

# Attaque de type Man-In-The-Middle sur réseau «dual-stack»

Global Security Days – 24 mars 2015

SUDKI Karim



# Introduction | Agenda

Introduction

Rappel IPv6

Théorie de l'attaque

pyMITM6

Conclusion

Q&A

# Introduction | Whoami

[SUDKI Karim]

Ingénieur sécurité @SCRT (2013)

[SCRT]

Organisateur d' Insomni'Hack  
19-20 mars, Genève

Partenaire de la St'Hack  
27 mars, Bordeaux



**STHACK**  
Ethical Hacking | CTF & Conférences

# Introduction | Subject

## [Actualité]

2011 PoC SLAAC Attack

2013 **DEFCON 21**

“MITM all the ipv6 things”

“ Fear the Evil FOCA: IPv6 attacks in Internet Connections ”

## [Domaines d'application]

Audits de sécurité

Internet des objets (IoT)

## [Intérêt]

Méthode alternative à “ARP Spoofing”

# IPv6 | History

## [Historique]

90's – Prédiction épuisement IPv4

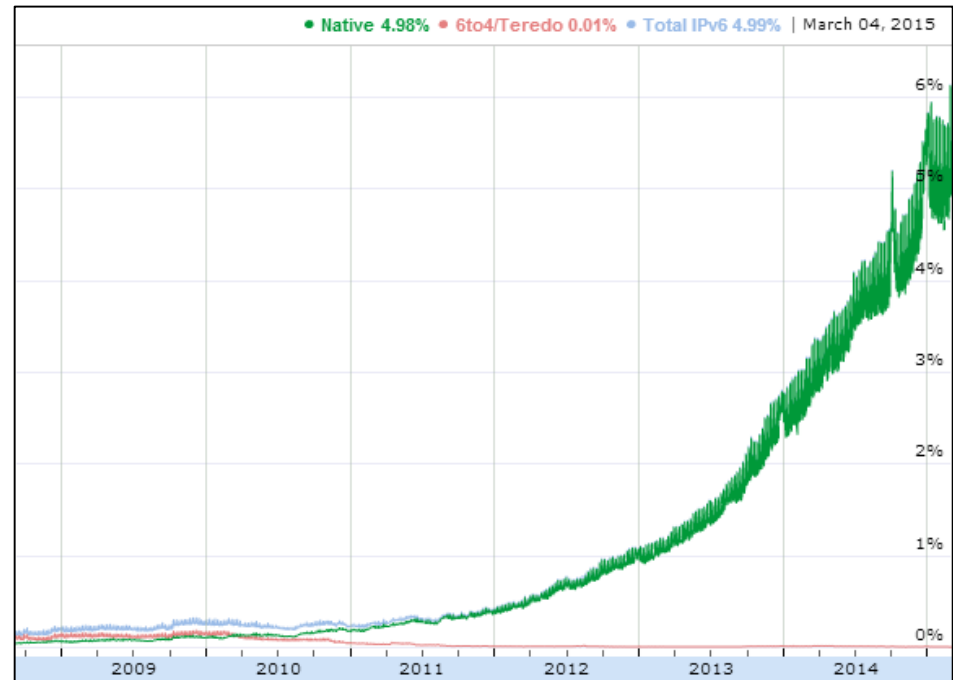
2011 – IPv6 Test Day

2012 – World IPv6 Launch

## [Constat]

Maigre utilisation sur Internet

Et dans les réseaux d'entreprise ?

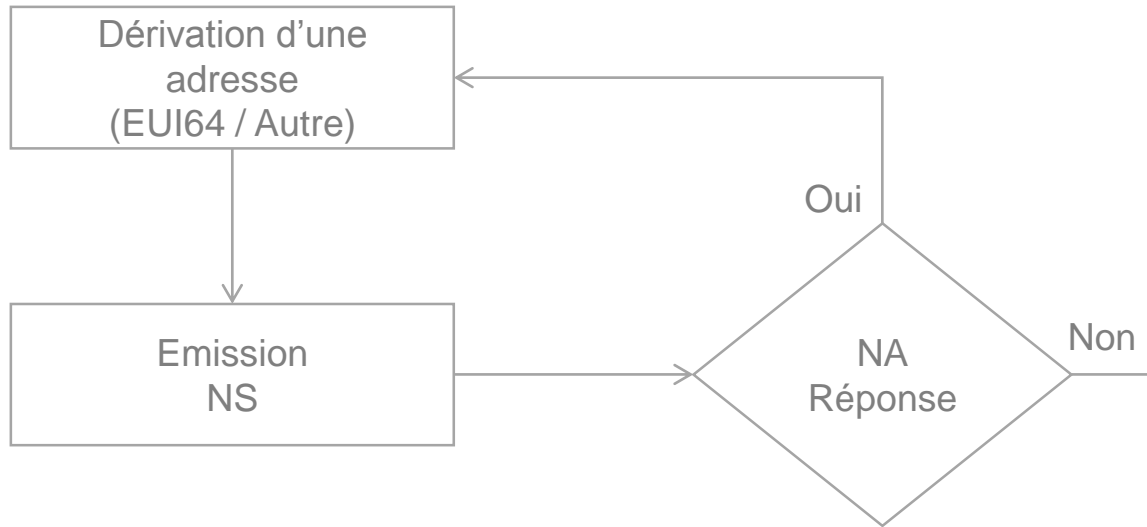


Source: <http://www.google.fr/ipv6/statistics.html>

# IPv6 | Overview

	IPv4	IPv6
<b>Adressage</b>	32bits	128 bits
<b>Notations</b>	A.B.C.D	AAAA:BBBB::CCCC:DDDD
<b>Exemples</b>	10.1.0.100	2001::db8:0:1  fe80::0202:b3ff:fe1e:8329
<b>Auto Configuration</b>	DHCP (stateful)	DHCPv6 (stateful) SLAAC (stateless)
<b>Protocole de voisins</b>	ARP	NDP (basé sur ICMPv6) <ul style="list-style-type: none"><li>- Router Advertisement (ff02::1)</li><li>- Router Solicitation (ff02::2)</li><li>- Neighbour Advertisement (ff02::1)</li><li>- Neighbour Solicitation (ff02::1:ff00:0)</li></ul>

# IPv6 | Basic Configuration



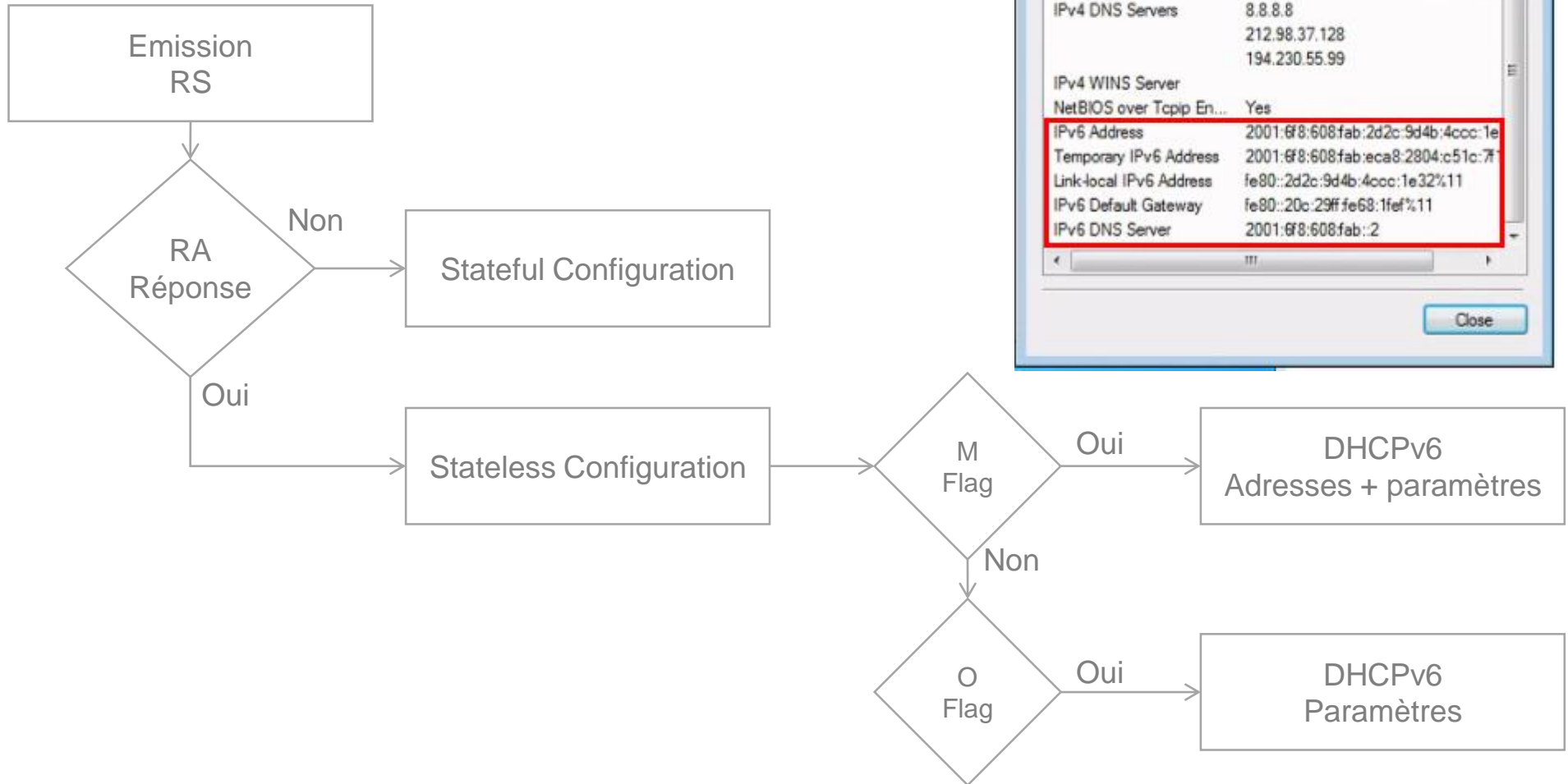
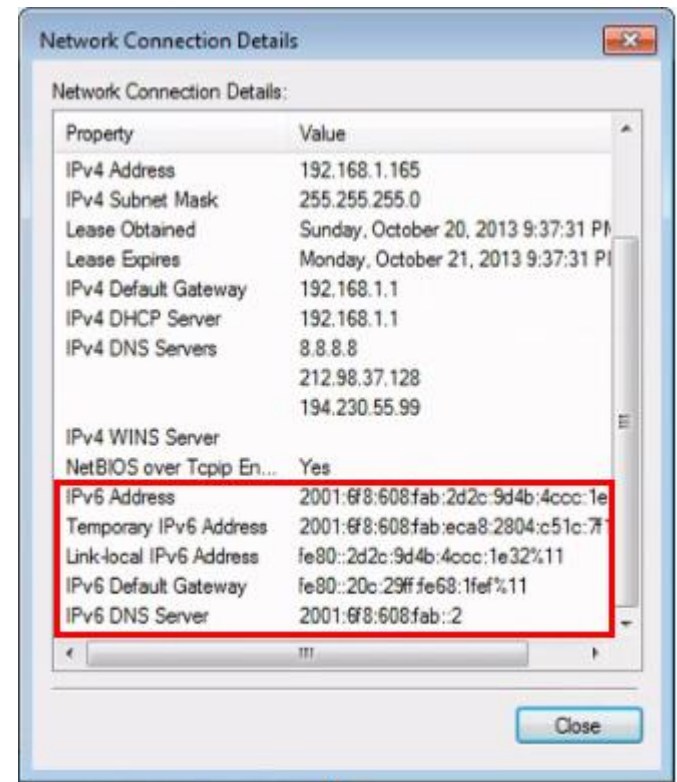
Network Connection Details

Property	Value
Connection-specific DN...	home
Description	Intel(R) Centrino(R) Advanced-N 6235
Physical Address	C4-85-08-73-2D-C8
DHCP Enabled	Yes
IPv4 Address	10.0.1.192
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	mercredi 18 mars 2015 16:58:58
Lease Expires	jeudi 19 mars 2015 16:59:00
IPv4 Default Gateway	10.0.1.1
IPv4 DHCP Server	10.0.1.1
IPv4 DNS Server	10.0.1.1
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	fe80::5c06fb74:ed89:ce45%12
IPv6 Default Gateway	
IPv6 DNS Server	

↓

Auto configuration

# IPv6 | Autoconfiguration





# IPv6 | Transition Mechanisms

## [Dual Stack]

Communication en IPv4 et/ou IPv6

## [Translation d'adresses]

Communication entre noeuds exclusivement IPv4 et IPv6

## [Tunnels]

Encapsulation de paquets IPv6 pour transport sur réseau IPv4

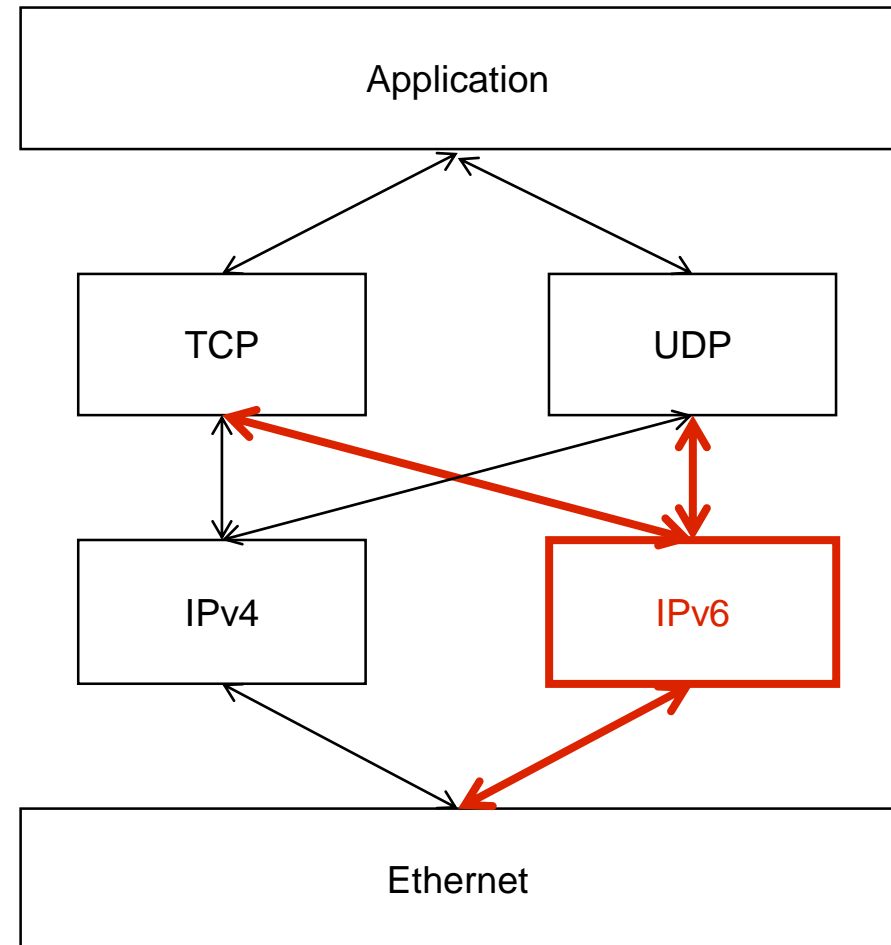
# IPv6 | Transition Mechanisms

## [Dual Stack]

Active par défaut (Win, Mac)

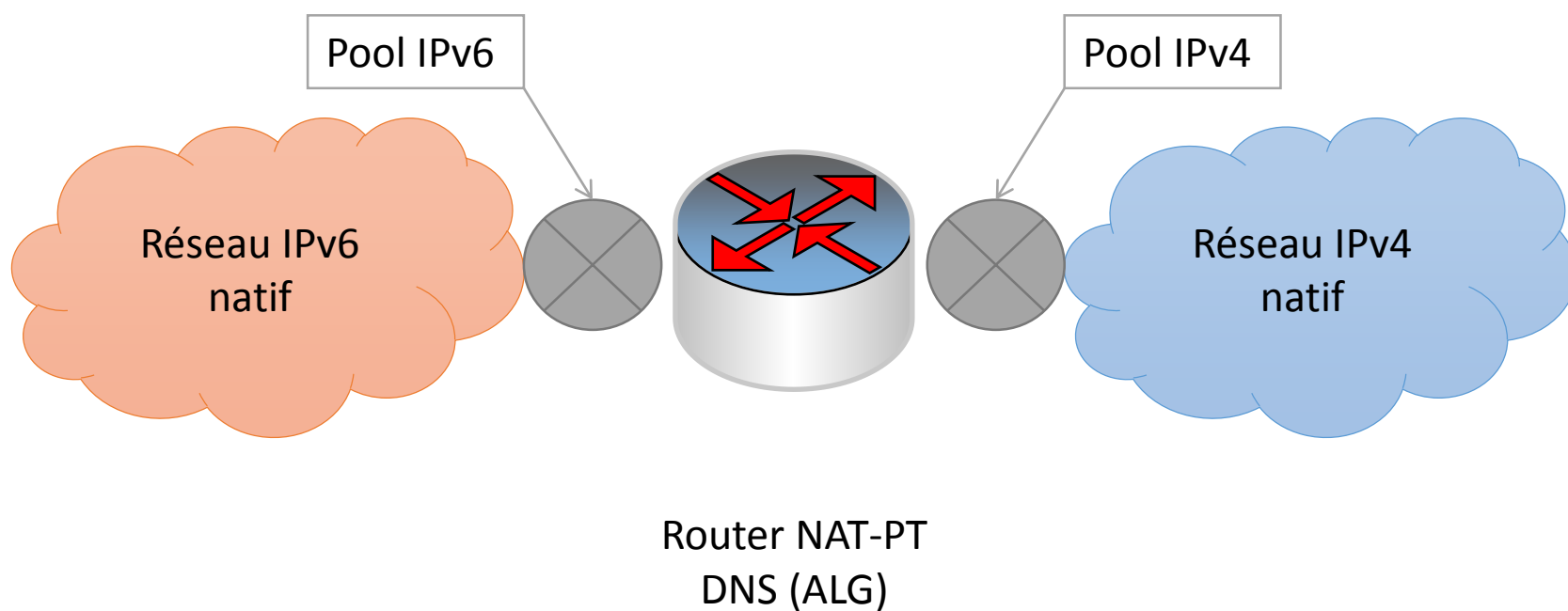
IPv6 préféré automatiquement

Piles indépendantes



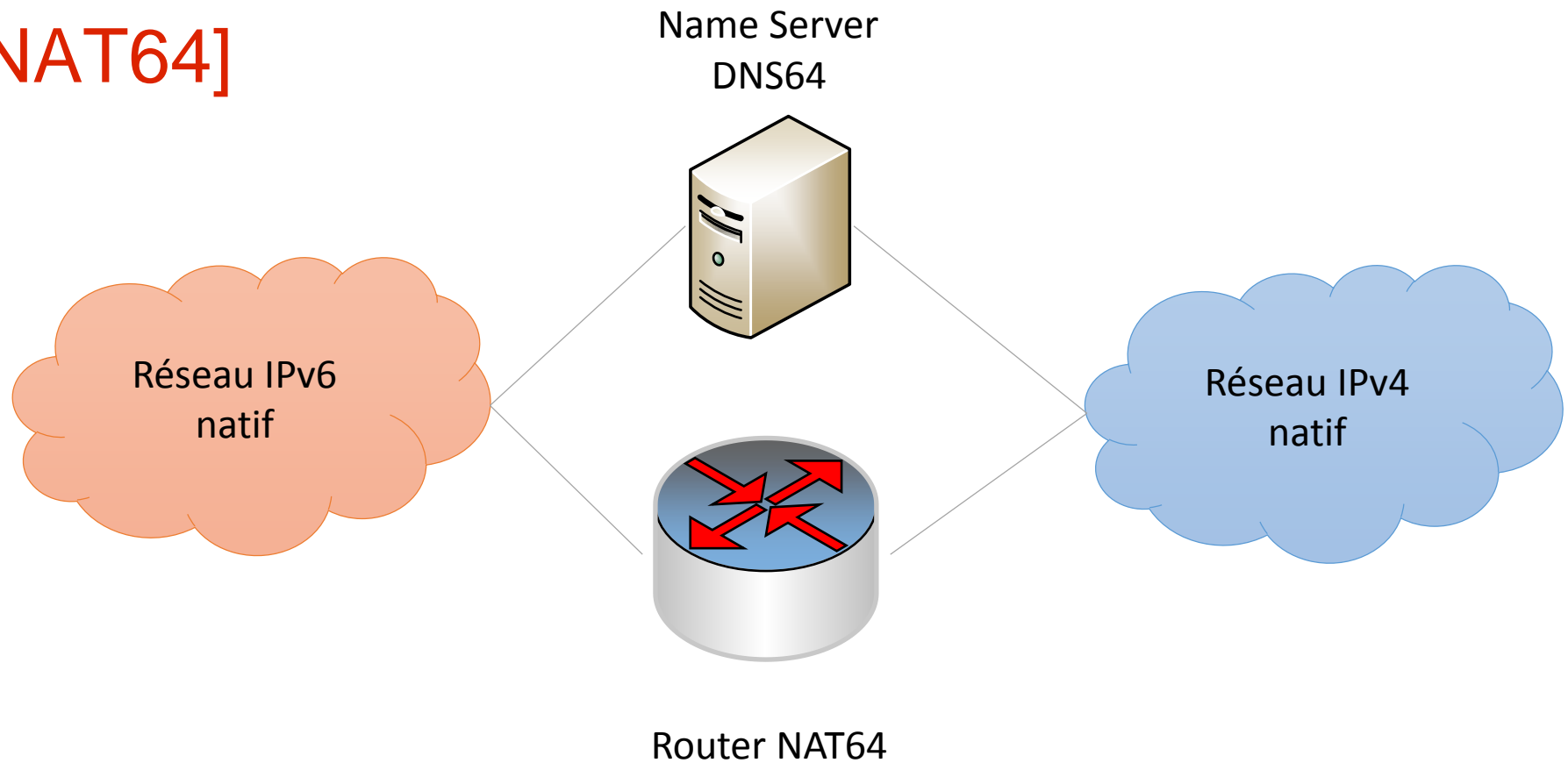
# IPv6 | Transition Mechanisms

## [NAT-PT]



# IPv6 | Transition Mechanisms

## [NAT64]



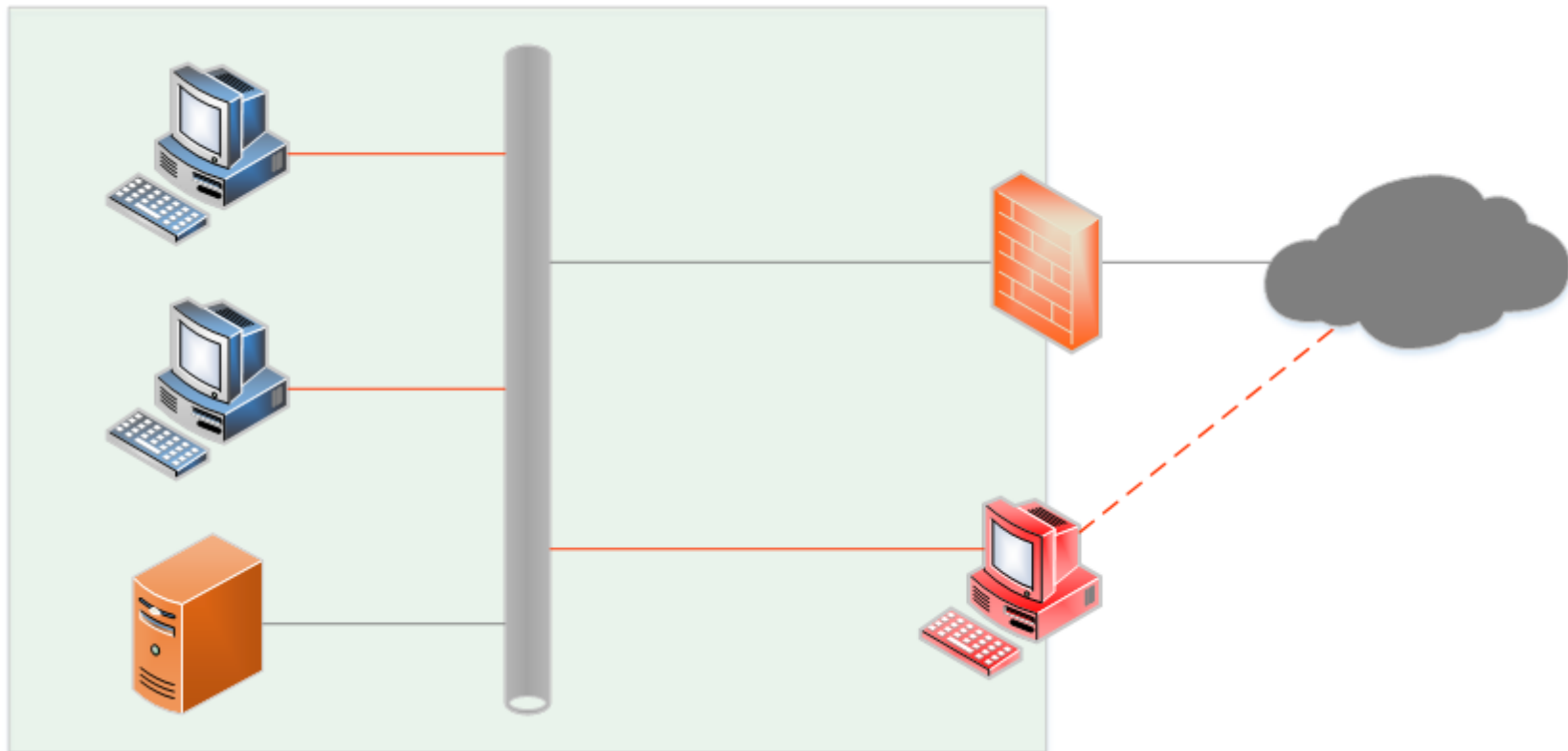
# IPv6 | Attacks

**Neighbour Advertisement (NA) Spoofing**

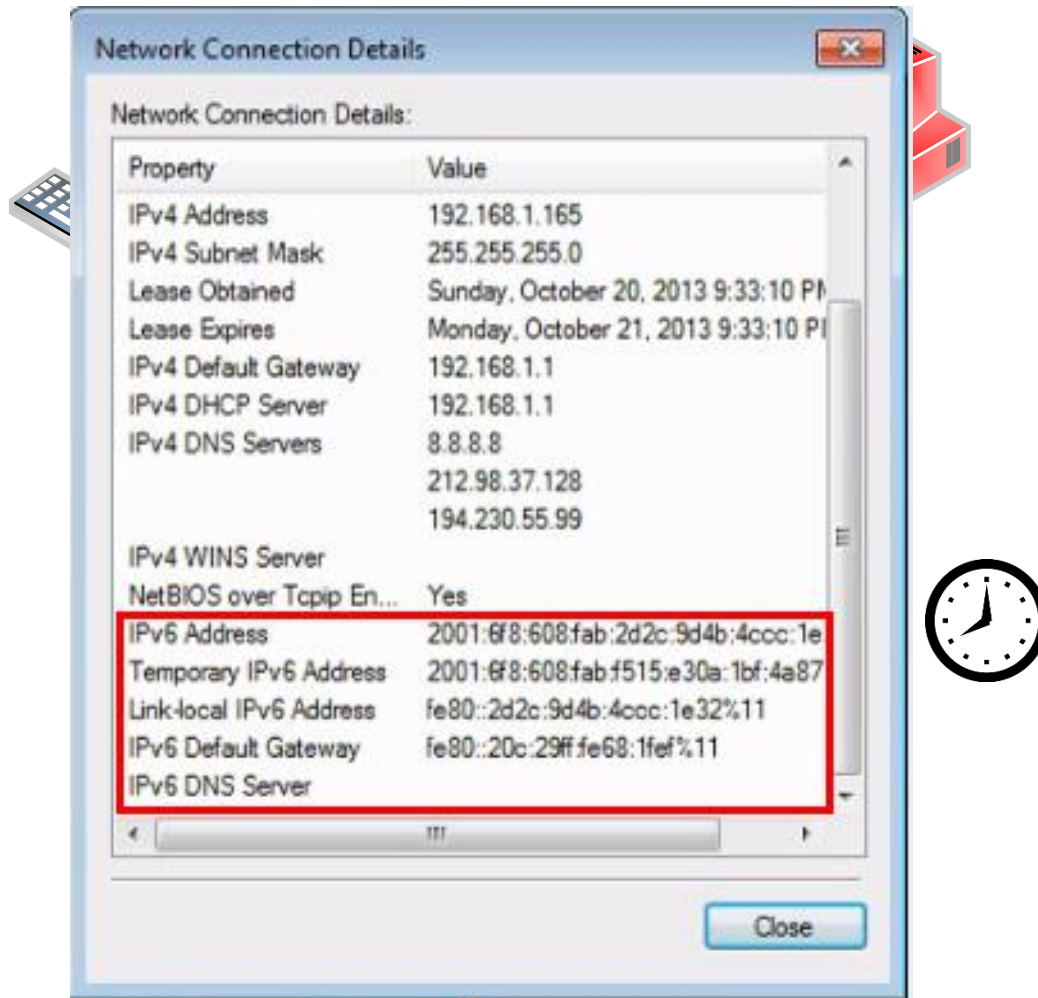
**StateLess Address Auto Configuration (SLAAC)**

**Web Proxy Autodiscovery Protocol (WPAD) (idem IPv4)**

# SLAAC Attack | Concept



# SLAAC Attack | Configuration



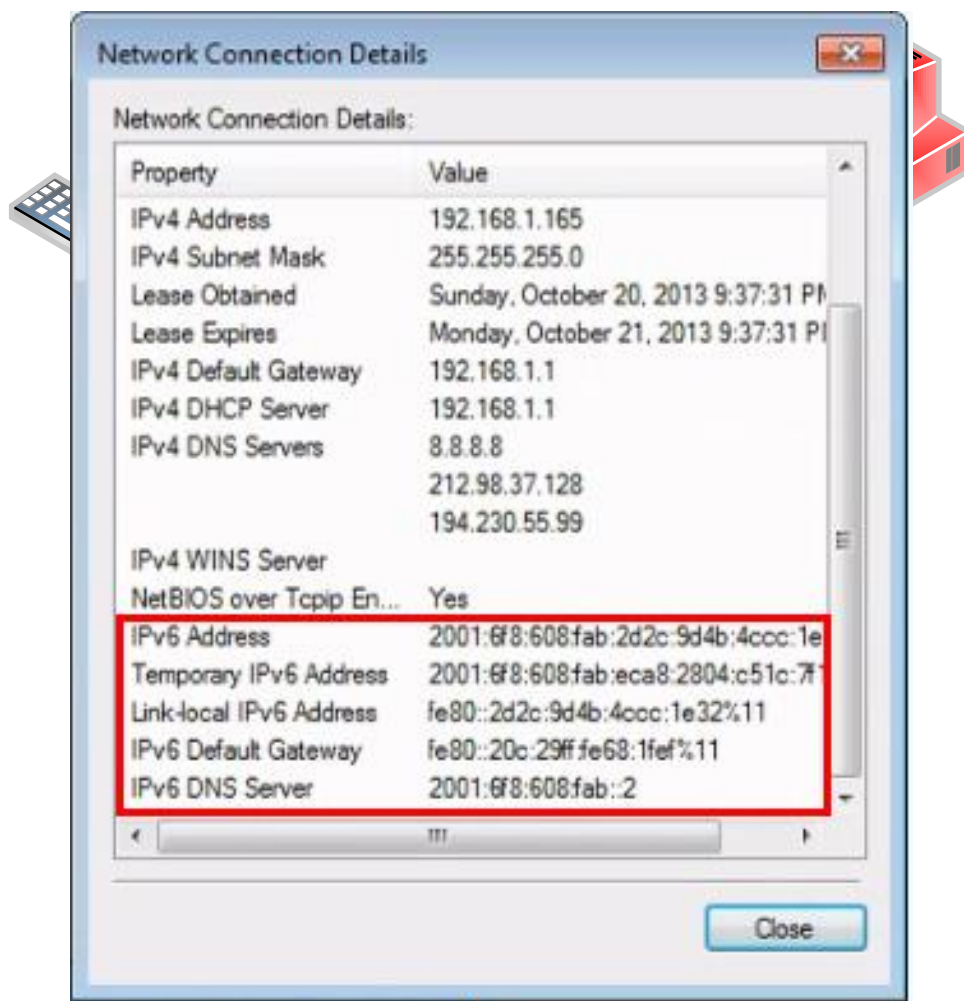
Network Connection Details

Network Connection Details:

Property	Value
IPv4 Address	192.168.1.165
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Sunday, October 20, 2013 9:33:10 PM
Lease Expires	Monday, October 21, 2013 9:33:10 PM
IPv4 Default Gateway	192.168.1.1
IPv4 DHCP Server	192.168.1.1
IPv4 DNS Servers	8.8.8.8 212.98.37.128 194.230.55.99
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
IPv6 Address	2001:6f8:608:fab:2d2c:9d4b:4ccc:1e
Temporary IPv6 Address	2001:6f8:608:fab:f515:e30a:1bf:4a87
Link-local IPv6 Address	fe80::2d2c:9d4b:4ccc:1e32%11
IPv6 Default Gateway	fe80::20c:29ff:fe68:1fef%11
IPv6 DNS Server	

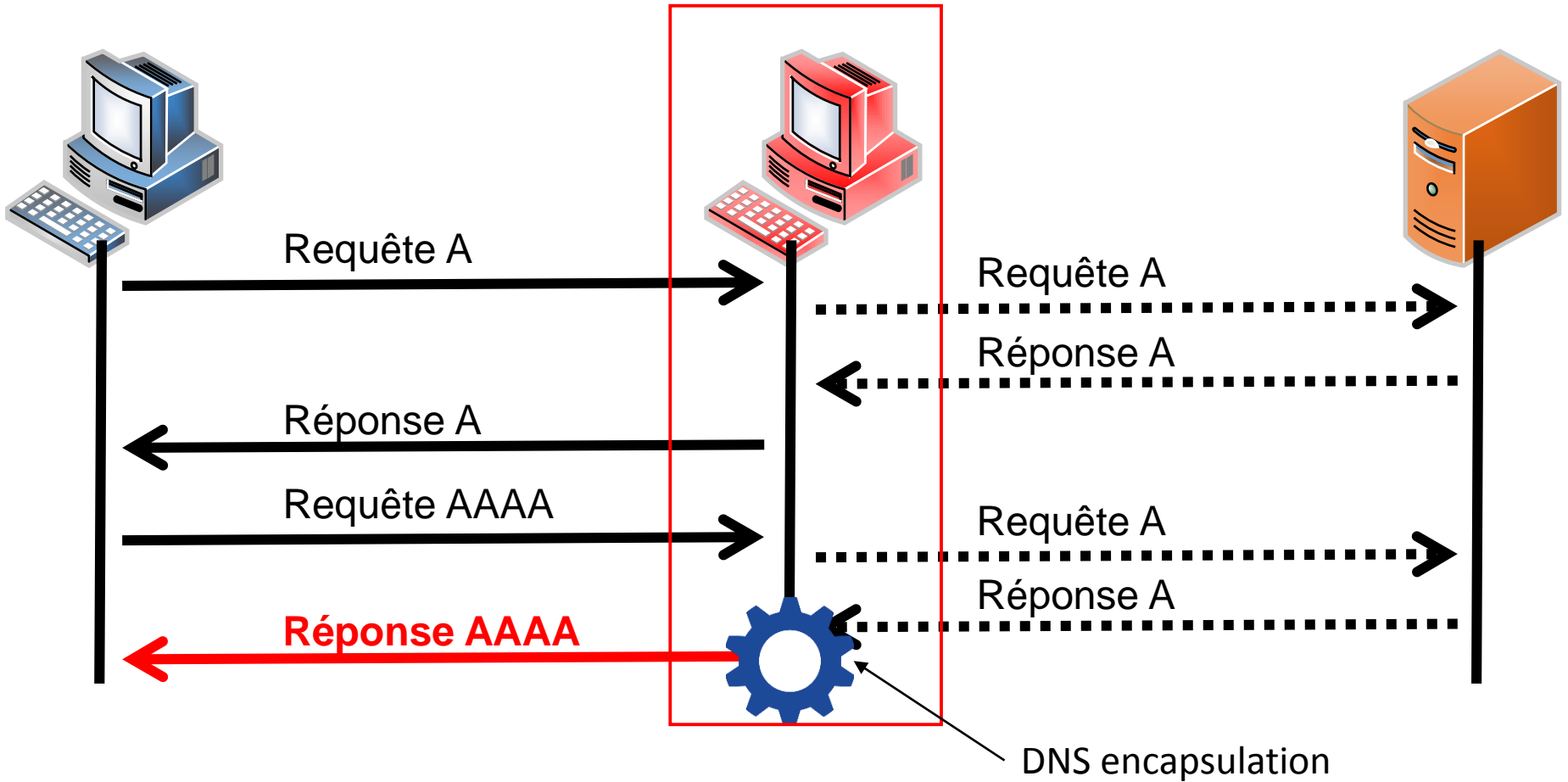
Close

# SLAAC Attack | Configuration



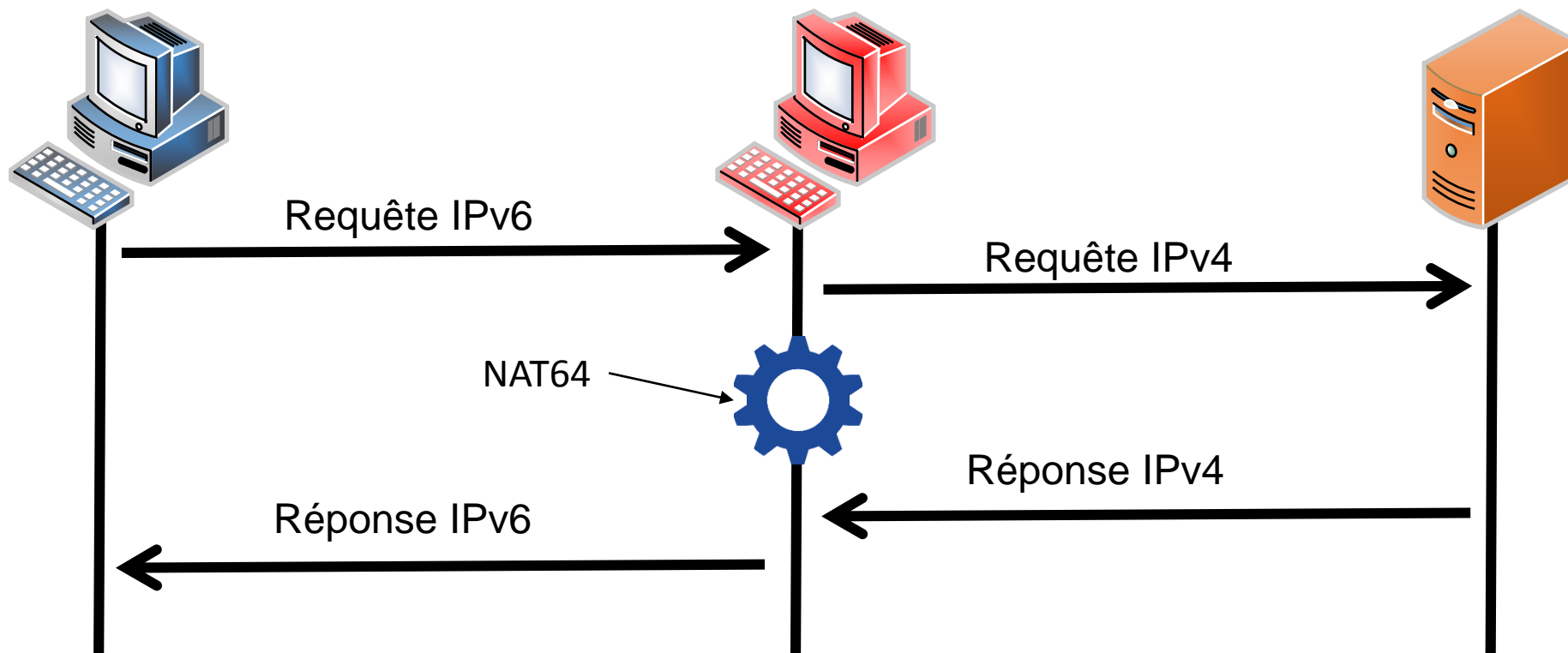


# SLAAC Attack | Name resolution



8	16	24	32	40	48	56	64	72	80	88	96	104	112	120	128
Préfixe IPv6												IPv4			

# SLAAC Attack | Network flow



# SLAAC Attack | State of the art

## [Suddensix]

Bash script pour automatisation installation + configuration  
Utilisation de paquets + protocole NAT-PT obsolètes

## [Evil FOCA]

Outil complet (multiples attaques IPv4 & IPv6)  
Windows

# SLAAC Attack | Wrap-up

## [Avantages]

Peu de paquets nécessaires au maintien de l'attaque

Contrôle du flux et du DNS

Sélection des victimes

Moins de protection IPv6 sur réseau IPv4

## [Inconvénient]

Mise en œuvre de l'attaque fastidieuse

**=> Création d'un outil pyMITM6 <=**

# pyMITM6 | Introduction

## [Développement]

- Python 2.x
- Licence GPLv2
- Utilisation des librairies standards => pas de dépendances

## [Modules]

- Interface
- Configuration
- Résolution de noms
- Traduction d'adresses

# pyMITM6 | Interface

```
[F] pyMITM6 - Target Selection
-----
IPv6 Targets                               Selected
fe80::8bf:40f2:74a9:7f8e                   [ ]
[I] fe80::5864:fa53:2369:99dc                [x]
fe80::e:edbc:83e0:42d4                     [ ]
fe80::ea06:88ff:fe95:f337                 [ ]
fe80::8a32:9bff:fe6c:7d3c                 [ ]
fe80::867a:88ff:fe7b:f5f8                 [ ]
```

# pyMITM6 | Configuration

## [Fonctionnalités]

- Configuration IPv6 de la victime
  - Emission de RA périodiquement
  - Emission de RA en réponse au RS
- Configuration du serveur DNS via DHCPv6 (Info requ.)

## [Implémentation]

- Sockets IPv6/raw

## [Prérequis]

- Préfixe IPv6 (config)
- Adresse IPv6 du Serveur DNS

# pyMITM6 | Name resolution

## [Fonctionnalités]

- Interception requêtes A et AAAA
- Interrogation serveur réel IPv4 ou du cache (requête A)
- Modification pour les réponses AAAA

## [Implémentation]

- Librairie python dnslib
- Socket IPv6/udp

8	16	24	32	40	48	56	64	72	80	88	96	104	112	120	128
Préfixe IPv6												IPv4			

## [Prérequis]

- Préfixe IPv6 (différent de celui de Configuration)



# pyMITM6 | Network Address Translation

## [Fonctionnalités]

- Traduction des adresses IPv6 en IPv4 (vice-versa)

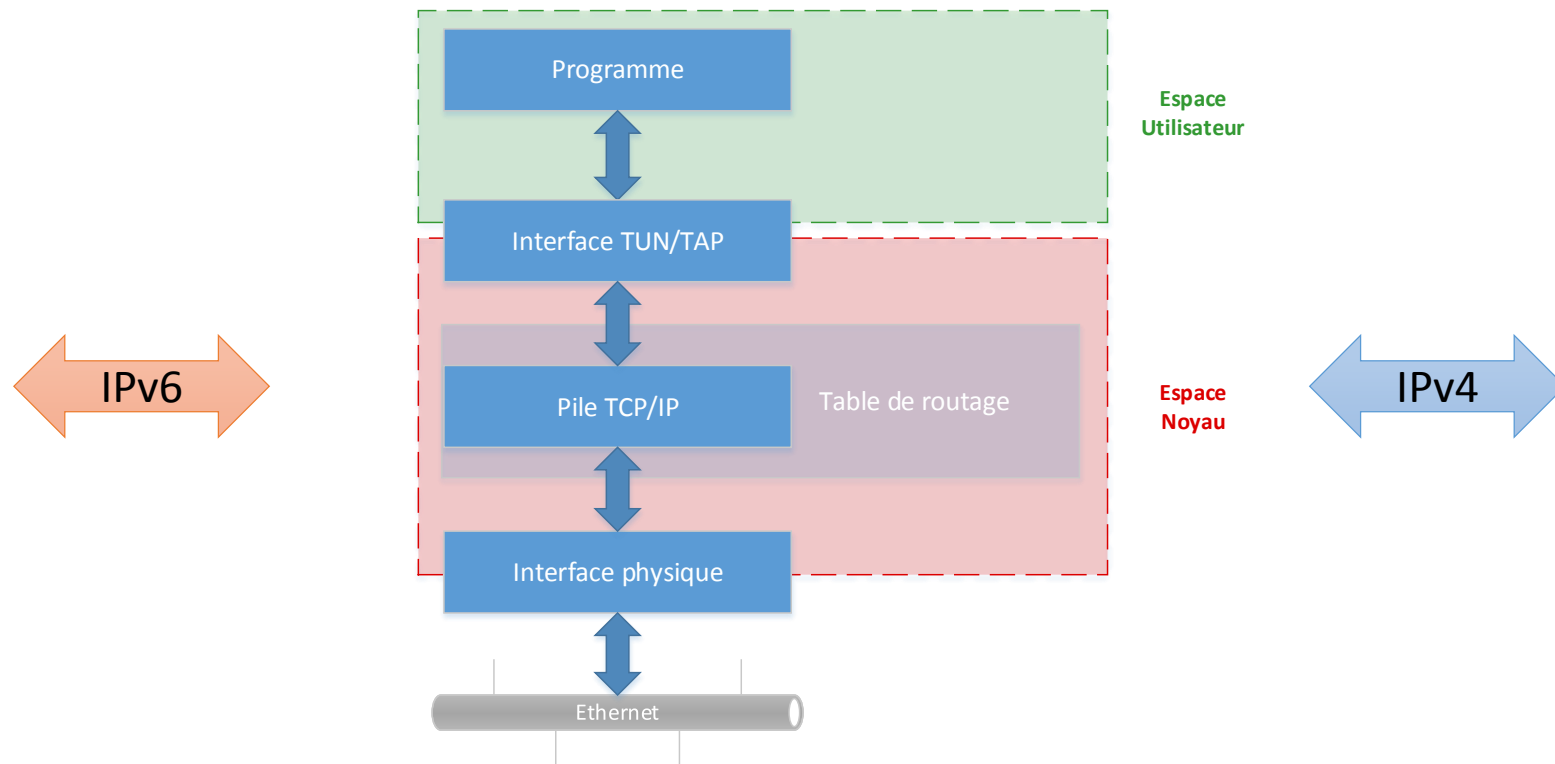
## [Implémentation]

- Algorithme SIIT [RFC 2765] (NAT64)
- Routage (linux)
- Interface TUN
- Source NAT (iptables)

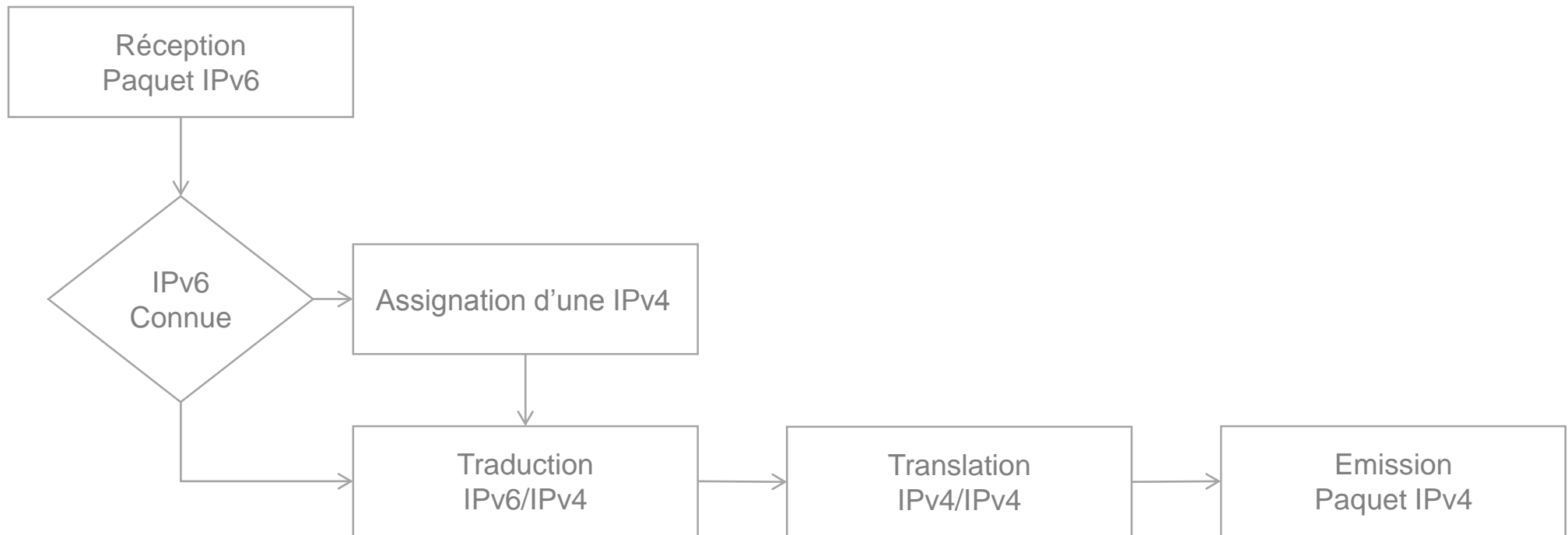
## [Prérequis]

- Plage d'adresses IPv4 (fonctionnement interne)

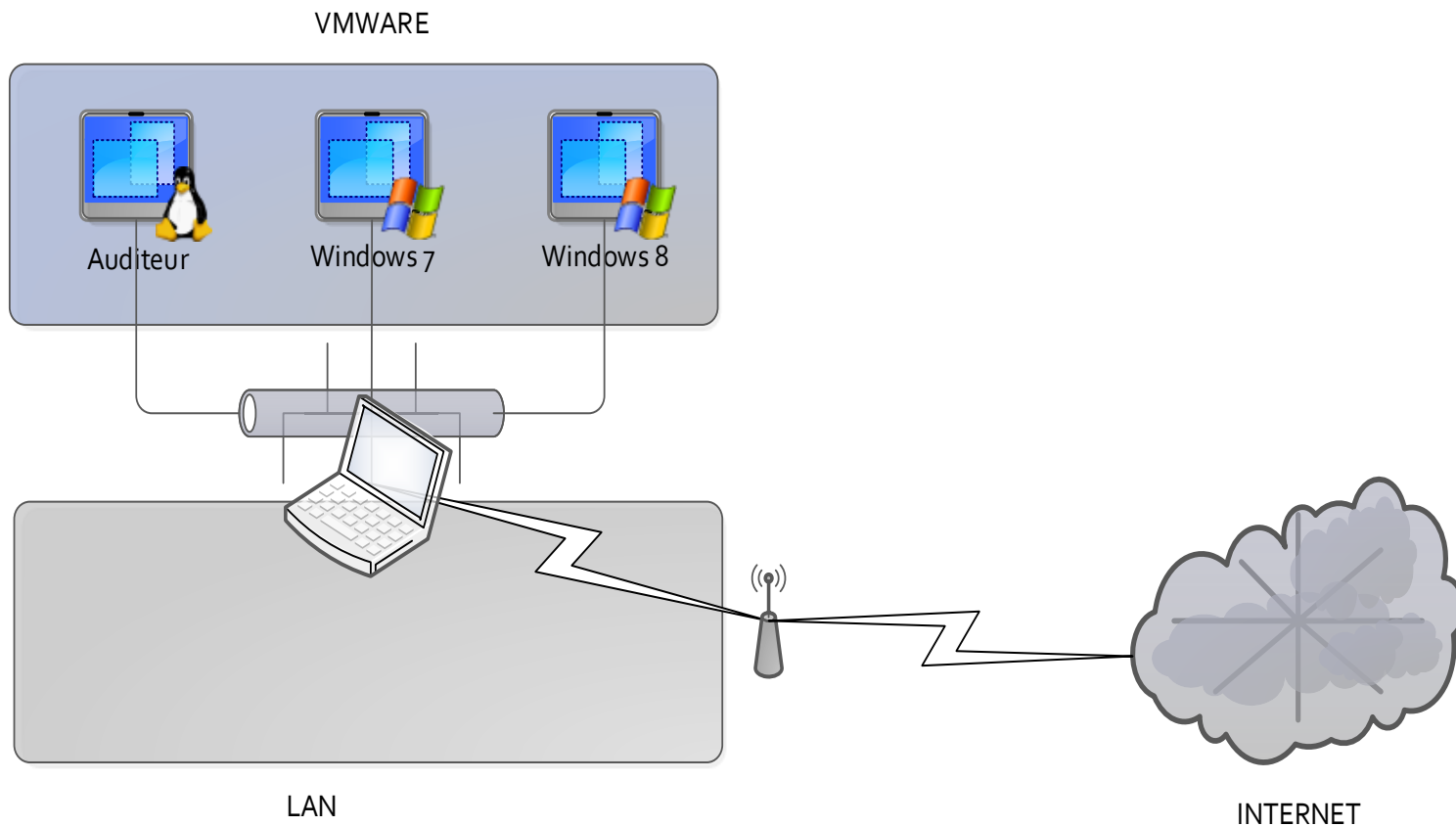
# pyMITM6 | Traduction d'adresses



# pyMITM6 | Traduction d'adresses



# pyMITM6 | Demo



# pyMITM6 | Limitations

Contournement des protections (RA Guard)

Améliorer l'implémentation DHCPv6 (Windows Server 2k12)

Interface graphique

WPAD (proxy)

# Protections

Désactivation de la pile IPv6

IPv6 Router Advertisement Guard [RFC 6105]

Monitoring NDP ( NDPMon )

# Conclusion

Attaque alternative à ARP Spoofing

Contrôle du flux réseau

Contrôle de la résolution de noms

Fallback en IPv4 automatique

Protection peu/pas implémentée

# Merci

[em@il]  
[twitter]

karim@scrt.ch  
@8008135\_