IPv6 Principles and Practice

Tommaso Pecorella
tommaso.pecorella@unifi.it

DaCoNetS - DINFO
Università degli Studi di Firenze

October 21, 2018

Outline

IPv6

IPv6 is the new IP protocol version. Its design goals are to fix the weak IPv4 points and to enhance its strengths.

IPv6 Pros

- Larger address space
- NATs are gone, history
- Simplified Header
- Autoconfiguration

IPv6

IPv6 is the new IP protocol version. Its design goals are to fix the weak IPv4 points and to enhance its strengths.

IPv6 Pros

- Larger address space
- NATs are gone, history
- Simplified Header
- Autoconfiguration

IPv4

- Each Internet host have an “address”
- The address is necessary for the routing
- To reach an host, its address must be **unique**

IPv4 $\rightarrow 2^{32}$addresses $\simeq$ 4billions, but they're **misused**

- there are some “private” addresses that can **not** be reached unless through complex (and extremely unreliable) NAT-traversal techniques

IPv4

- Each Internet host have an "address"
- The address is necessary for the routing
- To reach an host, its address must be **unique**

$$\text{IPv4} \rightarrow 2^{32}\text{addresses} \simeq 4\text{billions, but they're } \textbf{misused}$$

- there are some "private" addresses that can **not** be reached unless through complex (and extremely unreliable) NAT-traversal techniques

IPv4

- Each Internet host have an "address"
- The address is necessary for the routing
- To reach an host, its address must be **unique**

$$\text{IPv4} \rightarrow 2^{32}\text{addresses} \simeq 4\text{billions, but they're } \textbf{misused}$$

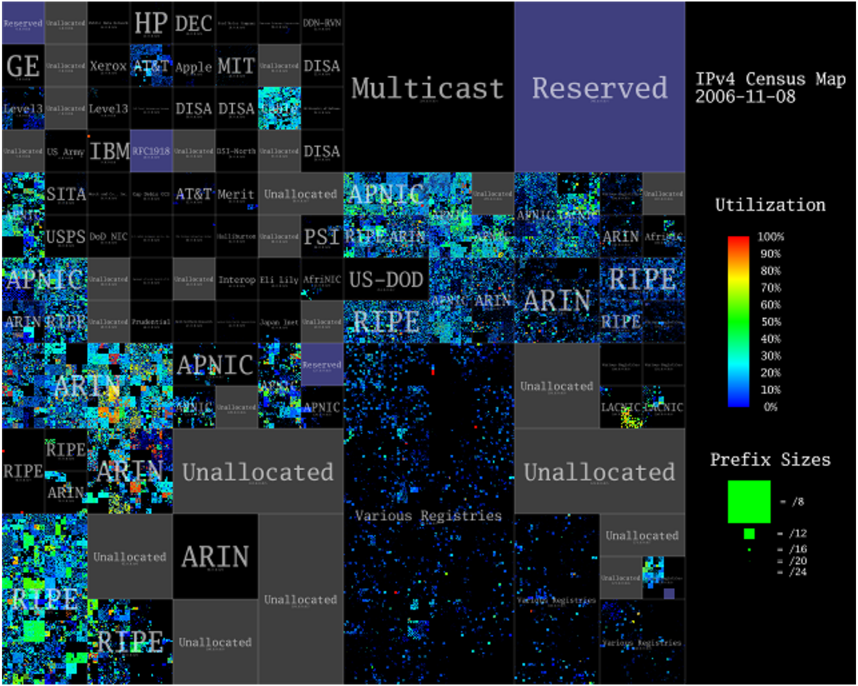
- there are some "private" addresses that can **not** be reached unless through complex (and extremely unreliable) NAT-traversal techniques

IPv4

- Each Internet host have an “address”
- The address is necessary for the routing
- To reach an host, its address must be **unique**

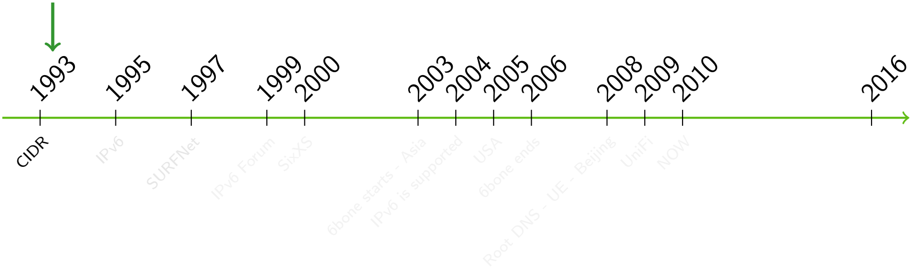
IPv4 $\rightarrow 2^{32}$addresses $\simeq$ 4billions, but they’re **misused**

- there are some “private” addresses that can **not** be reached unless through complex (and extremely unreliable) NAT-traversal techniques



IPv4 Census Map
2006-11-08
Multicast
Reserved
HP
DEC
DDN-RVN
GE
Xerox
AT&T
Apple
MIT
DISA
Level3
Level3
DISA
DISA
US Army
IBM
RFC1918
DSI-North
DISA
SITA
AT&T
Merit
Unallocated
APNIC
USPS
DoD NIC
Halliburton
PSI
RIPE
ARIN
APNIC
Interop
Eli Lily
AfriNIC
US-DOD
ARIN
RIPE
Prudential
Japan Inet
ARIN
Reserved
APNIC
LACNIC
LACNIC
Unallocated
Various Registries
Utilization
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
Prefix Sizes
= /8
= /12
= /16
= /20
= /24

IP addresses are exhausting for real?

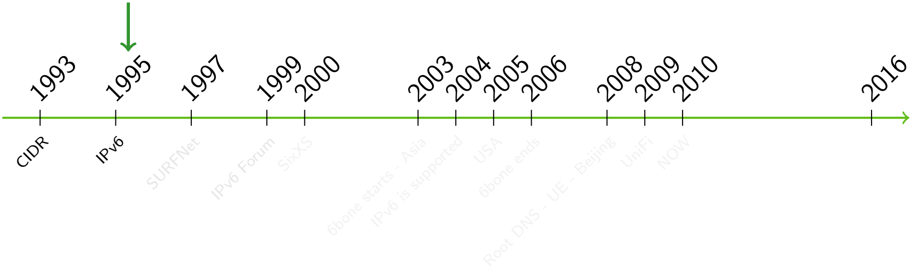


1993

- Class-based routing is dead. Welcome to CIDR.
  CIDR both helps routing table size and allows better IP pool allocation. The exhaustion is delayed.

.

IP addresses are exhausting for real?

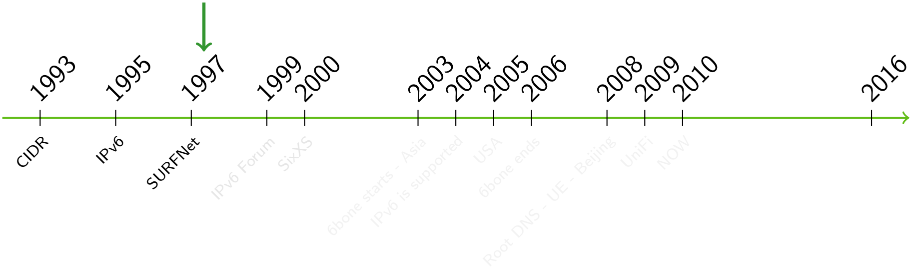


1995

- IPv6 is officially released (RFC 1752).

.

IP addresses are exhausting for real?

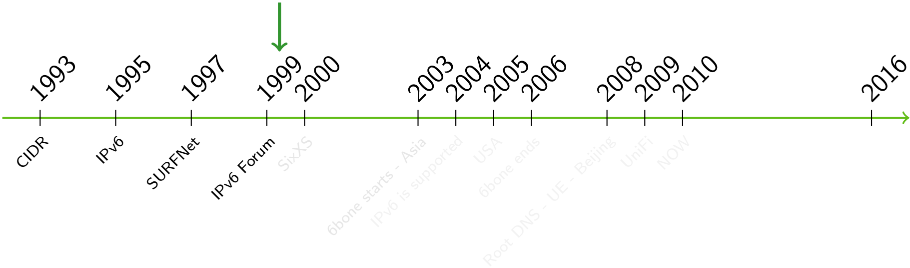


1997

- SURFNet, Netherlands's academic network, goes IPv6.

.

IP addresses are exhausting for real?

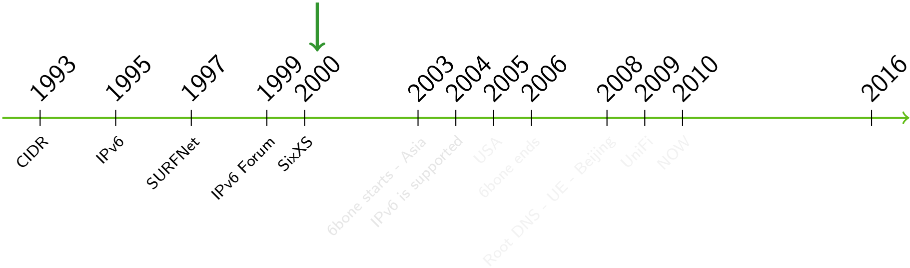


1999

- IPv6Forum and regional task forces are created.

.

IP addresses are exhausting for real?

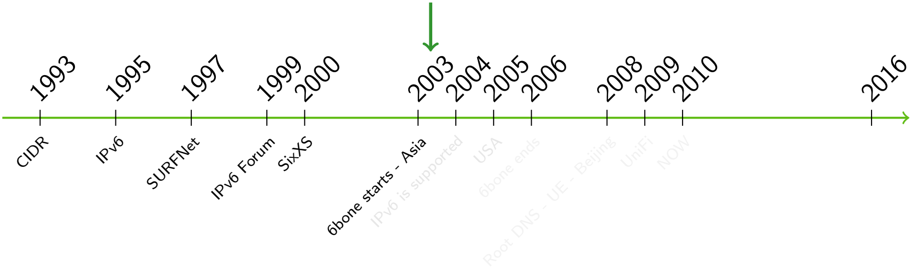


2000

- SixXS (one of the largest tunnel brokers) starts its operations.

.

IP addresses are exhausting for real?

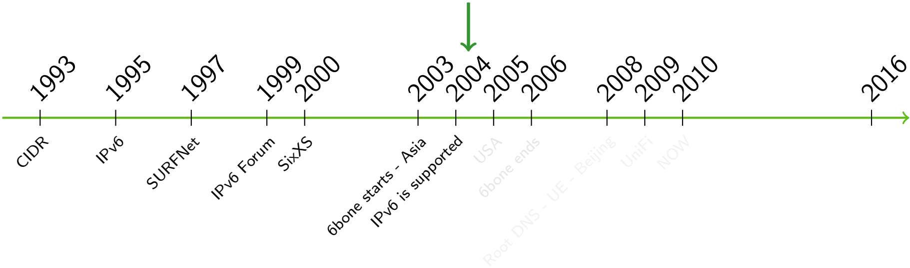


2003

- 6bone testbed
- Japan, China and South Korea announce their willingness to become leaders in IPv6.

.

IP addresses are exhausting for real?

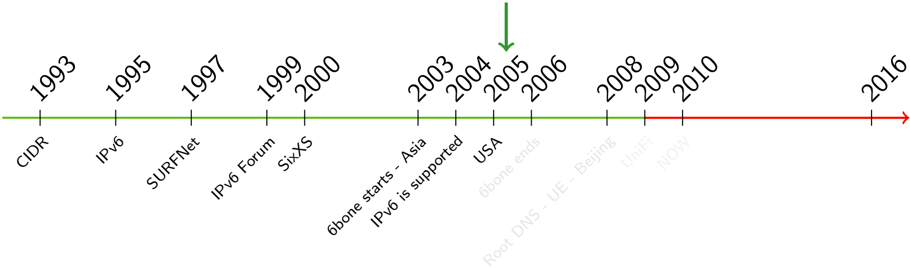


2004

- The majority of network nodes are supporting IPv6.

.

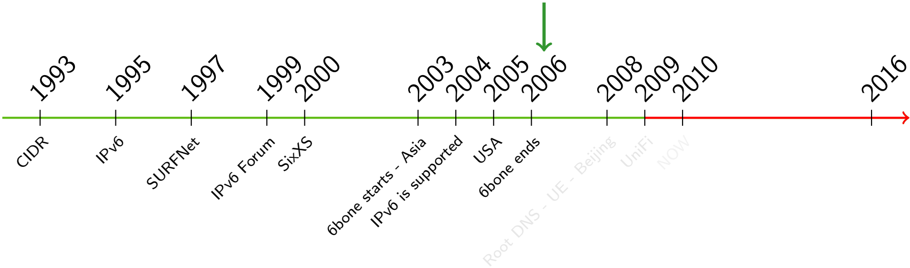
IP addresses are exhausting for real?



2005

- USA Government requires that all the federal agencies backbones have to migrate to IPv6 before 2008.
- Sify, India's ISP, gives IPv6 connectivity to its end-users.
  Tony Hain of Cisco Systems publishes a paper where he forecasts the end of IPv4 addresses between 2009 and 2016.

IP addresses are exhausting for real?

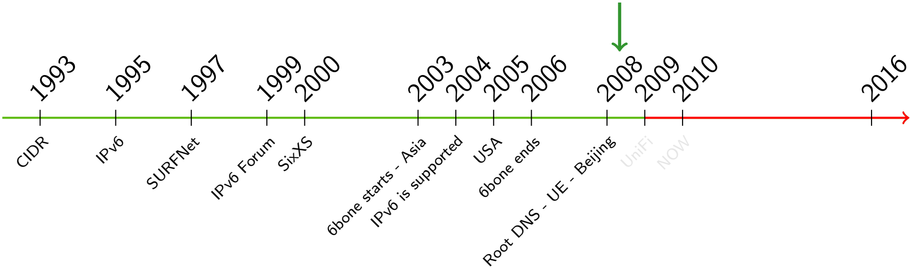


2006

- 6bone experiment ends with success.

.

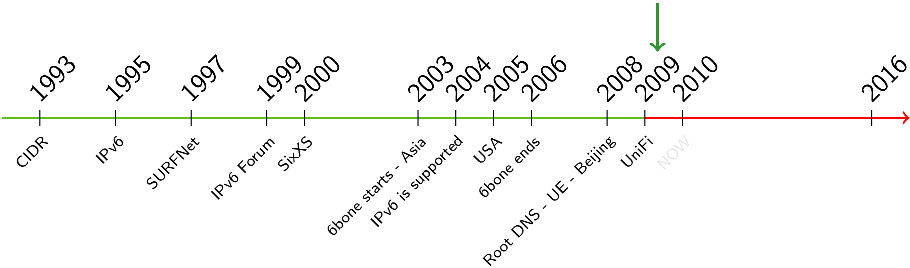
IP addresses are exhausting for real?



2008

- Root DNS can be reached also through IPv6.
- EU Commission set a goal of 25% population reached by IPv6 before 2010.
- China uses IPv6 to cover the Beijing Olympic Games. It's the biggest IPv6 use ever seen.

IP addresses are exhausting for real?

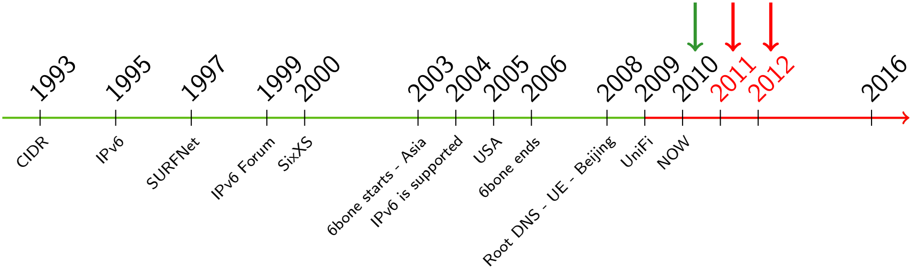


2009

- UniFi backbone is IPv6 along with a DNS server and a web server.

.

IP addresses are exhausting for real?



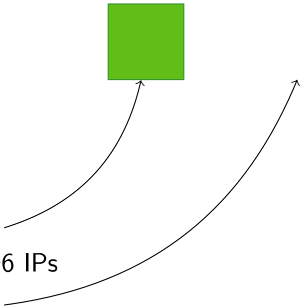
2010

- Geoff Huston's forecasts. The new address exhaustion timeline is updated to a date between September 2011 and May 2012.
- The end of the world date (according to Maya's calendar) is only a coincidence

- IPv4 Address Space

- IPv4 Address Space
  - $2^{32} = 4‘294‘967‘296$ IPs

- IPv4 Address Space
  - $2^{32} = 4‘294‘967‘296$ IPs
- IPv6 Address Space



- IPv4 Address Space
  - $2^{32} = 4‘294‘967‘296$ IPs
- IPv6 Address Space
  - $2^{128} = 340‘282‘366‘920‘938‘463‘463‘374‘607‘431‘768‘211‘456$ IPs

- IPv4 Address Space
  - $2^{32} =$ 4‘294‘967‘296 IPs
- IPv6 Address Space
  - $2^{128} =$ 340‘282‘366‘920‘938‘463‘463‘374‘607‘431‘768‘211‘456 IPs
  - Not quite right. To keep the proportion we should paint in white the whole Solar System!

- IPv4 Address Space
  - 2^{32} = 4‘294‘967‘296 IPs
- IPv6 Address Space
  - 2^{128} = 340‘282‘366‘920‘938‘463‘463‘374‘607‘431‘768‘211‘456 IPs
  - Not quite right. To keep the proportion we should paint in white the whole Solar System!
  - More than $6.66 \cdot 10^{23}$ addresses per square meter of the Earth’s surface (i.e., about 666 thousands’ billions of billions).

Network Address Translation (NAT)

Network Address Translation (NAT) is an IP address mangling technique used to allow multiple hosts to share the same (public) address.

- NAT allows a private IP adress to reach Internet, but not the opposite.
- It is possible to bypass a NAT, but it's unreliable as NATs can exhibit non-deterministic behaviours.
- You could be behind a NAT even if you have a public IP address: Large Scale NATs (LSN) are used by ISPs.

Network Address Translation (NAT)

Network Address Translation (NAT) is an IP address mangling technique used to allow multiple hosts to share the same (public) address.

- NAT allows a private IP adress to reach Internet, but not the opposite.
- It is possible to bypass a NAT, but it's unreliable as NATs can exhibit non-deterministic behaviours.
  - UPnP, STUN, NAT Traversal
- You could be behind a NAT even if you have a public IP address: Large Scale NATs (LSN) are used by ISPs.

Network Address Translation (NAT)

Network Address Translation (NAT) is an IP address mangling technique used to allow multiple hosts to share the same (public) address.

- NAT allows a private IP adress to reach Internet,
  <u>but not the opposite</u>.
- It is possible to bypass a NAT, but it's unreliable as NATs can exhibit non-deterministic behaviours.
  - UPnP, STUN, NAT Traversal
- You could be behind a NAT even if you have a public IP address: Large Scale NATs (LSN) are used by ISPs.

Network Address Translation (NAT)

Network Address Translation (NAT) is an IP address mangling technique used to allow multiple hosts to share the same (public) address.

- NAT allows a private IP adress to reach Internet, but not the opposite.
- It is possible to bypass a NAT, but it's unreliable as NATs can exhibit non-deterministic behaviours.
  - UPnP, STUN, NAT Traversal
- You could be behind a NAT even if you have a public IP address: Large Scale NATs (LSN) are used by ISPs.

Simplified Header

0–3	4–11	12–15	16–23	24–31
Ver.	Traffic Class	Flow Label		
Payload Length			Next Header	Hop Limit
Source Address				
Destination Address				

Simplified Header

0 3	4 11	12 15	16 23	24 31
Ver.	Traffic Class	Flow Label		
Payload Length		Ne		
Source Add				
Destination Ad				

IPv6 Pros

- Fixed length: 40 byte
- No more error checking
- No more fragmentation
- Header Extensions
- Better support for QoS tags
- IPSec is native
- MobileIPv6 is greatly simplified

Autoconfiguration

- Even without a router, IPv6 nodes are able to autonomously negotiate a local IPv6 address. (link-local unicast)
- The default router's behaviour is to broadcast its network so the nodes can automatically generate a valid IPv6 address. (global unicast)

Outline

IPv6 Addressing Scheme

IPv6 address space is so HUGE that a new addressing scheme is needed.

- **RFC4291** defines IPv6 addressing scheme.
- **RFC3587** defines IPv6 global unicast address format.

Moreover:

- Address is written using an Hexadecimal representation.
- Interfaces have *always* several IPv6 addresses.

IPv6 Address Types

There are a number of Address Types, and they might be confusing.

Unicast (one-to-one)

- global
- link-local
- site-local (deprecated)
- Unique Local (ULA)
- IPv4-compatible (deprecated)
- IPv6-mapped

- Multicast (one-to-many)
- Anycast (one-to-nearest)

There is no Broadcast, Multicast is used instead.

Textual Address Format

Preferred form for a 16-byte Global IPv6 Address is:

`2001:0DB8:3003:0001:0000:0000:6543:210F`

Compact form is:

`2001:DB8:3003:1::6543:210F`

Literal representation is:

- `[2001:DB8:3003:2:a00:20ff:fe18:964c]`
- `http://[2001:DB8::43]:80/index.html`

2001:DB8::/32

2001:DB8::/32 (2001 - Debate) is a *documentation-only* prefix.
Any documentation must use this prefix for examples.

Address Type Prefixes

Currently IANA allocated prefixes are:

- ::/128 (all zeroes) - Unspecified
- ::1/128 - Loopback
- 2000::/3 - Global Unicast [RFC4291]
- FC00::/7 - Unique Local Unicast [RFC4193]
- FE80::/10 - Link Local Unicast [RFC4291]
- FF00::/8 - Multicast [RFC4291]
- Anycast addreses are allocated from unicast prefixes
- 64:ff9b::/96 - IPv6-mapped IPv4 address [RFC6052]

Address Type Prefixes

Link-local addresses are used during auto-configuration and when no routers are present.

0 – 9	10 – 15	16 – 31
FE80		
0...0		
Interface		
ID		

The Interface ID can be built in a number of different ways. The most common is to derive it from the Interface MAC address.

IPv6 Interface IDs

The Interface ID can be assigned using:

- Auto-configured using 64-bit MAC address.
- Auto-configured using 48-bit MAC address (e.g., Ethernet) expanded into a 64-bit EUI-64 format.
- Assigned via DHCP.
- Manually configured.
- Auto-generated pseudo-random number (Win's default, crap).
- CGA (Cryptographically Generated Address) [RFC3972].
- Other methods (?)

IPv6 Interface IDs

Auto-configured using 48-bit MAC address:

00	Vendor	NIC specific part

02	Vendor	FF	FE	NIC specific part

E.g., `00:1f:5b:39:67:3c` maps into `021f:5bff:fe39:673c`

Assigned via DHCP

Good idea – configuration is a bit more complex than DHCPv4.

CGA (Cryptographically Generated Address)

I've not yet seen any implementation but it looks damn cool.

IPv6 Interfaces (plural!)

The thing to keep in mind is... each NIC have *at least* 3 IPv6 addresses, but probably many more.

- Loopback (::1/128, it's like "localhost")
- Link Local (FE80::xx:yy:zz:kk where xx:yy:zz:kk is from your MAC)
- Global Unicast (assigned in some way)
- All-Nodes Multicast address (FF02::1)
- All Routers Multicast Address (FF02::2, if it's a router)
- Solicited-Node Multicast Address (FF02::1:FF00:0000/104, if in auto-configuration)

IPv6 Interfaces (plural!)

The thing to keep in mind is... each NIC have *at least* 3 IPv6 addresses, but probably many more.

- Loopback (::1/128, it's like "localhost")
- Link Local (FE80::xx:yy:zz:kk where xx:yy:zz:kk is from your MAC)
- Global Unicast (assigned in some way)
- All-Nodes Multicast address (FF02::1)
- All Routers Multicast Address (FF02::2, if it's a router)
- Solicited-Node Multicast Address (FF02::1:FF00:0000/104, if in auto-configuration)

IPv6 Interfaces (plural!)

The thing to keep in mind is... each NIC have *at least* 3 IPv6 addresses, but probably many more.

- Loopback (::1/128, it's like "localhost")
- Link Local (FE80::xx:yy:zz:kk where xx:yy:zz:kk is from your MAC)
- Global Unicast (assigned in some way)
- All-Nodes Multicast address (FF02::1)
- All Routers Multicast Address (FF02::2, if it's a router)
- Solicited-Node Multicast Address (FF02::1:FF00:0000/104, if in auto-configuration)

IPv6 Interfaces (plural!)

The thing to keep in mind is... each NIC have *at least* 3 IPv6 addresses, but probably many more.

- Loopback (::1/128, it's like "localhost")
- Link Local (FE80::xx:yy:zz:kk where xx:yy:zz:kk is from your MAC)
- Global Unicast (assigned in some way)
- All-Nodes Multicast address (FF02::1)
- All Routers Multicast Address (FF02::2, if it's a router)
- Solicited-Node Multicast Address (FF02::1:FF00:0000/104, if in auto-configuration)

IPv6 Interfaces (plural!)

The thing to keep in mind is... each NIC have *at least* 3 IPv6 addresses, but probably many more.

- Loopback (::1/128, it's like "localhost")
- Link Local (FE80::xx:yy:zz:kk where xx:yy:zz:kk is from your MAC)
- Global Unicast (assigned in some way)
- All-Nodes Multicast address (FF02::1)
- All Routers Multicast Address (FF02::2, if it's a router)
- Solicited-Node Multicast Address (FF02::1:FF00:0000/104, if in auto-configuration)

IPv6 Interfaces (plural!)

The thing to keep in mind is... each NIC have *at least* 3 IPv6 addresses, but probably many more.

- Loopback (::1/128, it's like "localhost")
- Link Local (FE80::xx:yy:zz:kk where xx:yy:zz:kk is from your MAC)
- Global Unicast (assigned in some way)
- All-Nodes Multicast address (FF02::1)
- All Routers Multicast Address (FF02::2, if it's a router)
- Solicited-Node Multicast Address (FF02::1:FF00:0000/104, if in auto-configuration)

IPv6 Interfaces (plural!)

The thing to keep in mind is... each NIC have *at least* 3 IPv6 addresses, but probably many more.

- Loopback (::1/128, it's like "localhost")
- Link Local (FE80::xx:yy:zz:kk where xx:yy:zz:kk is from your MAC)
- Global Unicast (assigned in some way)
- All-Nodes Multicast address (FF02::1)
- All Routers Multicast Address (FF02::2, if it's a router)
- Solicited-Node Multicast Address (FF02::1:FF00:0000/104, if in auto-configuration)

IPv6 Interfaces (plural!)

The thing to keep in mind is... each NIC have *at least* 3 IPv6 addresses, but probably many more.

- Loopback (::1/128, it's like "localhost")
- Link Local (FE80::xx:yy:zz:kk where xx:yy:zz:kk is from your MAC)
- Global Unicast (assigned in some way)
- All-Nodes Multicast address (FF02::1)
- All Routers Multicast Address (FF02::2, if it's a router)
- Solicited-Node Multicast Address (FF02::1:FF00:0000/104, if in auto-configuration)

Auto-configuration

Auto-configuration is tricky and can lead to a number of disasters if an attacker wants to exploit it.

A node have to do the following steps:

1. Build its own Node ID
2. Join the Solicited-Node Multicast Address group and send out a DAD (Duplicate Address Detection) message.
3. Start using its Link Local IP to ask the router(s) for a Router Advertisement (RA)
4. Upon receiving the RA, build the Global Unicast Address
5. Do another DAD
6. Set Default Router
7. Surf the 'Net (maybe)

Auto-configuration

Auto-configuration is tricky and can lead to a number of disasters if an attacker wants to exploit it.

A node have to do the following steps:

1. Build its own Node ID
2. Join the Solicited-Node Multicast Address group and send out a DAD (Duplicate Address Detection) message.
3. Start using its Link Local IP to ask the router(s) for a Router Advertisement (RA)
4. Upon receiving the RA, build the Global Unicast Address
5. Do another DAD
6. Set Default Router
7. Surf the 'Net (maybe)

Auto-configuration (the problem)

There is only a small problem: the DNS

The RA carries the network prefix. It *can* carry the DNS address (RFC 6106). To obtain a DNS address you can:

1. Use the DNS from IPv4 stack, if you have dual-stack.
2. Have it manually configured (definitely a bad idea).
3. Use a DHCPv6.
4. Use RAs with DNS extension (RFC 6106).

Beware of the client compatibility to the above methods. Old OSes could not comply with them.

On-link and subnet - two different things

The difference is so subtle, and yet important, that there's a whole RFC about this: RFC 5942.

IPv4

The subnet is defined by the *address* and the *netmask*.
All hosts in the subnet are considered on-link (direct routing).

IPv6

There is *no netmask* - there is a *prefix*.
A host direct reachability is defined by its on-link status.
The on-link is *not a consequence* of having the same prefix...
... and it is *not limited to* having the same prefix.

Neighbors and RFC 4861

Neighbor solicitation

When a node has a unicast packet to send to a neighbor, but does not know the neighbor's link-layer address, it performs address resolution

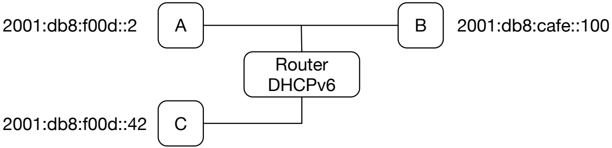
Problem is: *what is a neighbor*.

Neighbor definition

neighbors
: nodes attached to the same link

link
: a communication facility or medium over which nodes can communicate at the link layer, i.e., the layer immediately below IP.

Neighbors ? Example !



... assume that all the networks are /64.

- A and C: same prefix, but NOT on the same link.
- A and B NOT same prefix, but on the same link.

Consequence:

- A and C *can not* communicate directly.
- A and B *can* communicate directly.

What ?!?!?!?

Router Advertisement “on-link” (L) bit - if set, all the host haring the same prefix are on-link.
By default a node must consider any host as off-link.

If the router don’t set the on-link flag, any connection will go through the router. However...

1. The network performance will suffer. Fortunately...
2. ... Route Redirect messages will change the on-link property.

Note how elegant an attack can be.

Outline

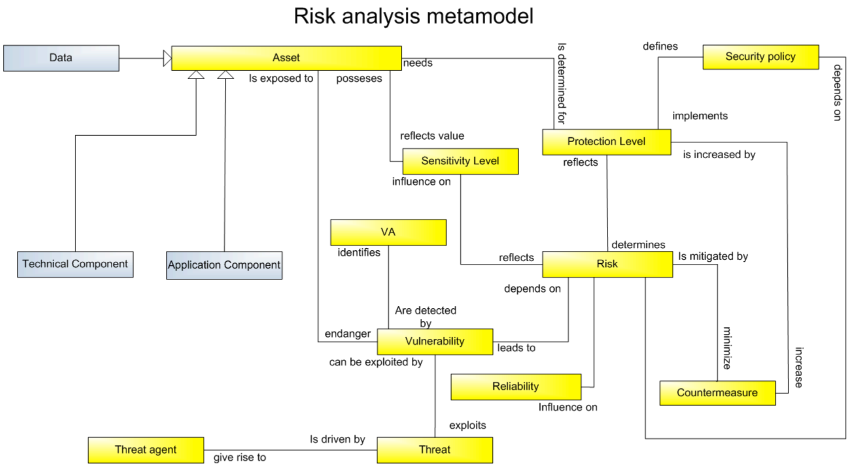
Security Plan

"Security" isn't about making things secure...
"Security" is about defining what *security* means for you
... and make it happen.

The steps to reach the target security have to follow a precise path:

- Understand the Enterprise Architecture and its goals.
- Define the Security Targets that have to be enforced.
  - e.g., robustness, failsafe operation (and percentage), admitted outage, confidentiality, etc.
- Analise Threats, Occurrence Probability and Attacker Capabilities.
- Define the Countermeasures.
- Measure the Effectiveness.

Security Plan



Partial example of Security Analysis, more on Ni2S3 deliverables.

Security Plan

Concentrating on the “bare bone” technical part does *not* adds security, it *just* add complexity.

On the other hand, we don’t have enough time to do a complete security class, so...

We will concentrate on the possible threats and countermeasures

Security Plan

Concentrating on the "bare bone" technical part does *not* adds security, it *just* add complexity.

On the other hand, we don't have enough time to do a complete security class, so...

We will concentrate on the possible threats and countermeasures

Security Plan

Concentrating on the "bare bone" technical part does *not* adds security, it *just* add complexity.

On the other hand, we don't have enough time to do a complete security class, so...

We will concentrate on the possible threats and countermeasures

IPv6 Threat model

The Threat Model in IPv6 is not that different from the one from IPv4 [RFC3552].

Threat Model

A THREAT MODEL describes the capabilities that an attacker is assumed to be able to deploy against a resource. It should contain such information as the resources available to an attacker in terms of information, computing capability, and control of the system.

For any system you have to define a Threat Model before even *thinking* to add or check security,

IPv6 Threat model

The IPv6 attacks should be divided into 2 main areas.

- IP-level attacks and vulnerabilities
- Upper-layer attacks and vulnerabilities

Upper-layer attacks and vulnerabilities is not our business, but you should always check for possible holes in the software. IPv6 addresses (and in particular IPv4-mapped ones) can raise application-level vulnerabilities.

Beware !

Do not assume that a "secure" IPv4 software is secure also for IPv6 just because it works.

IPv6 Threat model

The IPv6 attacks should be divided into 2 main areas.

- IP-level attacks and vulnerabilities
- Upper-layer attacks and vulnerabilities

Upper-layer attacks and vulnerabilities is not our business, but you should always check for possible holes in the software. IPv6 addresses (and in particular IPv4-mapped ones) can raise application-level vulnerabilities.

Beware !

Do not assume that a “secure” IPv4 software is secure also for IPv6 just because it works.

IPv6 Good News

The good news is:

- Fragmentation attack is not anymore possible - IPv6 doesn't have fragments !
- ARP is gone, so there is no ARP spoofing.
- IPSec is native, so you can expect to be able to use it massively.

On the other hand, considering IPv6 as something more easy-to-secure than IPv4 is a big mistake.
Moreover IPv6 is not (yet) massively deployed, so you should expect a lot of bad implementations, bugs and possible exploits.
So, the bottom line is...

YOU ARE NOT PREPARED

IPv6 Good News

The good news is:

- Fragmentation attack is not anymore possible - IPv6 doesn't have fragments !
- ARP is gone, so there is no ARP spoofing.
- IPSec is native, so you can expect to be able to use it massively.

On the other hand, considering IPv6 as something more easy-to-secure than IPv4 is a big mistake.
Moreover IPv6 is not (yet) massively deployed, so you should expect a lot of bad implementations, bugs and possible exploits.
So, the bottom line is...

YOU ARE NOT PREPARED

IPv6 Good News

The good news is:

- Fragmentation attack is not anymore possible - IPv6 doesn't have fragments !
- ARP is gone, so there is no ARP spoofing.
- IPSec is native, so you can expect to be able to use it massively.

On the other hand, considering IPv6 as something more easy-to-secure than IPv4 is a big mistake.
Moreover IPv6 is not (yet) massively deployed, so you should expect a lot of bad implementations, bugs and possible exploits.
So, the bottom line is...

YOU ARE NOT PREPARED

Why so many bad news ?

The bad news are not *that* bad, the point is to understand why there are bad news.

IPv6 aims to be *easier for the user*

Easy for the user does NOT means easy to administer, on the contrary!

- Auto-configuration means that an attacker can easily jump into your net and ask a lot of things about it.
- It also mean that an attacker can pretend to be something and everyone could trust it.
- IPv6 address space is HUGE, meaning that controlling it is more difficult (but also more difficult to scan).
- NATs are gone, and that's good, but network will need to be partitioned in the same way. So more firewalls.

Specific IPv6 things

IPv6 includes a lot of underestimated changes that have to be considered. As an example:

- ICMPv6 is used for a number of different purposes, so it can't be firewalled anymore.
- ICMP can be used for DOS in more creative ways /evil grin
- ARP is no more, bye bye Man in the Middle...
  but ND and NS give us a lot of fun toys to play with!
- CGA and DAD are even more fun... DOS for dummies !
- Some protocols can be forced to disable IPSec... D'oh!

Just as an example...
`http://freeworld.thc.org/papers/vh_thc-ipv6_attack.pdf`

Specific IPv6 things

IPv6 includes a lot of underestimated changes that have to be considered. As an example:

- ICMPv6 is used for a number of different purposes, so it can't be firewalled anymore.
- ICMP can be used for DOS in more creative ways /evil grin
- ARP is no more, bye bye Man in the Middle...
  but ND and NS give us a lot of fun toys to play with!
- CGA and DAD are even more fun... DOS for dummies !
- Some protocols can be forced to disable IPSec... D'oh!

Just as an example...
`http://freeworld.thc.org/papers/vh_thc-ipv6_attack.pdf`

Specific IPv6 things

IPv6 includes a lot of underestimated changes that have to be considered. As an example:

- ICMPv6 is used for a number of different purposes, so it can't be firewalled anymore.
- ICMP can be used for DOS in more creative ways /evil grin
- ARP is no more, bye bye Man in the Middle...
  but ND and NS give us a lot of fun toys to play with!
- CGA and DAD are even more fun... DOS for dummies !
- Some protocols can be forced to disable IPSec... D'oh!

Just as an example...
http://freeworld.thc.org/papers/vh_thc-ipv6_attack.pdf

Specific IPv6 things

IPv6 includes a lot of underestimated changes that have to be considered. As an example:

- ICMPv6 is used for a number of different purposes, so it can't be firewalled anymore.
- ICMP can be used for DOS in more creative ways /evil grin
- ARP is no more, bye bye Man in the Middle...
  but ND and NS give us a lot of fun toys to play with!
- CGA and DAD are even more fun... DOS for dummies !
- Some protocols can be forced to disable IPSec... D'oh!

Just as an example...
http://freeworld.thc.org/papers/vh_thc-ipv6_attack.pdf

Specific IPv6 things

IPv6 includes a lot of underestimated changes that have to be considered. As an example:

- ICMPv6 is used for a number of different purposes, so it can't be firewalled anymore.
- ICMP can be used for DOS in more creative ways /evil grin
- ARP is no more, bye bye Man in the Middle...
  but ND and NS give us a lot of fun toys to play with!
- CGA and DAD are even more fun... DOS for dummies !
- Some protocols can be forced to disable IPSec... D'oh!

Just as an example...
http://freeworld.thc.org/papers/vh_thc-ipv6_attack.pdf

Specific IPv6 things

IPv6 includes a lot of underestimated changes that have to be considered. As an example:

- ICMPv6 is used for a number of different purposes, so it can't be firewalled anymore.
- ICMP can be used for DOS in more creative ways /evil grin
- ARP is no more, bye bye Man in the Middle...
  but ND and NS give us a lot of fun toys to play with!
- CGA and DAD are even more fun... DOS for dummies !
- Some protocols can be forced to disable IPSec... D'oh!

Just as an example...
http://freeworld.thc.org/papers/vh_thc-ipv6_attack.pdf

Specific IPv6 things

IPv6 includes a lot of underestimated changes that have to be considered. As an example:

- ICMPv6 is used for a number of different purposes, so it can't be firewalled anymore.
- ICMP can be used for DOS in more creative ways /evil grin
- ARP is no more, bye bye Man in the Middle...
  but ND and NS give us a lot of fun toys to play with!
- CGA and DAD are even more fun... DOS for dummies !
- Some protocols can be forced to disable IPSec... D'oh!

Just as an example...
`http://freeworld.thc.org/papers/vh_thc-ipv6_attack.pdf`

Internet of Things bad news

Things are not that different for Internet of Things (or sensors networks).

- Way larger number of nodes make it possible for malicious devices to hop into your network.
- You'll need not only to recognize legitimate devices, but also to nullify attackers.
- Firewalls are not really feasible (not in the usual way).
- Multi-hop networks only make things worse.

The best approach to security is to *plan* it ahead.

Thanks to...

I'd like to thank Alessio Caiazza
`mailto:ac@alessiocaiazza.info`
who was both student and teacher at the same time.

Part of this presentation comes from a previous presentation we did together.

Part of this presentation comes also from 6deploy (www.6deploy.org).