IPv6 Neighbor Discovery (RFC 4861) Man-in-the-middle Protection

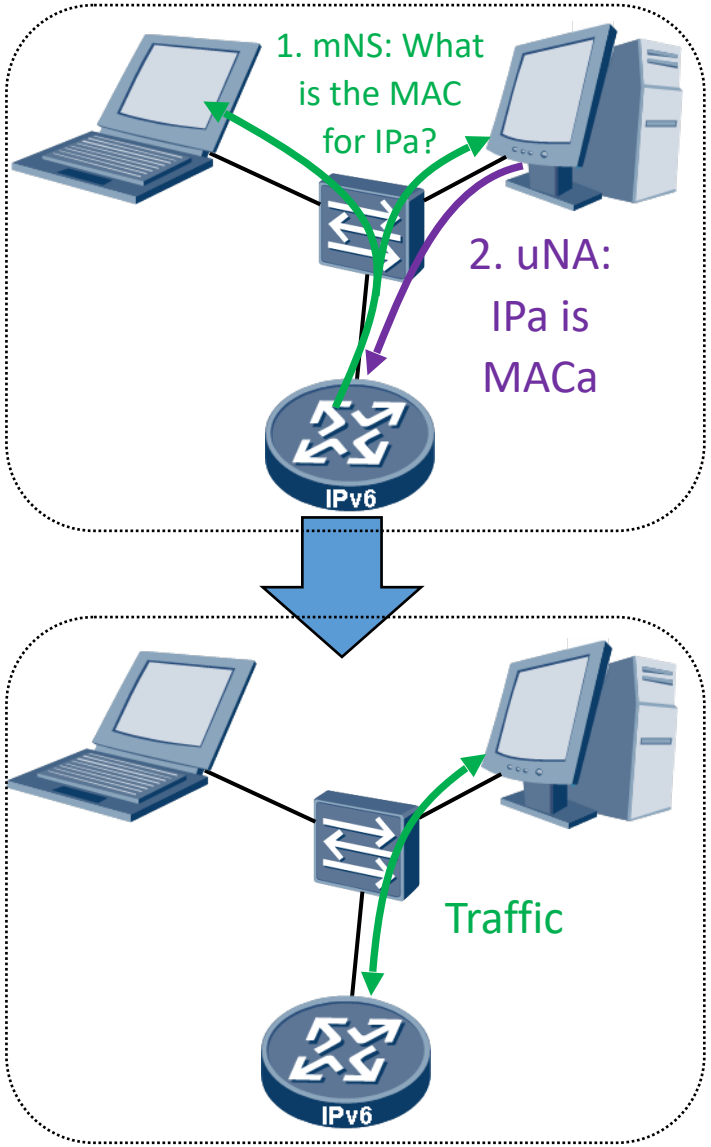
draft-vasilenko-6man-ND-MITM-protection

Eduard Vasilenko vasilenko.eduard@huawei.com

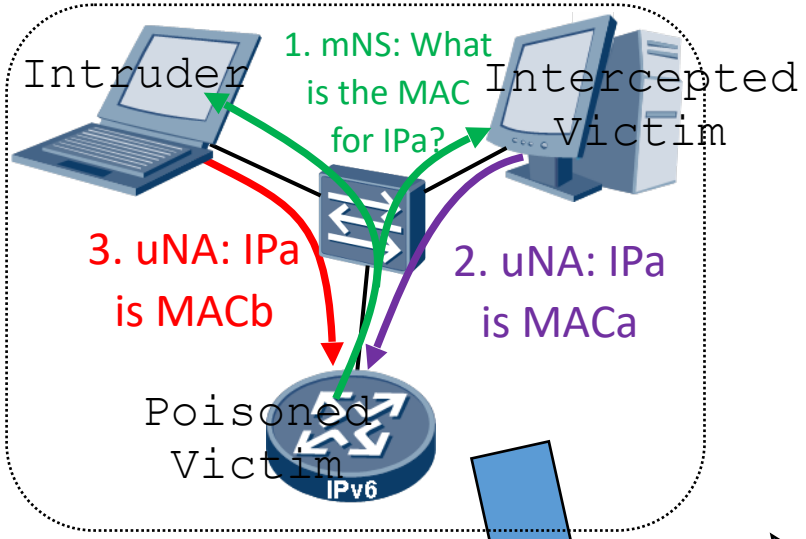
XiPeng Xiao xipengxiao@huawei.com

The Problem Statement: ND MITM (1)

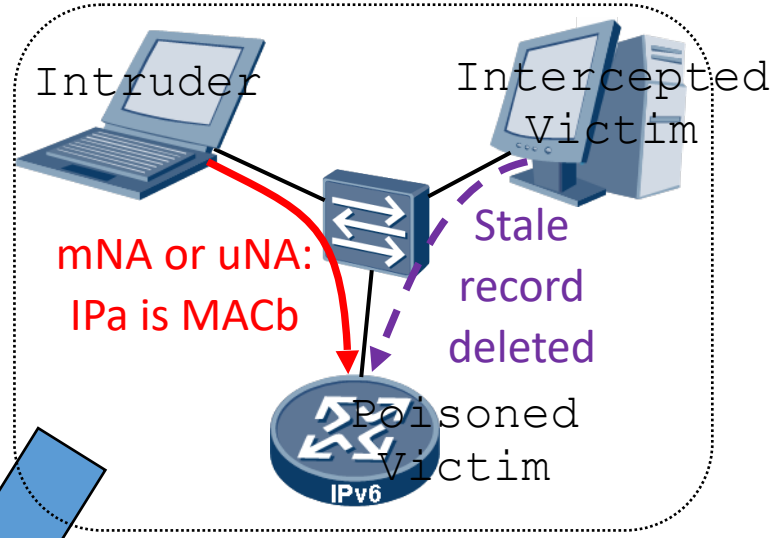
By Design (RFC 4861/2)

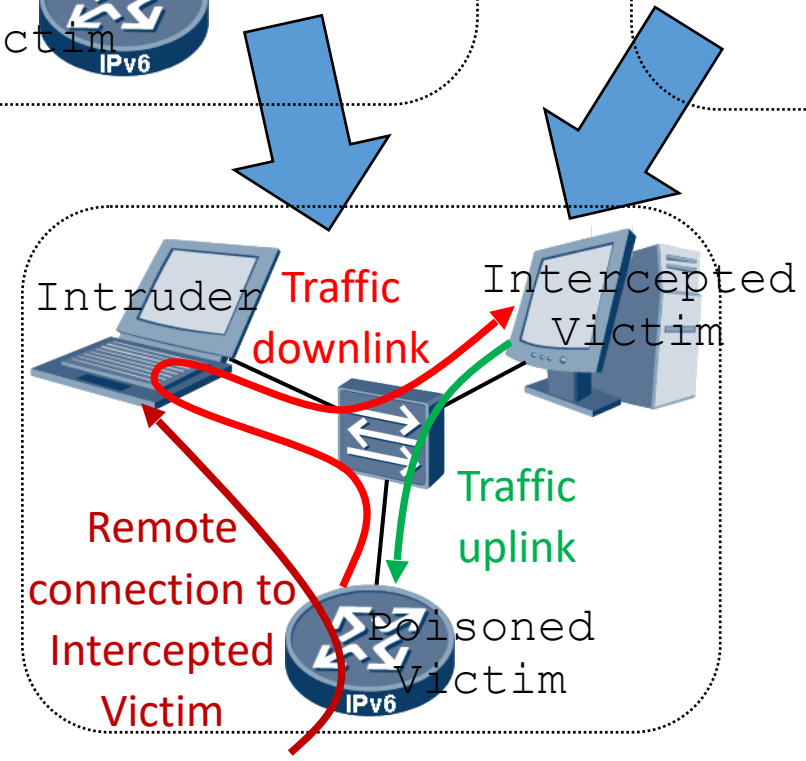


Attack in basic ND



Attack in GRAND environment

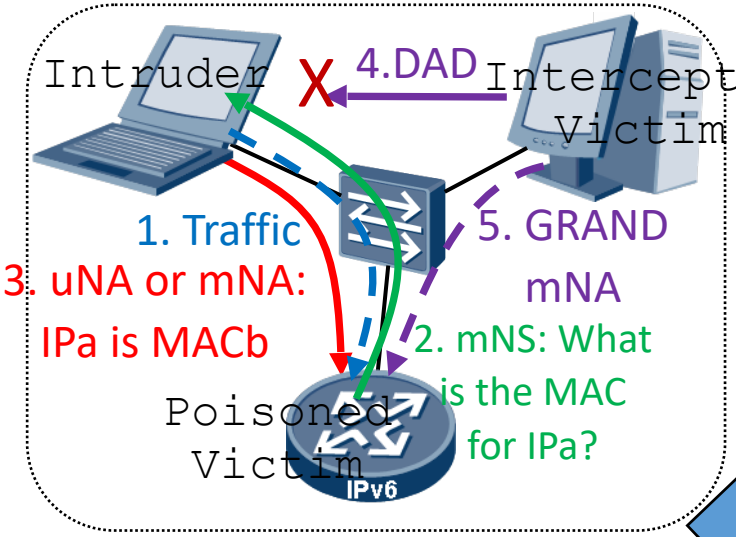




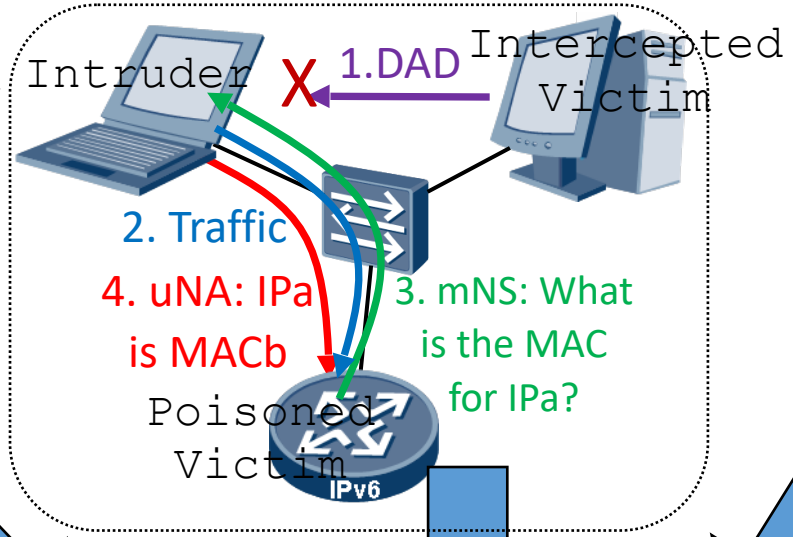
Problem statement:
When the Poisoned Victim would receive the IPa/ MACb association, it should check for duplicity of IPa by doing multicast.
This way, the Poisoned Victim has the opportunity to discover duplicity

The Problem Statement: ND MITM (2)

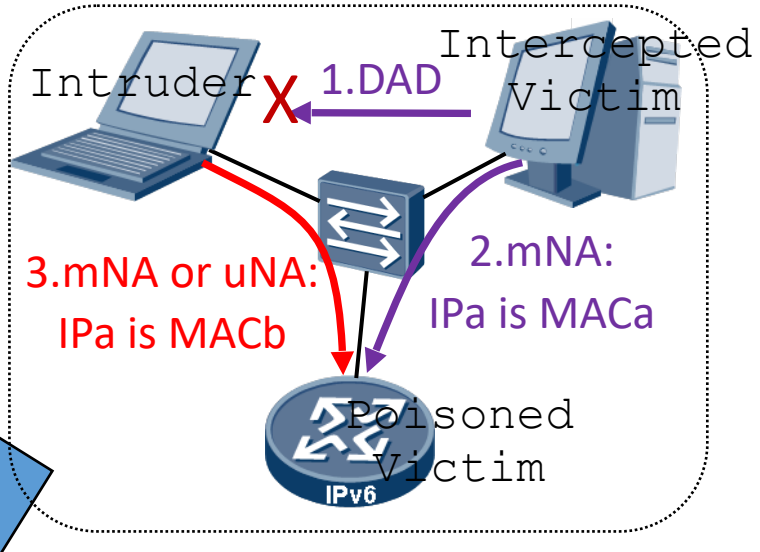
Attack: Be the 1st



Attack: start race by traffic

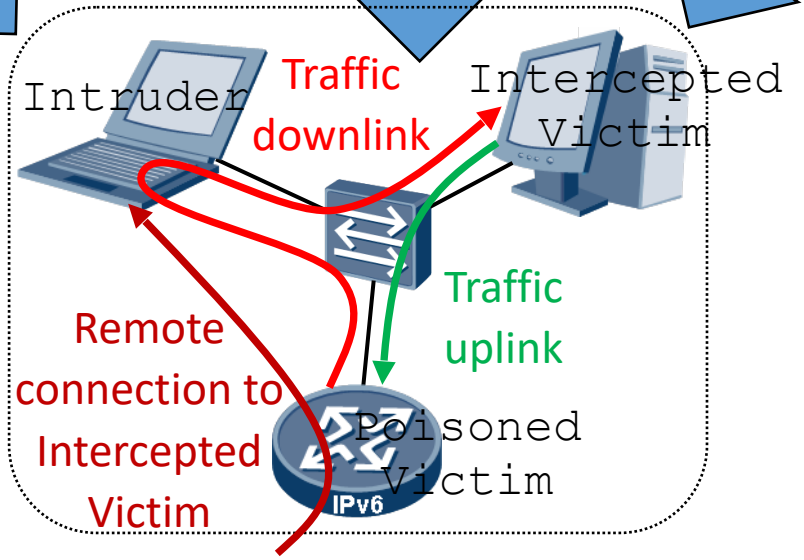


Attack: start race by uNA (GRAND environment)



2 cases are possible for this attack:

- Basic ND environment – cache record initialized by traffic
- GRAND environment – cache record could be initialized by traffic, multicast or unicast NA

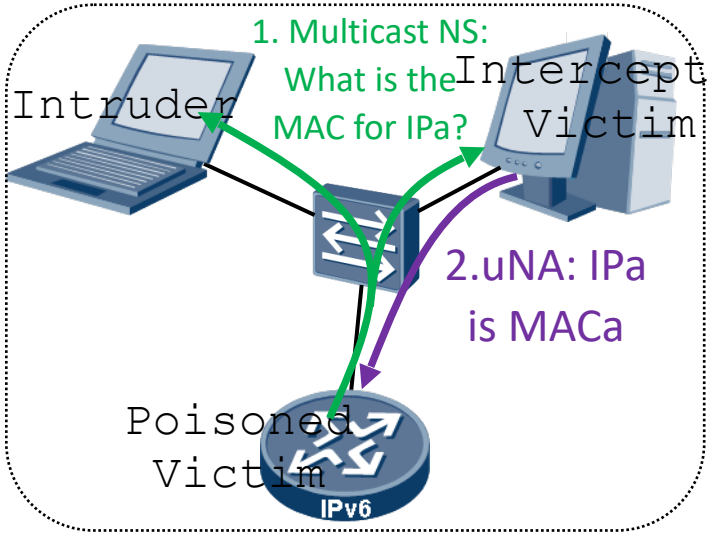


Race Attacks have some special characteristics:

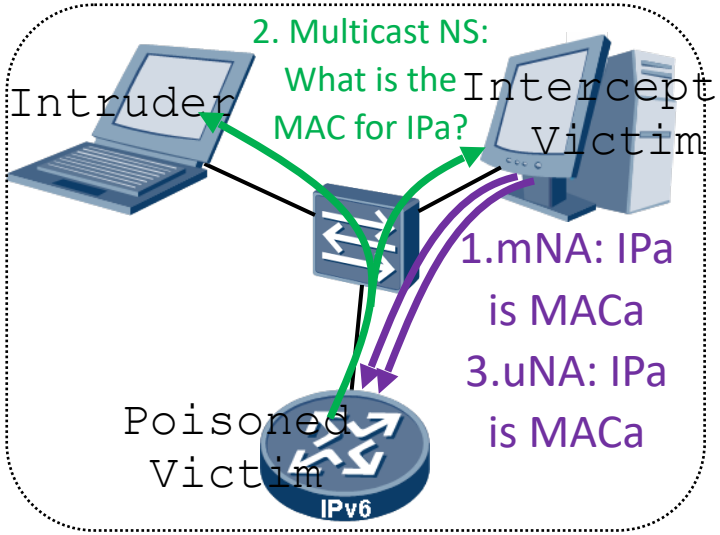
- should be finished inside RetransTimer (1sec is the plenty of time)
- prevent us from the possibility to inform Intercepted Victim to release the IP address – we have to block both

ND MITM Protection

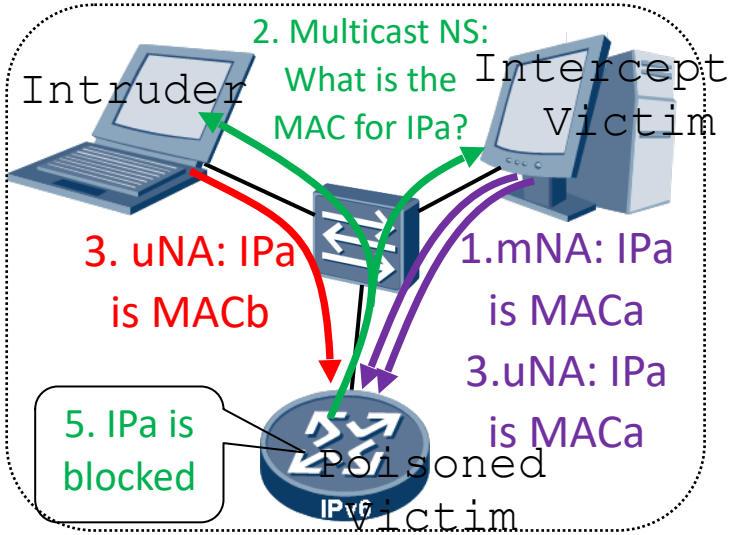
Basic ND √



GRAND environment √



Intruder in GRAND √



- Link Layer Address rewrite or initial write for any neighbor cache entry MUST be only as a result of *multicast* Neighbor Solicitation
- ”Security DAD” is mandatory: it SHALL be checked that not more than expected number of NA replies have been received in the response to *multicast* NS. It means for the majority of environments (default Duplicity_Level): not more than 1 reply

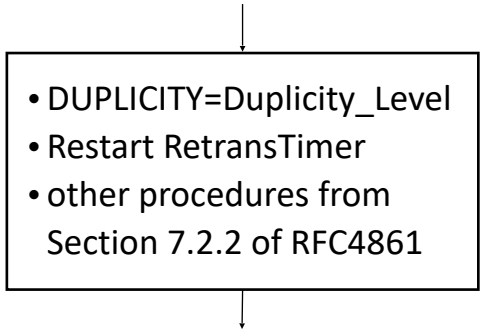
- ✓ Minimal changes to ND protocol
- ✓ Compatibility to all ND extensions published
- ✓ No need for additional functionality on layer 2 (switch)
- ✓ Anycast support (expected level of duplicate addresses)
- ✓ Active-standby clustering support (including VRRP)
- ✓ Could be introduced in production on any nodes ad-hoc
- × Depending on a scenario lead to 0%-100% multicast traffic increase, with the tendency to 0%

Examples on this slide is to analyze multicast impact, not to show how all Attacks are blocked

ND Extension Details

- DUPLICATE state - Target address has been put into dampening state for the time defined by Duplicate Timer, because SDAD (additional security check) has found duplicate address. Neighbor cache entry MUST not be used for traffic forwarding, all NS and NA for this target address SHALL be ignored. DUPLICATE entry SHOULD be deleted after Duplicate Timer expiration
- Duplicate Timer – measured in seconds, dampening time for duplicate IP address discovered by SDAD procedure. It SHOULD be copied from “Reachable Time” advertised by router (on router itself it is known as AdvReachableTime – section 6.2.1 of RFC4861)
- Duplicity_Level – number of NA responses that is accepted as legitimate for multicast NS solicitation. It permits to properly handle anycast addresses present on the link if maximum number of anycast addresses is known in advance. The node MUST have capability to provision Duplicity_Level on per-link granularity. 32-bit unsigned integer SHOULD be reserved for this counter

Sending NS –
Section 7.2.2 of RFC4861:



Receipt NA –
Section 7.2.5 of RFC4861: