邻居服务及广播流量攻击与防御

MUM 上海 2016/4/10

演讲人：熊茂祥

自我介绍

熊茂祥，武汉卓茵科技有限责任公司

-通过MIKROTIK官方MTCNA，MTCWE，MTCRE，MTCTCE技术认证

-编写并发布过10个以上ROS相关的应用程序，其中涉及到有分流，负载，限速，认证，CAPSMAN，系统日志服务端，用户上网日志采集，路由表采集，集中WINBOX管理，内网穿透管理等方面。

-用户分布在国内10个以上省市，并且在尼日利亚，马来西亚也分布了少量用户。

一. 邻居服务的简单介绍。

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或兼容CDP设备（Cisco发现协议）。

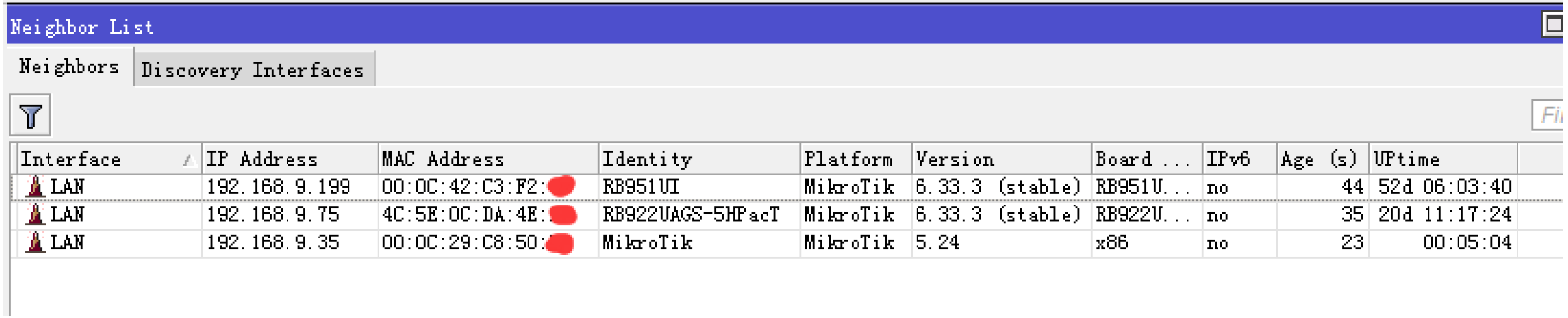
2.例如在同一个广播域中存在RB951，RB941，RB433，UBNT等设备。那么在RB951将可以在邻居菜单里看到RB941，RB433，UBNT等设备，并且可以显示对应邻居的MAC，IP，系统标识，系统版本等信息。

邻居服务带来的好处

1.大家最常用的是WINBOX的自动搜索功能，大家可以WINBOX里找到同广播域的Mikrotik设备，然后通过MAC来连接管理。

2.比较常用的还有在远程管理异地Mikrotik设备时也会用到，比如在异地的Mikrotik网络下新增了一个AP或者CRS，这个时候由于新增设备是没有进行设置的，我们需要通过远程在异地已运行的Mikrotik设备，然后利用邻居服务来发现这个设备，并使用MAC TELNET来进行基本配置。可以完全免去异地新增Mikrotik设备需要现场人员进行基本配置的过程。可以实现全远程操作添加调试设备，无需现场人员进行软操作配合，只需插线即可。

在Mikrotik系统里邻居服务如下图所示。



二. 如何使用该程序来攻击邻居服务。

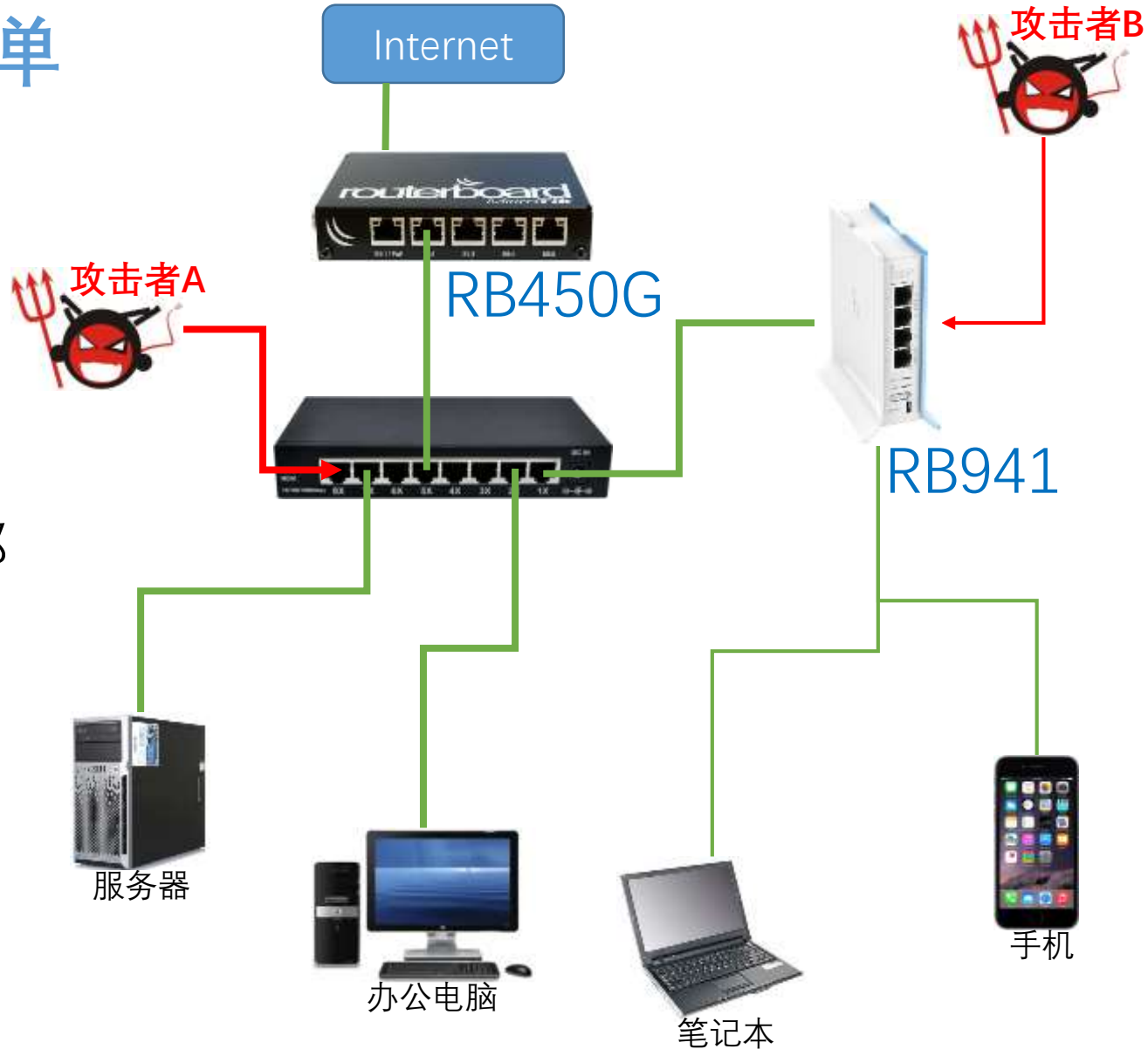
1.现在我们已经知道邻居服务的作用，那么假设在同一个广播域里有一个攻击者，模拟邻居服务来发送数据包。这样所有的邻居设备都会收到这个数据包，并且记录和显示在邻居菜单中。

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？

图中所展示的是一个很常见的单广播域网络。

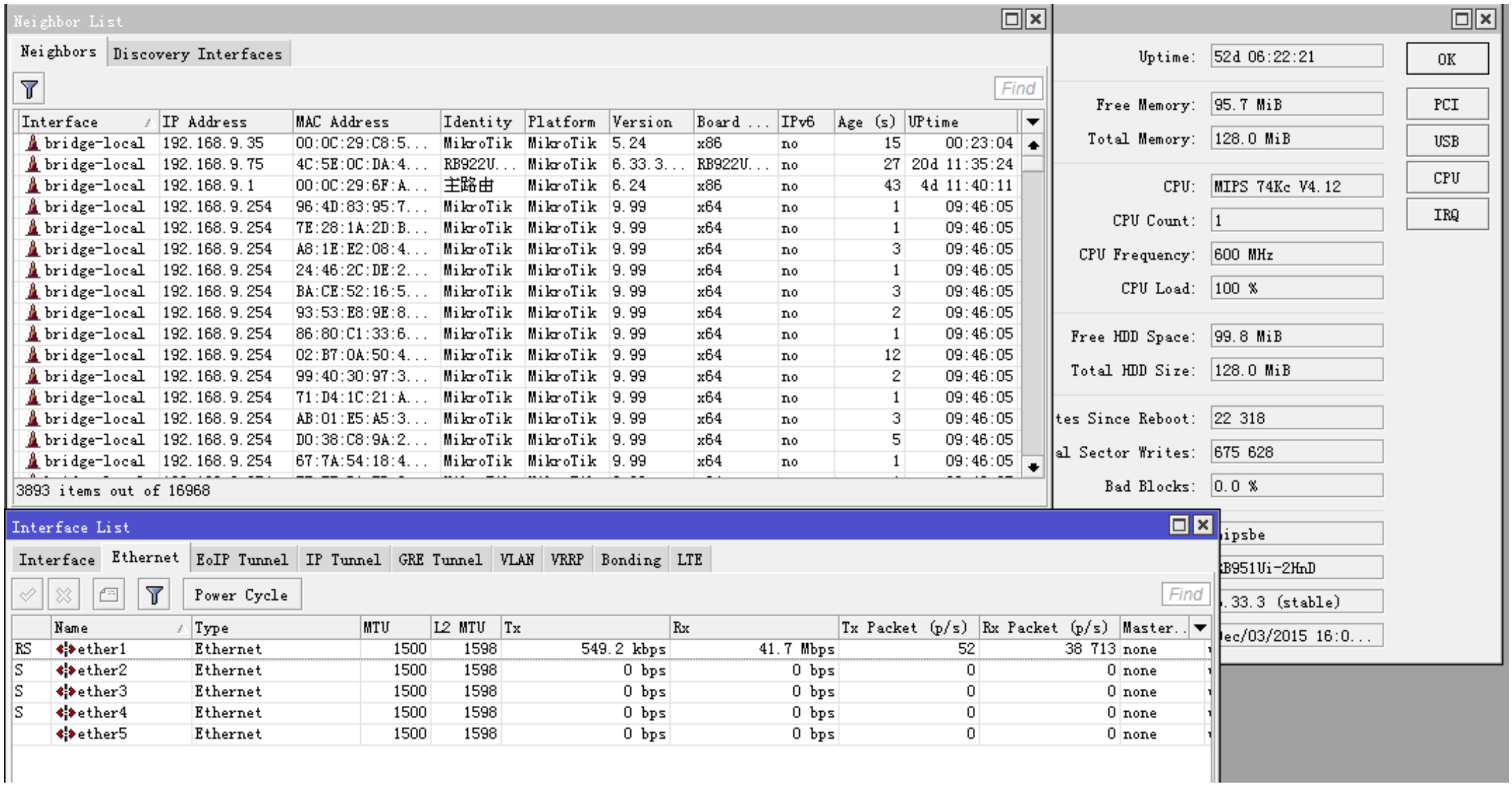
当攻击者A发起攻击时， RB450G和RB941将会迅速瘫痪，从而导致终端与互联网断开。
假设攻击者A的硬件足够强大，每秒发送足够多的数据包。网络内所有设备性能都将受影响，包括PC。所有设备将持续收到大量的广播数据包，硬件较差的设备CPU将持续高负载，甚至死机。

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。



3.攻击时除了邻居服务受影响，还会有什么服务受到影响？攻击威力将会有多大？

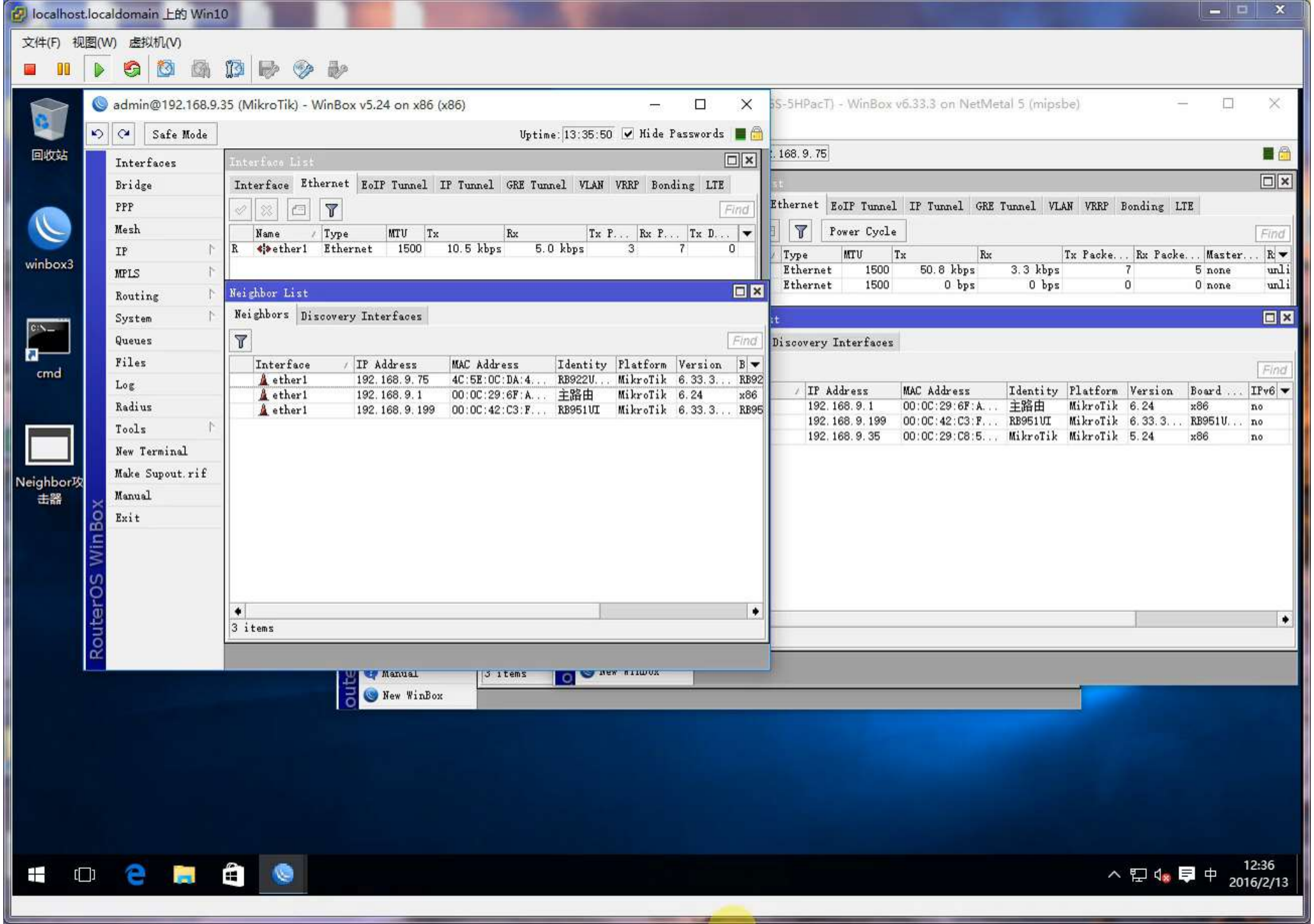
4.邻居服务的攻击可以让CPU持续100%负载，同时还有广播包的流量攻击。实际测试同广播域里的所有RB设备均会在3秒内失去响应，x86平台的ROS也会CPU负荷极大，甚至可能无法逃脱和RB同样结局。


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的强大。

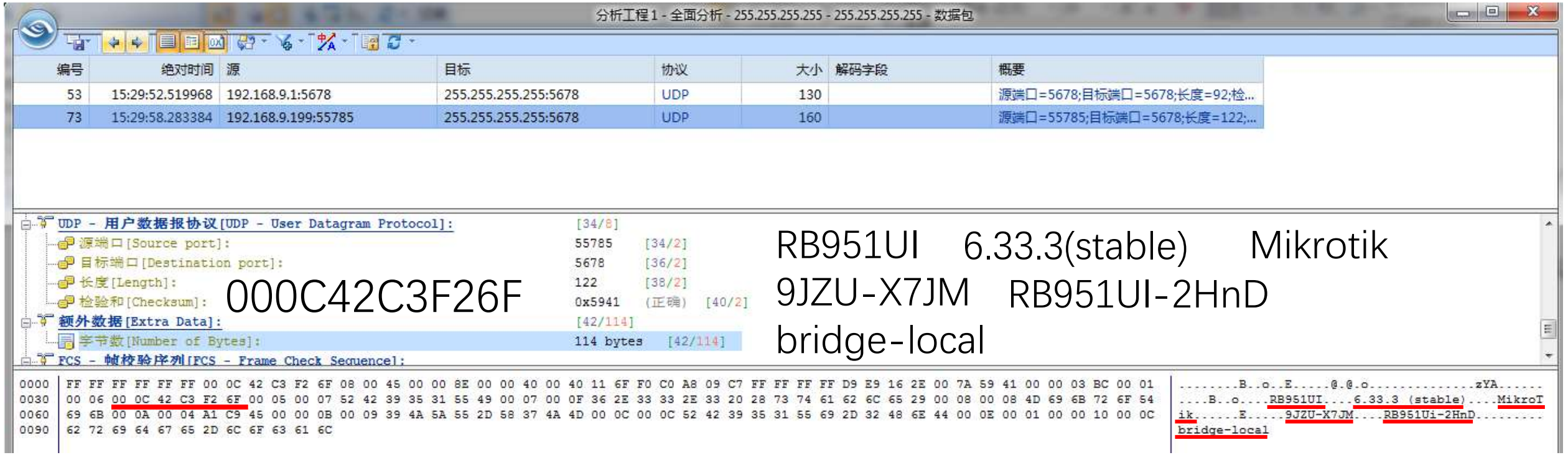
6.同时被攻击的还不止这一台RB951设备，而是整个广播域里的所有设备，包含非ROS系统的设备。（不具备邻居服务的设备会受到广播包流量攻击。具备邻居服务的设备会受到双重攻击。）

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。

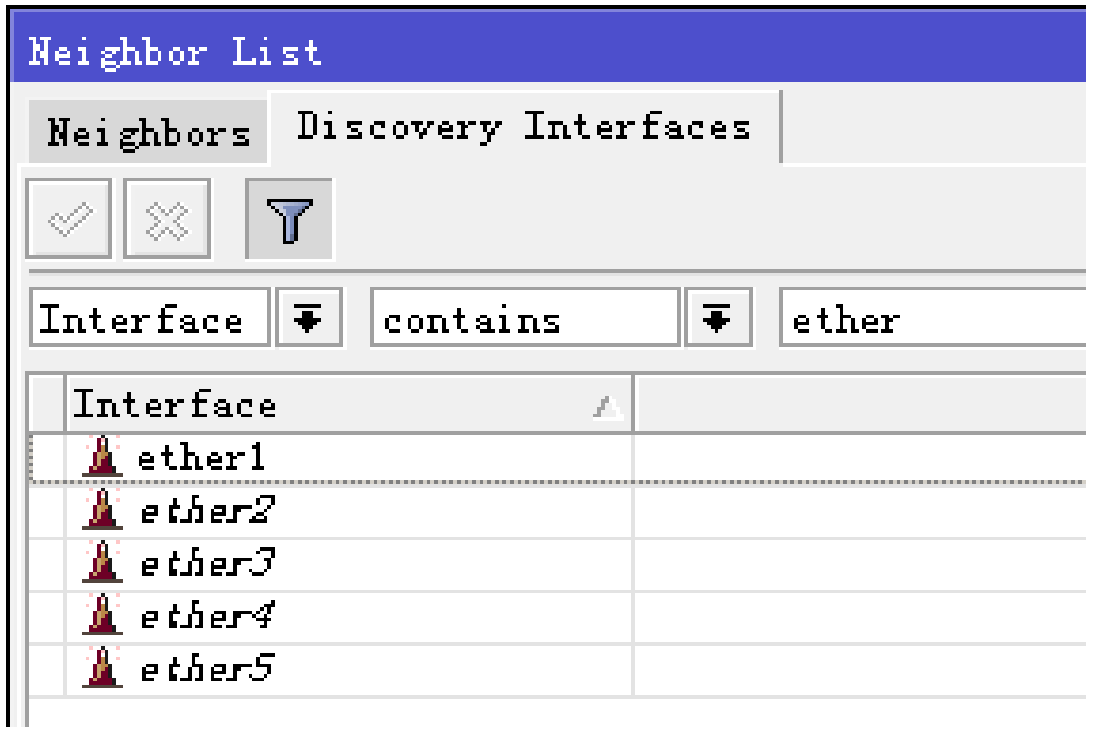

localhost.localdomain 上的 Win10
文件(F) 视图(W) 虚拟机(V)
admin@192.168.9.35 (MikroTik) - WinBox v5.24 on x86 (x86)
Safe Mode
Uptime: 13:35:50
Hide Passwords
Interfaces
Bridge
PPP
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
Make Supout.rif
Manual
Exit
RouterOS WinBox
Interface List
Interface Ethernet EoIP Tunnel IP Tunnel GRE Tunnel VLAN VRRP Bonding LTE
Name Type MTU Tx Rx Tx P... Rx P... Tx D...
R ether1 Ethernet 1500 10.5 kbps 5.0 kbps 3 7 0
Neighbor List
Neighbors Discovery Interfaces
Interface IP Address MAC Address Identity Platform Version
ether1 192.168.9.75 4C:5E:0C:DA:4... RB922U... MikroTik 6.33.3...
ether1 192.168.9.1 00:0C:29:6F:A... 主路由 MikroTik 6.24 x86
ether1 192.168.9.199 00:0C:42:C3:F... RB951UI MikroTik 6.33.3... RB95
3 items
Power Cycle
Type MTU Tx Rx Tx Packe... Rx Packe... Master...
Ethernet 1500 50.8 kbps 3.3 kbps 7 5 none
Ethernet 1500 0 bps 0 bps 0 0 none
Discovery Interfaces
IP Address MAC Address Identity Platform Version Board ... IPv6
192.168.9.1 00:0C:29:6F:A... 主路由 MikroTik 6.24 x86 no
192.168.9.199 00:0C:42:C3:F... RB951UI MikroTik 6.33.3... RB951U... no
192.168.9.35 00:0C:29:C8:5... MikroTik MikroTik 5.24 x86 no
New WinBox
回收站
winbox3
cmd
Neighbor攻击器
12:36
2016/2/13

三.邻居攻击数据包结构。

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。



四. 如何防御邻居服务攻击。



1.以下防范邻居服务攻击的方法

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])

2.以下为防范广播流量攻击的方法

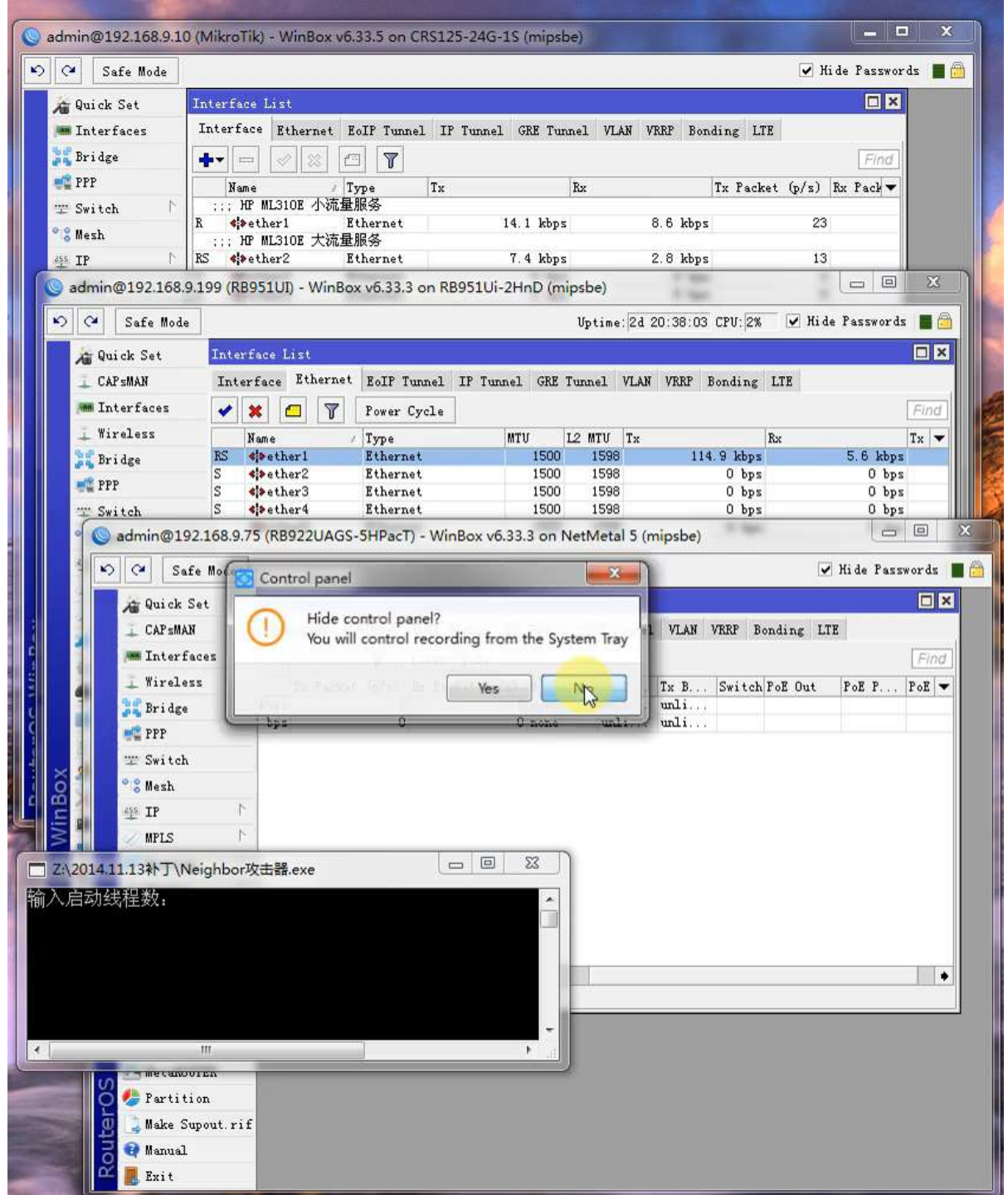
防御广播流量攻击需要使用交换机进行VLAN隔离，再使用三层交换转发至路由。如果使用802.1Q VLAN对接到路由,广播流量将仍然会转发到路由，这样当然是不行的。VLAN隔离后可以确保广播流量只存在于和攻击者同VLAN的网络中。

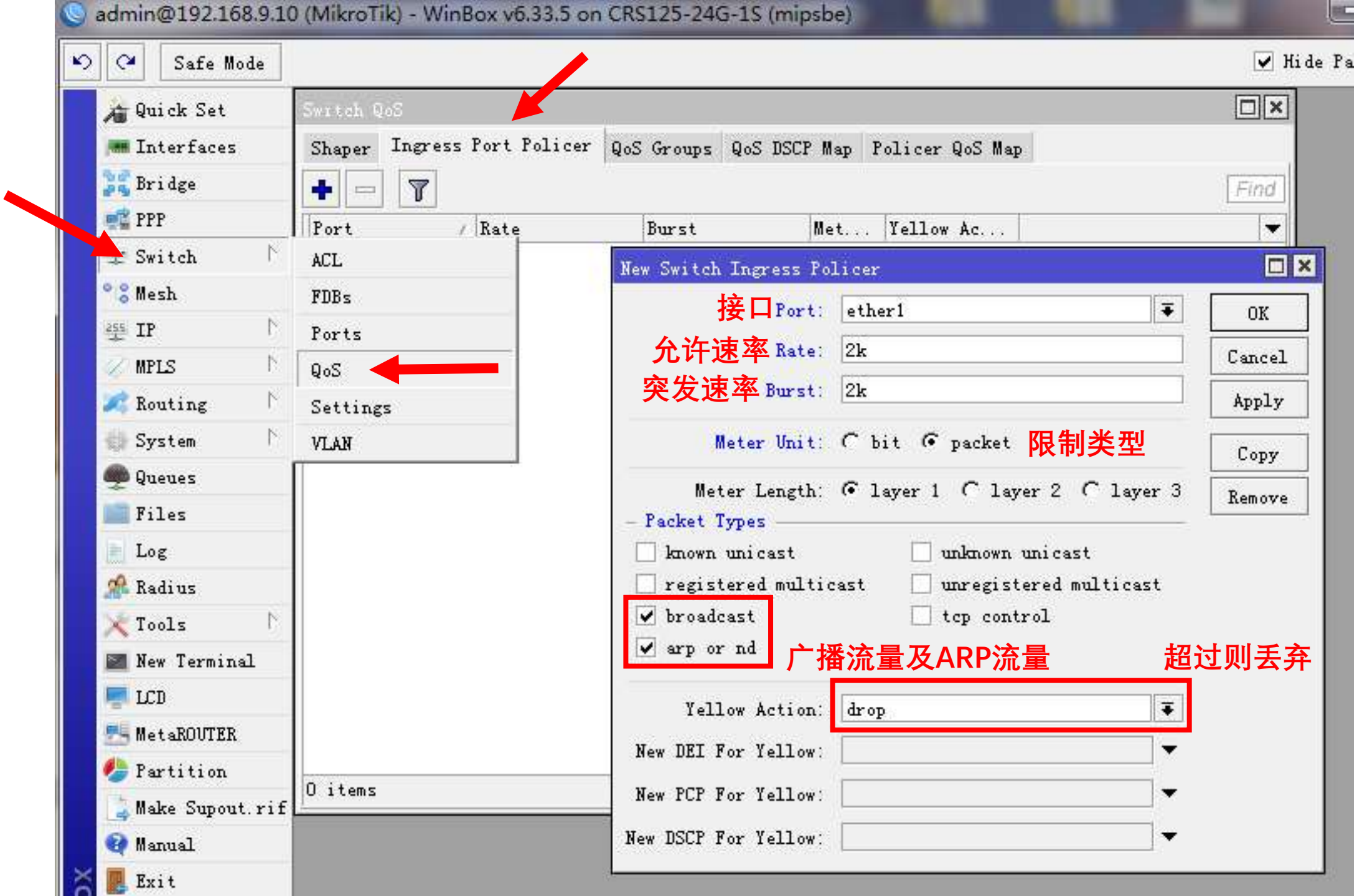
对于目前只有普通交换机的环境里，如果改变现有网络结构大家一定觉得很不方便，并且会有一些连带的设备需要改变配置，工作量很大。

大家一定想知道有没有更简单的防御方法，当然有！

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！

我们先来看看CRS是如何防御这类攻击的。


admin@192.168.9.10 (MikroTik) - WinBox v6.33.5 on CRS125-24G-1S (mipsbe)
Safe Mode
Hide Passwords
Quick Set
Interfaces
Bridge
PPP
Switch
Mesh
IP
Interface List
Interface
Ethernet
EoIP Tunnel
IP Tunnel
GRE Tunnel
VLAN
VRRP
Bonding
LTE
Find
Name
Type
Tx
Rx
Tx Packet (p/s)
HP ML310E 小流量服务
ether1
Ethernet
14.1 kbps
8.6 kbps
23
HP ML310E 大流量服务
ether2
7.4 kbps
2.8 kbps
13
admin@192.168.9.199 (RB951UI) - WinBox v6.33.3 on RB951Ui-2HnD (mipsbe)
Uptime: 2d 20:38:03
CPU: 2%
CAPsMAN
Wireless
Power Cycle
MTU
L2 MTU
ether3
ether4
0 bps
admin@192.168.9.75 (RB922UAGS-5HPacT) - WinBox v6.33.3 on NetMetal 5 (mipsbe)
Control panel
Hide control panel?
You will control recording from the System Tray
Yes
No
MPLS
Partition
Make Supout.rif
Manual
Exit
Z:\2014.11.13补丁\Neighbor攻击器.exe
输入启动线程数:
WinBox
RouterOS


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

运行以下脚本就可轻松实现全接口防御广播流量攻击

```
: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。

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。）

2.发送的数据包内容由随机伪造MAC地址加系统名称等固定信息

3.将伪造好的数据包发送到255.255.255.255完成最后攻击步骤。

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。

谢谢观看！