邻居服务及广播流量攻击与防御

Neighbor and broadcast attack/defense

MUM ShangHai 2016/4/10

Xiong MaoXiang

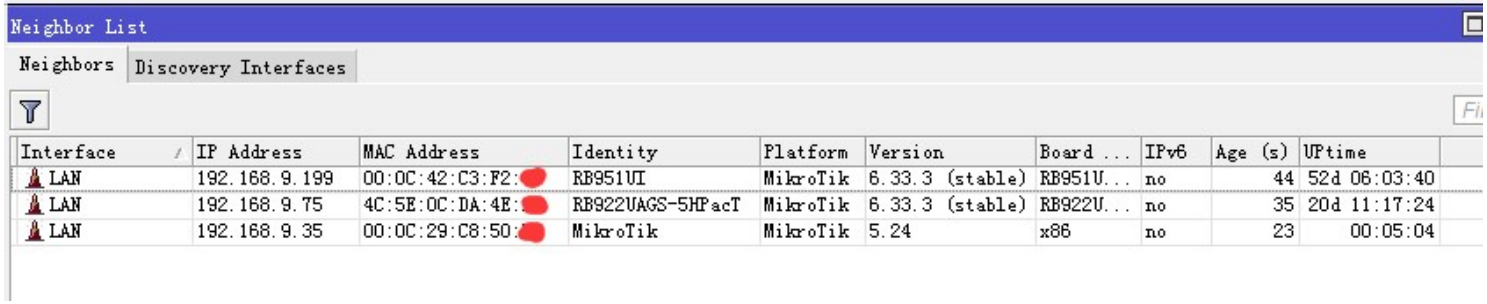
一. 邻居服务的简单介绍。
What is Neighbor in mikrotik

- 1. MikroTik邻居发现协议（MNDP）允许发现同在第2层广播域的其他设备和兼容CDP设备（Cisco发现协议）。
- MikroTik neighbor discovery protocol (MNDP) allows discovery of other devices in the second layer broadcast domain and compatible with CDP devices (Cisco Discovery Protocol)

- 2.例如在同一个广播域中存在RB951，RB941，RB433，UBNT等设备。那么在RB951将可以在邻居菜单里看到RB941，RB433，UBNT等设备，并且可以显示对应邻居的MAC，IP，系统标识，系统版本等信息。
- For example, in the same broadcast domain, there are RB951, RB941, RB433, UBNT, and other devices. Then in RB951 ‘s neighbor menu will see RB941, RB433, UBNT and other devices，and can display the corresponding neighbor's IP, MAC, system identification, system version and other information.

在Mikrotik系统里邻居服务如下图所示。

Neighbor in Mikrotik system is shown in the figure.



Interface	IP Address	MAC Address	Identity	Platform	Version	Board ...	IPv6	Age (s)	UPtime
LAN	192.168.9.199	00:0C:42:C3:F2:[redacted]	RB951UI	MikroTik	6.33.3 (stable)	RB951U...	no	44	52d 06:03:40
LAN	192.168.9.75	4C:5E:0C:DA:4E:[redacted]	RB922UAGS-5HPacT	MikroTik	6.33.3 (stable)	RB922U...	no	35	20d 11:17:24
LAN	192.168.9.35	00:0C:29:C8:50:[redacted]	MikroTik	MikroTik	5.24	x86	no	23	00:05:04

二. 如何使用该程序来攻击邻居服务。
How to use the program to attack a neighbor.

- 1.现在我们已经知道邻居服务的作用，那么假设在同一个广播域里有一个攻击者，模拟邻居服务发送数据包。这样所有的邻居设备都会收到这个数据包，并且记录 显示在邻居菜单中。
- Now we know the function of neighbor, then suppose there is an attacker in the same broadcast domain, it is analog neighbor to send data packets.So that all the neighbors will receive the data package records and display in the neighbor menu.

- 2.我们知道，如果邻居服务收到邻居服务包会占用CPU去处理这些信息。那么这个占用量可以被放大到多大呢？
- We know that if a neighbor receives a neighbor's package, it will take CPU to process the information. So how big is the amount of this occupation?

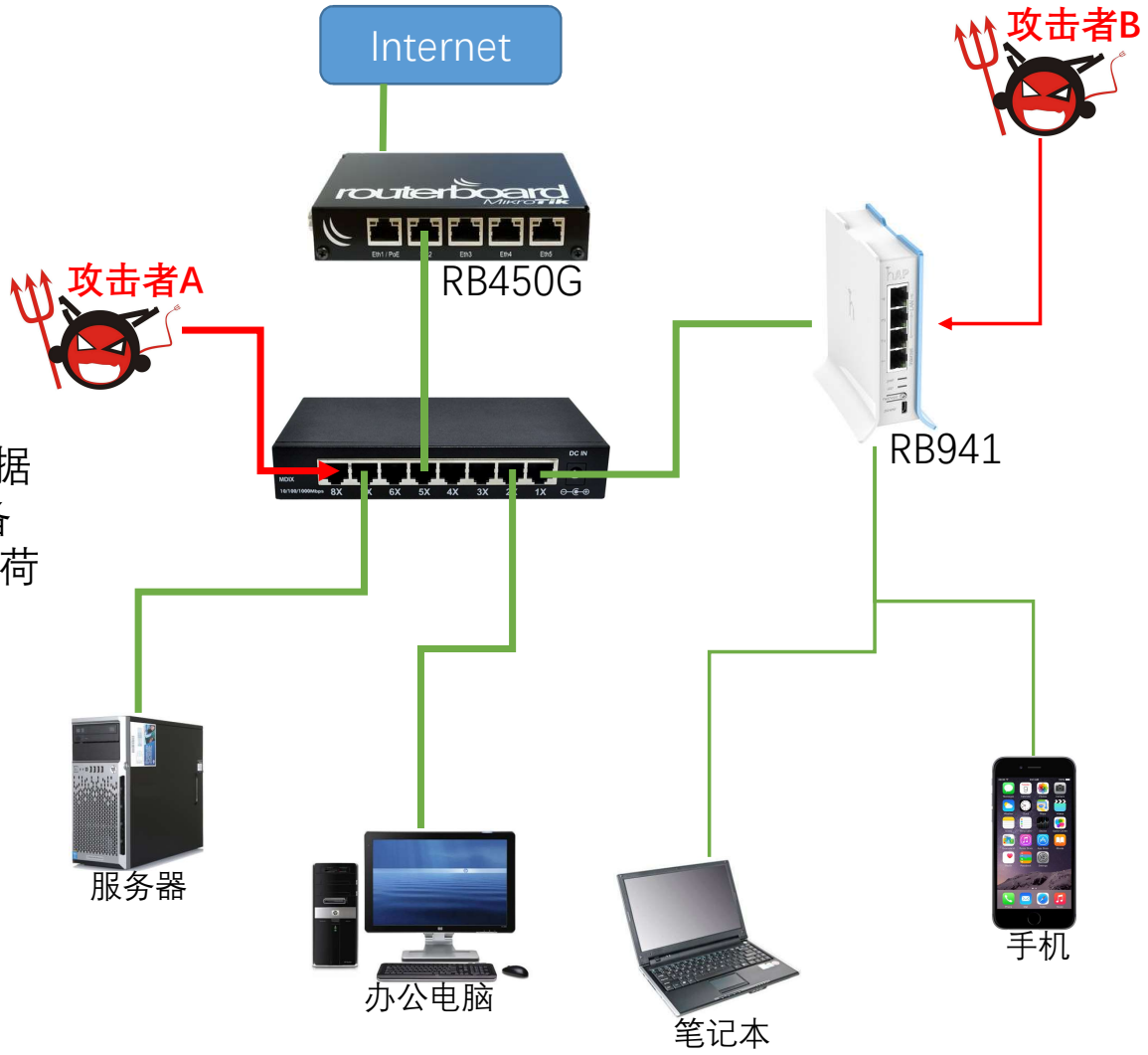
- 3.攻击时除了邻居服务受影响，还会有什么服务受到影响？攻击威力将有多大？
- When a neighbor is attacked, what services will be affected too? Attack power will be how much?

- 4.邻居服务的攻击可以让CPU持续100%负载，同时还有广播包的流量攻击。实测同广播域里的所有RB均会在3秒内失去响应，x86平台的ROS也会CPU负荷极大，甚至将无法逃脱和RB同样结局。
- The neighbor's attack will keep the CPU100% to load, at the same time, there are traffic attacks on broadcast packets.The measured results show that all the RB in the same broadcast domain will lose response within 3 seconds. CPU load of ROS on X86 platform is very great, and will not be able to avoid the same ending like RB.

图中所展示的是一个很常见的单广播域网络。

当攻击者A发起攻击时， RB450G和AP将会迅速瘫痪，从而导致互联网断开。
假设攻击者A的硬件足够强大，每秒发送足够多的数据包。所有网络所有设备都将瘫痪，包括PC。所有设备将收到大量的广播数据包，所有设备CPU将持续高负荷负载，硬件较差的设备将处于死机状态。

当攻击者B发起攻击时，由于是从无线连接的，所以攻击强度可能不足以瘫痪整个网络，但是也足以让当前网络质量大幅降低。

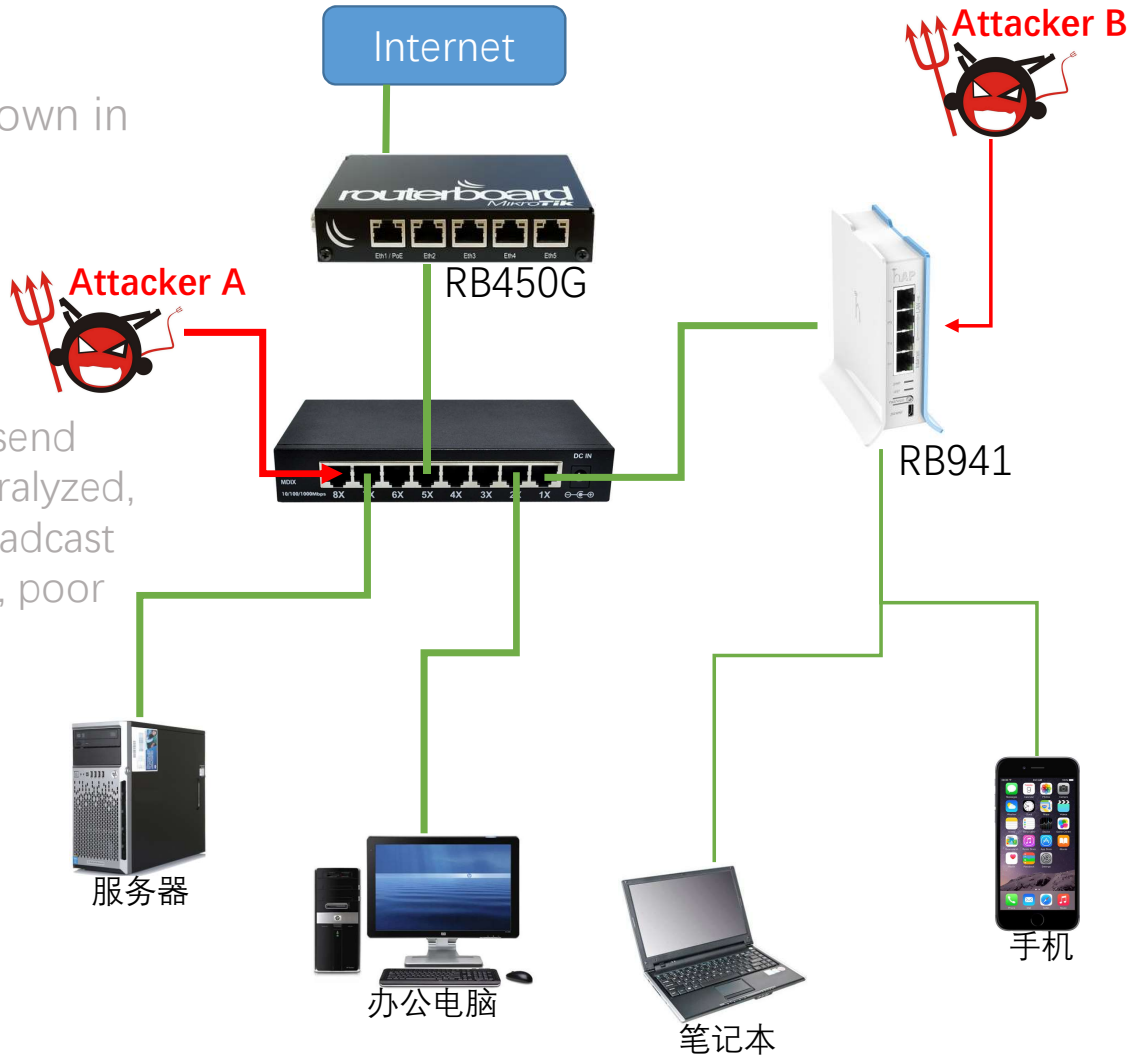


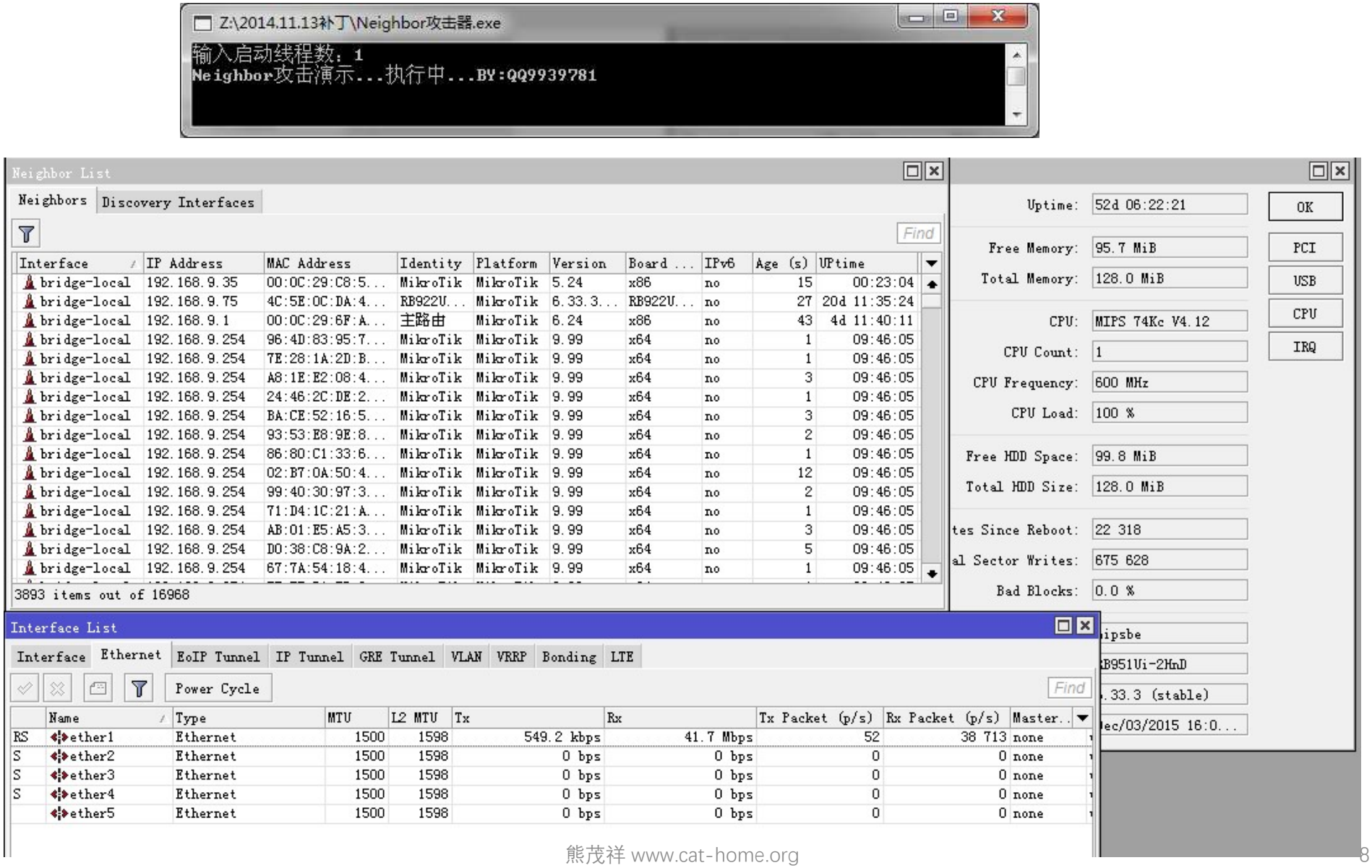
The common single broadcast domain network is shown in the picture.

When an attacker A attacks, RB450G and AP will quickly paralyzed, thus made the Internet to disconnect.

Assume that the attacker A hardware is strong enough to send enough packets per second. All network devices will be paralyzed, including PC. All devices will receive a large number of broadcast packets, all equipment CPU will continue to high load load, poor hardware equipment will be in a state of crash.

When an attacker B attacks, because it is from a wireless connection, so the strength of the attack may not be enough to disable the entire network,but it is enough to make the current network quality significantly reduced.




Z:\2014.11.13补丁\Neighbor攻击器.exe
输入启动线程数：1
Neighbor攻击演示...执行中...BY:QQ9939781
Neighbor List
Neighbors
Discovery Interfaces
Find
Interface
IP Address
MAC Address
Identity
Platform
Version
Board ...
IPv6
Age (s)
Uptime
bridge-local 192.168.9.35 00:0C:29:C8:5... MikroTik MikroTik 5.24 x86 no 15 00:23:04
bridge-local 192.168.9.75 4C:5E:0C:DA:4... RB922U... MikroTik 6.33.3... RB922U... no 27 20d 11:35:24
bridge-local 192.168.9.1 00:0C:29:6F:A... 主路由 MikroTik 6.24 x86 no 43 4d 11:40:11
bridge-local 192.168.9.254 96:4D:83:95:7... MikroTik MikroTik 9.99 x64 no 1 09:46:05
bridge-local 192.168.9.254 7E:28:1A:2D:B... MikroTik MikroTik 9.99 x64 no 1 09:46:05
bridge-local 192.168.9.254 A8:1E:E2:08:4... MikroTik MikroTik 9.99 x64 no 3 09:46:05
bridge-local 192.168.9.254 24:46:2C:DE:2... MikroTik MikroTik 9.99 x64 no 1 09:46:05
bridge-local 192.168.9.254 BA:CE:52:16:5... MikroTik MikroTik 9.99 x64 no 3 09:46:05
bridge-local 192.168.9.254 93:53:E8:9E:8... MikroTik MikroTik 9.99 x64 no 2 09:46:05
bridge-local 192.168.9.254 86:80:C1:33:6... MikroTik MikroTik 9.99 x64 no 1 09:46:05
bridge-local 192.168.9.254 02:B7:0A:50:4... MikroTik MikroTik 9.99 x64 no 12 09:46:05
bridge-local 192.168.9.254 99:40:30:97:3... MikroTik MikroTik 9.99 x64 no 2 09:46:05
bridge-local 192.168.9.254 71:D4:1C:21:A... MikroTik MikroTik 9.99 x64 no 1 09:46:05
bridge-local 192.168.9.254 AB:01:E5:A5:3... MikroTik MikroTik 9.99 x64 no 3 09:46:05
bridge-local 192.168.9.254 D0:38:C8:9A:2... MikroTik MikroTik 9.99 x64 no 5 09:46:05
bridge-local 192.168.9.254 67:7A:54:18:4... MikroTik MikroTik 9.99 x64 no 1 09:46:05
3893 items out of 16968
Uptime: 52d 06:22:21
Free Memory: 95.7 MiB
Total Memory: 128.0 MiB
CPU: MIPS 74Kc V4.12
CPU Count: 1
CPU Frequency: 600 MHz
CPU Load: 100 %
Free HDD Space: 99.8 MiB
Total HDD Size: 128.0 MiB
tes Since Reboot: 22 318
al Sector Writes: 675 628
Bad Blocks: 0.0 %
OK
PCI
USB
CPU
IRQ
ipsbe
B951Ui-2HnD
.33.3 (stable)
ec/03/2015 16:0...
Interface List
Interface
Ethernet
EoIP Tunnel
IP Tunnel
GRE Tunnel
VLAN
VRRP
Bonding
LTE
Power Cycle
Find
Name
Type
MTU
L2 MTU
Tx
Rx
Tx Packet (p/s)
Rx Packet (p/s)
Master..
RS ether1 Ethernet 1500 1598 549.2 kbps 41.7 Mbps 52 38 713 none
S ether2 Ethernet 1500 1598 0 bps 0 bps 0 0 none
S ether3 Ethernet 1500 1598 0 bps 0 bps 0 0 none
S ether4 Ethernet 1500 1598 0 bps 0 bps 0 0 none
ether5 Ethernet 1500 1598 0 bps 0 bps 0 0 none

- 5.以上图片充分展示了攻击威力之强大。
- These pictures fully demonstrate the power of attack is very powerful

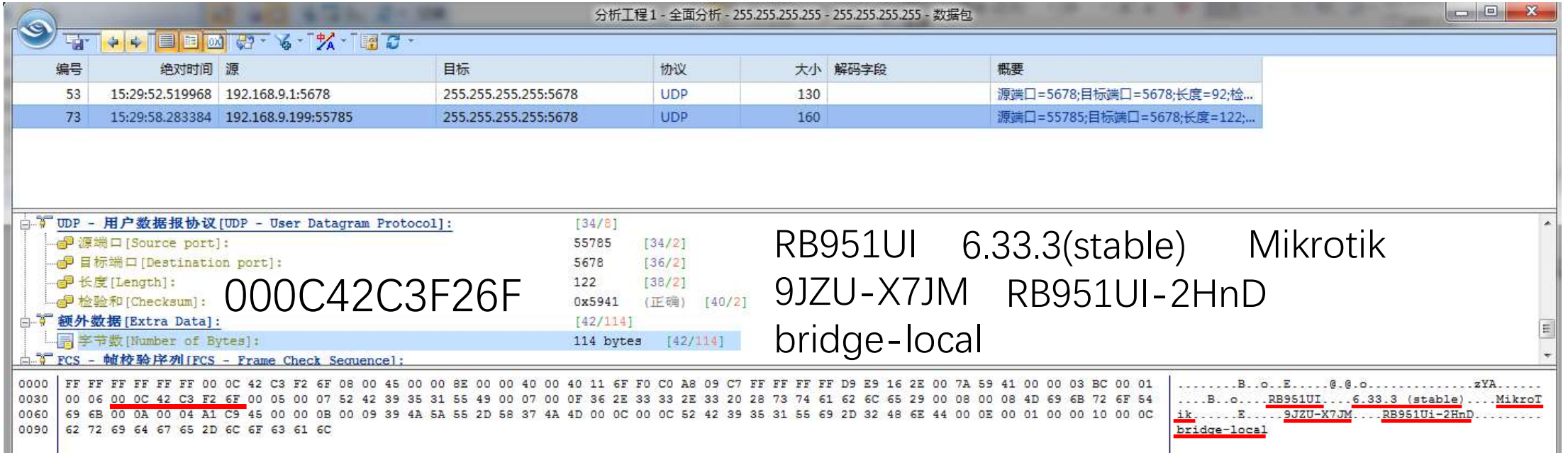
- 6.同时被攻击的不止这一台RB951设备，而是整个广播域里的所有设备，包含非ROS系统的设备。（不具备邻居服务的设备会受到广播包流量攻击。具备邻居服务的设备会受到双重攻击。）

- At the same time it is attacked more than one RB951 device, but the entire broadcast domain of all equipment , and contain the device which not installed ROS system.(the equipment without neighbor will be attacked by broadcast packets. the equipment with neighbor will going to be double under attack.)

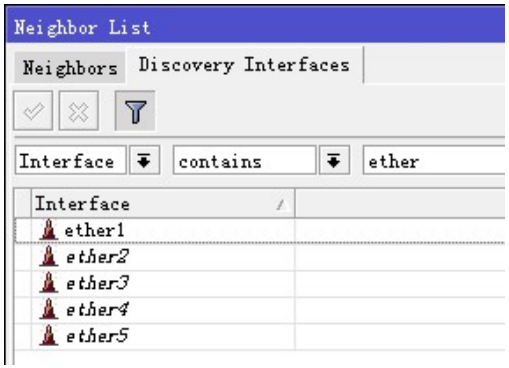
- 7.在普通网络环境中使用该程序进行攻击，和攻击者处于同一广播域的网络将极有可能瘫痪。
- In the common network environment to use the program to attack, the Internet with an attacker in the same broadcast domain is likely to be paralyzed.

三.邻居攻击数据包结构。
Neighbor attack packet structure.

1.邻居数据包由MAC，系统标识，系统版本，品牌，序列号，设备名，广播接口名组成。neighbor data package comprise by MAC, system identity, system version, brand, serial number, device name, broadcast interface name 。



四. 如何防御邻居服务攻击。
How to defense Neighbor attack.



- 1.以下防范邻居服务攻击的方法
- The following is the way to guard against neighbor attacks.

Mikrotik邻居服务使用UDP 5678端口。我们可以关闭邻居服务里的所有接口。这样即使收到邻居服务的数据包也不会进行处理。(/ip neighbor discovery disable [find])

Mikrotik neighbor using UDP 5678 port. We can shut down all the interfaces of our neighbor's . Even if a packet is received from a neighbor, it will not be processed.

- 2.以下为防范广播流量攻击的方法
- The following is the way to preventing broadcast traffic attack

防御广播流量攻击需要使用交换机进行广播域隔离，或使用3层交换转发至路由。如果使用802.1Q VLAN到路由,流量将仍然会转发到上级设备。

- Defense broadcast traffic attacks require the use the switch for broadcast domain isolation, or use the 3 layer switch to forward to the routing. If use VLAN 802.1Q to the route, traffic will still be forwarded to the superior device.

对于目前只有普通交换机的环境里，如果改变现有网络结构大家一定觉得很不方便，并且会有一些连带的设备需要改变配置，工作量很大。

For the current environment of the common switch, if you change the existing network structure, we must find it very inconvenient, and there will be some of the equipment needs to change the configuration, add a lot of work.

大家一定想知道有没有更简单的防御方法，当然有！

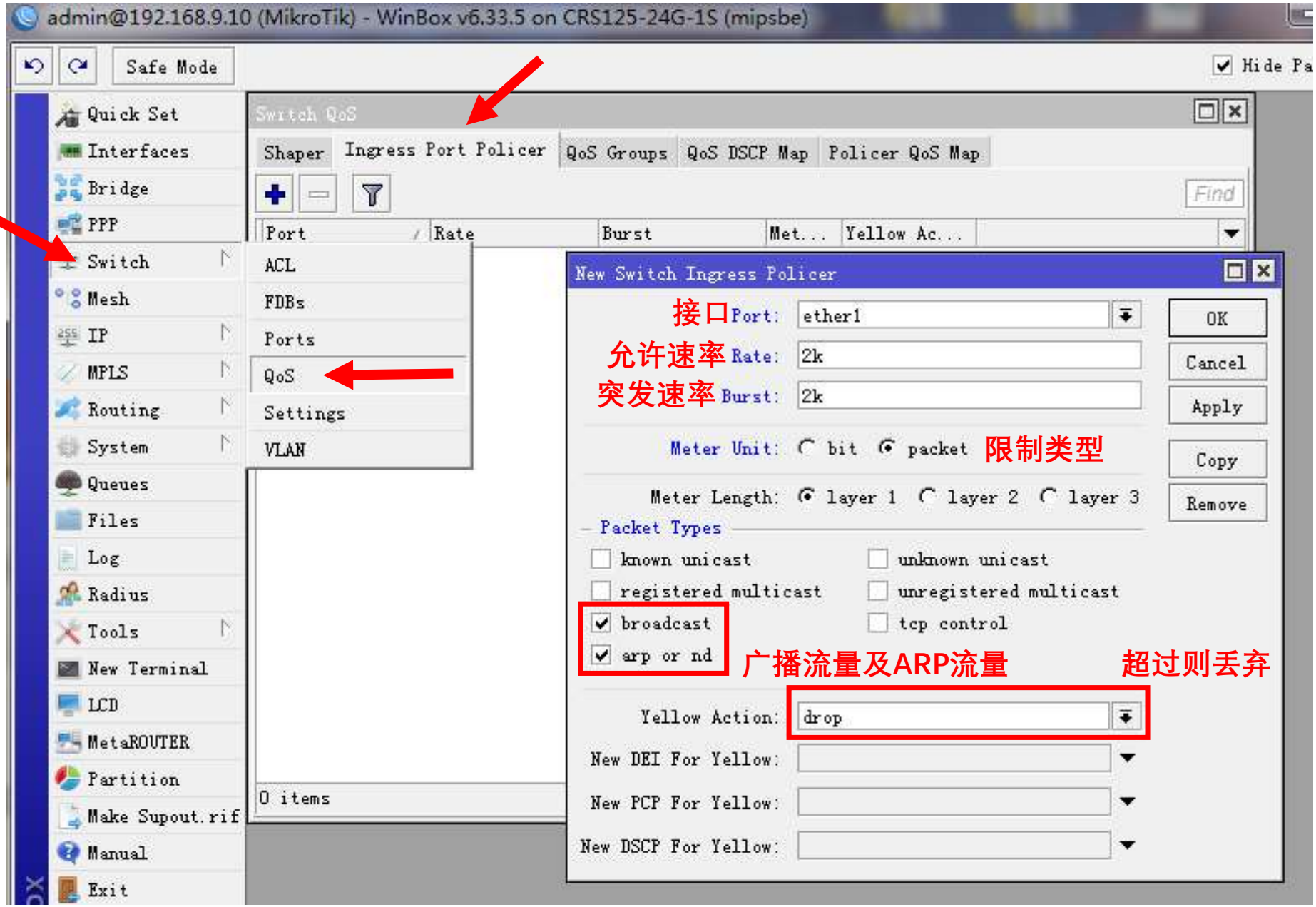
We all want to know that there is no more simple way to defend this, of course!

现在只需要将普通交换机更换为CRS就可以轻松防御这种广播攻击。有多轻松呢？3秒完工！

Now only need to replace the common switch to CRS can easily defend against such a broadcast attack. How easy is it? 3 seconds to complete!

我们先来看看CRS是如何防御这类攻击的。

Let's take a look at how CRS's defense against this type of attack.


admin@192.168.9.10 (MikroTik) - WinBox v6.33.5 on CRS125-24G-1S (mipsbe)
Safe Mode
Hide Pa
Quick Set
Interfaces
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
LCD
MetaROUTER
Partition
Make Supout.rif
Manual
Exit
ACL
FDBs
Ports
QoS
Settings
VLAN
Switch QoS
Shaper
Ingress Port Policer
QoS Groups
QoS DSCP Map
Policer QoS Map
Find
Port
Rate
Burst
Met...
Yellow Ac...
0 items
New Switch Ingress Policer
接口Port:
ether1
允许速率Rate:
2k
突发速率Burst:
2k
Meter Unit:
bit
packet
限制类型
Meter Length:
layer 1
layer 2
layer 3
Packet Types
known unicast
unknown unicast
registered multicast
unregistered multicast
broadcast
tcp control
arp or nd
广播流量及ARP流量
超过则丢弃
Yellow Action:
drop
New DEI For Yellow:
New PCP For Yellow:
New DSCP For Yellow:
OK
Cancel
Apply
Copy
Remove

说好的3秒完工的方式如下

Following that the completion of the way of 3 seconds

运行以下脚本就可轻松实现全接口防御广播流量攻击

Run the script can easily achieve full interface radio traffic attack defense

```
:foreach interid in=[/interface ethernet find ] do={
:global interna [/interface ethernet get $interid name]
/interface ethernet switch ingress-port-policer add burst=2k meter-unit=packet packet-types=arp-or-nd,broadcast port=$interna rate=2k}
```

五. 公开编译好的程序及程序源码。
make public the compiled program and the program source code.

- 1.程序采用VB.NET编写，支持并发启动多个攻击线程。启动的攻击线程越多，造成的攻击效果越大。（公开的源码仅支持单线程。）
- Program using VB.NET constructed, Supports the simultaneous launch of 1 to 4 attack threads. The more attacking thread is started, the bigger the attack effect is.（ Open source only supports single thread ）

- 2.发送的数据包内容由伪造MAC地址加系统名称等固定信息。
- The content of the data packet is composed of the forged MAC address and the system name.

- 3.将伪造好的数据包发送到255.255.255.255完成最后攻击步骤。
- The forged packets are sent to 255.255.255.255 to complete the final attack step.

- 由于幻灯片不便展示过长的源码内容及编译好的程序，有需要的观众可以与我联系获取。
- Due to the inconvenience of showing too long the source content and compile the program, there is a need for the audience can contact me to get.

谢谢观看！

Thanks for watching ！