



IoT, IPv6 and the new ISP challenges for Internet security

European MUM – 2017

Milan / Italy

Wardner Maia

Wardner Maia

Electronic and Telecommunications Engineer;
Internet Service Provider since 1995;
Training Business since 2002;
Certified Mikrotik Trainer since 2007;
MD Brasil IT & Telecom CTO;
Member of the board of directors of LACNIC.

MD Brasil

ISP (radio and optical), ~ 6.000 customers
Distributor and training center

Previous Participations on European MUMs

- 1) Wireless Security (2008 – Krakow/PL)
- 2) Wireless Security for OLPC project (2009 – Prague/CZ)
- 3) Layer 2 Security (2010 – Wroclaw/PL)
- 4) Routing Security (2011 – Budapest/HU)
- 5) IPv6 Security (2012 - Warsaw/PL)
- 6) BGP Filtering (2013 – Zagreb/CR)
- 7) MPLS VPNs Security (2014 – Venice/IT)
- 8) Network Simulation (2015 – Prague/CZ)
- 9) DDoS – detection and mitigation (2016 – Ljubljana/SL)

Today: IoT, IPv6 and new ISP challenges for Internet Security

<http://mikrotikbrasil.com.br/artigos>



One year ago... February, 2016

EUROPE ON FEBRUARY 25 - 26, 2016

Registration Closed

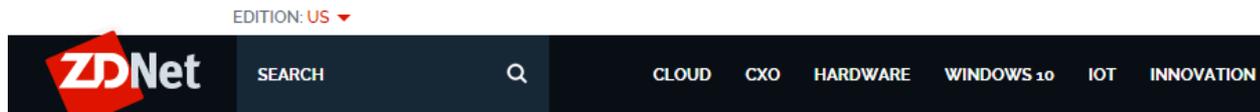


DDoS attacks increase in number, endanger small organizations



Marcos Ortiz Valmaseda
Senior Product Marketing Manager & Content Marketing Strategist at GET // Freelance Copywriter

Follow



MUST READ **SAMSUNG STARTS ANDROID MARSHMALLOW ROLLOUT FOR GALAXY S6, S6 EDGE**

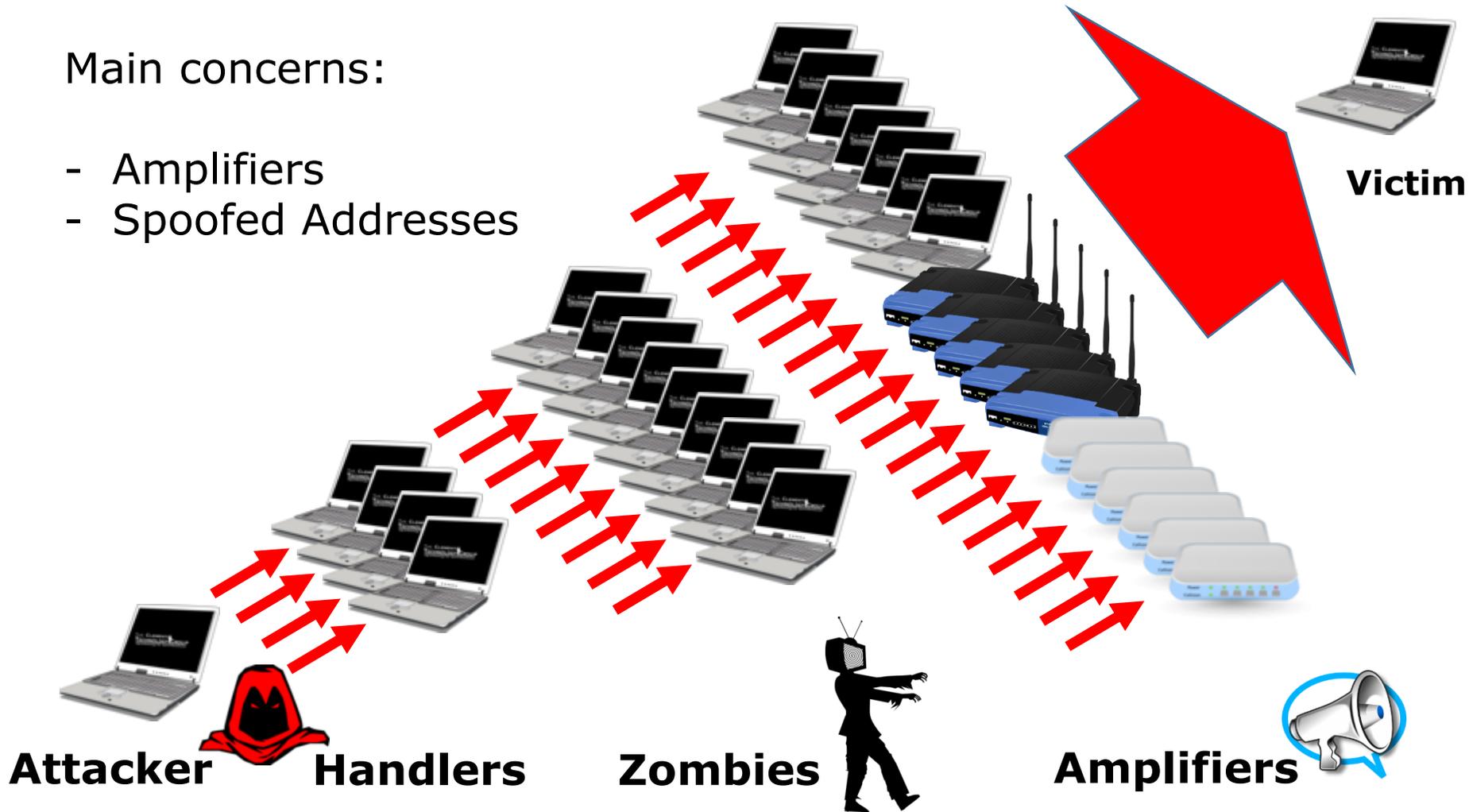
DDoS Attacks: Size doesn't matter



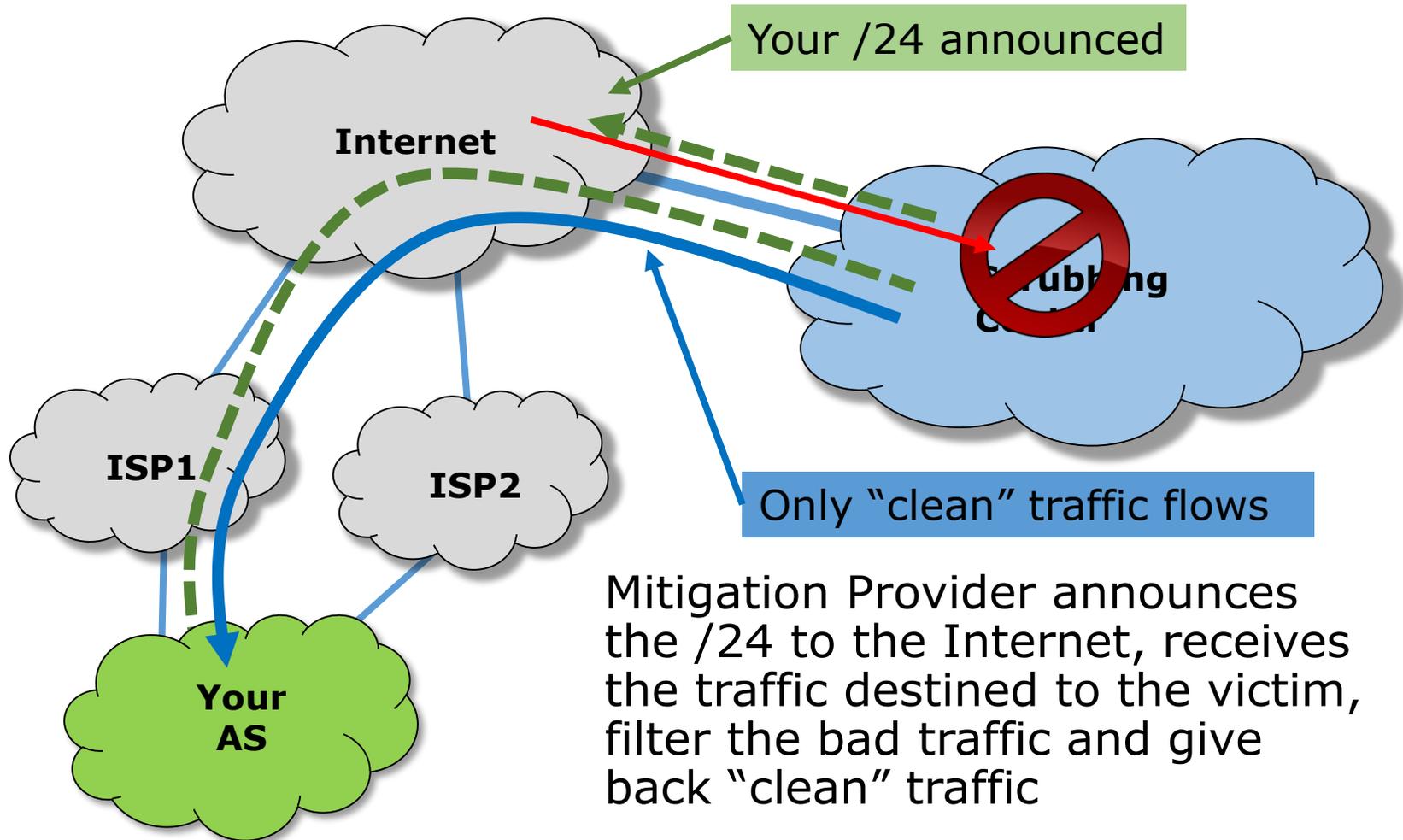
Anatomy of a DRDoS attack

Main concerns:

- Amplifiers
- Spoofed Addresses

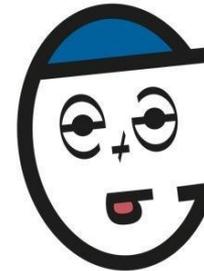


Mitigation On the Cloud

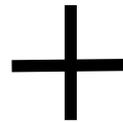


Mitigation Provider announces the /24 to the Internet, receives the traffic destined to the victim, filter the bad traffic and give back "clean" traffic

Mikrotik Traffic Flow



ExaBGP



Detection and mitigation schema based on Open Source tools (Fastnetmon, ExaBGP, InfluxDB and Grafana) interacting with RouterOS



2016, what a year!



May, 2016

WISPs CPE attacked

More than 200 thousand people without Internet access! (only in our region)



15/05/2016 17h05 - Atualizado em 15/05/2016 17h05

Ataque hacker deixa milhares de pessoas sem internet na região

Mais de 200 mil pessoas estão sem acesso a internet via rádio há três dias. Transmissão só deve ser normalizada em uma semana.

WISP's CPE attacked



15/05/2016 17h05 - Atualizado em 15/05/2016 17h05

Ataque hacker deixa milhares de pessoas sem internet na região

Mais de 200 mil pessoas estão sem acesso a internet via rádio há três dias. Transmissão só deve ser normalizada em uma semana.

A Smart "WORM"

- An EXPLOIT, exploited a flaw in the http/https service;
- Once one equipment was infected it starts to scan the neighborhood to find other targets;
- That is the reason that people called it a "worm" ou "Virus"

WISP's CPE attacked



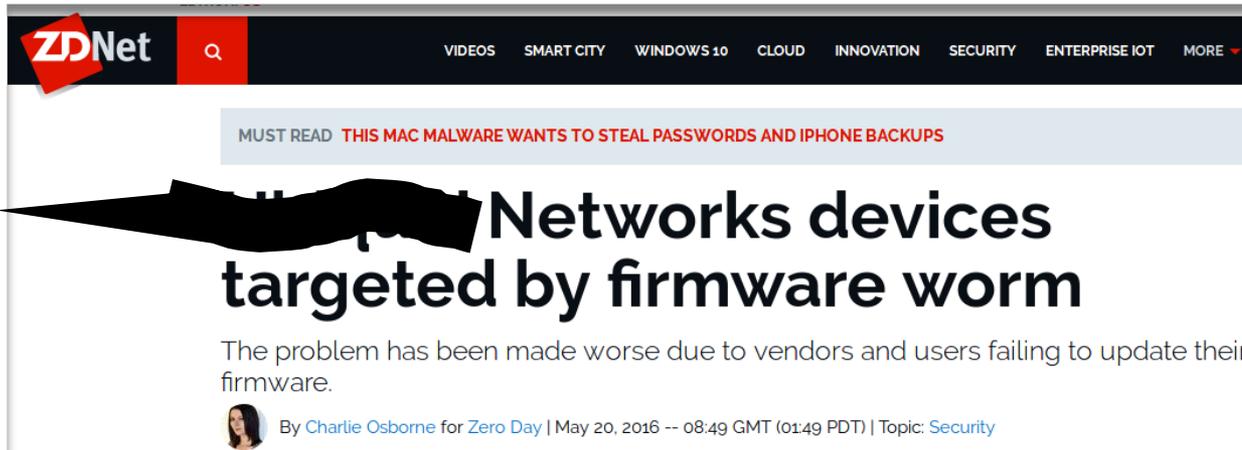
15/05/2016 17h05 - Atualizado em 15/05/2016 17h05

Ataque hacker deixa milhares de pessoas sem internet na região

Mais de 200 mil pessoas estão sem acesso a internet via rádio há três dias. Transmissão só deve ser normalizada em uma semana.

A Smart "WORM"

- There are many variants of the "Virus". With the most common WISPs had their Equipment reset and password changed to "n[REDACTED]r"
- WISPs loose the access to the equipment an have to go to the towers and remote location to fix the problem.
- Some Customers stayed without service for more than a week!!!



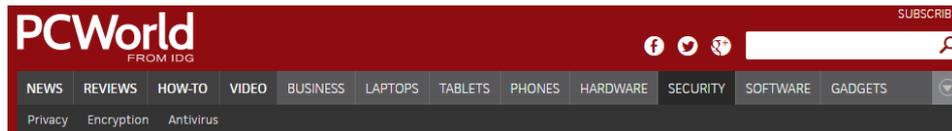
ZDNet VIDEOS SMART CITY WINDOWS 10 CLOUD INNOVATION SECURITY ENTERPRISE IOT MORE

MUST READ THIS MAC MALWARE WANTS TO STEAL PASSWORDS AND IPHONE BACKUPS

[REDACTED] Networks devices targeted by firmware worm

The problem has been made worse due to vendors and users failing to update their firmware.

By Charlie Osborne for Zero Day | May 20, 2016 -- 08:49 GMT (01:49 PDT) | Topic: Security



PCWorld FROM IDG

NEWS REVIEWS HOW-TO VIDEO BUSINESS LAPTOPS TABLETS PHONES HARDWARE SECURITY SOFTWARE GADGETS

Privacy Encryption Antivirus

Home / Security

NEWS Worm infects unpatched [REDACTED] wireless devices

The vulnerability has been known for almost a year, but many users haven't applied the patches



SecurityIntelligence Analysis and Insight for Information Security Professionals

NEWS 34 TOPICS INDUSTRIES

NEWS May 23, 2016 @ 2:00 PM [REDACTED] Routers Attacked by Worm



Ubiquiti Netw alert this week update their a was in respon company's ro performed by

The alert note payloads are exploit How

May 2016

WISP's CPE attacked

The flaw was previously known by the Manufacturer, thanks a **Bug Bounty Program**.

The manufacturer did **release an update** with a correction but **didn't emphasize the importance of doing that update**.



On the other hand, the affected WISPs didn't do the firmware update and weren't using other **good practices** for security, disabling unnecessary services, changing ports, restricting access from a known IP, etc.

WISP's CPE attacked

I have to highlight the work of Alexandre Correa (Onda Internet)

<https://www.linkedin.com/in/ajcorrea/>

who did a great job helping ISPs with problems making some scripts to find vulnerable equipment and automatically correcting them.

The scripts are available at Github:
<https://github.com/ajcorrea/cleanmf>





July, 2016

DDoS Hackers Exposed

pastebin.com/Rg1xT68V

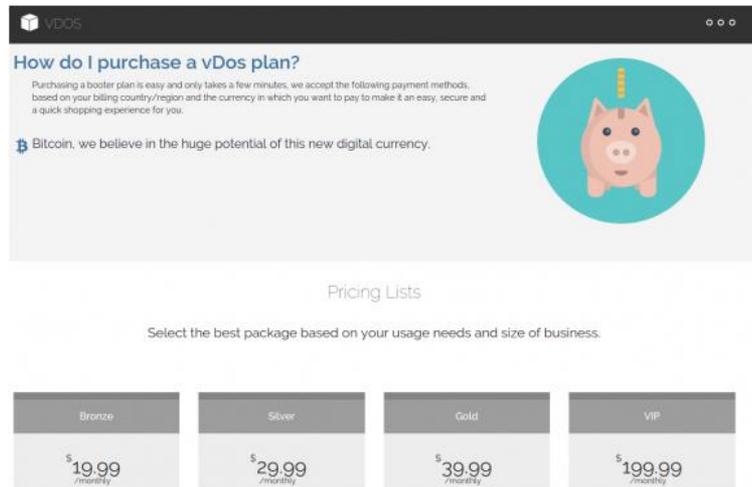
July, 2016



BLOG ADVERTISING

08 Israeli Online Attack Service 'vDOS' Earned \$600,000 in Two Years

SEP 16



vDOS

How do I purchase a vDos plan?

Purchasing a booster plan is easy and only takes a few minutes, we accept the following payment methods, based on your billing country/region and the currency in which you want to pay to make it an easy, secure and a quick shopping experience for you.

Bitcoin, we believe in the huge potential of this new digital currency.



Pricing Lists

Select the best package based on your usage needs and size of business.

Bronze	Silver	Gold	VIP
\$19.99 /monthly	\$29.99 /monthly	\$39.99 /monthly	\$199.99 /monthly

The vDos home page.

Brian Krebs, an investigative reporter known for his works about profit-seeking hacker organizations, revealed the vDOS web site.

Soon after Krebs report, two men were arrested and the Web site was taken offline.



September, 2016

Hackers Fightback!

Hackers Fightback!

September, 2016

≡ BUSINESS INSIDER ENTERPRISE

Akamai kicked journalist Brian Krebs' site off its servers after he was hit by a 'record' cyberattack



≡ FORTUNE | Google Rescues a Security Blogger Under Attack from Hackers

MEDIA AND TECHNOLOGY

Google Rescues a Security Blogger Under Attack from Hackers

Brian's blog received a DDoS of 620 Gbps and the hosting company kicked the site off!

Google shield program "rescued" the Security Blogger



2016 September, October

OVH massive attack

September 2016



Home > Virus & Threats



150,000 IoT Devices Abused for Massive DDoS Attacks on OVH

~ 1 Tbps attack



October 2016



BRIEF

14K web domains dropped Dyn following massive DDoS attack

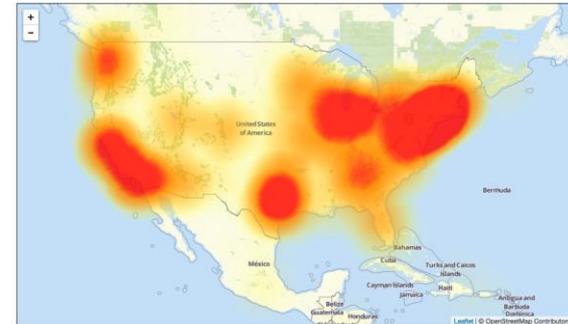


Home > Security

NEWS

DNS provider Dyn hit by DDoS attack that takes out major sites

Twitter, GitHub, Etsy, Spotify, The New York Times and the Boston Globe were knocked offline



MUST READ FROM MALWARE TO CYBER-SPIES, THE 15 BIGGEST THREATS ONLINE, RANKED

Dyn DDoS part 2: The hackers strike back



2016, November

Routers, again...

Deutsche Telekom Routers Attacked



More than 900k routers of Deutsche Telekom German users went offline

November 28, 2016 By Pierluigi Paganini



welivesecurity
News, views, and insight from the ESET security community

All Posts Latest Research How To Multimedia Papers Our Experts

900,000 Germans knocked offline, as critical router flaw exploited

BY GRAHAM CLULEY POSTED 29 NOV 2016 - 03:55PM

MALWARE

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE FORUMS

RISK ASSESSMENT —

Newly discovered router flaw being hammered by in-the-wild attacks

Researchers detect barrage of exploits targeting potentially millions of devices.

DAN GOODIN - 11/28/2016, 7:21 PM

November 2016

Deutsche Telekom

- The attack exploited the older TR-064 protocol, through port 7547.
- Port 7547 is the same used by TR-069
- The attacker managed to inject code in the routers making them download malicious software;
- The routers can be turned on robots for DDoS attacks.





2016

Lessons Learned



Internet of Things

Welcome to the world of connected everything



TECHNOLOGY LAB —

How one rent-a-botnet army of cameras, DVRs caused Internet chaos

Attacks that took down Dyn appear to have been "rented" from multiple botnets.

SEAN GALLAGHER - 10/25/2016, 6:45 PM



MUST READ [MICROSOFT ISSUES CRITICAL SECURITY PATCHES, BUT LEAVES ZERO-DAY FLAWS AT RISK](#)

Surveillance cameras sold on Amazon infected with malware

A security researcher has discovered malicious code embedded within cameras offered for sale on the e-commerce platform.



By [Charlie Osborne](#) for Zero Day | April 11, 2016 -- 09:53 GMT (02:53 PDT) | Topic: [Security](#)

Mirai Botnet



Ethical hackers claim Mirai is “tip of the iceberg”, as Deutsche Telekom boosts security after attack

Latest News

01 December 2016



December 2016

“**Mirai**,” a malware strain that enslaves poorly secured Internet of Things (IoT) devices like wireless routers and security cameras into a botnet for use in large cyberattacks.



<https://krebsonsecurity.com>



To end 2016 with a flourish...

Mirai Source Code Released!



*"When I first go in DDoS industry, I wasn't planning on staying in it long. I made my money, **there's lots of eyes looking at IoT now**, so it's time to GTFO.*

So today, I have an amazing release for you..."

Anna-senpai



How Powerful are the “Things” of the Internet of Things?

How Many Things are there in the IoT?

Gartner
 WHY GARTNER ANALYSTS RESEARCH EVENTS CONSULTING ABOUT

Search

Newsroom

Press Release

Share: [Tweet](#) [in Share](#) 1,183 [G+](#) +43

STAMFORD, Conn., November 10, 2015 [View All Press Releases](#)

Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015

Table 1: Internet of Things Units Installed Base by Category (Millions of Units)

Category	2014	2015	2016	2020
Consumer	2,277	3,023	4,024	13,509
Business: Cross-Industry	632	815	1,092	4,408
Business: Vertical-Specific	898	1,065	1,276	3,990
Grand Total	3,807	4,902	6,392	20,797

Source: Gartner (November 2015)

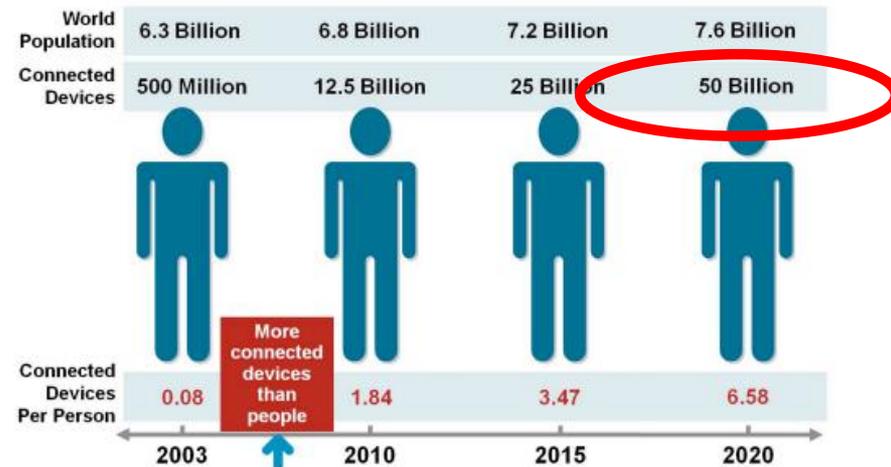
IEEE SPECTRUM

Follow on: [f](#) [t](#) [in](#) [+](#) [m](#)

Engineering Topics ▾ Special Reports ▾ Blogs ▾ Multimedia ▾

Tech Talk | Telecom | Internet

Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated

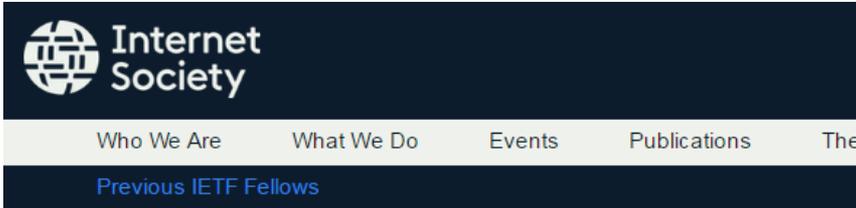


Source: Cisco IBSG, April 2011



Anything else to Highlight in 2016?

2016 IPv6 20 years old!



Home » Blog » Tech Matters » Celebrating New Year 2016 with 10% IPv6!

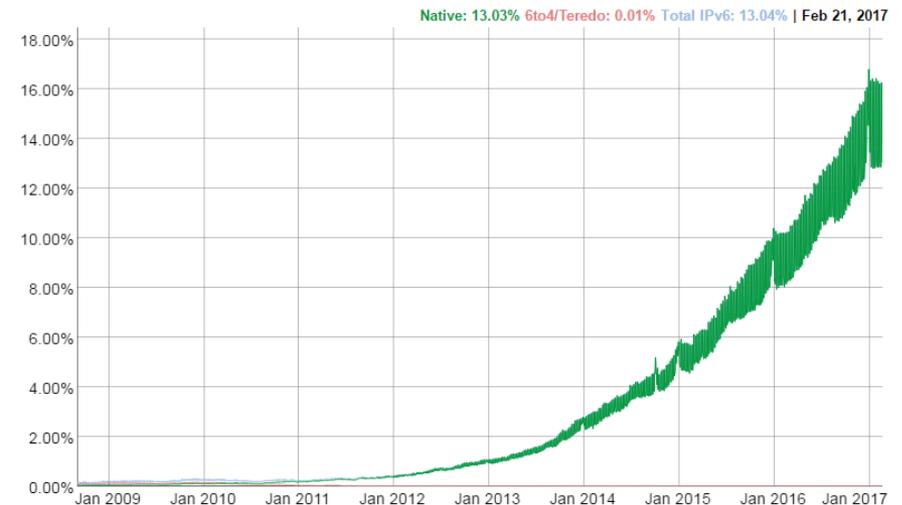
Celebrating New Year 2016 with 10% IPv6!

📅 04 January 2016 🗨️ Tech Matters



IPv6 Adoption

We are continuously measuring the availability of IPv6 connectivity among Google users. The graph shows the percentage of users that access Google over IPv6.





Internet Architecture Board

[Home](#) [About](#) [Activities](#) [Documents](#) [Liaisons](#) [Appeals](#) [IAB Mailing Lists](#)

← Please comment on IAOC candidates for IAB selection

IAB Statement on IPv6

Posted on 2016-11-07
by Cindy Morgan

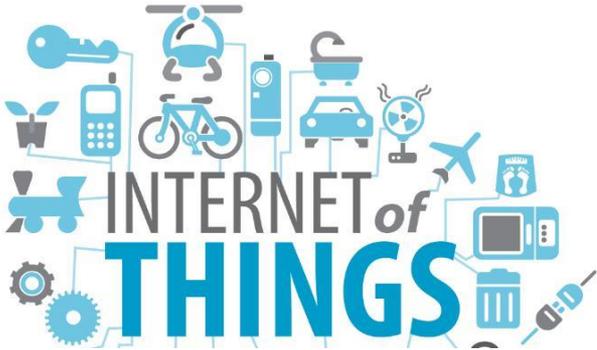
<https://www.iab.org/2016/11/07/iab-statement-on-ipv6/>

...

“The IAB expects that the IETF **will stop requiring IPv4 compatibility in new or extended protocols**. Future IETF protocol work will then optimize for and depend on IPv6.”

...

New Internet Scenario



IoT + IPv6 - NAT

**As an ISP, should I
care?**



Home > Internet



DEFENSIVE COMPUTING

By Michael Horowitz | Follow

About  Defensive Com computing dev than focus on t aims to be educ opinions.

OPINION

Blame the ISPs rather than the routers



ENDPOINT

9/29/2015
10:35 AM

Survey: Consumers Would Switch ISPs for Better Security

IoT and IoT security is sure an ISP's responsibility!

Since this retrospective has been made...

Presentation Goals

1) Good practices to secure the “things” of the IoT that are **under our control** (ISP);

2) Good practices to provide a **minimum of security** for our customers’ “things”;

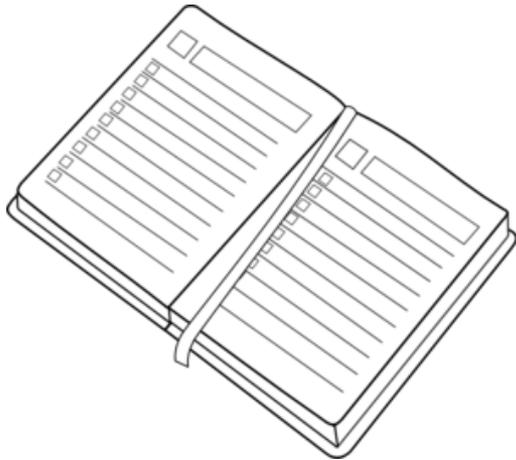
3) How to manage security implementation in large scale in a **pro-active an automated way.**



*The complete working solution in a small ISP using **open-source and free tools** will be showed.*

Introduction, motivation, relevant facts ✓

Reminder of good practices to secure RouterOS equipment at Outside Plant and at Customer Premises;



IPv6 protocol - issues, configurations and some recommended practices;

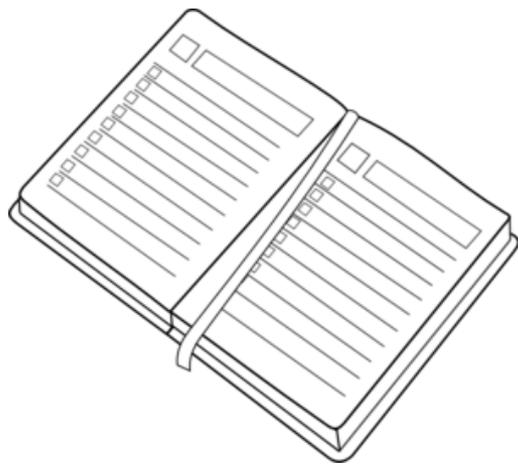
Customer Security – How to provide a minimum of security keeping neutrality and privacy;

Large scale security management – A real case implementation.



21'

Introduction, motivation, relevant facts ✓



Reminder of good practices to secure RouterOS equipment at Outside Plant and at Customer Premises;

IPv6 protocol - issues, configurations and some recommended practices;

Customer Security – How to provide a minimum of security keeping neutrality and privacy;

Large scale security management – A real case implementation.



16'



Physical Security

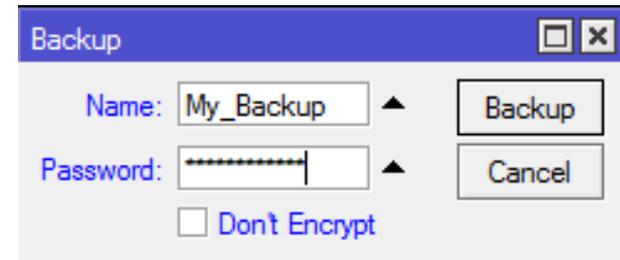




Physical Security

Equipment Outside Plant or in Customer Premises

- Disable unused Interfaces;
- Take care about local Backups. Do not leave them inside the boxes;
- Don't use local database for users. Use Radius instead;
- If you Technicians convinced you that it is absolutely necessary a local login, consider to create one but restrict it to ssh, and the use a RSA key;



Creating and uploading a RSA key

```
maia@xps:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/maia/.ssh/id_rsa): mdadm-ssh
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in mdadm-ssh.
Your public key has been saved in mdadm-ssh.pub.
The key fingerprint is:
SHA256:6A4QANxds2fmF/BsWp5v0C2vUc+qZUT24MKm2x0eleE maia@xps
The key's randomart image is:
```

```
+---[RSA 2048]----+
| = . . . 0 . |
| 0 . . . 0 + |
| . . . + * +. |
| . . . = . + + 0 0 0 |
| . . . So = + 0 0 E o |
| . . . . 0 0 0 + 0 . |
| . . . . + = . 0 |
| . . . 0 . = 0 + |
| . . . . 0 0 + |
+----[SHA256]-----+
maia@xps:~$ █
```

```
maia@xps:~$ ftp 192.168.1.1
Connected to 192.168.1.1.
220 AP-Maia FTP server (MikroTik 6.38.5) ready
Name (192.168.1.1:maia): admin
331 Password required for admin
Password:
230 User admin logged in
Remote system type is UNIX.
ftp> put mdadm-ssh.pub
local: mdadm-ssh.pub remote: mdadm-ssh.pub
200 PORT command successful
150 Opening ASCII mode data connection for '/mdadm-ssh.pub'
226 ASCII transfer complete
391 bytes sent in 0.03 secs (14.3910 kB/s)
ftp> █
```



Creating a user with restricted rights

Group <mdadm-ssh>

Name:

Policies:

<input type="checkbox"/> local	<input type="checkbox"/> telnet
<input checked="" type="checkbox"/> ssh	<input type="checkbox"/> ftp
<input checked="" type="checkbox"/> reboot	<input checked="" type="checkbox"/> read
<input checked="" type="checkbox"/> write	<input checked="" type="checkbox"/> policy
<input type="checkbox"/> test	<input type="checkbox"/> winbox
<input type="checkbox"/> password	<input type="checkbox"/> web
<input type="checkbox"/> sniff	<input type="checkbox"/> sensitive
<input type="checkbox"/> api	<input type="checkbox"/> romon
<input type="checkbox"/> dude	<input type="checkbox"/> tikapp

Skin:

User <mdadm-ssh>

Name:

Group:

Allowed Address:

Import SSH Key

User:

Key File:

```
maia@xps:~$ ssh -l mdadm-ssh -p 6922 -i /home/maia/mdadm-ssh 192.168.1.1
mdadm-ssh@192.168.1.1's password:
```

- Consider a script to “visit” your outside boxes and change regularly (e.g weekly) the local access credentials.

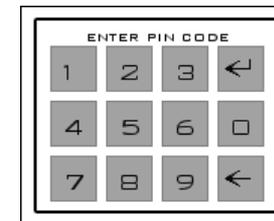
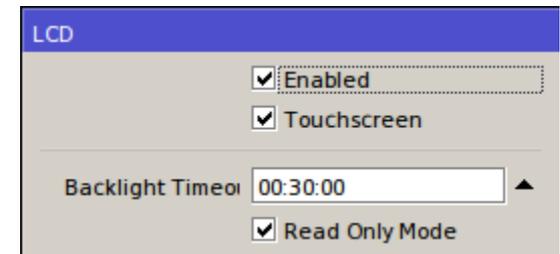


Physical Security



LCD

If you really need the LCD on, make sure LCD is on read-only mode. otherwise, the PIN code (default = 1234) will be asked and someone who has it can add an IP address, reboot or even reset the router.





Protected Bootloader

Allows the protection of RouterOS configuration and files from a physical attacker by disabling ether boot.

Can be enabled and disabled only from within RouterOS after login;

When this setting is enabled - reset button, reset pin-hole is and console access is disabled;

Special package for this is provided.

https://wiki.mikrotik.com/wiki/Manual:RouterBOARD_settings#Protected_bootloader



Layer 2 Security





Layer 2 Security

There are a lot of issues in Layer 2 that have to be considered depending on the specific topology and features used;

- Mac Flooding
- MNDP / CDP
- DHCP Starvation
- Vlan hopping attack
- Spanning tree attacks
- ARP poisoning attacks
- Deauth attack



Layer 2 Security

RouterOS has several features that can be used to mitigate Layer 2 issues, like:

- Bridge Filtering
- Layer 2 Isolation
- Management Protection (Wireless)

Use and overuse RouterOS features!

Reference = MUM 2010 Wroclaw / Poland:

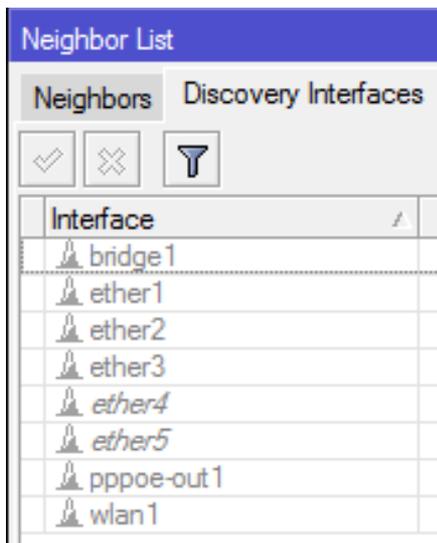
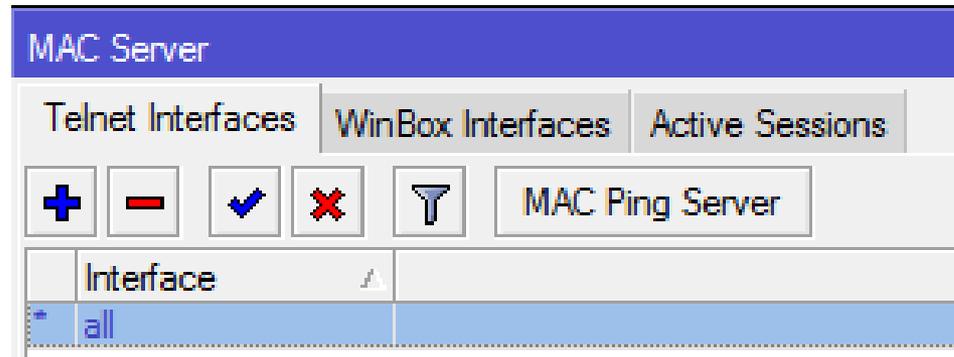
[Layer 2 Security – Attacks and Countermeasures using MikroTik RouterOS](#)



Layer 2 Security

MAC-Server

Disable MAC-Server for Telnet and Winbox whenever possible. If "necessary" enable only on specific interfaces



MNDP

Disable Discovery Interfaces whenever possible to avoid MNDP attacks.



Layer 2 Security (Wireless)

Interface Wireless

Default Authentication
 Default Forward
 Hide SSID
 Multicast Helper:

In case you have more than one Wireless interface, use also Horizon, or Bridge Filters

Bridge Port <wlan1>

General Status

Interface: wlan1
 Bridge: bridge1
 Priority: 80
 Path Cost: 10
 Horizon: 5

Bridge Port <wlan2>

General Status

Interface: wlan2
 Bridge: bridge2
 Priority: 80
 Path Cost: 10
 Horizon: 5

Bridge Filter Rule <>

General Advanced

Chain: forward

Interfaces

In. Interface: wlan1
 Out. Interface: wlan2

Bridge Filter Rule <>

ARP STP Action Statistics ...

Action: drop



Layer 2 Security (Wireless)

Interface Wireless

Security Profile <PSK>

General RADIUS EAP Static Keys

EAP Methods: EAP-TLS

TLS Mode: verify certificate

TLS Certificate: 58_cert.pem_0

Use strong encryption methods,
preferably using Certificates

Management Protection: required

Management Protection Key:

Protect against **Deauth Attack**
and MAC spoofing, specially in
Point to Point links



Services Security





IP Services

IP Service List			
	Name	Port	Available From
X	api	8728	
X	api-ssl	8729	
X	ftp	21	
	ssh	9922	192.168.77.1
X	telnet	23	
	winbox	8292	192.168.77.1
X	www	80	
X	www-ssl	443	

Disable unnecessary services;

Change default ports;

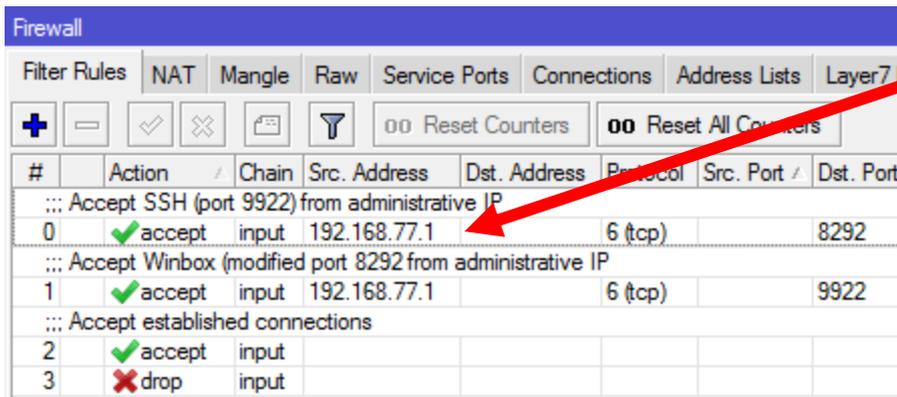
Restrict access from a particular IP

Can sounds a little bit paranoid, but besides the above, **for running services** it's important to block also in /ip firewall (see next slide)



Services Security

IP Firewall



#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port
::: Accept SSH (port 9922) from administrative IP							
0	✓ accept	input	192.168.77.1		6 (tcp)		8292
::: Accept Winbox (modified port 8292 from administrative IP							
1	✓ accept	input	192.168.77.1		6 (tcp)		9922
::: Accept established connections							
2	✓ accept	input					
3	✗ drop	input					

On Input channel restrict the access to services only for administrative IPs; **

** Although it seems redundant, the reason to block services/ports also in /ip firewall was pointed by **Tom Smyth** (wirelessconnect.eu):

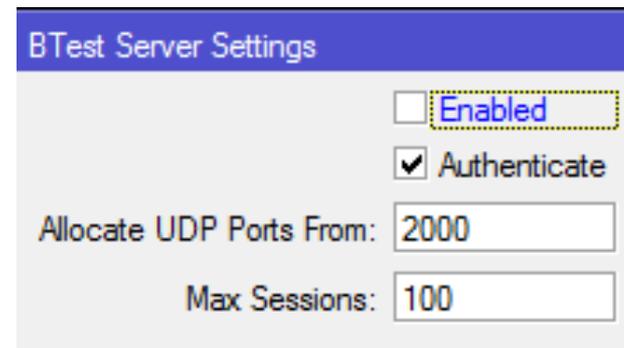
*"As far as I am aware and from tests I carried out about 7 or 8 years ago the allowed from IP addresses in IP services menu uses TCP wrappers and actually allows TCP connections from any address (**regardless of what IPs you specified**) the decision to allow or deny a user login is taken after the connection is made so there could be a window for the exploit to be uploaded."*



Services Security

Bandwidth Test Server

There is no reason to leave Bandwidth test server enabled by default. Enable it only when and where you want to test something



BTest Server Settings

Enabled

Authenticate

Allocate UDP Ports From:

Max Sessions:



Enable Strong Crypto

Since v.30 Mikrotik has changed ssh module, introducing stronger encryption algorithms and methods.

```
[mdadm-ssh@AP-Maia] > ip ssh set strong-crypto=yes  
[mdadm-ssh@AP-Maia] > █
```

Strong crypto is disabled by default and should be considered whenever the impacts on hardware resources would not be a problem.



Services disabled by default that should be kept disabled:

```
/ip upnp  
/ip smb  
/ip socks  
...
```

If you are not sure which services are running in your box, try to find them with nmap:

```
maia@xps:~$ sudo nmap -A -T4 192.168.88.1  
[sudo] password for maia:  
  
Starting Nmap 7.01 ( https://nmap.org ) at 2017-03-29 15:22 CEST
```



Routing Security

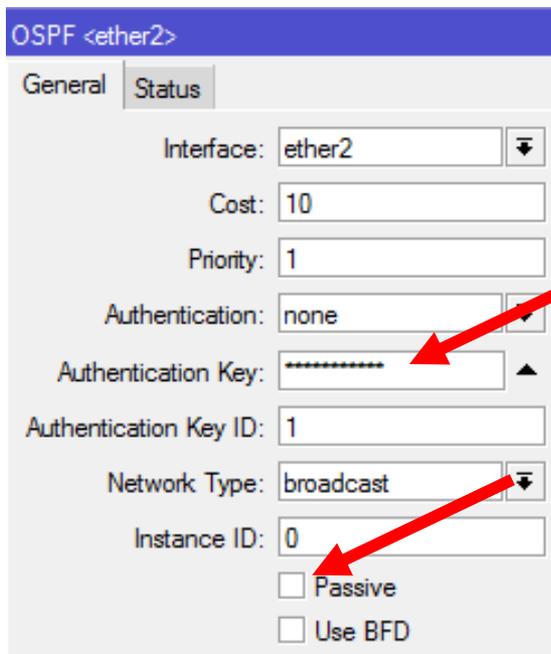




Routing Security

OSPF and OSPFv3

- Use encryption;
- Set interfaces to passive mode on links where clients are connected in;
- Drop protocol 89 on appropriate Interfaces.



OSPF <ether2>

General Status

Interface: ether2

Cost: 10

Priority: 1

Authentication: none

Authentication Key: [redacted]

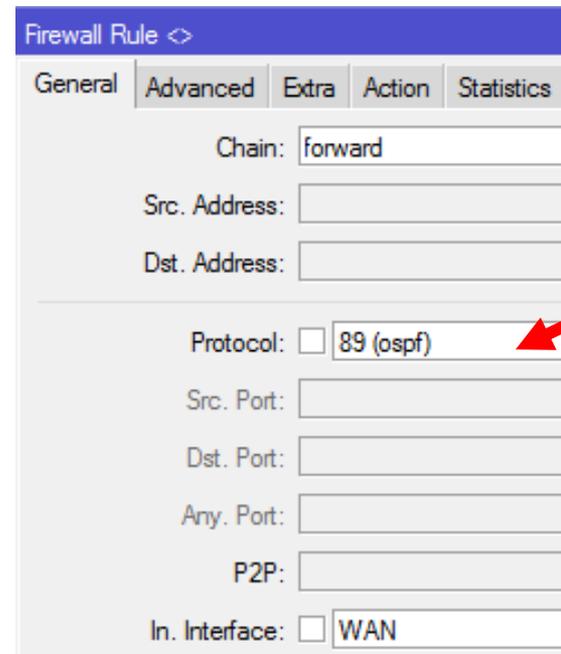
Authentication Key ID: 1

Network Type: broadcast

Instance ID: 0

Passive

Use BFD



Firewall Rule <>

General Advanced Extra Action Statistics

Chain: forward

Src. Address:

Dst. Address:

Protocol: 89 (ospf)

Src. Port:

Dst. Port:

Any. Port:

P2P:

In. Interface: WAN

[Routing Security – Hungary MUM 2011](#)



Routing Security

BGP Peer <peer1>

General | Advanced | Status

Name: peer1

Instance: default

Remote Address: 1.1.1.1

Remote Port:

Remote AS: 1111

TCP MD5 Key: *****

Nexthop Choice: default

Multihop

Route Reflect

Hold Time: 180

Keepalive Time:

TTL: 2

BGP

- Use MD5 encryption;
- Use TTL "hack";
- Filter BOGONs prefixes;
- Filter unwanted prefixes, like own prefix;
- Filter too large AS-Path;
- etc...

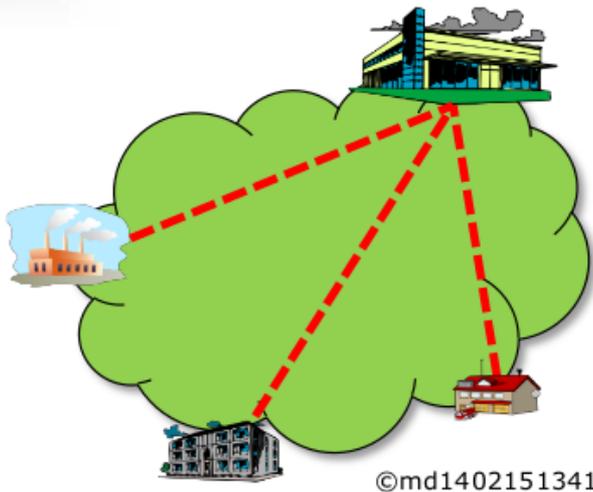
[Routing Security – Hungary MUM 2011](#)
[BGP Filtering – Croatia MUM 2013](#)



Routing Security

MPLS VPNs

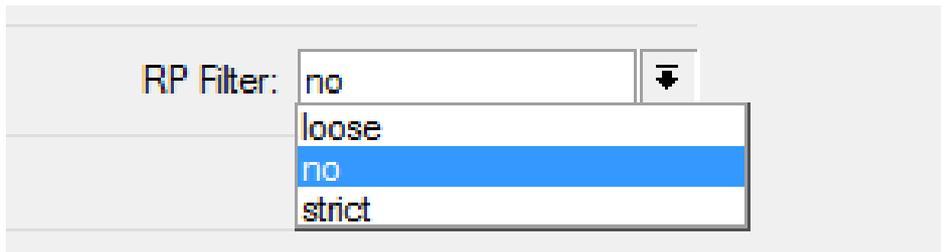
- Use only static routing between CE - > PE;
- Do not give your customer access to CE routers;
- Protect network against spoofing using uRPF;
- Consider using IPSec between PEs



[MPLS VPN Security – Italy MUM 2014](#)



uRPF Filter



RP Filter: no

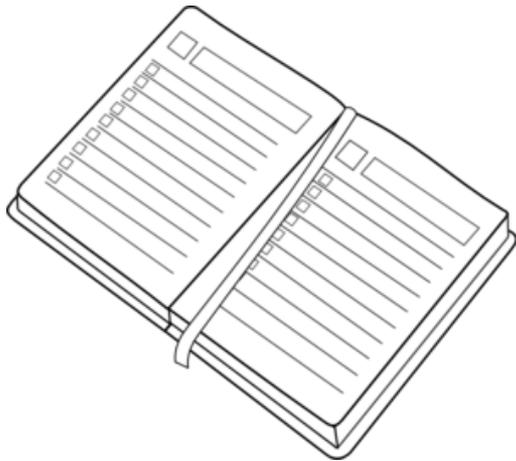
- loose
- no
- strict

To avoid spoofing from your customers it is **very important** to enable URPF;

- **strict mode:** the packet must be received on the interface that the router would use to forward the return packet
- **loose mode:** for a received packet, router has to have some route to deliver the return packet.

Introduction, motivation, relevant facts; ✓

Reminder (check list) of good practices to secure RouterOS equipment at Outside Plant and at Customer Premises; ✓



IPv6 protocol - issues, configurations and some recommended practices;

Customer Security – How to provide a minimum of security keeping neutrality and privacy;

Large scale security management – A real case implementation.



30'

Misconceptions about IPv6 Security

Misconceptions about IPv6 security

1) IPv6 is more secure than IPv4 because it uses IPsec

IPsec was originally developed for IPv6 and backported to IPv4. It was a **mandatory feature**.

RFC 6434 (<https://tools.ietf.org/html/rfc6434>), changed from mandatory to optional

SHOULD != MUST



IPsec

2) Scanning is impossible in IPv6

The smallest recommended network (/64) has the current Internet IPv4 space squared. This makes traditional (sequential) scan methods pointless.

However, selective techniques based on the way addresses are formed and configured can make a successful scanning.

Besides that, multicast addresses can be used to gather information inside the network, identifying routers, routers, OSPF, routers, etc.



Scanning



Some articles about scanning, by [Fernando Gont](#)

Vast IPv6 address space actually enables IPv6 attacks

<http://searchsecurity.techtarget.com/tip/Analysis-Vast-IPv6-address-space-actually-enables-IPv6-attacks>

How to use DNS reverse mapping to scan IPv6 addresses

<http://searchsecurity.techtarget.com/tip/How-to-use-DNS-reverse-mapping-to-scan-IPv6-addresses>

DNS reverse address mapping: Exploiting the scanning technique

<http://searchsecurity.techtarget.com/tip/DNS-reverse-address-mapping-Exploiting-the-scanning-technique>

Multicast addresses in IPv6

Address	Description
FF02::1	Find Nodes on a subnet
FF02::2	Return Local Subnet Routers
FF02::5	OSPF Routers
FF02::6	Designed OSPF Routers (DR's)
FF02::9	RIP Routers
FF02::D	PIM Routers
FF02::1:2	DHCP Agents



Scanning

Misconceptions about IPv6 security

ff02::1 (All Hosts)

```
maia@maia-laptop:~$ sudo ping6 -I wlan0 ff02::1
PING ff02::1(ff02::1) from fe80::223:14ff:fe21:d4a8 wlan0: 56 data bytes
64 bytes from fe80::223:14ff:fe21:d4a8: icmp_seq=1 ttl=64 time=0.097 ms
64 bytes from fe80::a00:27ff:fe20:1052: icmp_seq=1 ttl=64 time=0.328 ms (DUP!)
64 bytes from fe80::a00:27ff:fe20:1052: icmp_seq=1 ttl=64 time=0.392 ms (DUP!)
64 bytes from fe80::20c:42ff:fe61:b3c3: icmp_seq=1 ttl=64 time=0.917 ms (DUP!)
64 bytes from fe80::20c:42ff:fe0c:a003: icmp_seq=1 ttl=64 time=1.20 ms (DUP!)
64 bytes from fe80::20c:42ff:fe3a:8e24: icmp_seq=1 ttl=64 time=1.63 ms (DUP!)
64 bytes from fe80::223:14ff:fe21:d4a8: icmp_seq=2 ttl=64 time=0.107 ms
64 bytes from fe80::a00:27ff:fe20:1052: icmp_seq=2 ttl=64 time=0.299 ms (DUP!)
64 bytes from fe80::a00:27ff:fe20:1052: icmp_seq=2 ttl=64 time=0.375 ms (DUP!)
```

ff02::2 (All Routers)

```
maia@maia-laptop:~$ sudo ping6 -I wlan0 ff02::2
PING ff02::2(ff02::2) from fe80::223:14ff:fe21:d4a8 wlan0: 56 data bytes
64 bytes from fe80::20c:42ff:fe61:b3c3: icmp_seq=1 ttl=64 time=8.77 ms
64 bytes from fe80::20c:42ff:fe61:b3c3: icmp_seq=2 ttl=64 time=0.804 ms
64 bytes from fe80::20c:42ff:fe61:b3c3: icmp_seq=3 ttl=64 time=0.904 ms
64 bytes from fe80::20c:42ff:fe61:b3c3: icmp_seq=4 ttl=64 time=0.832 ms
```

ff02::5 (All OSPF Routers)

```
maia@maia-laptop:~$ sudo ping6 -I wlan0 ff02::5
PING ff02::5(ff02::5) from fe80::223:14ff:fe21:d4a8 wlan0: 56 data bytes
64 bytes from fe80::20c:42ff:fe61:b3c3: icmp_seq=1 ttl=64 time=0.826 ms
64 bytes from fe80::20c:42ff:fe0c:a003: icmp_seq=1 ttl=64 time=1.26 ms (DUP!)
64 bytes from fe80::20c:42ff:fe61:b3c3: icmp_seq=2 ttl=64 time=0.870 ms
64 bytes from fe80::20c:42ff:fe0c:a003: icmp_seq=2 ttl=64 time=1.17 ms (DUP!)
64 bytes from fe80::20c:42ff:fe61:b3c3: icmp_seq=3 ttl=64 time=0.804 ms
64 bytes from fe80::20c:42ff:fe0c:a003: icmp_seq=3 ttl=64 time=1.15 ms (DUP!)
```

ff02::1:2 (All DHCP Servers)

```
maia@maia-laptop:~$ sudo ping6 -I wlan0 ff02::1:2
PING ff02::1:2(ff02::1:2) from fe80::223:14ff:fe21:d4a8 wlan0: 56 data bytes
64 bytes from fe80::20c:42ff:fe61:b3c3: icmp_seq=1 ttl=64 time=9.80 ms
64 bytes from fe80::20c:42ff:fe3a:8e24: icmp_seq=1 ttl=64 time=10.3 ms (DUP!)
64 bytes from fe80::20c:42ff:fe61:b3c3: icmp_seq=2 ttl=64 time=0.916 ms
64 bytes from fe80::20c:42ff:fe3a:8e24: icmp_seq=2 ttl=64 time=1.25 ms (DUP!)
64 bytes from fe80::20c:42ff:fe61:b3c3: icmp_seq=3 ttl=64 time=0.820 ms
64 bytes from fe80::20c:42ff:fe3a:8e24: icmp_seq=3 ttl=64 time=2.56 ms (DUP!)
```



Scanning

<http://mum.mikrotik.com/presentations/PL12/maia.pdf>
<https://www.youtube.com/watch?v=zZ6s1nVe-O0>

4) Because my network doesn't have IPv6, I don't have to care about IPv6 security

Even if your network doesn't support IPv6, you should care about IPv6 security, because of:

- Automatic transition techniques (Teredo, 6to4)
- Possible attacks on public hotspots

Please, see:

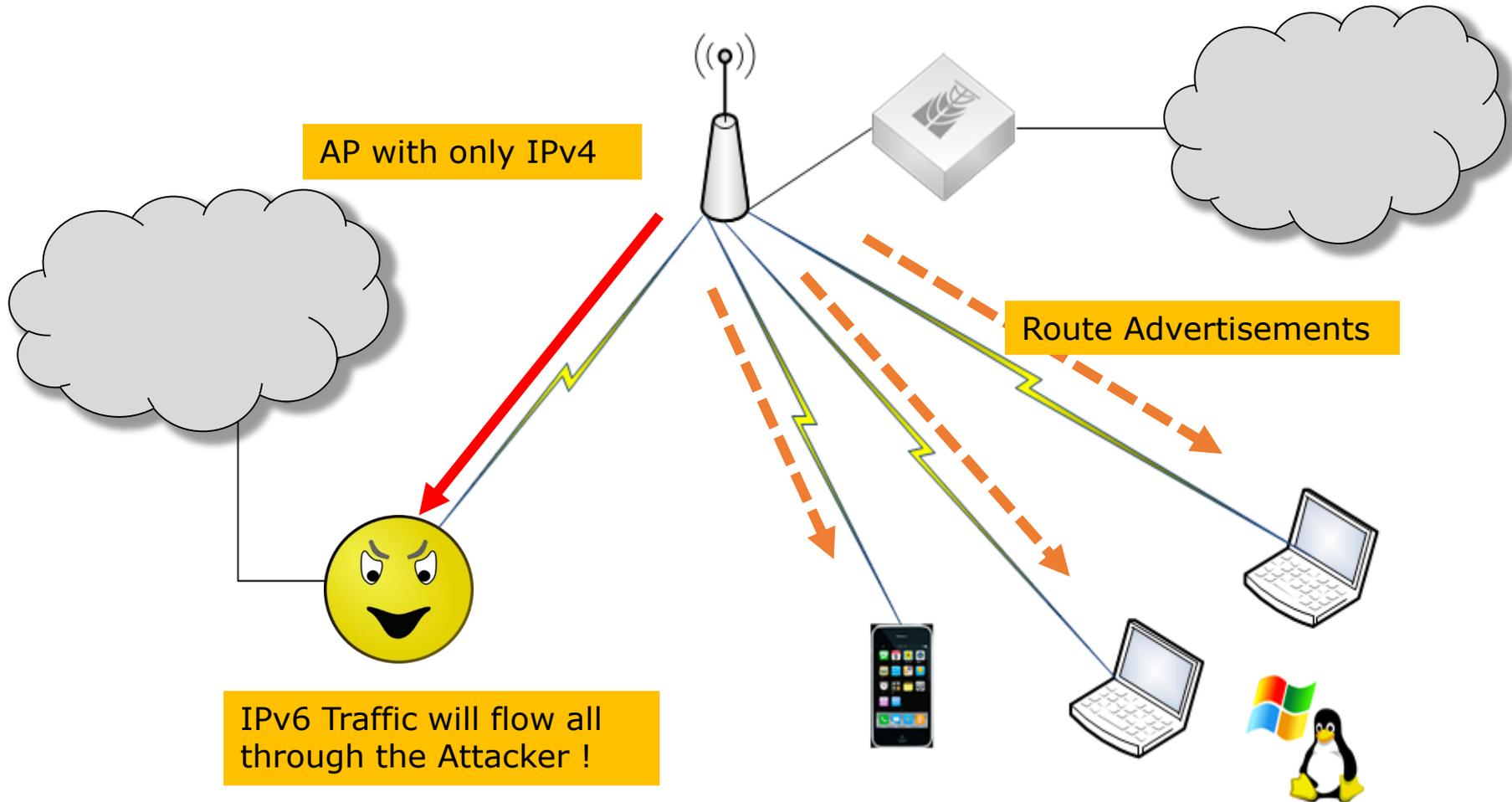
<http://mum.mikrotik.com/presentations/PL12/maia.pdf>

<https://www.youtube.com/watch?v=zZ6s1nVe-00>



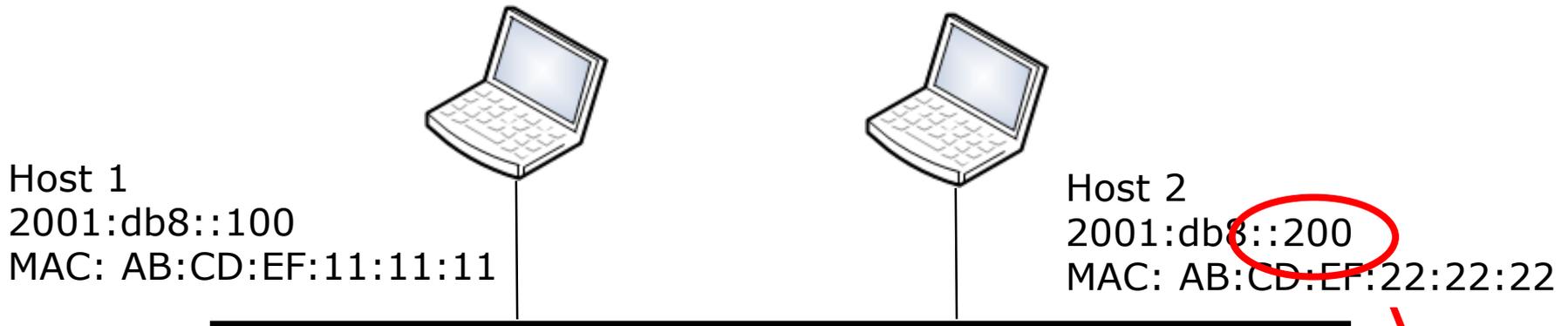
I don't care about IPv6 security

Abusing a Hotspot IPv4 only



Some IPv6 security issues

Neighbor discovery on IPv6



Neighbor Solicitation

(ICMPv6 Type 135)
Who is 2001:db8:200?

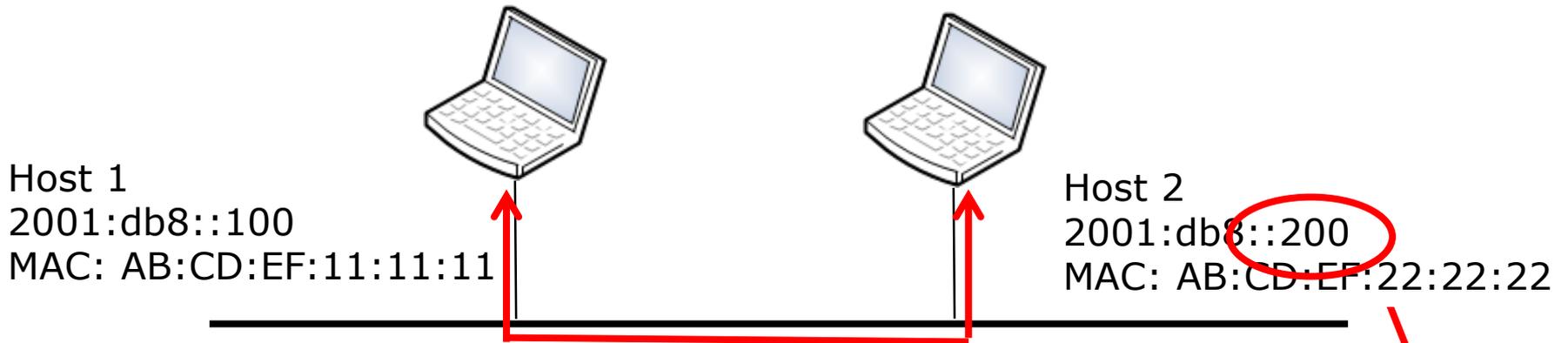
To: FF02::1:FF00:0200

To: 2001:db8::100

Neighbor Advertisement

(ICMPv6 Type 136)
2001:db8::200 is at AB:CD:EF:22:22:22

Neighbor discovery on IPv6



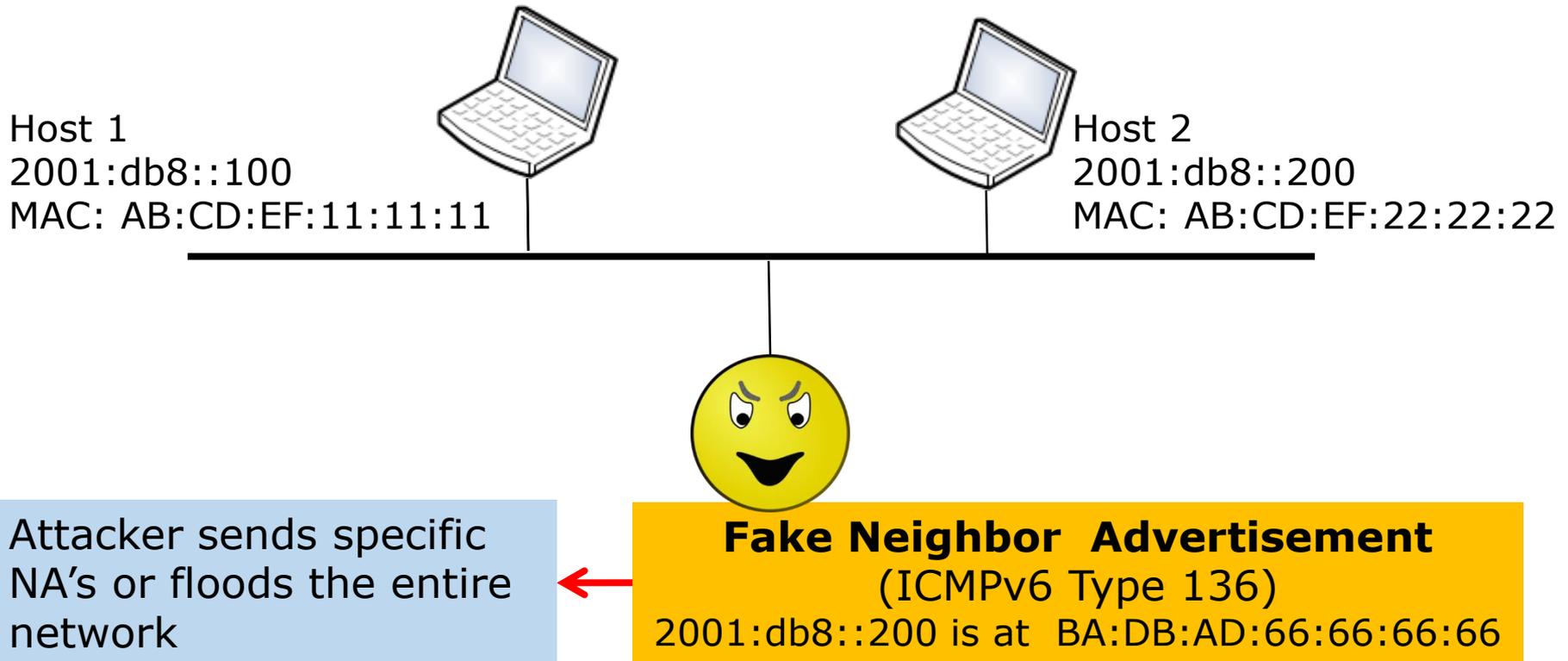
Neighbor Solicitation
(ICMPv6 Type 135)
Who is 2001:db8:200?

To: FF02::1:FF00:0200

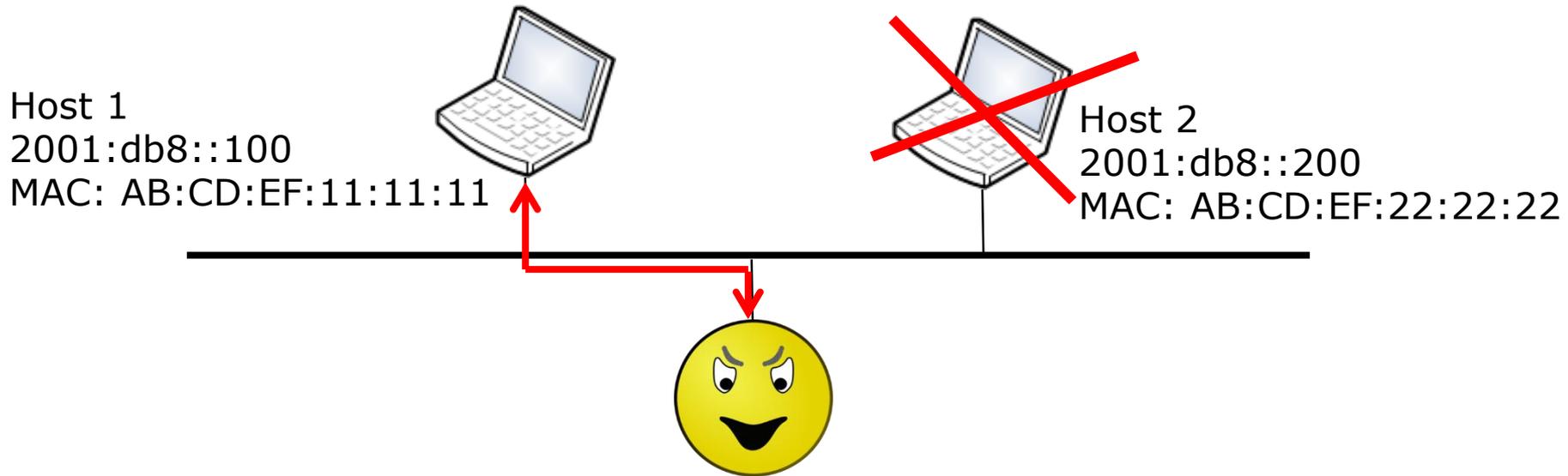
To: 2001:db8::100

Neighbor Advertisement
(ICMPv6 Type 136)
2001:db8::200 is at AB:CD:EF:22:22:22

Exploring Neighbor Discovery

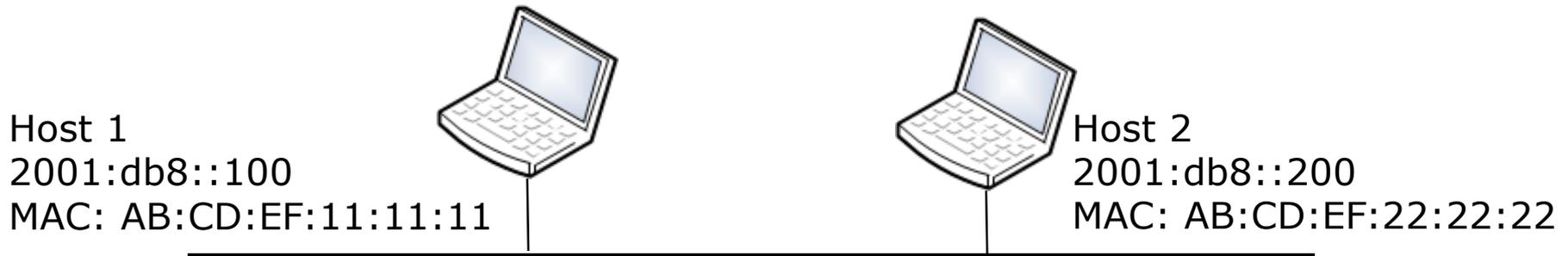


Exploring Neighbor Discovery



Host 1 thinks 2001:db8::200 is the attacker and send traffic layer 2 to it

Man-In-The-Middle



To: 2001:db8::100

Fake Neighbor Advertisement

(ICMPv6 Type 136)

2001:db8::200 is at BA:DB:AD:66:66:66:66

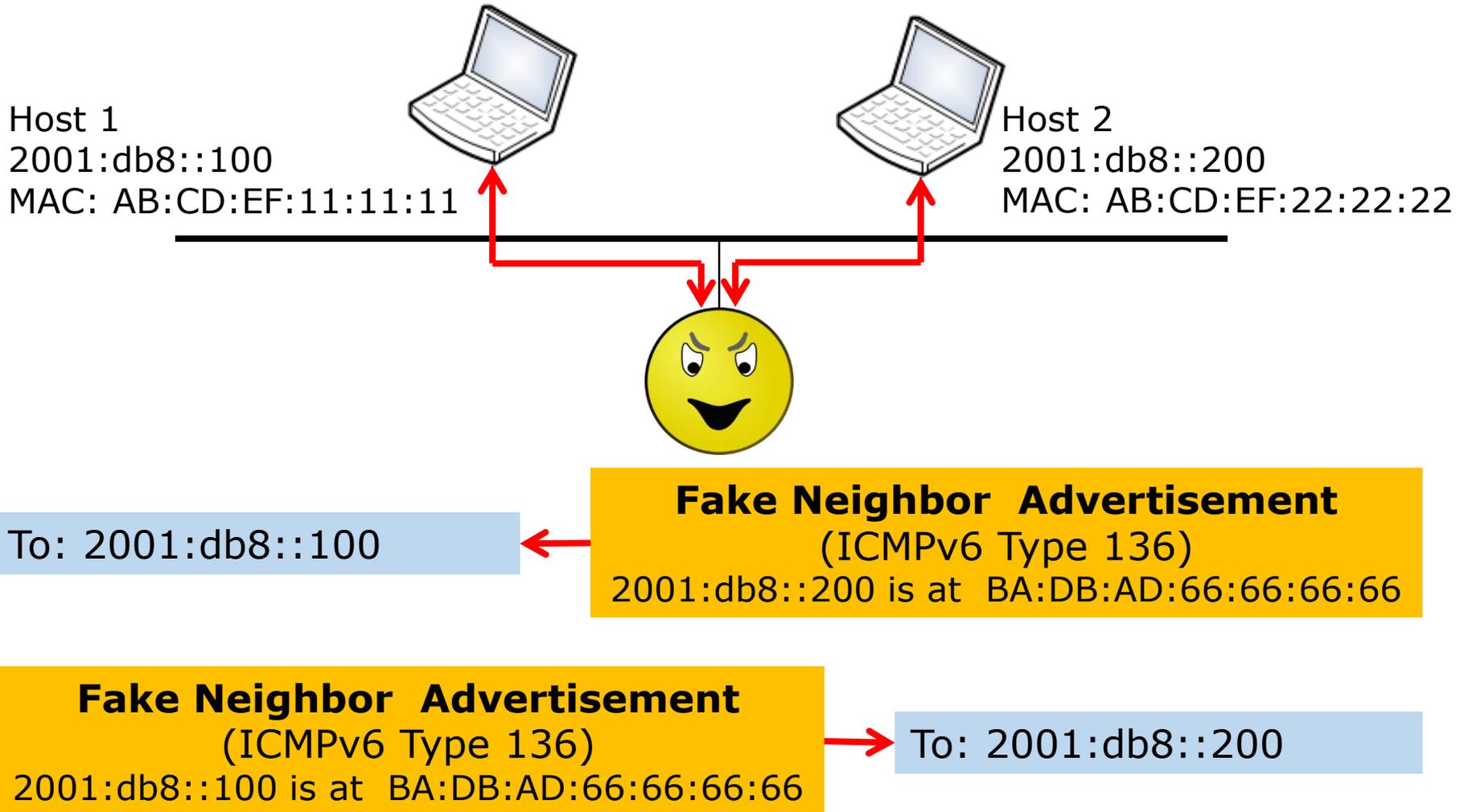
Fake Neighbor Advertisement

(ICMPv6 Type 136)

2001:db8::100 is at BA:DB:AD:66:66:66:66

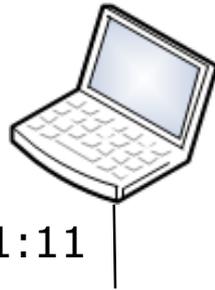
To: 2001:db8::200

Man-In-The-Middle



DAD – Duplicate Address Detection

After a boot or an IP change, DAD must be executed before using any IPv6 address (including link local address).

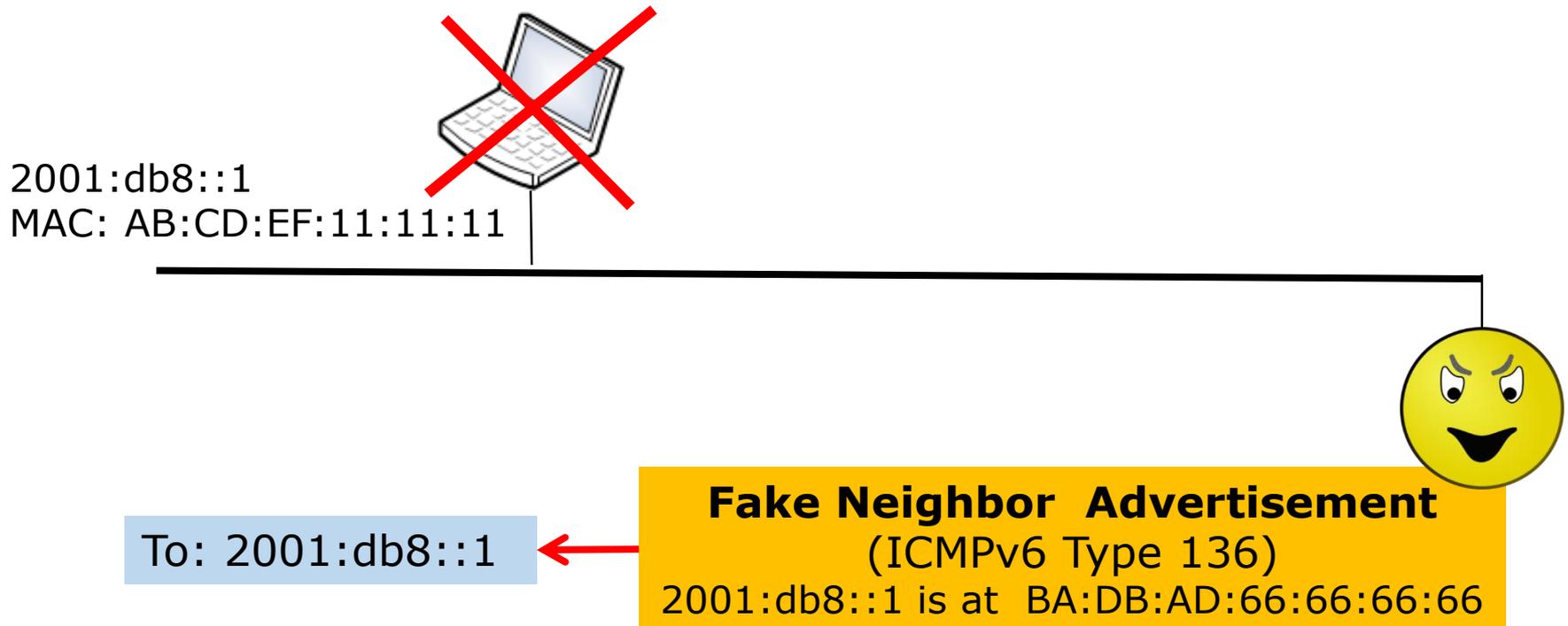


2001:db8::1
MAC: AB:CD:EF:11:11:11

Neighbor Solicitation
(ICMPv6 Type 135)
Who is 2001:db8:1 ?

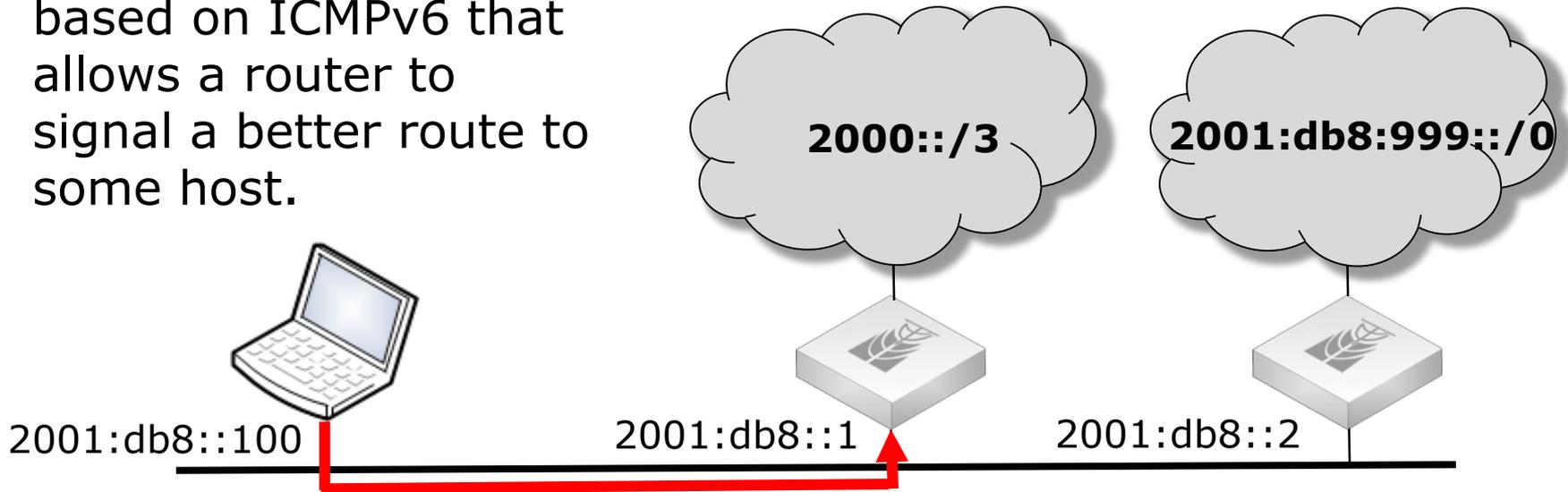
To: FF02::1:FF00:0001

If the host receives somehow a response, it will not use the IP for communications.



DAD exploitation can be used to cause a DoS to a specific device, the whole network or to impersonate some device.

Redirection is a feature based on ICMPv6 that allows a router to signal a better route to some host.

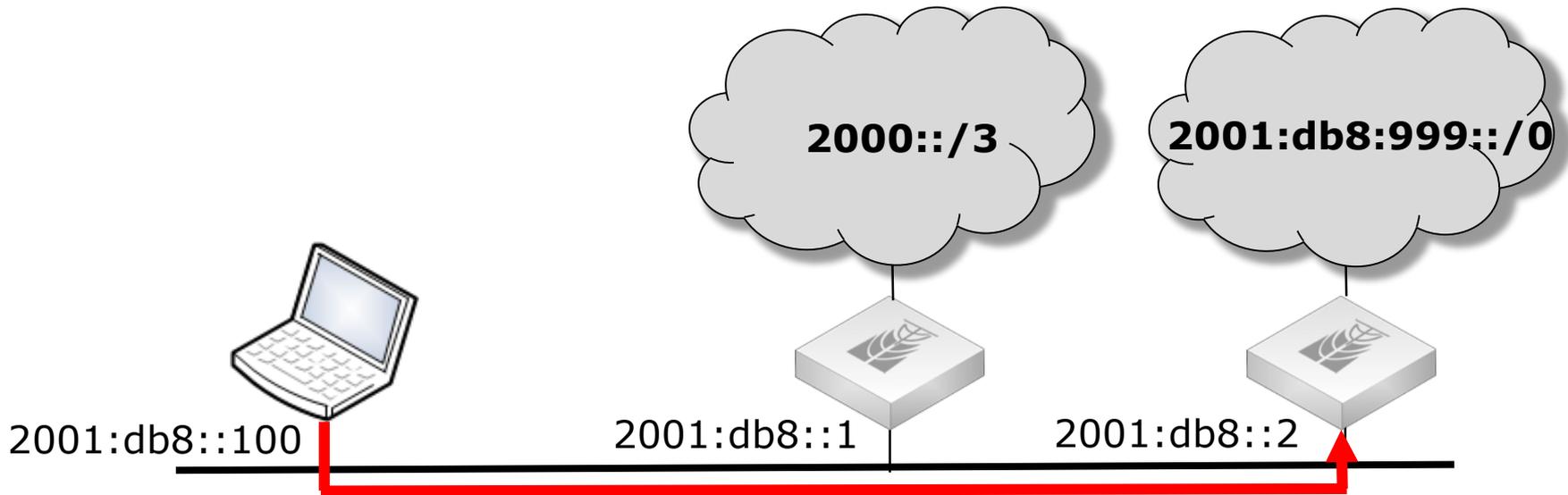


Packet to 2001:db8::999::X → To default gateway (2001:db8::1)

To 2001:db8::100

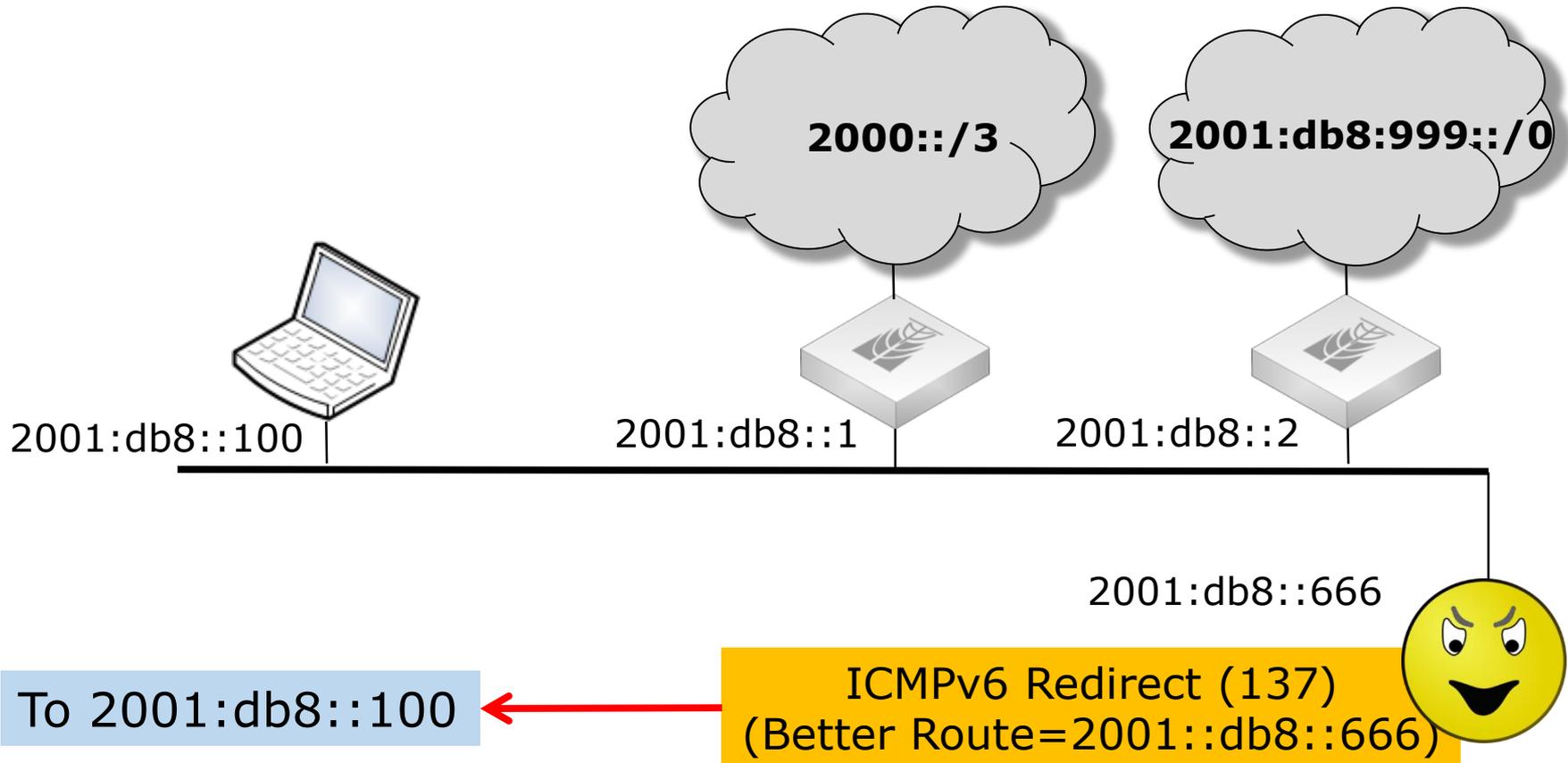
ICMPv6 Redirect (137)
(Better Route=2001::db8::2)

ICMPv6 Redirects

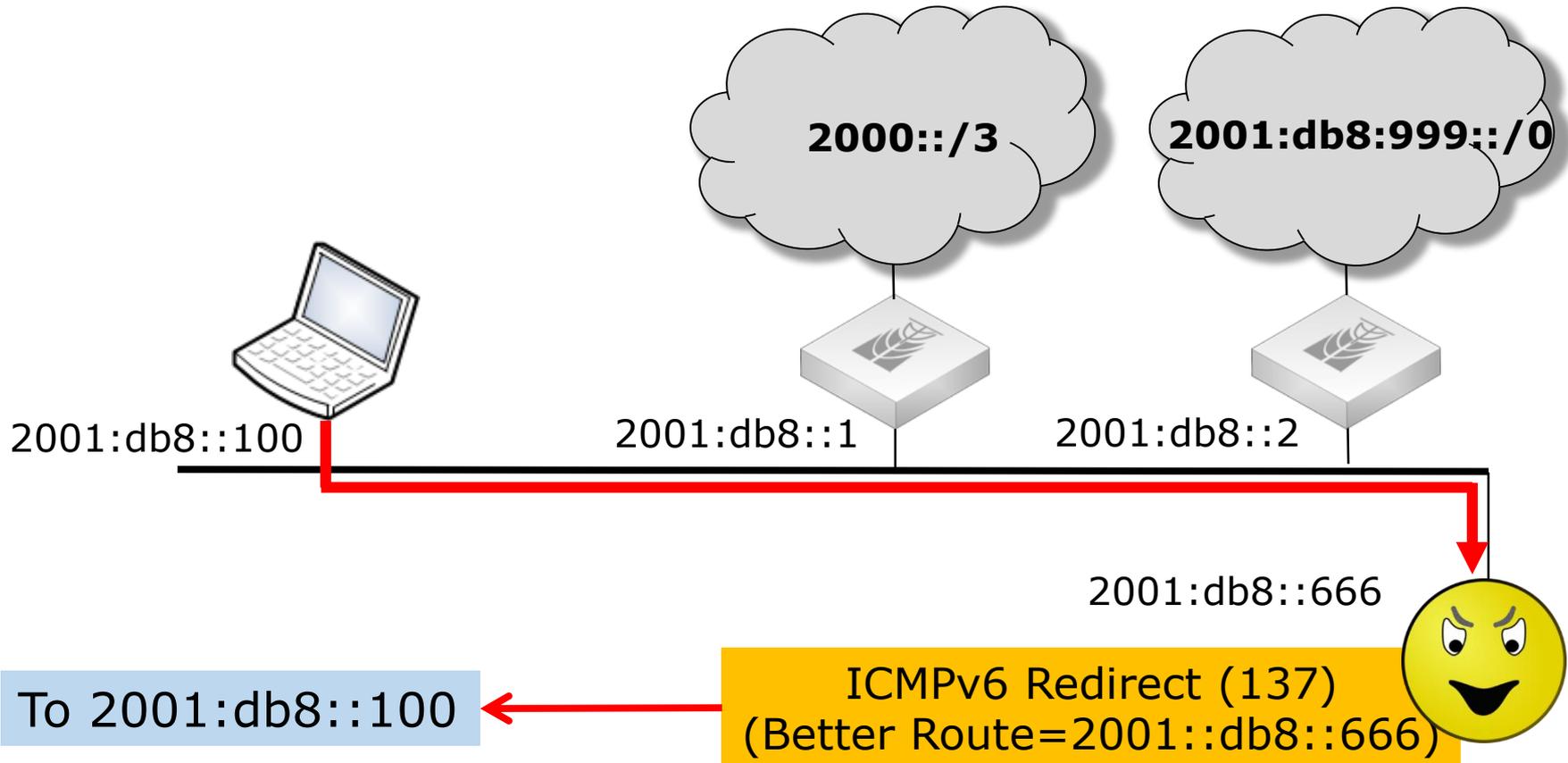


Further communication to `2001:db8:999::/0` will be sent through `2001:db8::2`

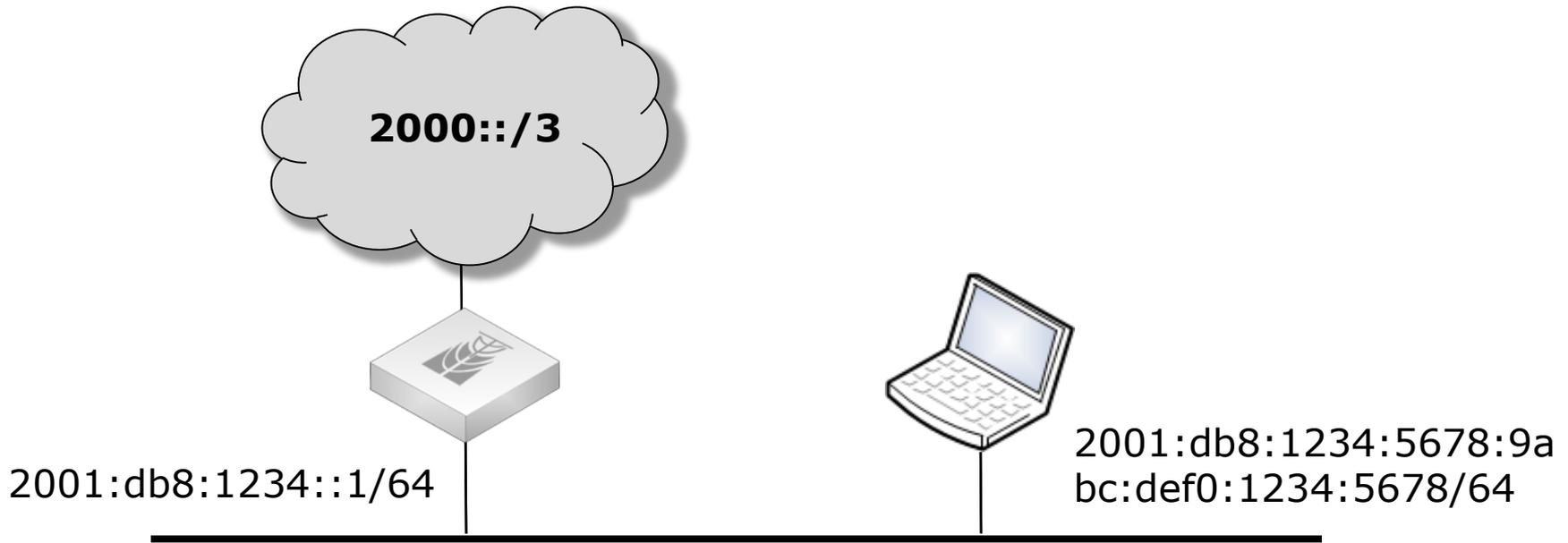
Exploring ICMPv6 Redirects



Exploring ICMPv6 Redirects



Router Advertisement



Router Advertisement

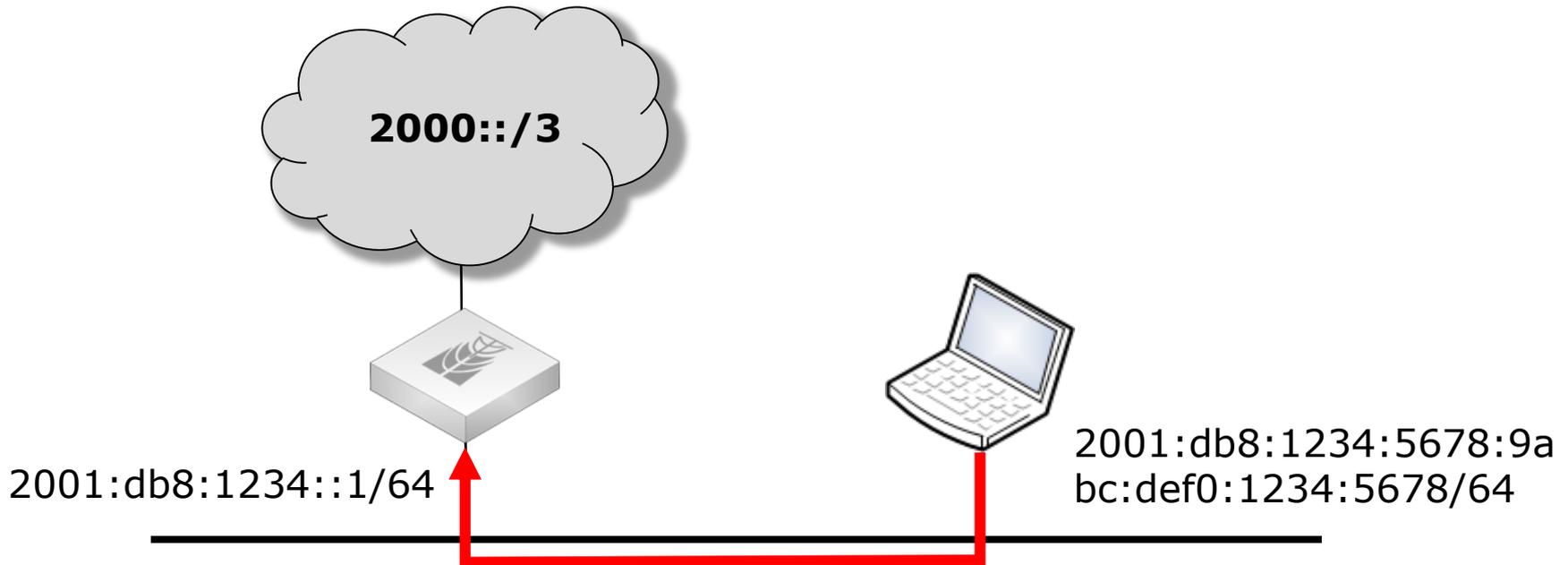
(ICMPv6 Type 134)

Source: Link-local address

Contents: Options, prefixes,
lifetime, auto configuration flag

To: FF02::1 (All nodes on link)

Router Advertisement



Router Advertisement

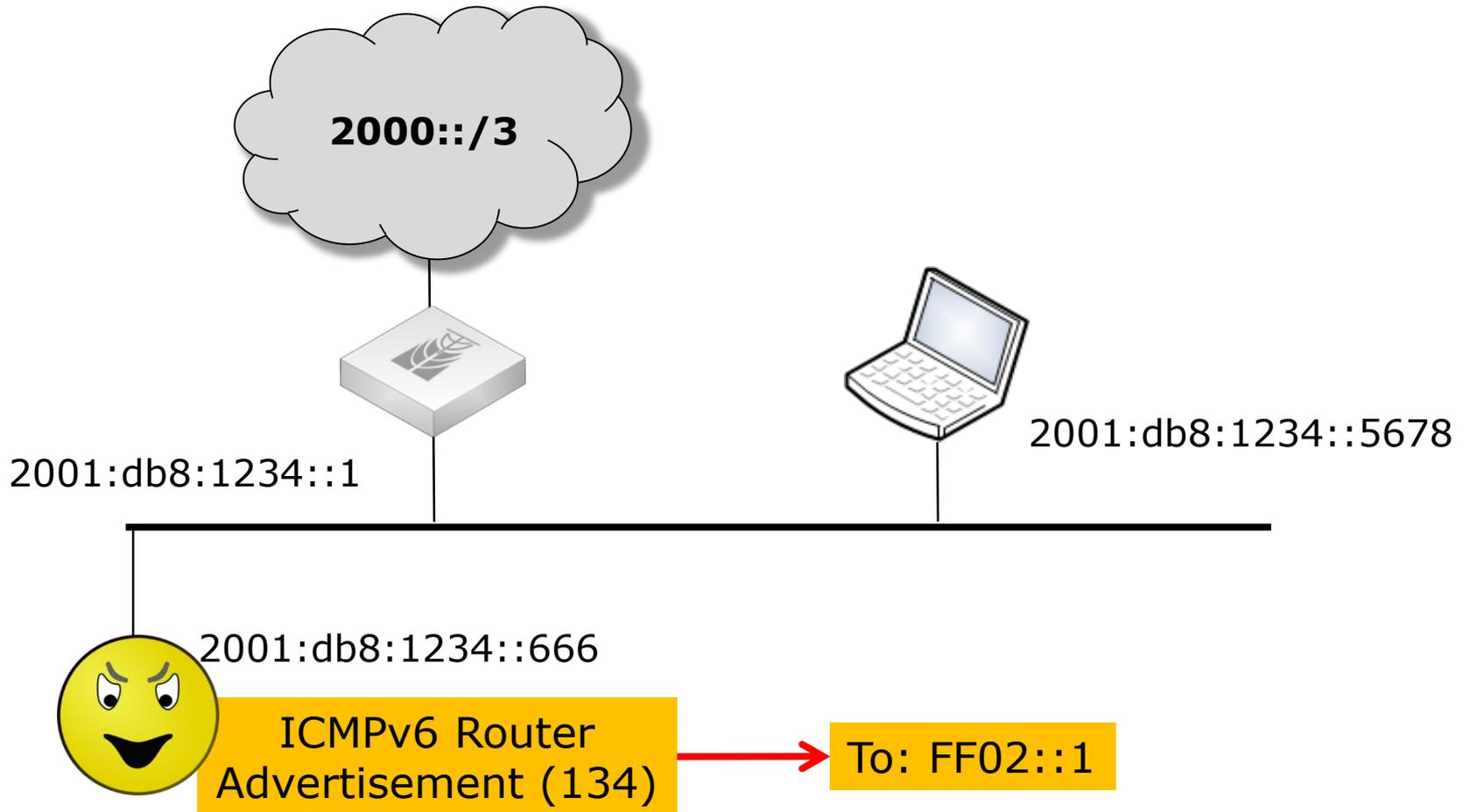
(ICMPv6 Type 134)

Source: Link-local address

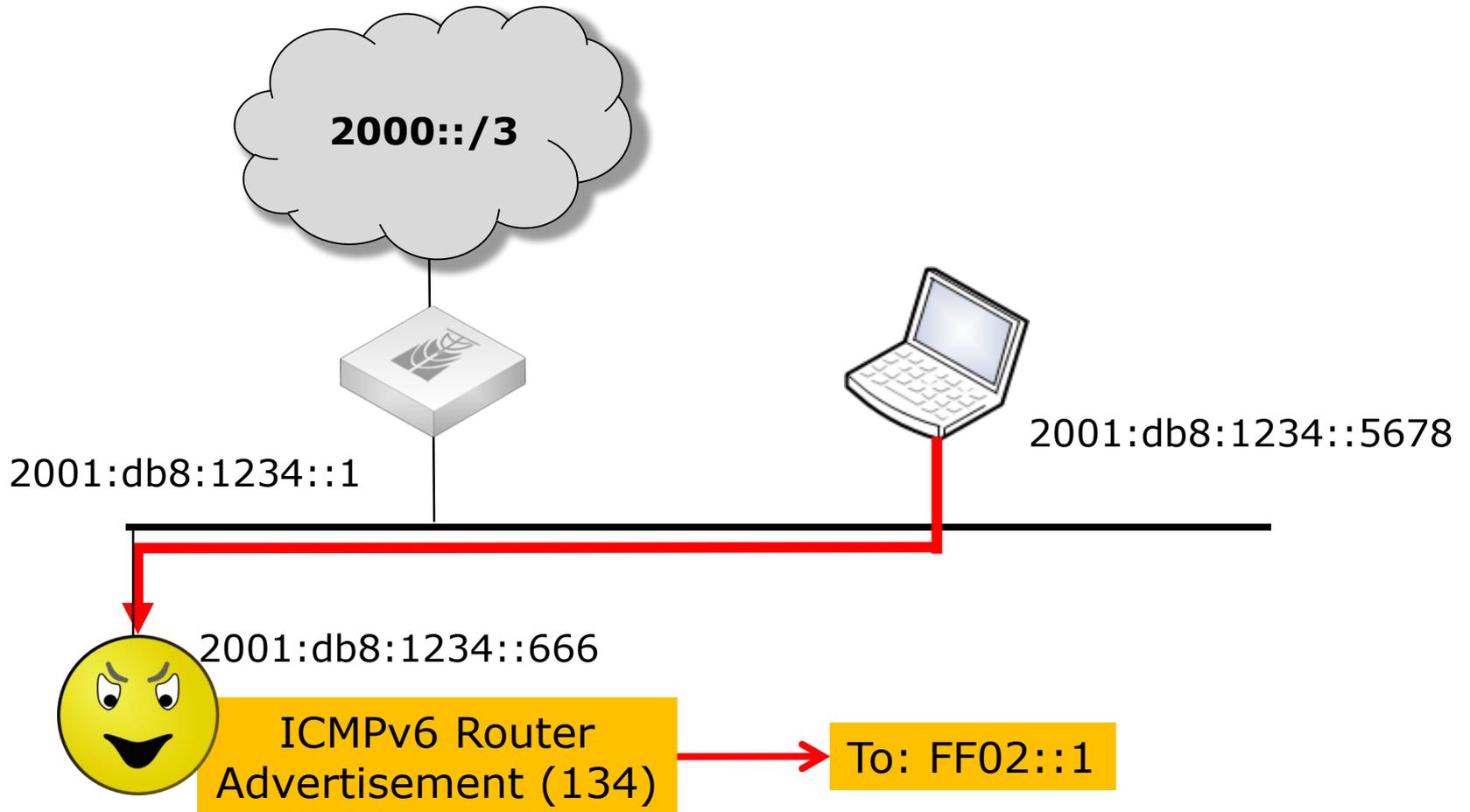
Contents: Options, prefixes,
lifetime, auto configuration flag

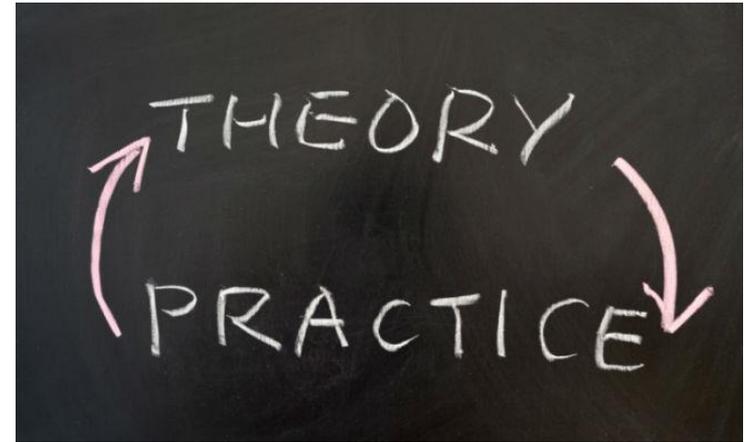
To: FF02::1 (All nodes on link)

Exploring Router Advertisement



Exploring Router Advertisement





**Do those stuff sound
too theoretical?**

Does this stuff sound
too theoretical?

```
maia@xps:~$ sudo apt-get install thc-ipv6
```

```
maia@xps:~$ atk6-
atk6-address6          atk6-fake_mld26      atk6-implementation6
atk6-alive6            atk6-fake_mld6       atk6-implementation6d
atk6-covert_send6     atk6-fake_mldrouter6 atk6-inject_alive6
atk6-covert_send6d    atk6-fake_pim6       atk6-inverse_lookup6
atk6-denial6          atk6-fake_router26  atk6-kill_router6
atk6-detect-new-ip6   atk6-fake_router6   atk6-ndpexhaust26
atk6-detect_sniffer6 atk6-fake_solicit6   atk6-ndpexhaust6
atk6-dnsdict6         atk6-firewall6      atk6-node_query6
atk6-dnsrevenue6     atk6-flood_advertise6 atk6-parasite6
atk6-dnssecwalk       atk6-flood_dhcp6    atk6-passive_discovery6
atk6-dos_mld          atk6-flood_mld26    atk6-randicmp6
atk6-dos-new-ip6     atk6-flood_mld6     atk6-redir6
atk6-dump_dhcp6       atk6-flood_mldrouter6 atk6-redirsniff6
atk6-dump_router6    atk6-flood_redir6   atk6-rsmurf6
atk6-exploit6         atk6-flood_router26 atk6-sendpees6
atk6-extract_hosts6  atk6-flood_router6  atk6-sendpeesmp6
atk6-extract_networks6 atk6-flood_rs6      atk6-smurf6
atk6-fake_advertise6 atk6-flood_solicit6 atk6-thcping6
atk6-fake_dhcp6       atk6-four2six       atk6-thcsyn6
atk6-fake_dns6d      atk6-fragmentation6 atk6-toobig6
atk6-fake_dnsupdate6 atk6-fuzz_dhcp6     atk6-trace6
atk6-fake_mipv6      atk6-fuzz_ip6
maia@xps:~$ █
```



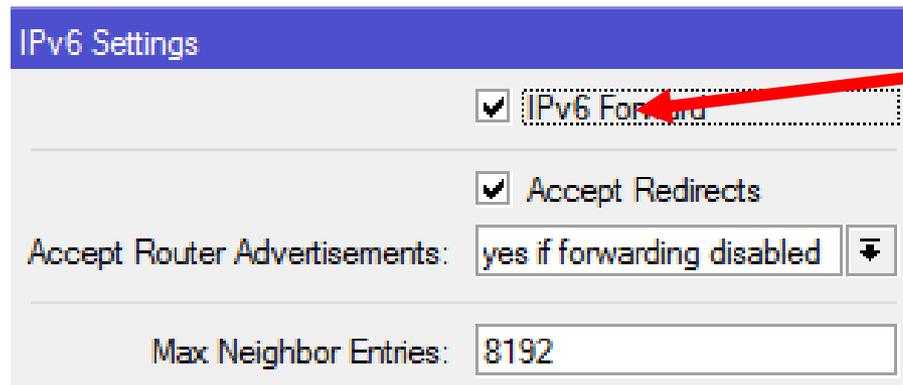


IPv6 Settings



Securing IPv6 Equipment

IPv6 Settings (default)



IPv6 Settings

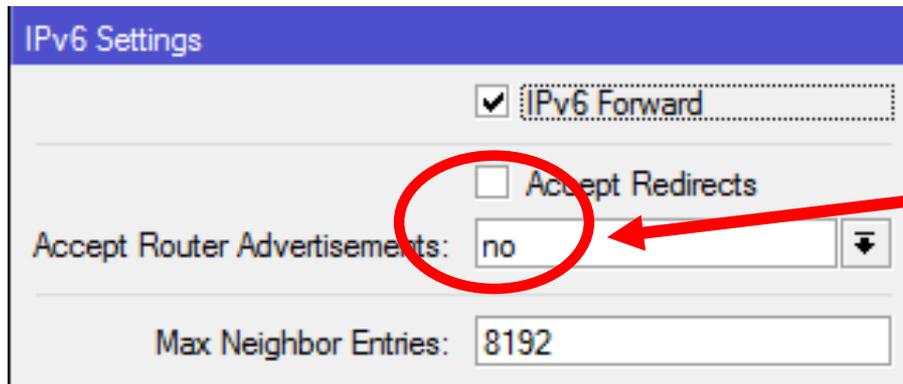
IPv6 Forward

Accept Redirects

Accept Router Advertisements: yes if forwarding disabled

Max Neighbor Entries: 8192

Disable IPv6 Forward on equipment that do not need to route packets from interfaces based on IPv6



IPv6 Settings

IPv6 Forward

Accept Redirects

Accept Router Advertisements: no

Max Neighbor Entries: 8192

Do not accept redirects avoiding potential man-in-the-middle attack;

Do not accept router advertisements.

Using Link Local Addresses



RFC 7404

RFC 7404 "Using only Link-Local addresses inside an IPv6 Network" is a document intended for informational purposes that discusses the advantages and disadvantages of this technique;

For this approach to work properly, for all routers, a global routable IPv6 address must be configured in a loopback interface;

Using only LLAs on infrastructure links **reduces the attack surface** of a router.

<https://tools.ietf.org/html/rfc7404>



Firewalling



Packets to be dropped:

- Packets with a multicast source address
- Packets with a multicast destination address over or equal to the router multicast scope
- Packets non-Internet Routable : bogon address, unspecified address, loopback address, documentation address, ULA...



Illegal Addresses

IPv6 Firewall			
Filter Rules			
Mangle Raw Connections Address Lists			
+ - ✓ ✗ [icon] [icon] 00 Reset Counters 00 Rese			
#	Action	Chain	Src. Address
::: Loopback Address			
36	✗ drop	Illegal Addresses	::1
::: IPv4 Compatible addresses			
37	✗ drop	Illegal Addresses	::/96
::: Other Compatible Addresses			
38	✗ drop	Illegal Addresses	::224.0.0.0/100
39	✗ drop	Illegal Addresses	::127.0.0.0/104
40	✗ drop	Illegal Addresses	::/104
41	✗ drop	Illegal Addresses	::255.0.0.0/104
::: False 6to4 packets			
42	✗ drop	Illegal Addresses	2002:e000::20
43	✗ drop	Illegal Addresses	2002:700::/24
44	✗ drop	Illegal Addresses	2002::/24
45	✗ drop	Illegal Addresses	2002:f00::/24
46	✗ drop	Illegal Addresses	2002:a00::/24
47	✗ drop	Illegal Addresses	2002:ac10::/28
48	✗ drop	Illegal Addresses	2002:c0a8::/32



::: Link Local Addresses			
49	✗ drop	Illegal Addresses	fe80::/10
::: Site Local Addresses (dprecated)			
50	✗ drop	Illegal Addresses	fec0::/10
::: Unique-local packets			
51	✗ drop	Illegal Addresses	fc00::/7
::: Multicast Packets (as a source address)			
52	✗ drop	Illegal Addresses	ff00::/8
::: Documentation Addresses			
53	✗ drop	Illegal Addresses	2001:db8::/32
::: 6bone Addresses (deprecated)			
54	✗ drop	Illegal Addresses	3ffe::/16



Multicast Filtering

IPv6 Firewall

Filter Rules | Mangle | Raw | Connections | Address Lists

+ - ✓ ✗ [icon] [icon] 00 Reset Counters 00 Reset All Counters

#	Action	Chain	Src. Address	Dst. Address	Protocol
::: Allow Link-Local Scope					
12	✓ accept	Multicast_Filters	ff02::/16		
::: Allow Link-Local Scope					
11	✓ accept	Multicast_Filters		ff02::/16	
10	✗ drop	Multicast_Filters	fec0::/10		
::: Deny other Multicasts					
14	✗ drop	Multicast_Filters	ff00::/8		
::: Deny deprecated by RFC 3879					
9	✗ drop	Multicast_Filters		fec0::/10	
::: Deny other Multicasts					
13	✗ drop	Multicast_Filters		ff00::/8	

Firewalling ICMPv6 Filtering



RFC 4890

Recommendations for Filtering ICMPv6 Messages in Firewalls

<https://www.ietf.org/rfc/rfc4890.txt>

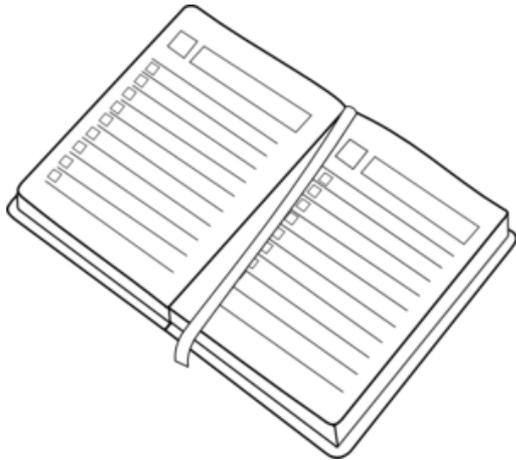
Basically, RFC 4890 allows unexpected inbound :

- echo request
- some ICMPv6 error messages
- some mobile IPv6 messages
- authenticated headers



Custom channel ICMPv6_Control

IPv6 Firewall						
Filter Rules						
Mangle Raw Connections Address Lists						
<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>						
<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>						
<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>						
<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>						
#	Action	Chain	Protocol	ICMP Options/ICMP Type	ICMP Options/ICMP Code	E
::: Accept Destination Unreachable (type 1)						
24	<input checked="" type="checkbox"/> accept	ICMPv6_Control	58 (icmpv6)	1 (destination unreachable)		
::: Accept Packet too big (type 2)						
25	<input checked="" type="checkbox"/> accept	ICMPv6_Control	58 (icmpv6)	2 (packet too big)		
::: Accept Time exceeded (type 3, code 0)						
26	<input checked="" type="checkbox"/> accept	ICMPv6_Control	58 (icmpv6)	3 (limit exceeded)		0
::: Accept Parameter problem (type 4, code 1)						
27	<input checked="" type="checkbox"/> accept	ICMPv6_Control	58 (icmpv6)	4 (bad header)		1
::: Accept Parameter problem (type 4)						
28	<input checked="" type="checkbox"/> accept	ICMPv6_Control	58 (icmpv6)	4 (bad header)		2
::: Accept Parameter problem (type 4, code 2)						
29	<input checked="" type="checkbox"/> accept	ICMPv6_Control	58 (icmpv6)	4 (bad header)		
::: Accept limited Echo Requests (type 128) - 5/sec, burst 10						
30	<input checked="" type="checkbox"/> accept	ICMPv6_Control	58 (icmpv6)	128 (echo request)		
::: Accept limited Echo Replies (type 129) - 5/sec, burst 10						
31	<input checked="" type="checkbox"/> accept	ICMPv6_Control	58 (icmpv6)	129 (echo reply)		



Introduction, motivation, relevant facts; ✓

Reminder of good practices to secure RouterOS equipment at Outside Plant and at Customer Premises; ✓

IPv6 protocol - issues, configurations and some recommended practices; ✓

Customer Security – How to provide a minimum of security keeping neutrality and privacy;

Large scale security management – A real case implementation.



40'

Security in a World without NAT



NAT was invented to extend IPv4 life and not for Security;

However, NAT gives as a “bonus” a stateful Firewall hiding internal topology from the Internet!

[T]he Internet of Things is going to drive a large population of connected devices, but most of those devices should never connect outside of their own local network.

Paul Vixie
CEO, Farsight Security

Security in a World without NAT

Thinking as a final Customer

If I don't want my devices external connected:

- In the IPv4+NAT World, I do nothing!;
- In the IPv6 World, I have to take care with SLAAC and configure them with a ULA or place Firewall rules;

If I want my devices connected:

- In the IPv4+NAT World, I have to do the appropriate dst-nat rule;
- In the IPv6 World, I do nothing!

[T]he Internet of Things is going to drive a large population of connected devices, but most of those devices should never connect outside of their own local network.

Paul Vixie
CEO, Farsight Security

**What does the
customer expect
from her/his ISP?**

What does the customer expect from her/his ISP?



nominum

[← BACK TO NEWS & EVENTS](#)

Consumers Want Simple Online Protection



YouGov UK

PRESS RELEASE

Consumers Want Simple Online Protection

Survey shows consumers want simpler online protection from Internet Service Providers. Growth of connected devices in the home leaves consumers feeling more vulnerable.

[READ MORE](#)

http://nominum.com/press_item/survey-shows-consumers-want-simpler-online-protection-from-internet-service-providers/

What does the customer expect from her/his ISP?

1,106 consumers polled in the United States.

- **63%** would like it if their current ISP provided one simple solution to increase security across all their connected devices.
- **51%** agreed they would **switch to another provider** if they offered a higher level of online protection, without additional monthly charges.
- **22%** have never changed their home gateway password at all !!!

Security in a World without NAT

What is allowed to an ISP?

- Drop lower ports (0 – 1023)?
- Drop connections initiated from external World?
- Do nothing?

What about net neutrality, privacy, etc.?

What does your country's regulation say?

Securing IPv6 CPEs



RFC 4864

Local Network Protection for IPv6

<https://tools.ietf.org/html/rfc4864>

RFC 6092

Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service.

<https://tools.ietf.org/html/rfc6092>

draft-ietf-v6ops-balanced-ipv6-security

Balanced Security for IPv6 Residential CPE

<https://www.ietf.org/archive/id/draft-ietf-v6ops-balanced-ipv6-security-01.txt> (expired & archived)



RFC 6092 Simple security in IPv6 Gateway CPE

RFC 6092 provides best practices recommendations (50 in total)

- Recommends implementation of stateful firewall which only allow incoming traffic **if initiated from inside the network;**
- However, RFC imposes a “transparent” mode of operation, **that users can turn on.** In this mode the CPE forwards all unsolicited flows regardless of forwarding direction;
- **IPsec traffic is always permitted**, inbound and outbound;

/ipv6 firewall – Forward channel

IPv6 Firewall				
Filter Rules				
Mangle Raw Connections Address Lists				
+ - [check] [x] [info] [filter] 00 Reset Counters 00 Rese				
#	Action	Chain	Protocol	IC
::: Transparent mode				
15	X [check] accept	forward		
::: Accept connections originated inside the network				
16	[check] accept	forward		
::: Accept established connections				
17	[check] accept	forward		
::: Accept related connections				
18	[check] accept	forward		
::: Accept IPsec-esp				
19	[check] accept	forward	50 (ipsec-esp)	
::: Accept IPsec-ah				
20	[check] accept	forward	51 (ipsec-ah)	
::: Accept TCP connections to port 500				
21	[check] accept	forward	6 (tcp)	
::: Accept TCP connections from port 500				
22	[check] accept	forward	6 (tcp)	

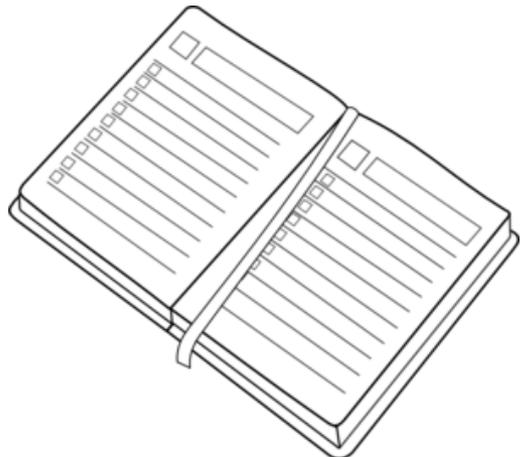


22	[check] accept	forward	6 (tcp)
::: Jump to ICMPv6 Control			
23	[fish] jump	forward	58 (icmpv6)
::: Jump to Bogons and Illegal Addresses blocking			
51	[fish] jump	forward	
::: Jump to Illegal Multicast Addresses			
52	[fish] jump	forward	
::: Drop all the rest			
82	[x] drop	forward	

(Work in progress)

- Existing users are being communicated about the new security features and could opt to stay as they are (no default security).
- Silence means security policies will be implemented.
- New users will strongly advised to opt for the security policies.
- **Anytime, users can turn off** the features enabling the transparent mode at customers' portal.

Agenda



Introduction, motivation, relevant facts; ✓

Reminder of good practices to secure RouterOS equipment at Outside Plant and at Customer Premises; ✓

IPv6 protocol - issues, configurations and some recommended practices; ✓

Customer Security – How to provide a minimum of security keeping neutrality and privacy; ✓

Large scale security management – A real case implementation.



48'

After security measures implemented and tested...



Time to Relax?

Bad things happen all the time...

- Some damaged equipment is replaced “on a rush” to reestablish the service and technicians forget to do all appropriate configuration;
 - Someone in the staff change something for testing purposes and forget to roll back;
 - A more skilled customer turns transparent mode on but is running some kind of malware;
 - The manufacturer releases an important security update.
- ...

Time to Relax?



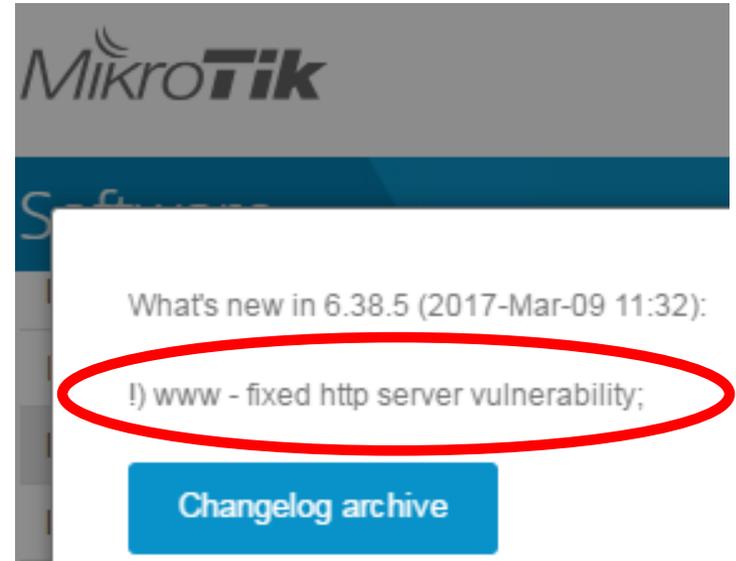
The Register
Biting the hand that feeds IT

DATA CENTRE SOFTWARE SECURITY TRANSFORMATION DEVOPS BUSINESS PERSONAL TECH

Security

That CIA exploit list in full: The good, the bad, and the very ugly

We went through 8,000 documents so you don't have to



MikroTik

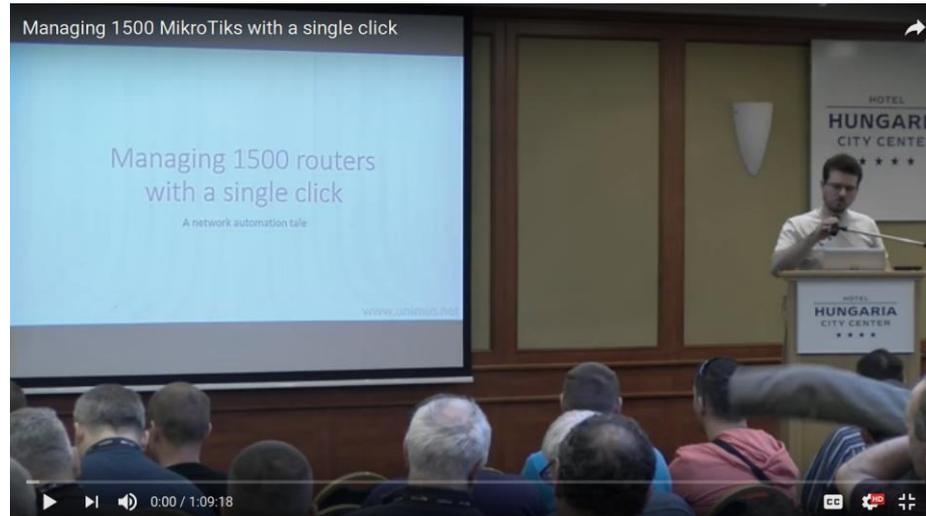
Software

What's new in 6.38.5 (2017-Mar-09 11:32):

!) www - fixed http server vulnerability;

[Changelog archive](#)

Thank you Mikrotik Guys for the quick fix!



Managing 1500 Mikrotik with a single click

Thanks to Tomas Kimak for the great presentation at 2016 Hungary MUM:

<https://mum.mikrotik.com/2016/HU/agenda/EN#>

Tools for monitoring/controlling



+



Telegram

Tools for monitoring/controlling



iTop is a free software for managing hardware, software and associated services enabling to centralize data about devices, software, users, locations, etc. It allows to streamline the Helpdesk, manage quality of services and govern the IT environment (ITSM).

Together with the other tools it will be used security related incidents management in a formal way.

Open source tool with no license nor limitations

<https://www.combodo.com/itop-193>

Tools for monitoring/controlling

ZABBIX

Zabbix is a software designed for real-time monitoring that can be used for several monitoring applications

Security regular checks like open ports or services, firmware versions and even physical access can be easily performed by Zabbix and timely notifications sent to exclude breaches or minimize losses from illegal actions.

Zabbix is Open Source and comes at no cost.

<http://www.zabbix.com/>

Tools for monitoring/controlling/ messaging

RANCID

RANCID (Really Awesome New Cisco Config Differ) is a free tool that monitors a router's (or more generally a device's) configuration, including software and hardware (cards, serial numbers, etc) and uses [CVS \(Concurrent Version System\)](#), [Subversion](#) or [Git](#) to maintain history of changes.

<http://www.shrubbery.net/rancid/>

Tools for monitoring/controlling/ messaging



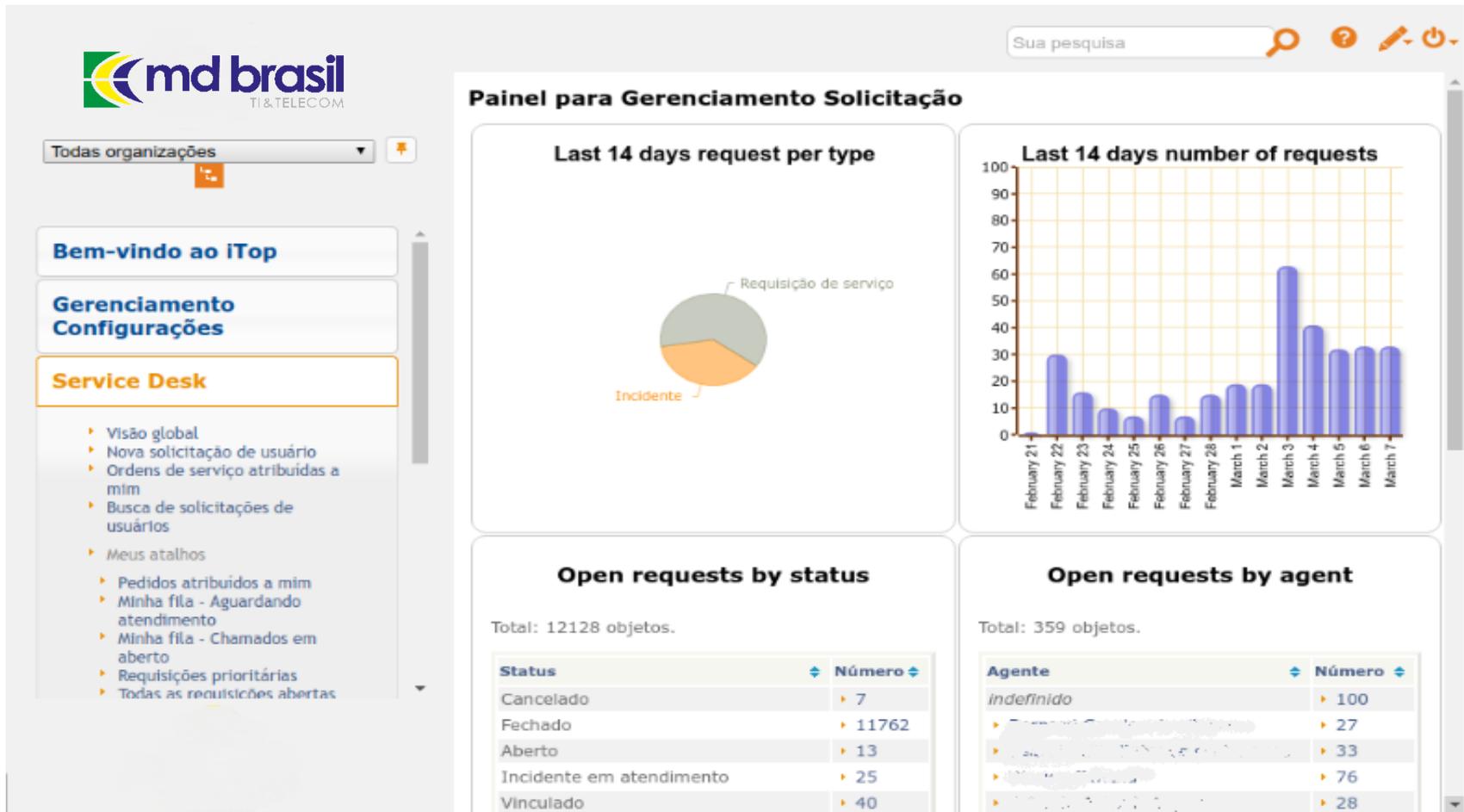
Telegram is a cloud-based mobile (IOS and Android) and desktop messaging app (Windows, MacOS and Linux).

Telegram has an open API and a Bot API, allowing to interact with other systems. <https://telegram.org/>

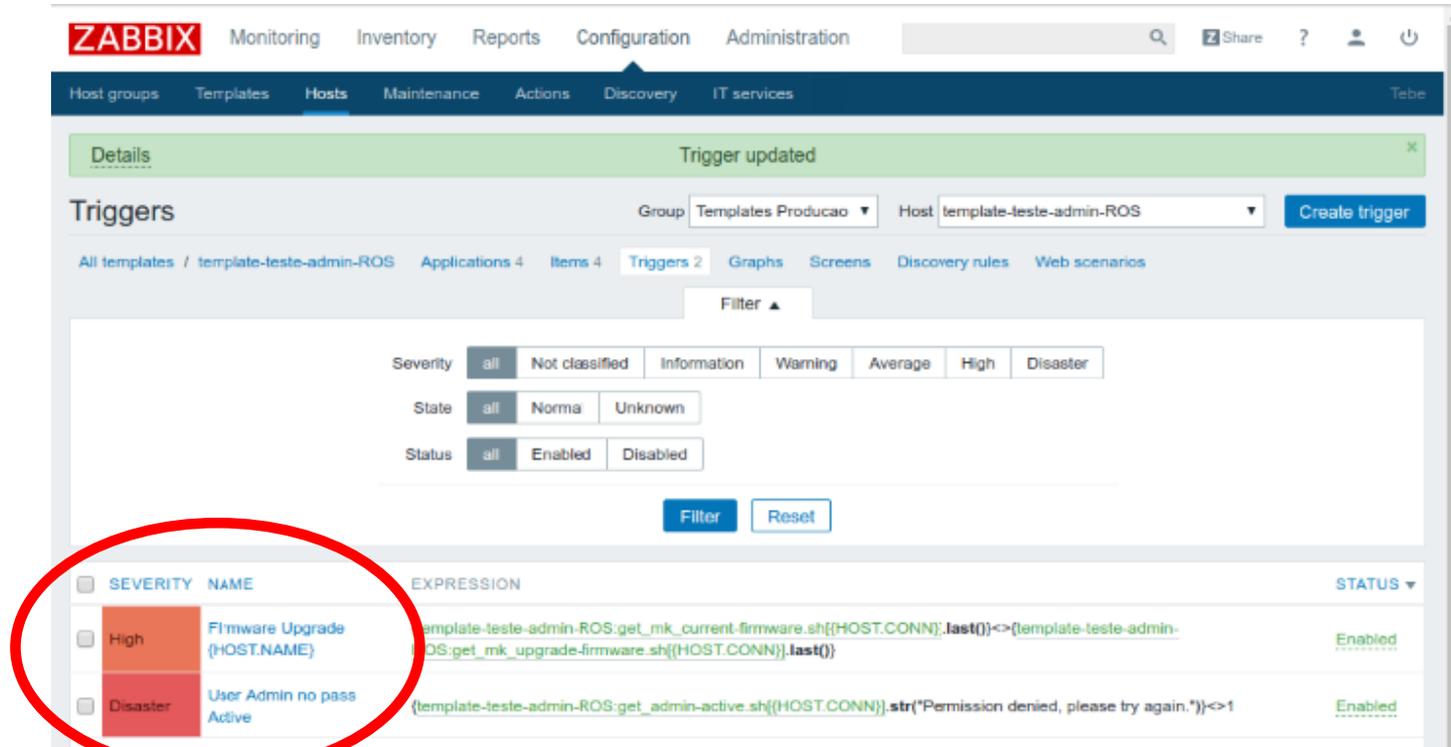
Integration with Telegram uses BatBot API
batbot.sh is a bash script that can reply messages and execute commands:

<https://github.com/theMiddleBlue/BaTbot>

Itop Dashboard



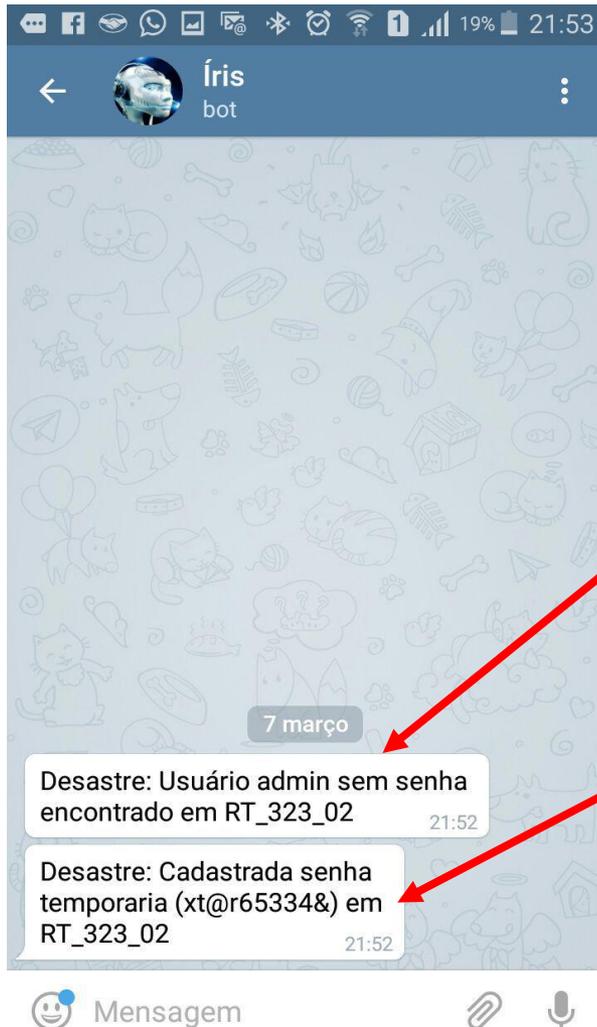
Zabbix configuration



The screenshot shows the Zabbix web interface with the 'Triggers' page selected. The interface includes a navigation bar with 'ZABBIX' and various menu items like 'Monitoring', 'Inventory', 'Reports', 'Configuration', and 'Administration'. Below the navigation bar, there are tabs for 'Host groups', 'Templates', 'Hosts', 'Maintenance', 'Actions', 'Discovery', and 'IT services'. A green notification bar at the top says 'Trigger updated'. The main content area shows a list of triggers with filters for Severity, State, and Status. Two triggers are highlighted with a red circle:

SEVERITY	NAME	EXPRESSION	STATUS
High	Firmware Upgrade (HOST.NAME)	template-teste-admin-ROS.get_mk_current_firmware.sh{([HOST.CONN]).last()}<>[template-teste-admin-ROS:get_mk_upgrade_firmware.sh{([HOST.CONN]).last()}]	Enabled
Disaster	User Admin no pass Active	(template-teste-admin-ROS:get_admin_active.sh{([HOST.CONN]).str("Permission denied, please try again.")}><1	Enabled

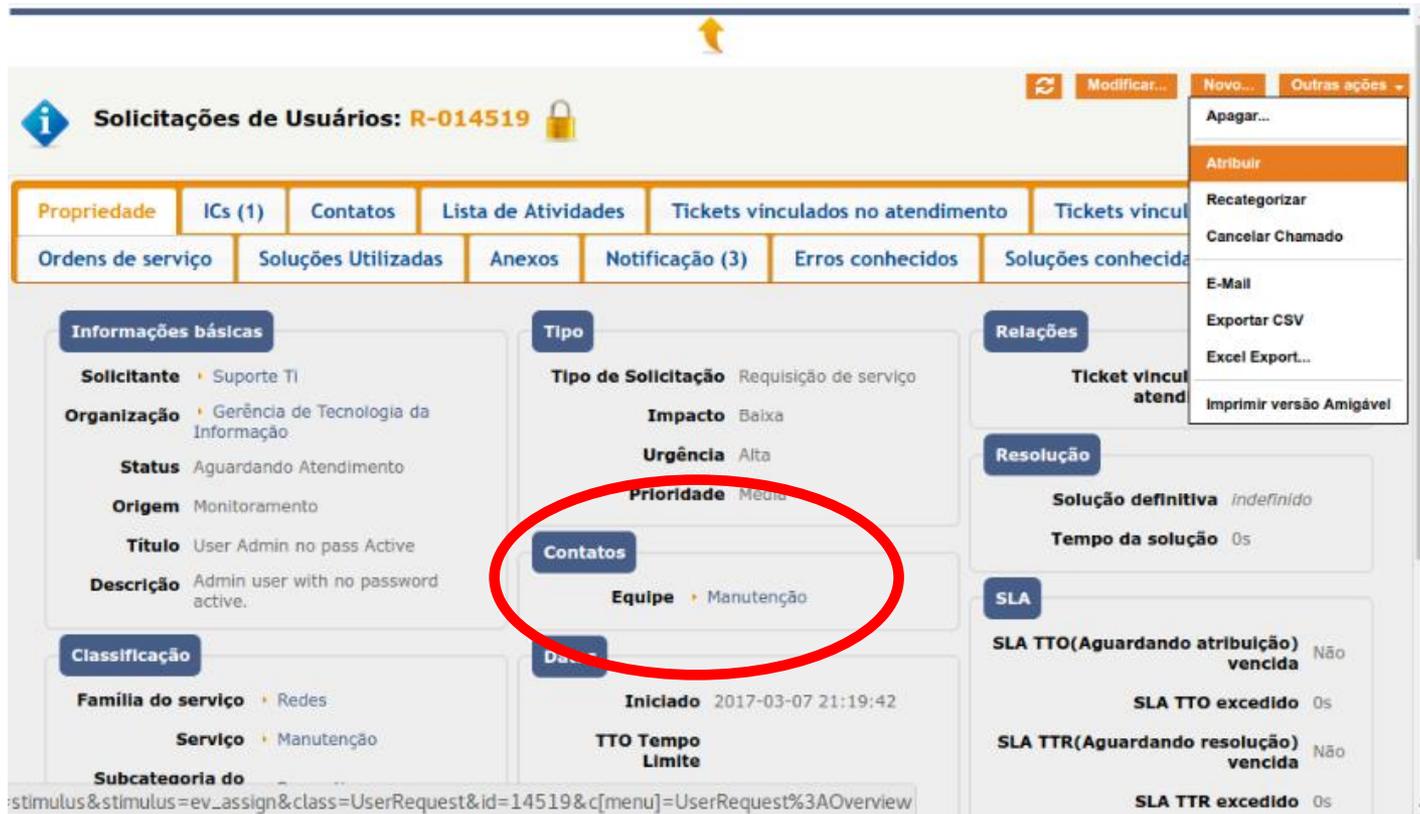
For instance, we selected 2 events – Firmware upgrade (Severity High) and Router with user=admin, no password (Severity Disaster)



Telegram

A notification is made via Telegram to the group of responsible technicians.

And Zabbix automatically configure a temporary random password!



Solicitações de Usuários: R-014519

Propriedade | ICs (1) | Contatos | Lista de Atividades | Tickets vinculados no atendimento | Tickets vinculados no atendimento

Ordens de serviço | Soluções Utilizadas | Anexos | Notificação (3) | Erros conhecidos | Soluções conhecidas

Informações básicas

Solicitante Suporte TI

Organização Gerência de Tecnologia da Informação

Status Aguardando Atendimento

Origem Monitoramento

Título User Admin no pass Active

Descrição Admin user with no password active.

Classificação

Família do serviço Redes

Serviço Manutenção

Subcategoria do

Tipo

Tipo de Solicitação Requisição de serviço

Impacto Baixa

Urgência Alta

Prioridade Média

Contatos

Equipe Manutenção

Relações

Ticket vinculado no atendimento

Resolução

Solução definitiva indefinido

Tempo da solução 0s

SLA

SLA TTO(Aguardando atribuição) vencida Não

SLA TTO excedido 0s

SLA TTR(Aguardando resolução) vencida Não

SLA TTR excedido 0s

iTOP registers the event notifying back office. One service ticket is generated.

Framework in action

Atribuir - R-014519

Agente -- seleccione um --
 -- seleccione um --
 Cancelar

Informações
 Solicitante: [Redacted]
 Organização: [Redacted]
 Status: Aguardando Atendimento
 Origem: Monitoramento
 Título: User Admin no pass Active
 Descrição: Admin user with no password active.

Classificação
 Família do serviço: Redes
 Serviço: Manutenção
 Subcategoria do serviço: Preventiva
 Contrato do cliente: Contrato Serviços Preventivas
 Item funcional principal: Indefinido

Tipo
 Tipo de Solicitação: Requisição de serviço
 Impacto: Baixa
 Urgência: Alta
 Prioridade: Média

Relações
 Ticket vinculado no atendimento: Indefinido

Resolução
 Solução definitiva: Indefinido
 Tempo da solução: 0s

SLA
 SLA TTO(Aguardando atribuição) vencida: Não
 SLA TTO excedido: 0s
 SLA TTR(Aguardando resolução) vencida: Não
 SLA TTR excedido: 0s

Contatos
 Equipe: Manutenção

Dados
 Inicializado: 2017-03-07 21:19:42
 TTO Tempo Limite
 TTR Tempo Limite
 Pendência acumulada: Decorrido, Não iniciado
 Última Atualização

Atribuir - R-014519

Agente Wesley Zanella
 Cancelar Atribuir

Informações
 Solicitante: [Redacted]
 Organização: [Redacted]
 Status: [Redacted]
 Origem: [Redacted]
 Título: [Redacted]
 Descrição: [Redacted]

Classificação
 Família do serviço: Redes
 Serviço: Manutenção
 Subcategoria do serviço: Preventiva
 Contrato do cliente: Contrato Serviços Preventivas
 Item funcional principal: Indefinido

Tipo
 Tipo de Solicitação: Requisição de serviço
 Impacto: Baixa
 Urgência: Alta
 Prioridade: Média

Relações
 Ticket vinculado no atendimento: Indefinido

Resolução
 Solução definitiva: Indefinido
 Tempo da solução: 0s

SLA
 SLA TTO(Aguardando atribuição) vencida: Não
 SLA TTO excedido: 0s
 SLA TTR(Aguardando resolução) vencida: Não
 SLA TTR excedido: 0s

Contatos
 Equipe: Manutenção

Dados
 Inicializado: 2017-03-07 21:19:42
 TTO Tempo Limite
 TTR Tempo Limite
 Pendência acumulada: Decorrido, Não iniciado
 Última Atualização

Aguarde!

Propriedade | ICs (1) | Contatos | Lista de Atividades | Tickets vinculados no atendimento | Tickets vinculados na solução

Ordens de serviço | Soluções Utilizadas | Anexos | Notificação (6) | Erros conhecidos | Soluções conhecidas | Histórico

Informações básicas
 Solicitante: Suporte TI
 Organização: Gerência de Tecnologia da Informação
 Status: Requisição de serviço em atendimento
 Origem: Monitoramento
 Título: User Admin no pass Active
 Descrição: Admin user with no password active.

Classificação
 Família do serviço: Redes
 Serviço: Manutenção
 Subcategoria do serviço: Preventiva
 Contrato do cliente: Contrato Serviços Preventivas
 Item funcional principal: Indefinido

Tipo
 Tipo de Solicitação: Requisição de serviço
 Impacto: Baixa
 Urgência: Alta

Contatos
 Agente: Wesley Zanella

Dados
 Inicializado: 2017-03-07 21:19:42
 Última atualização: 2017-03-07 21:33:41
 Data de Atribuição: 2017-03-07 21:33:41
 TTO Tempo Limite
 TTR Tempo Limite

Relações
 Ticket vinculado no atendimento: Indefinido

Resolução
 Solução definitiva: Indefinido
 Tempo da solução: 0s

SLA
 SLA TTO(Aguardando atribuição) vencida: Não
 SLA TTO excedido: 0s
 SLA TTR(Aguardando resolução) vencida: Não
 SLA TTR excedido: 0s

Agendamento

Back office forward to the appropriate technician who receives e-mail and telegram notification to fix the problem

Resolver - R-014519

Solução

usuário e senha configurados no equipamento e no sistema

É uma solução de contorno? Não

Solução selecionada -- seleccione um --

Cancelar Resolver

Informações básicas

Solicitante Suporte TI

Organização Gerência de Tecnologia da Informação

Status Requisição de serviço em atendimento

Tipo

Tipo de Solicitação Requisição de serviço

Impacto Baixa

Urgência Alta

Prioridade Média

Relações

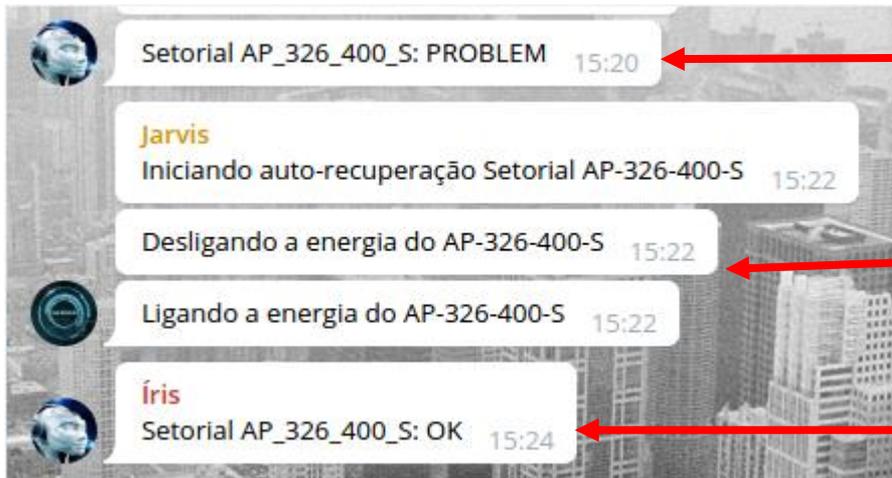
Ticket vinculado no atendimento indefinido

Resolução

The responsible technician fix the problem and inform iTOP closing the ticket

Framework in action

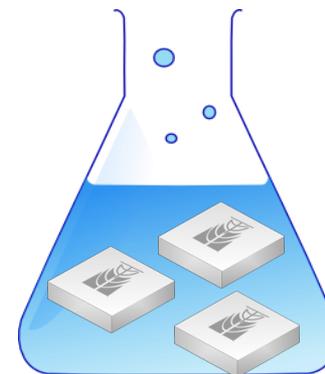
Many actions can be done automatically, like rebooting an irresponsive equipment.



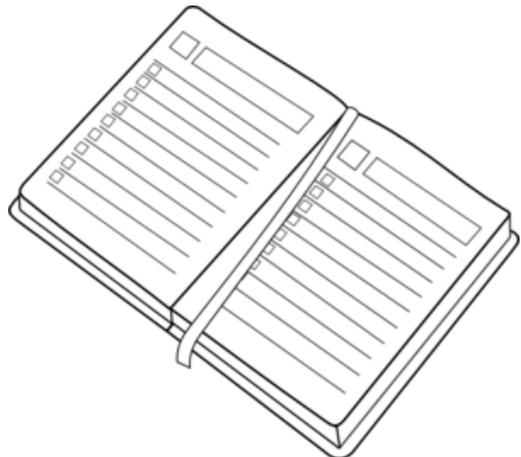
An access point is presenting problems;

Automatic reboot via RB 750UP;

Access point is now alive.



Online Demo



Introduction, motivation, relevant facts; ✓

Reminder of good practices to secure RouterOS equipment at Outside Plant and at Customer Premises; ✓

IPv6 protocol - issues, configurations and some recommended practices; ✓

Customer Security – How to provide a minimum of security keeping neutrality and privacy; ✓

Large scale security management – A real case implementation. ✓



60'

Securing Networks with Mikrotik RouterOS – Tom Smyth

<https://mum.mikrotik.com//presentations/HR13/legend.pdf>

IPV6 Security by Scott Hogg, Eric Vyncke

<http://www.ciscopress.com/store/ipv6-security-9781587055942>

RFC 4890

Recommendations for Filtering ICMPv6 Messages in Firewalls

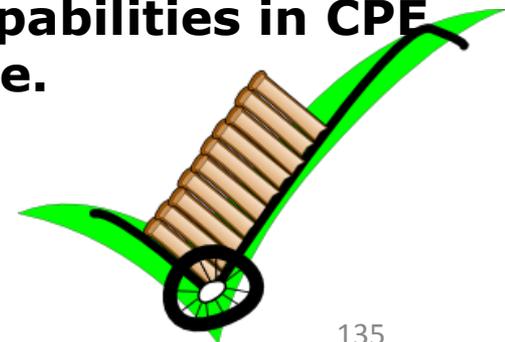
<https://www.ietf.org/rfc/rfc4890.txt>

RFC 4864 - Local Network Protection for IPv6

<https://tools.ietf.org/html/rfc4864>

RFC 6092 - Recommended Simple Security Capabilities in CPE for Providing Residential IPv6 Internet Service.

<https://tools.ietf.org/html/rfc6092>





Extra Slides



Input Channel (1/2)

```
/ipv6 firewall
```

```
add action=accept chain=input comment="Accept Established and  
Related Connections" connection-state=established,related
```

```
add action=accept chain=input comment="Accept Connections  
from IPv6 administrative addresses" src-address-  
list="Administrative IPv6 Adressess"
```

```
add action=accept chain=input comment="Accept DHCPv6 (UDP  
ports 547->546)" dst-port=546 protocol=udp src-port=547
```



Input Channel (2/2)

```
/ipv6 firewall
```

```
add action=accept chain=input comment="Accept DHCPv6 (TCP  
ports 547->546)" dst-port=546 protocol=tcp src-port=547
```

```
add action=jump chain=input comment="Jump to ICMPv6 Control"  
connection-state="" jump-target=ICMPv6_Control
```

```
add action=drop chain=input comment="Drop all the rest"
```



Output Channel (1/2)

```
/ipv6 firewall
```

```
add action=accept chain=output comment="Accept Established and  
Related Connections" connection-state=established,related
```

```
add action=accept chain=output comment="Accept Connections  
from IPv6 administrative addresses" src-address-  
list="Administrative IPv6 Adressess"
```

```
add action=accept chain=output comment="Accept DHCPv6 (UDP  
ports 546->547)" dst-port=547 protocol=udp src-port=546
```



Output Channel (1/2)

```
/ipv6 firewall
```

```
add action=accept chain=output comment="Accept DHCPv6 (TCP  
ports 546->547)" dst-port=547 protocol=tcp src-port=546
```

```
add action=jump chain=output comment="Jump to ICMPv6  
Control" connection-state="" jump-target=ICMPv6_Control
```

```
add action=drop chain=output comment="Drop all the rest"
```



Forward Channel (1/3)

/ipv6 firewall filter

```
add action=accept chain=forward comment="Transparent mode"  
disabled=yes
```

```
add action=accept chain=forward comment="Accept connections  
originated inside the network" connection-state=new out-  
interface=pppoe-out1
```

```
add action=accept chain=forward comment="Accept established  
connections" connection-state=established,related
```



Forward Channel (2/3)

/ipv6 firewall filter

```
add action=accept chain=forward comment="Accept IPsec-esp"  
connection-state=related protocol=ipsec-esp
```

```
add action=accept chain=forward comment="Accept IPsec-ah"  
connection-state=related protocol=ipsec-ah
```

```
add action=accept chain=forward comment="Accept TCP connections  
to port 500" dst-port=500 protocol=tcp
```

```
add action=accept chain=forward comment="Accept TCP connections  
from port 500" protocol=tcp src-port=500
```



Forward Channel (3/3)

```
/ipv6 firewall filter
```

```
add action=jump chain=forward comment="Jump to Bogons and  
Illegal Addresses blocking" jump-target="Illegal Addresses"
```

```
add action=jump chain=forward comment="Jump to Illegal Multicast  
Adresses" jump-target="Illegal Addresses"
```

```
add action=jump chain=forward comment="Jump to ICMPv6 Control"  
jump-target=ICMPv6_Control protocol=icmpv6
```

```
add action=drop chain=forward comment="Drop all the rest"
```



ICMPv6 Control (1/5)

```
/ipv6 firewall filter
```

```
add action=accept chain=ICMPv6_Control comment="Accept  
Destination Unreacheable (type 1)" icmp-options=1:0-255 protocol=  
icmpv6
```

```
add action=accept chain=ICMPv6_Control comment="Accept Packet  
too big (type 2)" icmp-options=2:0-255 protocol=icmpv6
```

```
add action=accept chain=ICMPv6_Control comment="Accept Time  
exceeded (type 3, code 0)" icmp-options=3:0 protocol=icmpv6
```



ICMPv6 Control (2/5)

/ipv6 firewall filter

```
add action=accept chain=ICMPv6_Control comment="Accept  
Parameter problem (type 4, code 1)" icmp-options=4:1 protocol=  
icmpv6
```

```
add action=accept chain=ICMPv6_Control comment="Accept  
Parameter problem (type 4)" icmp-options=4:2 protocol=icmpv6
```

```
add action=accept chain=ICMPv6_Control comment="Accept  
Parameter problem (type 4, code 2)" icmp-options=4:0-255  
protocol=icmpv6
```



ICMPv6 Control (3/5)

/ipv6 firewall filter

```
add action=accept chain=ICMPv6_Control comment="Accept limited  
Echo Requests (type 128) - 5/sec, burst 10" icmp-options=128:0-255  
protocol=icmpv6
```

```
add action=accept chain=ICMPv6_Control comment="Accept limited  
Echo Replies (type 129) - 5/sec, burst 10" icmp-options=129:0-255  
limit=5,10:packet protocol=icmpv6
```

```
add action=accept chain=ICMPv6_Control comment="Accept 143,  
code 0, hop limit 255" hop-limit=equal:255 icmp-options=143:0  
protocol=icmpv6
```



ICMPv6 Control (4/5)

/ipv6 firewall filter

```
add action=accept chain=ICMPv6_Control comment="Accept 133,  
code 0, hop limit 255" hop-limit=equal:255 icmp-options=133:0  
protocol=icmpv6
```

```
add action=accept chain=ICMPv6_Control comment="Accept 134,  
code 0, hop limit 255" hop-limit=equal:255 icmp-options=134:0  
protocol=icmpv6
```

```
add action=accept chain=ICMPv6_Control comment="Accept 135,  
code 0, hop limit 255" hop-limit=equal:255 icmp-options=135:0  
protocol=icmpv6
```



ICMPv6 Control (5/5)

/ipv6 firewall filter

```
add action=accept chain=ICMPv6_Control comment="Accept 136,  
code 0, hop limit 255" hop-limit=equal:255 icmp-options=136:0  
protocol=icmpv6
```

```
add action=drop chain=ICMPv6_Control protocol=icmpv6
```



Illegal Addresses (1/6)

/ipv6 firewall filter

```
add action=drop chain="Illegal Addresses" comment="Loopback Address" src-address>:::1/128
```

```
add action=drop chain="Illegal Addresses" comment="IPv4 Compatible addresses" src-address>:::/96
```

```
add action=drop chain="Illegal Addresses" comment="Other Compatible Addresses" src-address>:::224.0.0.0/100
```

```
add action=drop chain="Illegal Addresses" src-address>:::127.0.0.0/104
```



Illegal Addresses (2/6)

```
/ipv6 firewall filter
```

```
add action=drop chain="Illegal Addresses" src-address=::/104
```

```
add action=drop chain="Illegal Addresses" src-  
address=::255.0.0.0/104
```

```
add action=drop chain="Illegal Addresses" comment="False 6to4  
packets" src-address=2002:e000::20/128
```

```
add action=drop chain="Illegal Addresses" src-  
address=2002:7f00::/24
```



Illegal Addresses (3/6)

```
/ipv6 firewall filter
```

```
add action=drop chain="Illegal Addresses" src-address=2002::/24
```

```
add action=drop chain="Illegal Addresses" src-address=2002:ff00::/24
```

```
add action=drop chain="Illegal Addresses" src-address=2002:a00::/24
```

```
add action=drop chain="Illegal Addresses" src-address=2002:ac10::/28
```



Illegal Addresses (4/6)

/ipv6 firewall filter

```
add action=drop chain="Illegal Addresses" src-  
address=2002:c0a8::/32
```

```
add action=drop chain="Illegal Addresses" comment="Link Local  
Addresses" src-address=fe80::/10
```

```
add action=drop chain="Illegal Addresses" comment="Site Local  
Addresses (deprecated)" src-address=fec0::/10
```

```
add action=drop chain="Illegal Addresses" comment="Unique-local  
packets" src-address=fc00::/7
```



Illegal Addresses (5/6)

/ipv6 firewall filter

```
add action=drop chain="Illegal Addresses" comment="Multicast  
Packets (as a source address)" src-address=ff00::/8
```

```
add action=drop chain="Illegal Addresses"  
comment="Documentation Adresses" src-address=2001:db8::/32
```

```
add action=drop chain="Illegal Addresses" comment="6bone  
Addresses (deprecated)" src-address=3ffe::/16
```

```
add action=drop chain=Multicast_Filters comment="Deny deprecated  
by RFC 3879" dst-address=fec0::/10
```



Illegal Addresses (6/6)

```
/ipv6 firewall filter
```

```
add action=drop chain=Multicast_Filters src-address=fec0::/10
```

```
add action=accept chain=Multicast_Filters comment="Allow Link-Local Scope" dst-address=ff02::/16
```

```
add action=accept chain=Multicast_Filters comment="Allow Link-Local Scope" src-address=ff02::/16
```

```
add action=drop chain=Multicast_Filters comment="Deny other Multicasts" dst-address=ff00::/8
```

```
add action=drop chain=Multicast_Filters comment="Deny other Multicasts" src-address=ff00::/8
```

10 years of Official Training



**Questions, comments,
suggestion and critics**

maia@mdbrasil.com.br



Grazie!