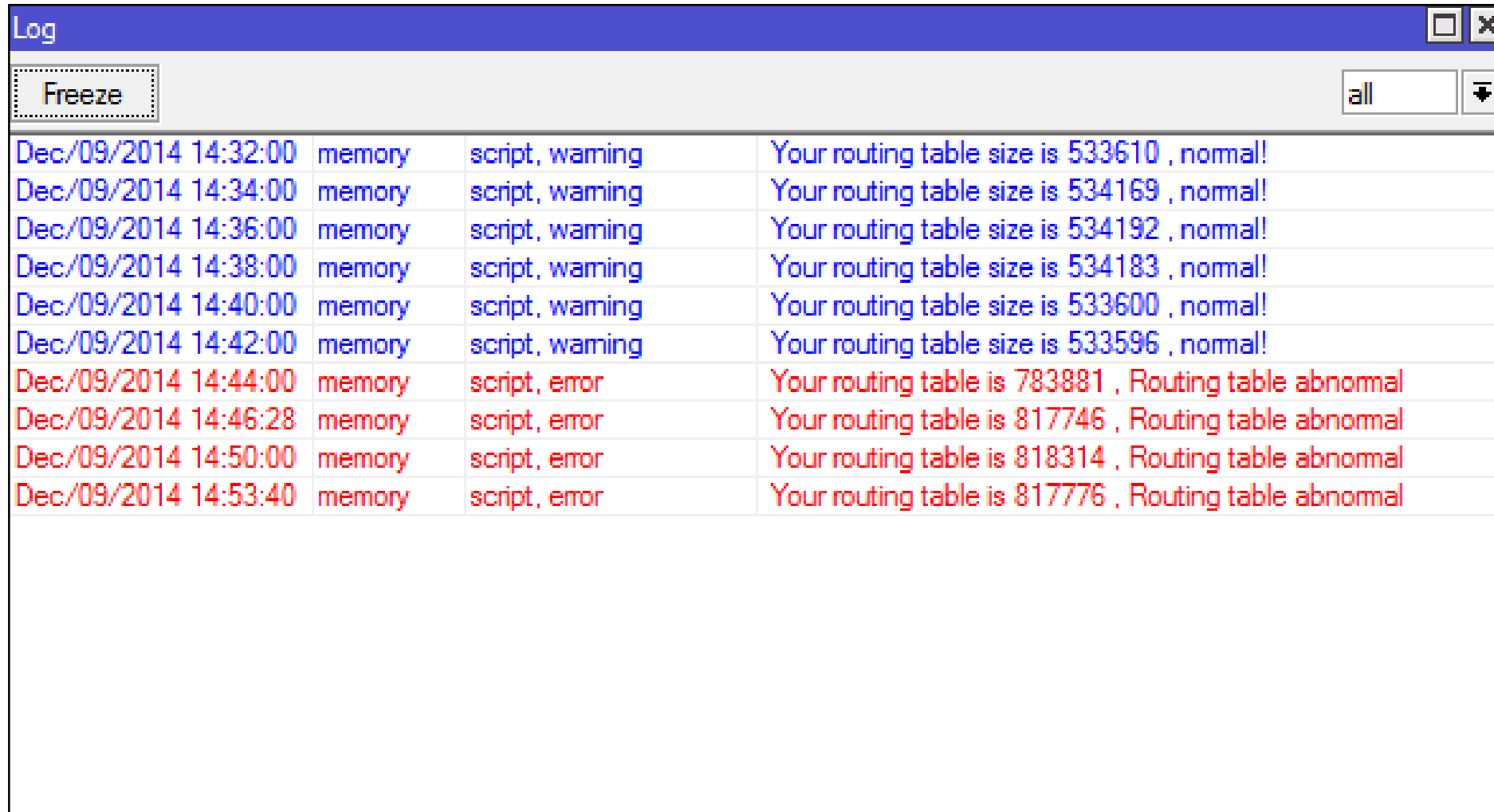
```
/system script
```

```
add name =detect-route
```

```
source=":local routeSize [/ip route print count-only];
```

```
:if ($routeSize > 5400000) do={/log error " Your routing table is $routeSize , Routing table abnormal"} else={/log warning " Your routing table size is $routeSize , normal!"}
```


Detect Route Flapping



The screenshot shows a log window with a blue title bar and a search bar containing 'Freeze'. The log entries are as follows:

Timestamp	Source	Severity	Message
Dec/09/2014 14:32:00	memory	script, warning	Your routing table size is 533610 , normal!
Dec/09/2014 14:34:00	memory	script, warning	Your routing table size is 534169 , normal!
Dec/09/2014 14:36:00	memory	script, warning	Your routing table size is 534192 , normal!
Dec/09/2014 14:38:00	memory	script, warning	Your routing table size is 534183 , normal!
Dec/09/2014 14:40:00	memory	script, warning	Your routing table size is 533600 , normal!
Dec/09/2014 14:42:00	memory	script, warning	Your routing table size is 533596 , normal!
Dec/09/2014 14:44:00	memory	script, error	Your routing table is 783881 , Routing table abnormal
Dec/09/2014 14:46:28	memory	script, error	Your routing table is 817746 , Routing table abnormal
Dec/09/2014 14:50:00	memory	script, error	Your routing table is 818314 , Routing table abnormal
Dec/09/2014 14:53:40	memory	script, error	Your routing table is 817776 , Routing table abnormal

RPKI (Resource Public Key Infrastructure)

- http://en.wikipedia.org/wiki/Resource_Public_Key_Infrastructure
- RPKI is a first step to secure BGP
- It allows to certify (and verify) that a prefix is advertised by original AS (in other words that an IP points to its legitimate owner)
- Not yet support by MikroTik RouterOS 6
- Will be included in **RouterOS V7 ???**

If you have any other questions or would like me to clarify anything else, please, let me know. I am always glad to help in any way I can



THANK YOU
FOR YOUR TIME

CONTACT

ADDRESS: Jakarta & Semarang, Indonesia

WEBSITE: www.training-mikrotik.com

EMAIL: ropix@id-networkers.com

TELEPHONE: +62 8156583545



@mymikrotik



www.facebook.com/ropix



id.linkedin.com/in/ropix/



[rofiq.fauzi](https://soundcloud.com/rofiq-fauzi)

“If you cannot survive in the tired of learning, then you will be suffering by the pain of stupidity” *(Imam Syafi’i)*

