

# Routing Loop Attacks using IPv6 Tunnels

Gabi Nakibly & Michael Arov

National EW Research & Simulation Center

Rafael - Advanced Defense Systems

*[gabin@rafael.co.il](mailto:gabin@rafael.co.il)*

# Introductions

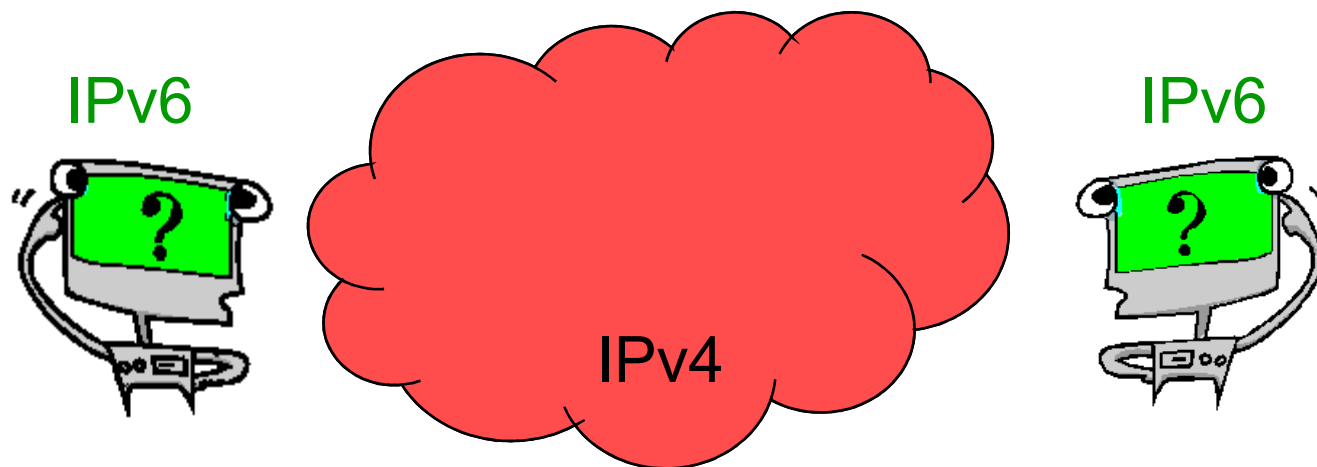
- National EW Research & Simulation Center
  - Provides research and analysis services on all things related to electronic warfare.
    - including computer security
  - Funded mostly by the government
- Rafael - Advanced Defense Systems Ltd.
  - Develops and manufactures hi-tech defense systems
  - Around 1.5B\$ of annual sales worldwide

# Overview

- Automatic IPv6 tunnels are an essential part of any migration plan to IPv6.
  - 6to4, ISATAP and Teredo
- These tunnels introduce an overlay routing state.
  - With no explicit configuration changes
- This can be abused to create routing loops → DoS!
  - We exhibit five such attacks.
- These attacks exploit the very design of the tunnels.
  - All IPv6 implementations are potentially vulnerable!
- All attacks were tested and validated on Windows machines.

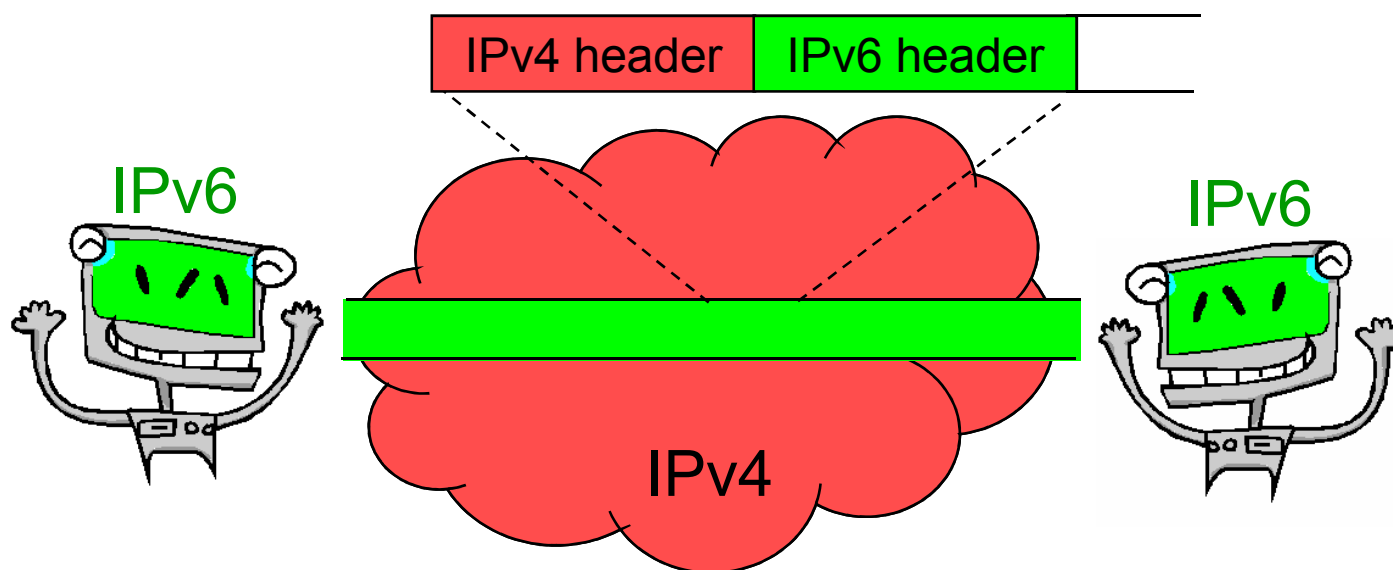
# IPv6 Migration Problem

- No overnight migration.
  - IPv6 is NOT backward compatible with IPv4.
- How IPv6 hosts can talk over a network that hasn't been migrated yet?



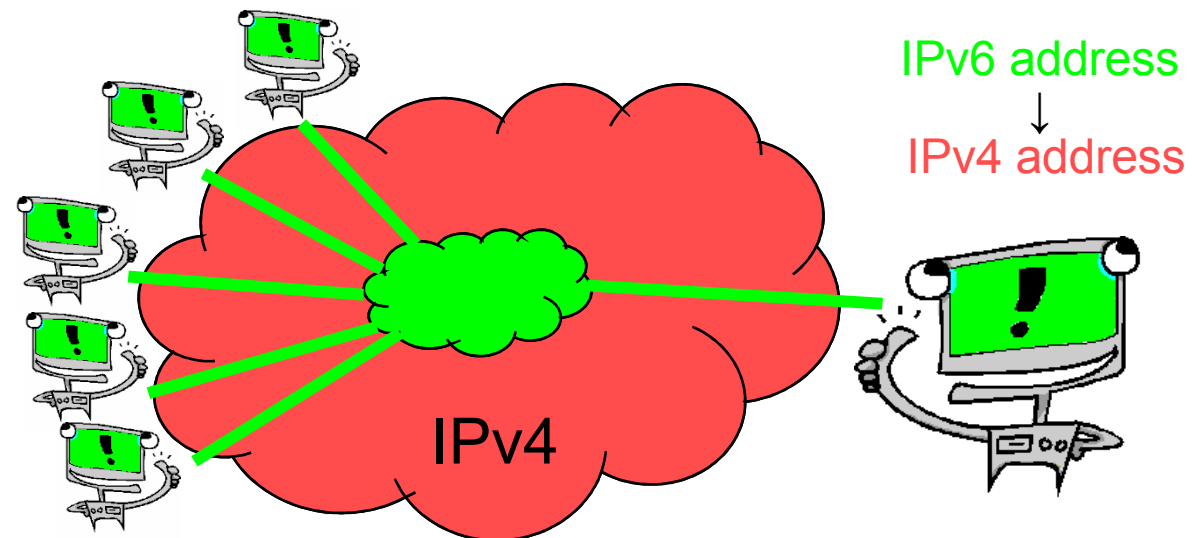
# The Solution: Tunnels

- The IPv6 packets are sent encapsulated with IPv4 header.
- However,
  - each end point must know it's peer's IPv4 address
  - all end points must be explicitly configured...



# Automatic Tunnels

- The IPv6 address is chosen so that the IPv4 address can be extracted from it.
- One can join and leave the tunnel without reconfiguring the other peers.

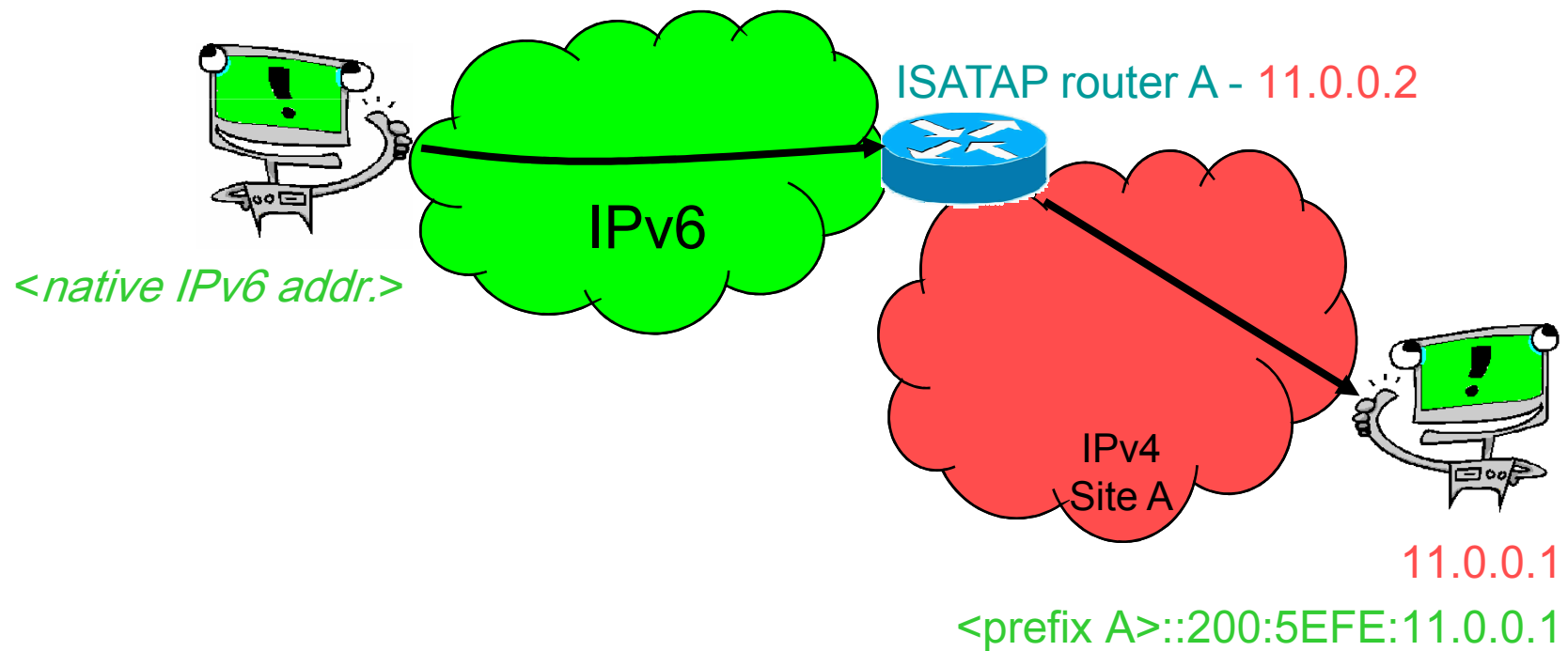


# ISATAP

- Intra-Site Automatic Tunnel Addressing Protocol [RFC 5214]
- Used to connect IPv6 hosts over an IPv4 site
- Supported by all major OSs
- Address format:
  - *< tunnel prefix >:0200:5EFE:< IPv4 address >*
  - Example: 2001:DB8::0200:5EFE:11.0.0.1

# ISATAP

11.0.0.2	<native IPv6 addr.>
→	→
11.0.0.1	<prefix A>::200:5EFE:11.0.0.1

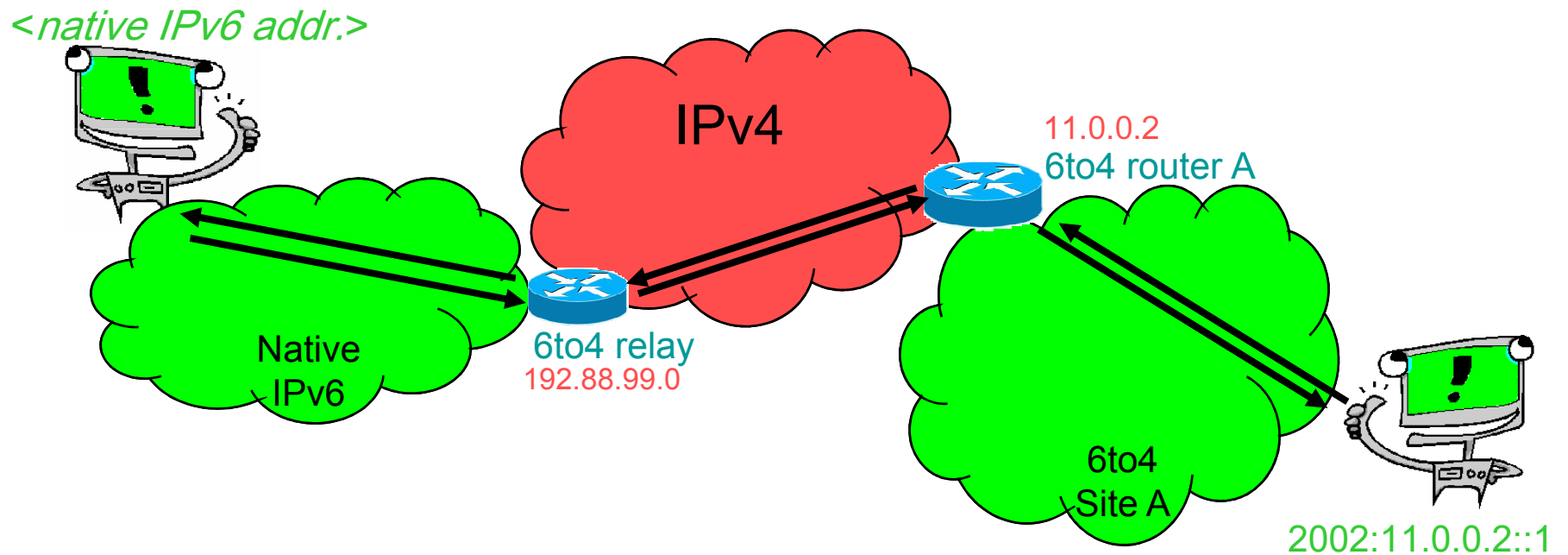
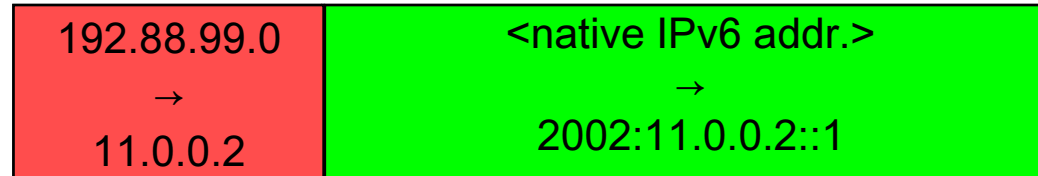




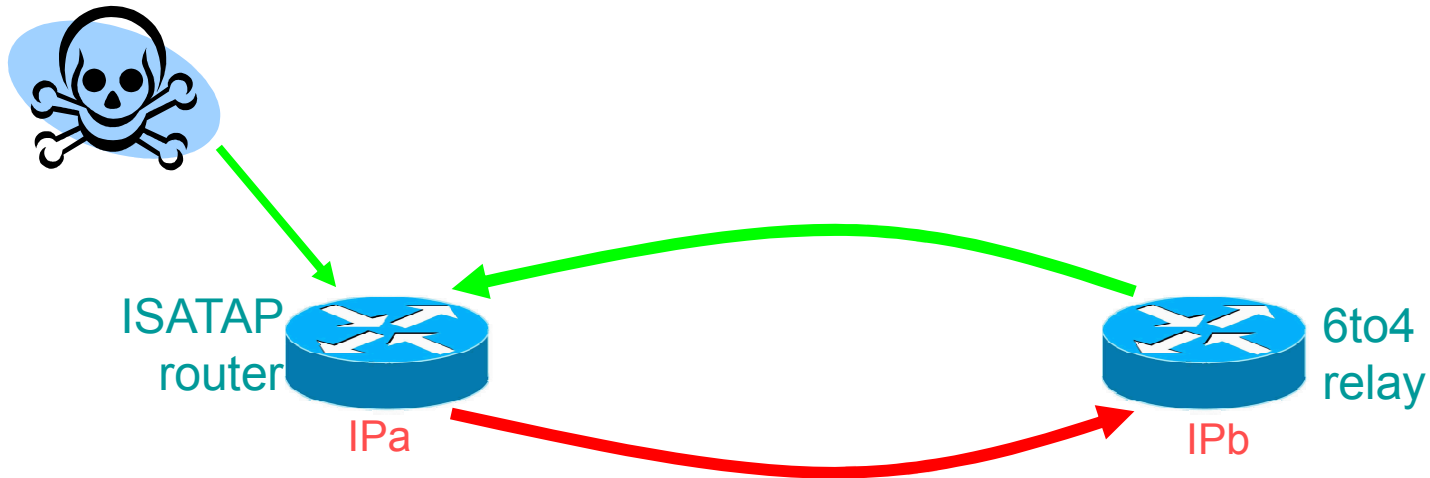
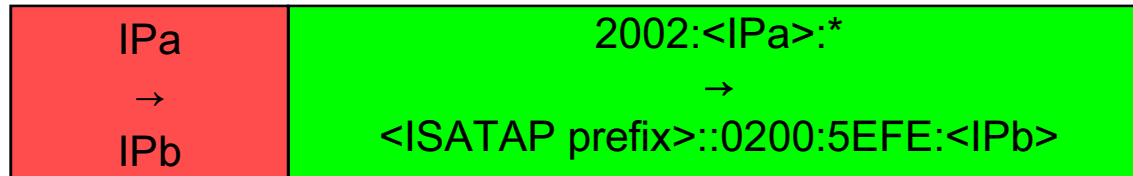
# 6to4

- Connects IPv6 sites over IPv4 Internet [RFC 3056]
- Supported by all major OSs
- IPv6 address prefix given to a site:
  - $2002:<IPv4\ address>::/48$ 
    - Where *<IPv4 address>* is the address of the site's border router.
  - Example:  $11.0.0.1 \rightarrow 2002:11.0.0.1::/48$

# 6to4




# Attack #1: ISATAP Router & 6to4 Relay



# Teredo

- A tunnel that is meant to connect hosts behind IPv4 NATs [RFC4380].

- Encapsulation: 

- Enabled by default on Vista.

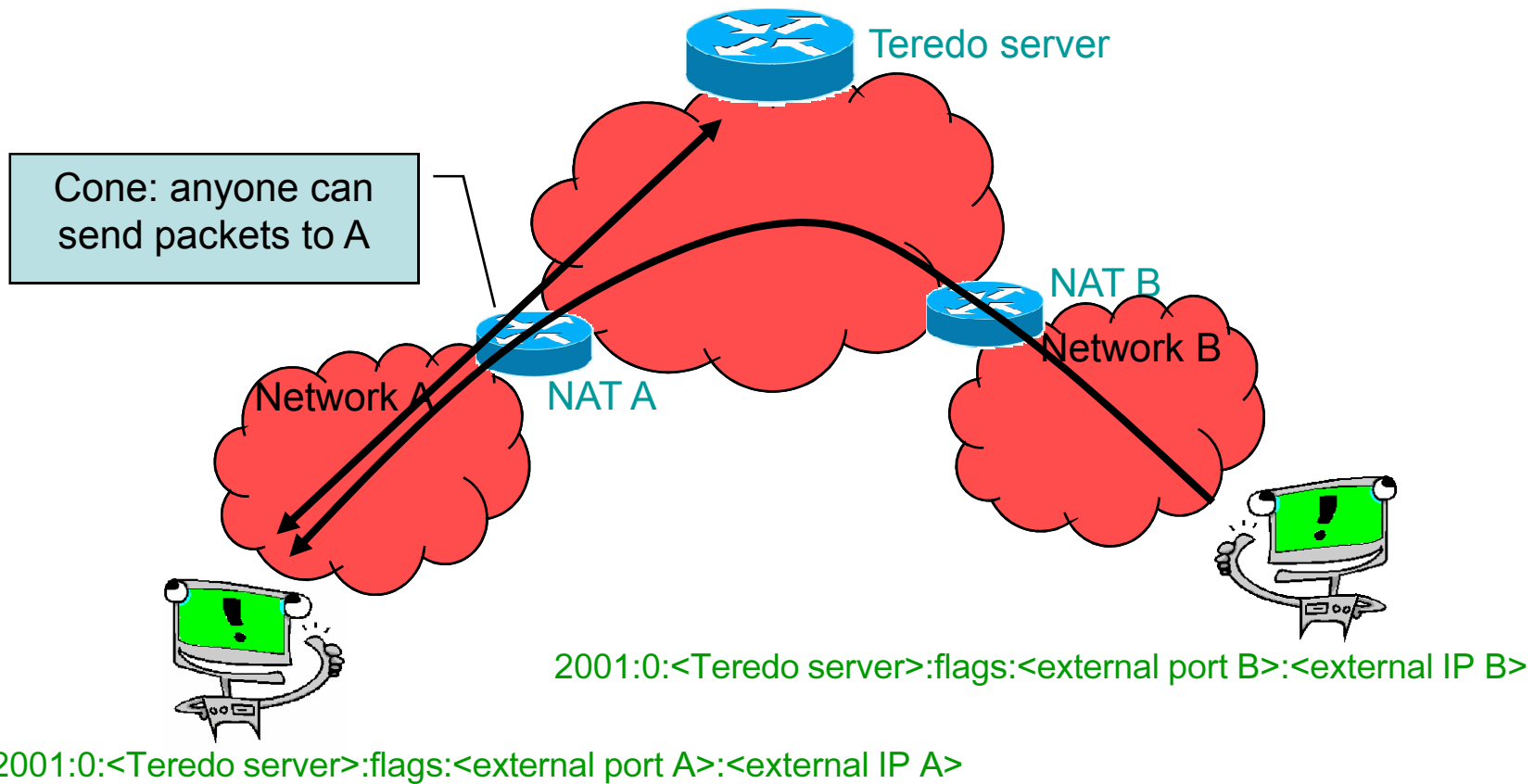
- Address format:

- 2001:0:0:0:Flags:0:0:0:0

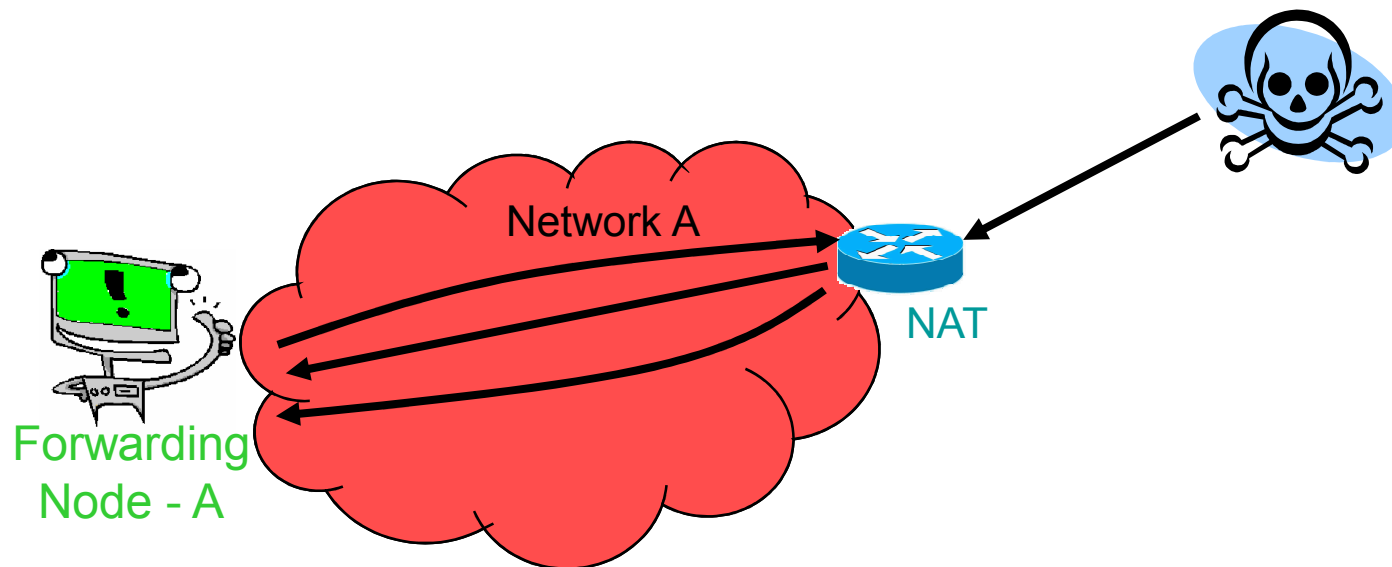
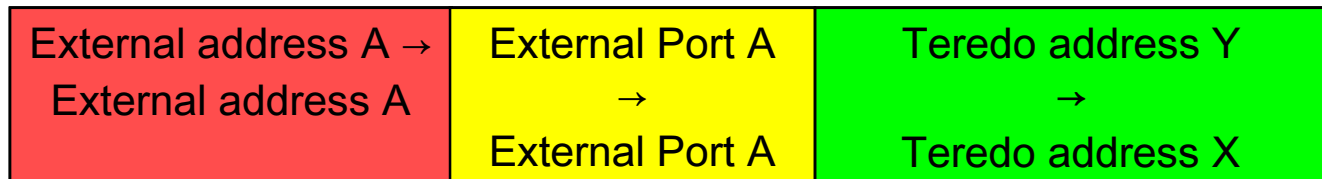
Teredo Server
Ext. Client
Ext. Client  
IPv4 address
UDP port
IPv4 address

# Teredo

Internal address B → External address A	Internal port B → External port A	Teredo address B → Teredo address A
---	---	---



# Attack #2: Forwarding node & NAT



We define two bogus Teredo addresses (that do NOT belong to A):

Teredo address X - 2001:0:XXXX:flags:<ext. port A>:<ext. IP A>

Teredo address Y - 2001:0:YYYY:flags:<ext. port A>:<ext. IP A>

Assumptions about the NAT:

- Cone
- Supports hair-pin routing with source translation

# Other Attacks in the Paper

- We present two other attacks that follow the same lines as the first one
  - ISATAP router and 6to4 relay swap roles
  - Two ISATAP routers
- We present an infinite self loop attack on a Teredo server
  - Using a crafted Teredo bubble

# Applicability

- All attacks use spoofed packets, hence may be foiled by:
  - egress filtering at the attacker's network
  - uRPF
- Attacks that involve ISATAP will fail when protocol-41 filtering at the site's border is employed.



# Mitigation Measures

- The attacks can be fully mitigated by addressing their root cause:
  - Forwarding out an IPv6 packet that is routed back to an IPv4 interface via a tunnel.
- Hence the following check must be employed:
  - A local IPv4 address must not be embedded in the IPv6 destination address.
  - This check must correspond to all the tunnels' address formats.

# Conclusions

- The migration to IPv6 must employ automatic IPv6 tunnels
  - These tunnels introduce overlay routing state.
- An attacker can exploit inconsistencies in the routing states to introduce routing loops.
- These are vulnerabilities in the standard and they must be mitigated by it.