OLD VULNERABILITIES IN NEW PROTOCOLS? HEADACHES ABOUT IPV6 FRAGMENTS

Eric Vyncke (@evyncke)
Cisco

RSA CONFERENCE EUROPE 2013

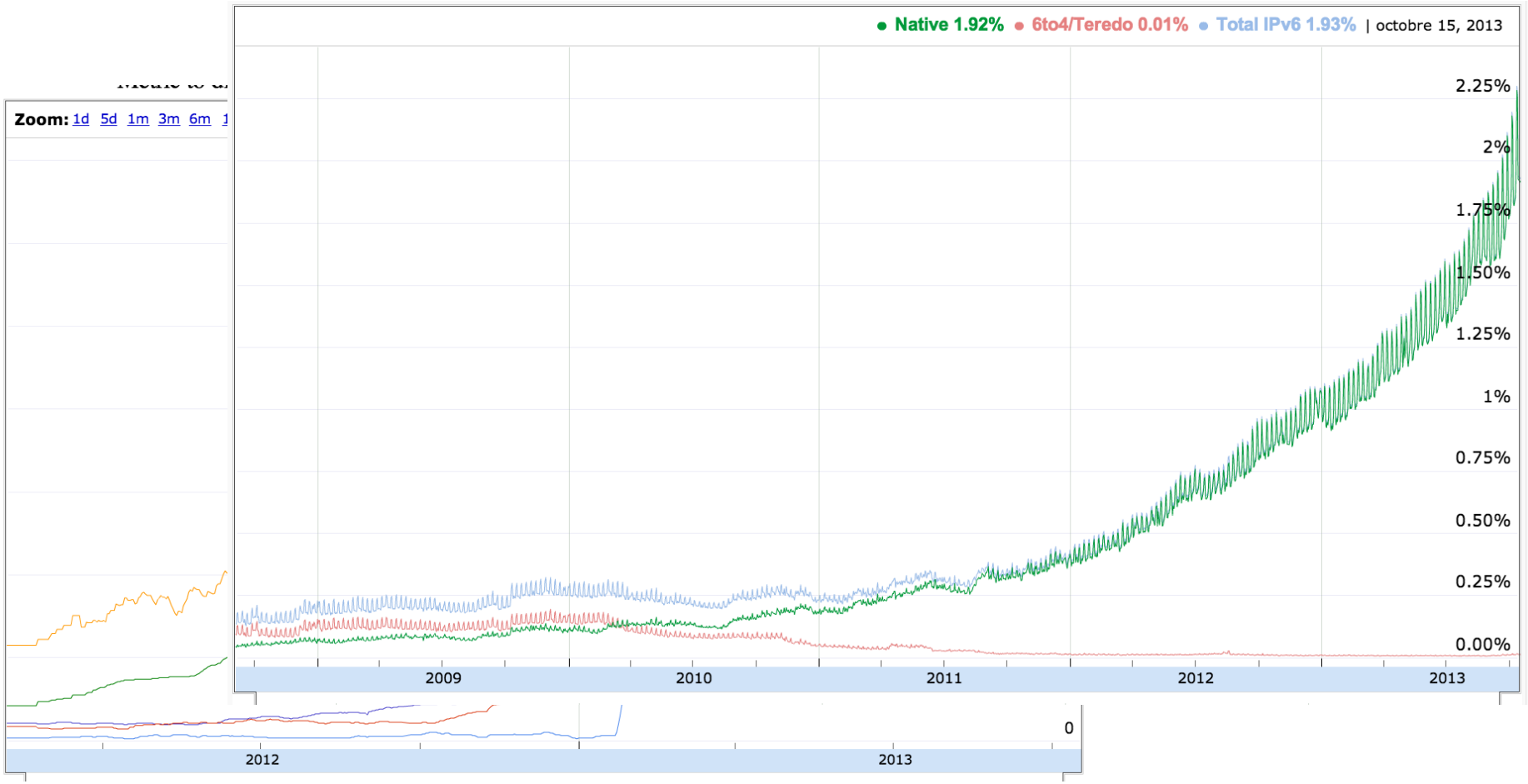
Session ID: ARCH W01

Session Classification: Advanced

Agenda

- Status of WorldWide IPv6 Deployment
- IPv6 refresher: extension headers and fragmentation
- Processing IPv6 extension headers
- “Hacking” with fragmentation and mitigation techniques

IPv6 is Here to Stay



Sources: http://www.google.com/ipv6/statistics.html & http://vyncke.org/ipv6status and http://6lab.cisco.com

IPv6 Refresher

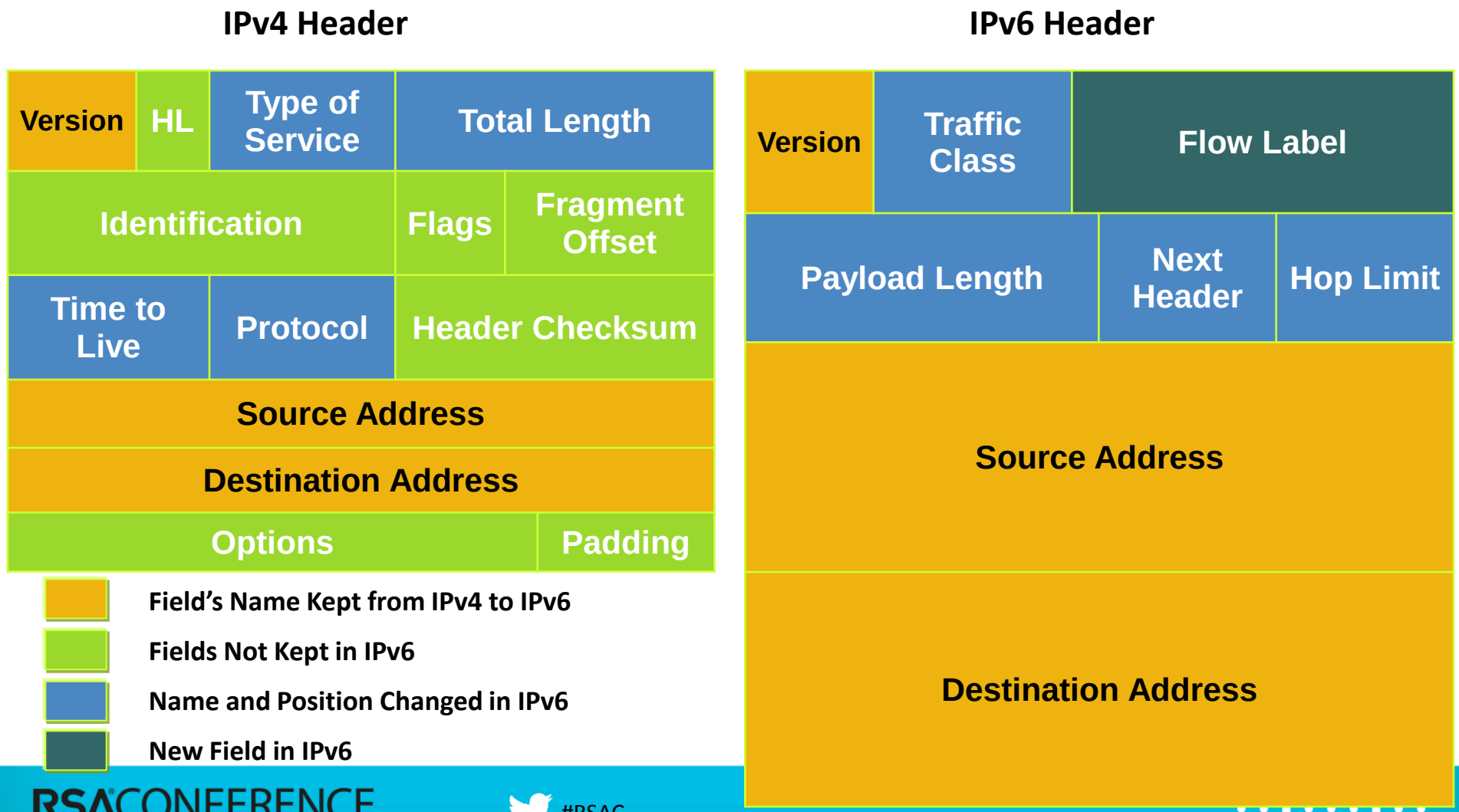
#RSAC

RSA CONFERENCE EUROPE 2013

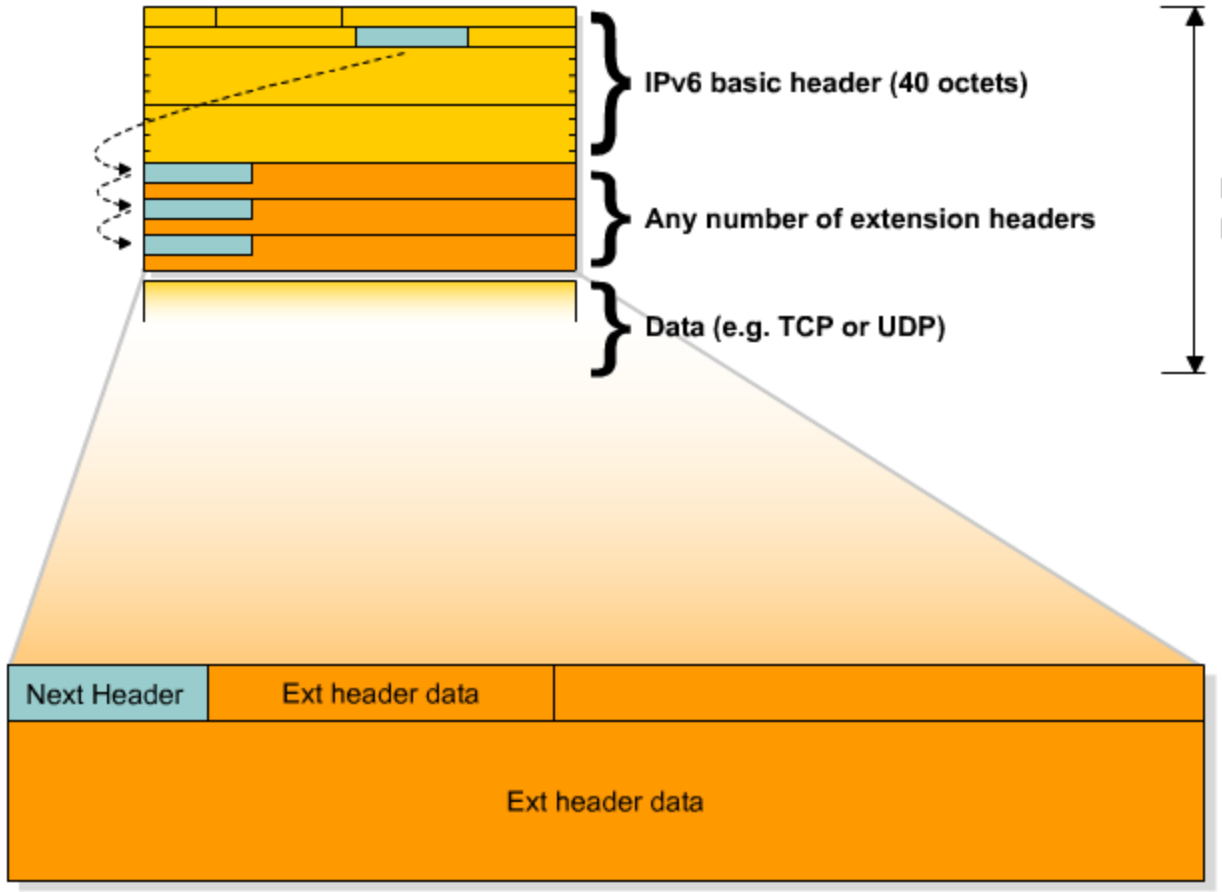
IPv6 in One Slide

- IPv6 is IPv4 with larger addresses
  - 128 bits vs. 32 bits
  - **NAT no more needed => easier for applications**
    - **Simpler hence more security**
- Data-link layer unchanged: Ethernet, xDSL, …
- Transport layer unchanged: UDP, TCP, …
- Applications "unchanged": HTTP, SSL, SMTP, …
- IPv6 is not really BETTER than IPv4 because it is 'new'
  - IPv6 has been specified in 1995…
  - IPsec is identical in IPv4 & IPv6
  - **Only benefit is a much larger address space**

IPv4 and IPv6 Header Comparison



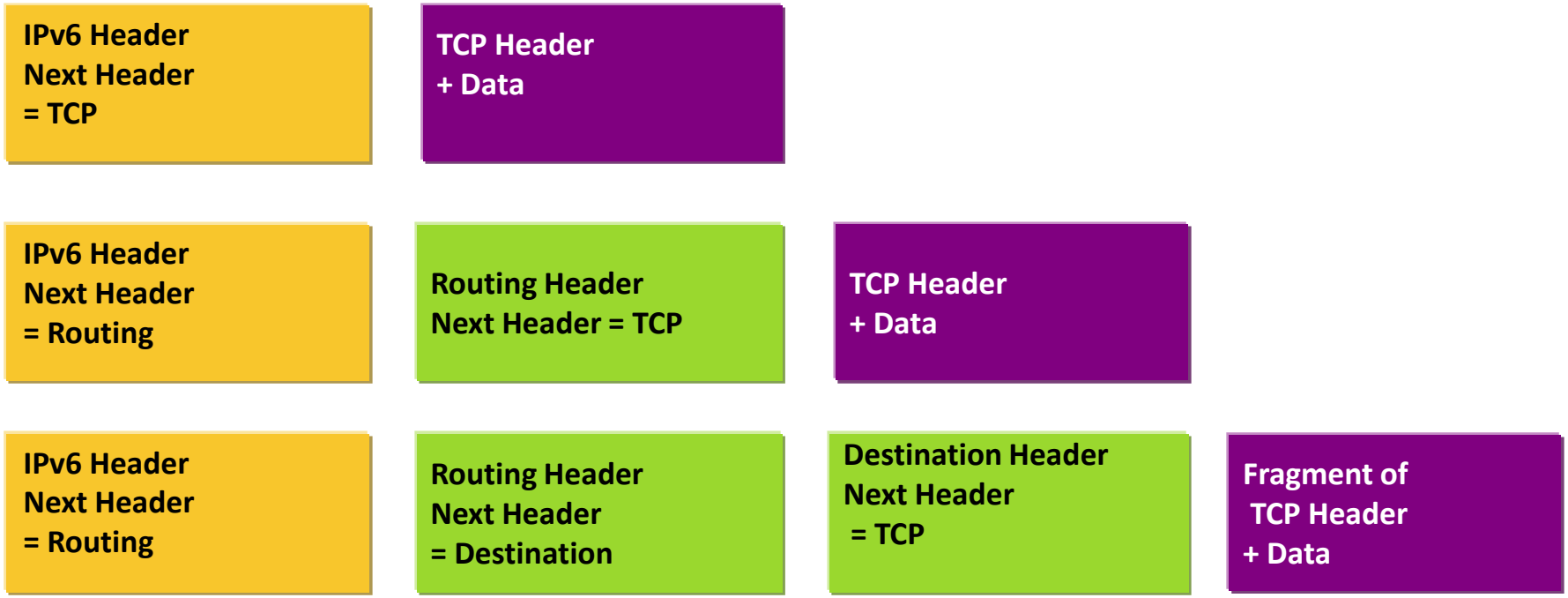
Extension Headers (RFC2460)



- Processed only by node identified in IPv6 Destination Address field => much lower overhead than IPv4 options
  - exception: Hop-by-Hop Options header
- Eliminated IPv4's 40-octet limit on options
  - In IPv6, limit is total packet size, or Path MTU in some cases

Extension Headers

- Extension headers are daisy chained



IPv6 Attacks with Strong IPv4 Similarities

Good news
IPv4 IPS signatures can be re-used

- Application layer attacks
  - The majority of vulnerabilities on the Internet today are at the application layer, something that IPSec will do nothing to prevent
- Rogue devices
  - Rogue devices will be as easy to insert into an IPv6 network as in IPv4
- Man-in-the-Middle Attacks (MITM)
  - Without strong mutual authentication, any attacks utilizing MITM will have the same likelihood in IPv6 as in IPv4
- Flooding
  - Flooding attacks are identical between IPv4 and IPv6
- Sniffing
  - IPv6 is no more or less likely to fall victim to a sniffing attack than IPv4

Processing IPv6 Extension Headers

#RSAC

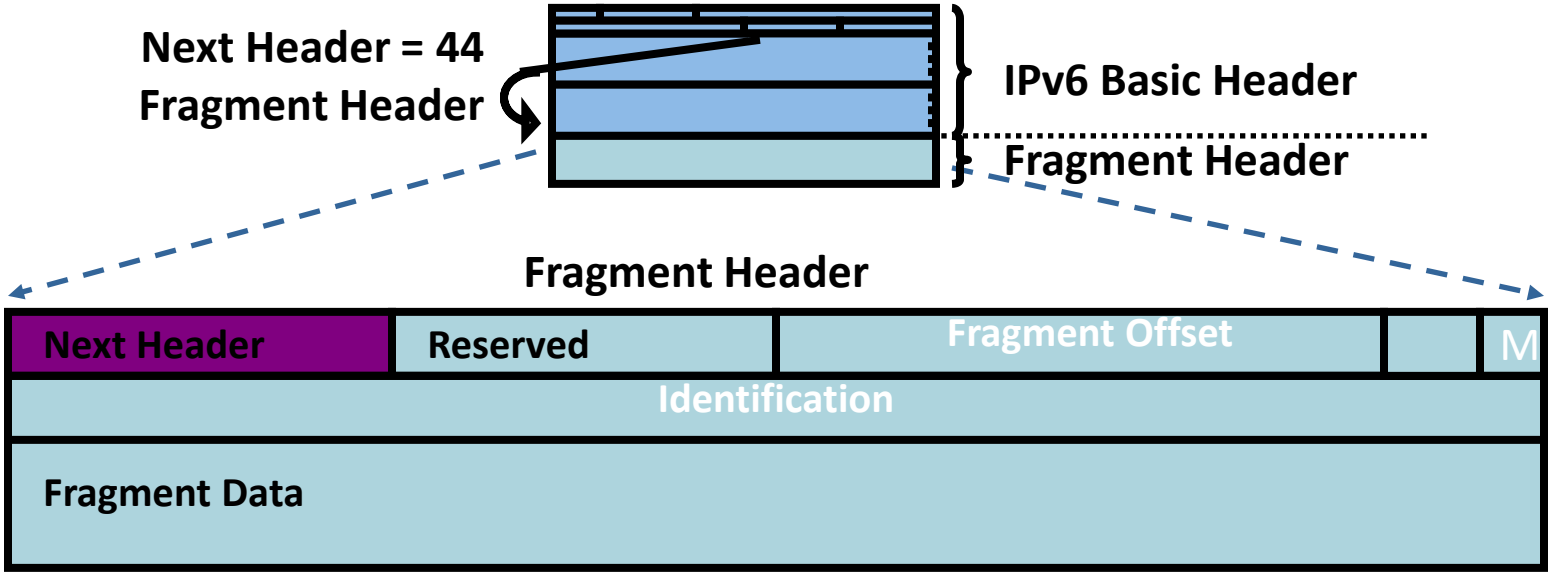
RSA CONFERENCE EUROPE 2013

Parsing the Extension Header Chain

- Finding the layer 4 information is not trivial in IPv6
  - Skip all known extension header
  - Until either known layer 4 header found => **MATCH**
  - Or unknown extension header/layer 4 header found... => **NO MATCH**

Fragment Header: IPv6

- In IPv6 fragmentation is done only by the end system
  - Tunnel end-points are end systems => Fragmentation / re-assembly can happen inside the network
- Reassembly done by end system like in IPv4
- Attackers can still fragment in intermediate system on purpose
- ==> a great obfuscation tool



Atomic IPv6 Fragments

- See: RFC 6946
- Def: *fragment which is both the first (offset=0) and the last (M=0)*
  - Used when a link MTU on the path < 1280 per RFC 2460 (sect 5)
  - Host caches this ‘feature’ per destination when receiving ICMPv6 packet-too-big
- Can be forged by sending a spoofed ICMPv6 packet-too-big
  - A trick must be used to ensure that the error message contains a copy of a valid packets
  - But, several OS do not even check, so why bother?
- Mitigation: anti-spoofing

Fragmentation Used in IPv4 by Attackers ... Also applicable to IPv6 of course

- Great evasion techniques
  - Some firewalls do not process fragments except for the first one
  - Some firewalls cannot detect overlapping fragments with different content
- IPv4 tools like whisker, fragrout, etc.
- Makes firewall and network intrusion detection harder
- Used mostly in DoSing hosts, but can be used for attacks that compromise the host
  - Send a fragment to force states (buffers, timers) in OS
  - See also: http://insecure.org/stf/secnet_ids/secnet_ids.html 1998!

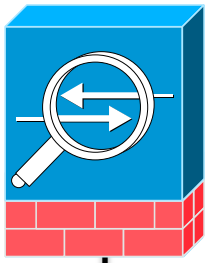
Hacking with fragmentation

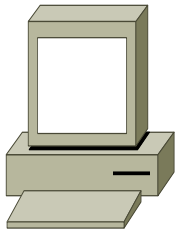
#RSAC

RSA CONFERENCE EUROPE 2013

Playing Tricks with Fragments /1

- Assuming stateful IPS (or even firewall) prefers the last fragment and host the first fragment...





Data = ATTACK

ID=n, OFF=10

Data = GOOD

ID=n, OFF=10

Data = ATTACK

ID=n, OFF=10

Data = GOOD

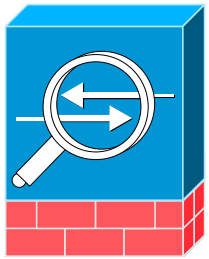
ID=n, OFF=10

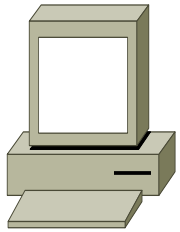
After re-assembly:
GOOD

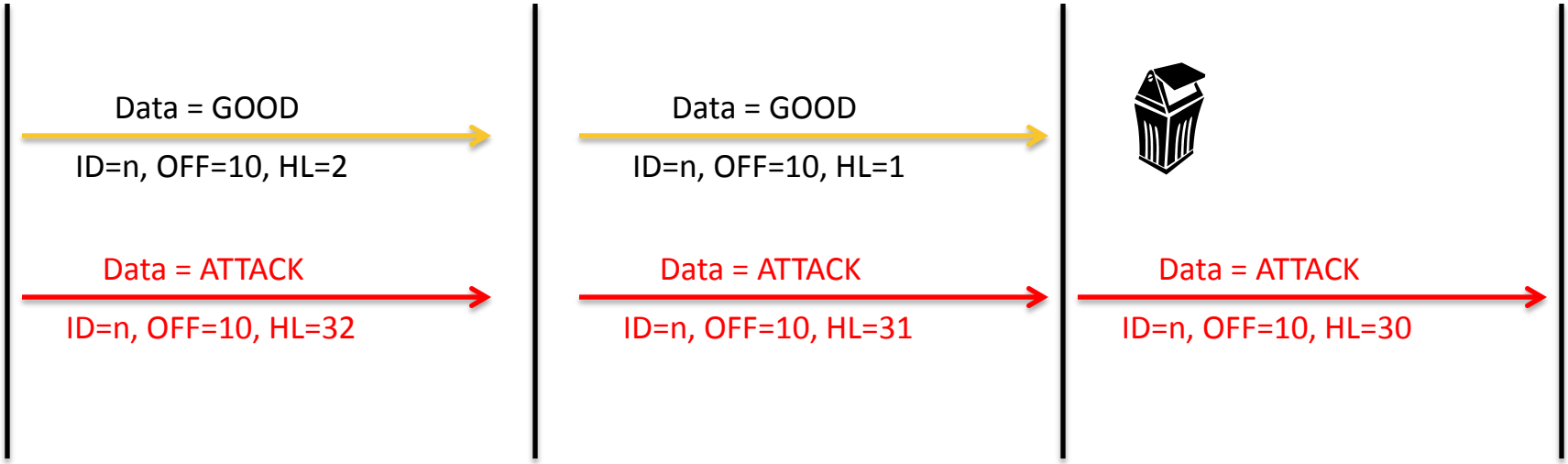
After re-assembly:
ATTACK

Playing Tricks with Fragments /2

- Assuming stateful IPS/firewall prefers the first fragment...

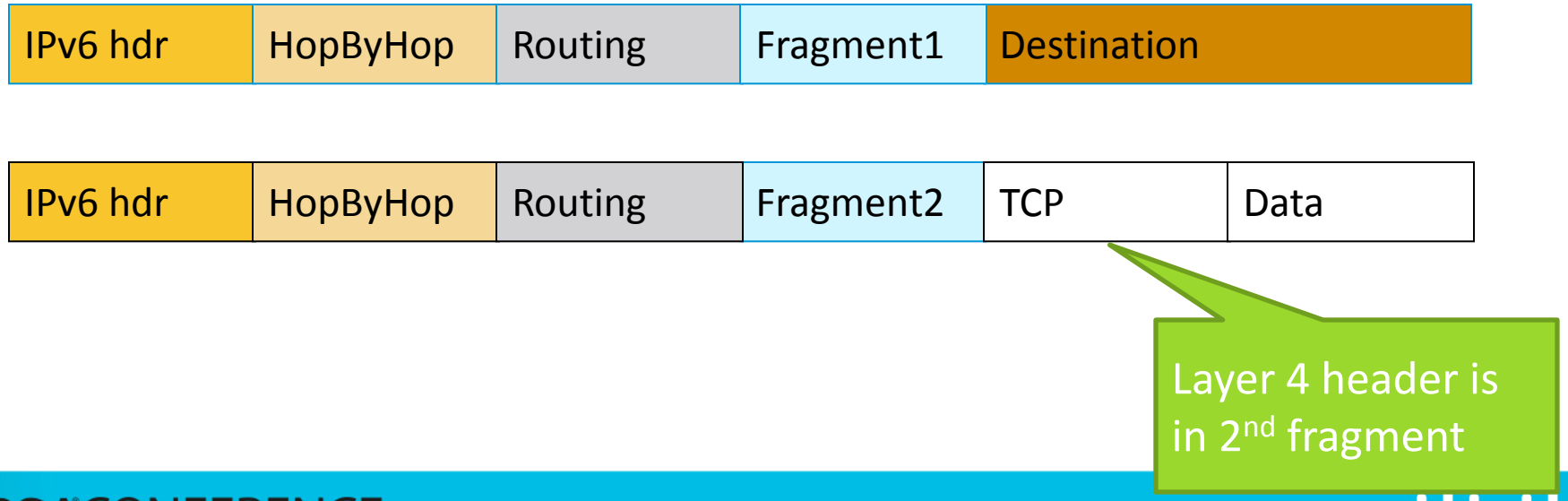






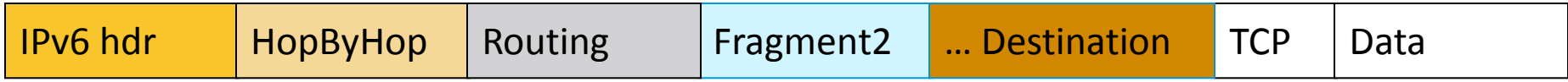
Parsing the Extension Header Chain Fragmentation Matters!

- Extension headers chain can be so large than it must be fragmented!
- RFC 3128 is not applicable to IPv6
- Layer 4 information could be in 2nd fragment



Parsing the Extension Header Chain Fragments and Stateless Filters

- RFC 3128 is not applicable to IPv6
- Layer 4 information could be in 2nd fragment
- But, stateless firewalls could not find it if a previous extension header is fragmented



Layer 4 header is in 2nd fragment, Stateless filters have no clue where to find it!

Overlapping Fragments Issues – RFC 5722

- Also in IPv4
- Can hinder NIDS/firewall
- Can bypass stateless ACL, e.g. ‘established’ sessions

IPv6 hdr	Frg ID=n O=0	TCP DST=80, ACK	Filler

✔

IPv6 hdr	Frg ID=n O=12	SYN	Attack

✔

At host:	TCP DST=80, ACK	SYN	Attack

✖

- RFC 5722 => drop overlapping fragments
- FreeBSD, Ubuntu 11.10 and Windows 7 implement RFC 5722 hence no worries for them

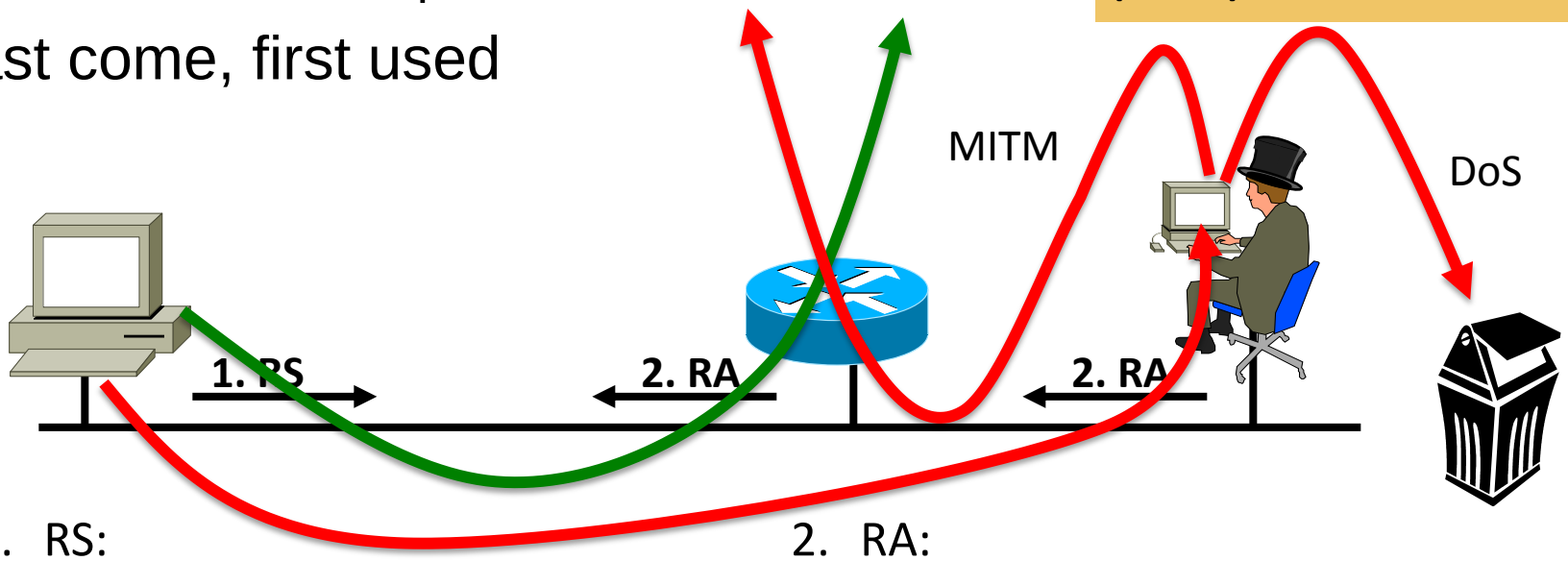
IPv6 Fragmentation & ACL Fragment Keyword (vendor specific)

- This makes matching against the first fragment non-deterministic:
  - layer 4 header might not be there but in a later fragment
  - ⇒ Need for stateful inspection
- `fragment` keyword matches
  - Non-initial fragments (same as IPv4)
- `undertermined-transport` keyword does not match
  - If non-initial fragment
  - Or if TCP/UDP/SCTP and ports are in the fragment
  - Or if ICMP and type and code are in the fragment
  - Else Everything else matches (including OSPFv3, RSVP, GRE, EIGRP, PIM …)
  - Only for deny ACE

Rogue Router Advertisement

- Router Advertisements contain:
  - Prefix to be used by hosts
  - Data-link layer address of the router
  - Miscellaneous options: MTU, DHCPv6 use, …
- Last come, first used

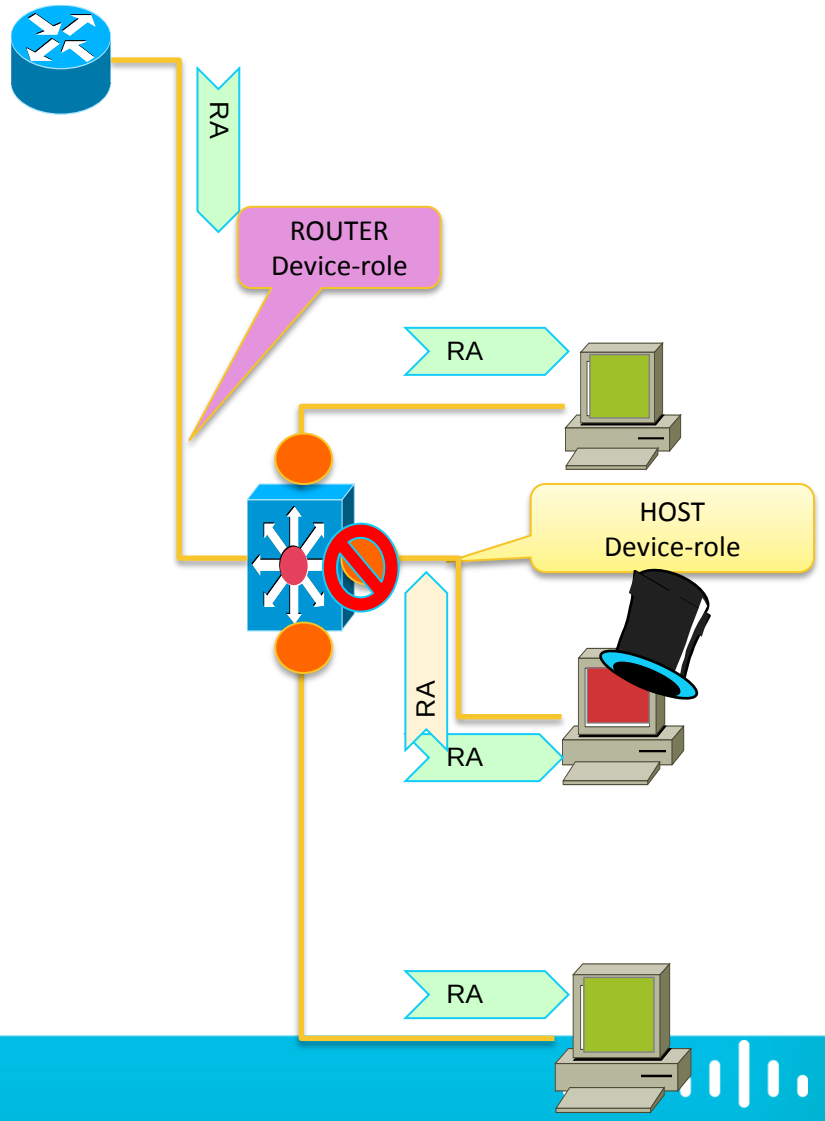
RA w/o Any Authentication Gives Exactly Same Level of Security as DHCPv4 (None)



1. RS:
   - –Data = Query: please send RA
2. RA:
   - –Data= options, **prefix**, lifetime, A+M+O flags

Mitigating Rogue RA: RFC 6101

- Multiple switches implement RFC 6101 by using stateless filtering of ICMP Router Advertisements



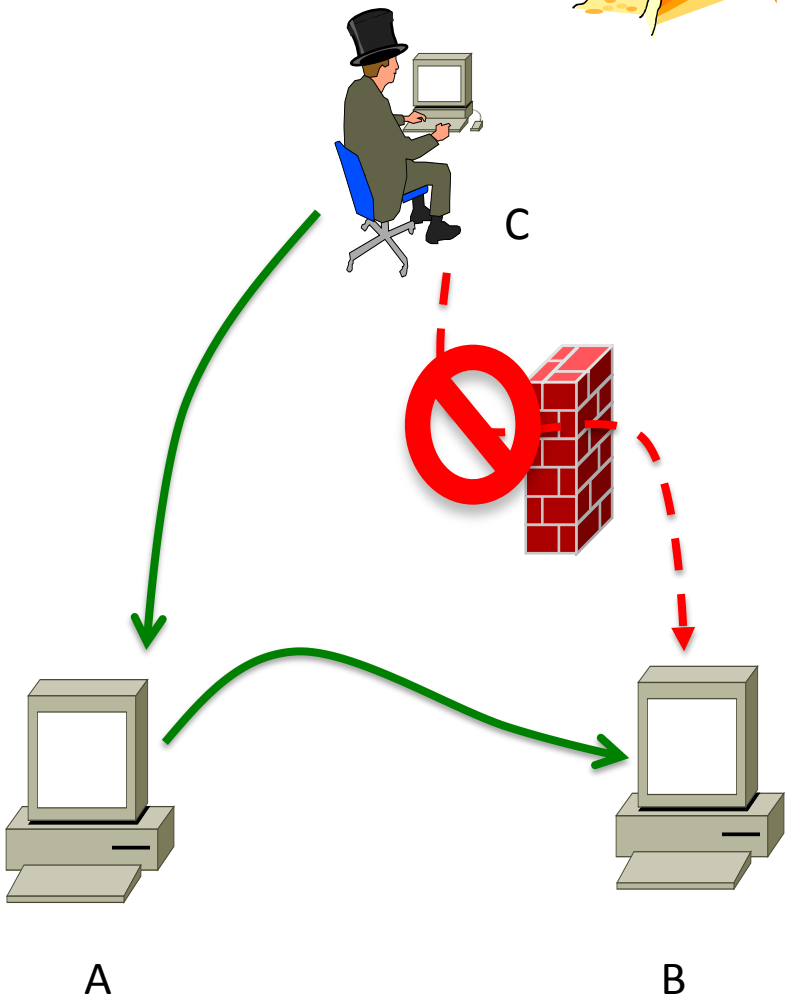
Parsing the Extension Header Chain Fragments and Stateless Filters (RA Guard)

- RA Guard works like a stateless ACL filtering ICMP type 134
- THC **`fake_router6 -FD`** implements this attack which bypasses RA Guard
- Partial work-around: block all fragments sent to ff02::1
- If supported, ***deny undetermined-transport*** blocks this attack (work item at IETF)
  - RFC 6980

ICMP header is in 2nd fragment,
RA Guard has no clue where to find it!

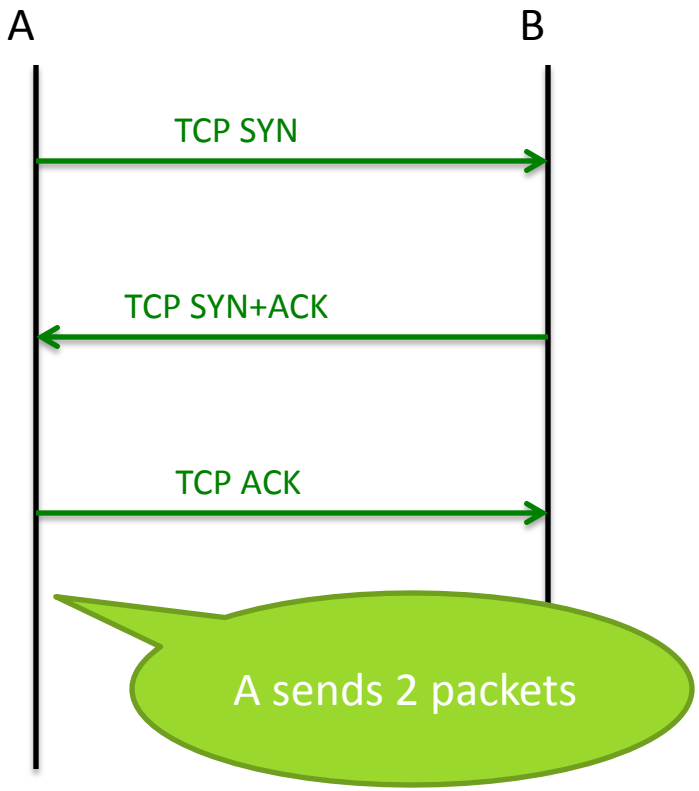
Predictable Fragment ID...

- RFC 2460 about ID field "*The Identification must be different than that of any other fragmented packet sent recently* with the same Source Address and Destination Address*"
- In IPv4, this was leveraged for blind scanning...
  - Allows a remote host C to detect the TCP/UDP ports opened between A and B
    - Either for anonymous scan of B
    - Or is C can only reach A (DMZ)
- See also draft-gont-6man-predictable-fragment-id

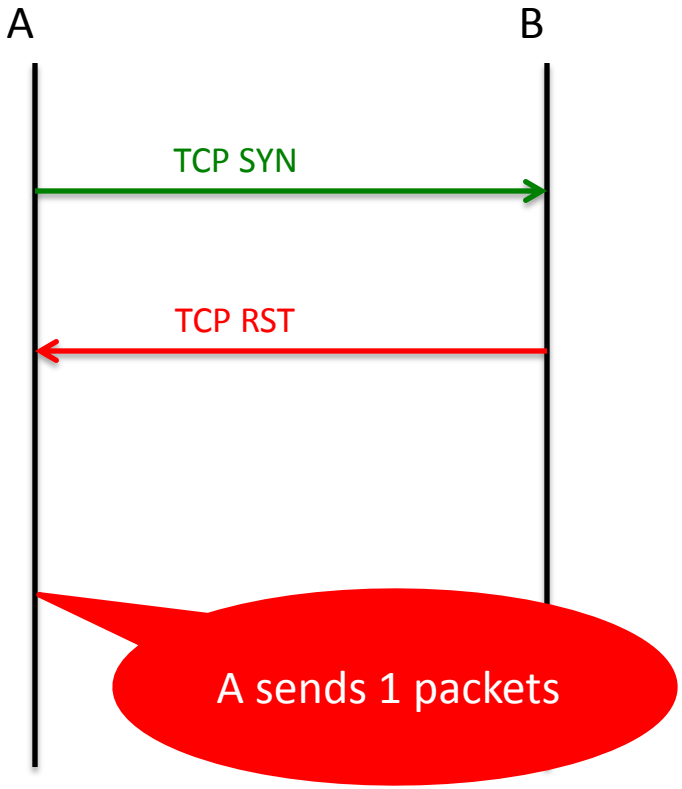


Review of TCP 3-way Handshake

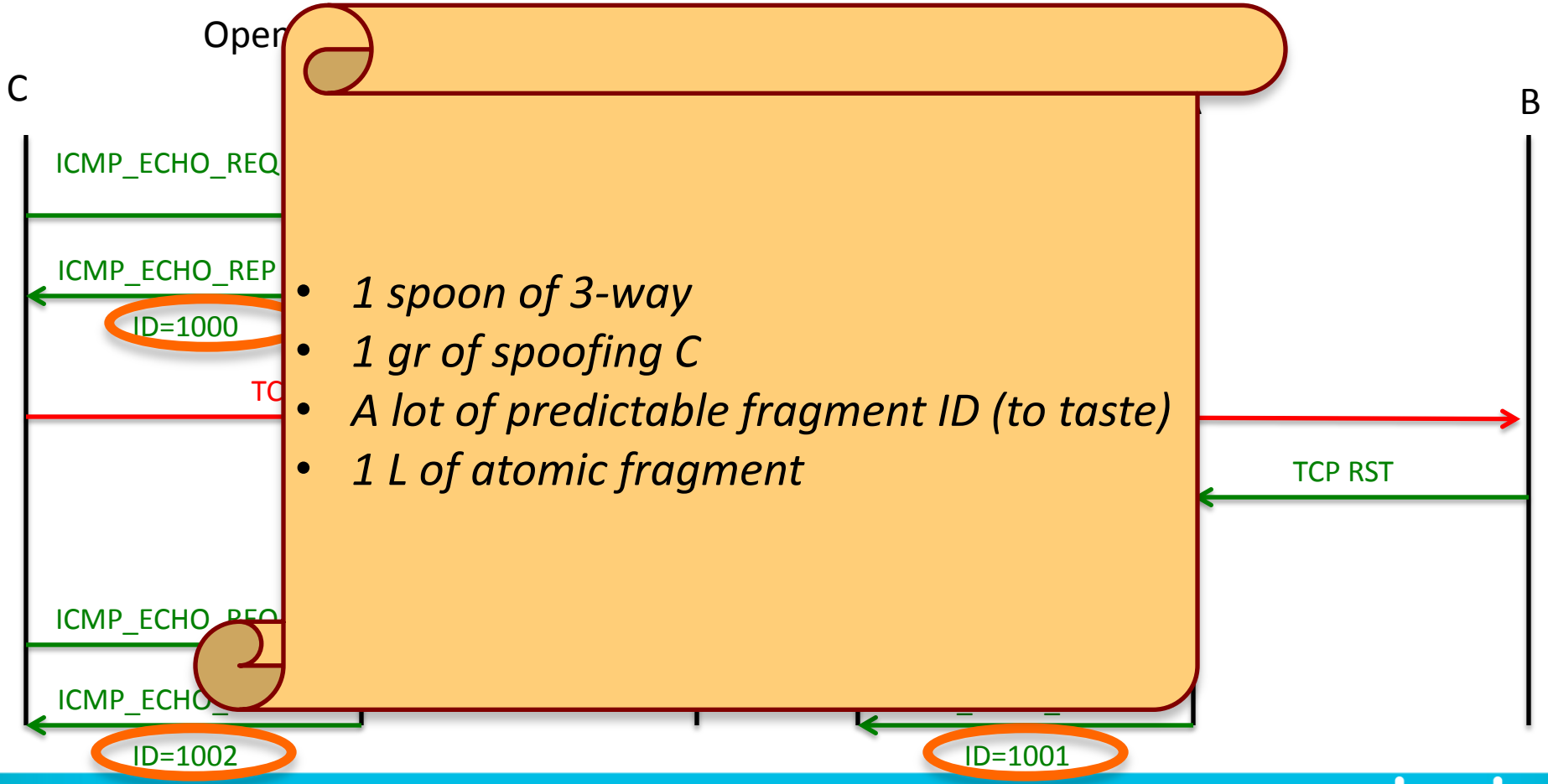
Open Port



Closed Port



Blind Scanning Recipe



Summary

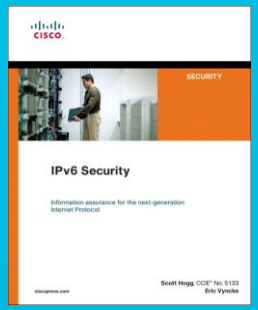
KEY TAKE AWAY

- Fragmentation caused several issues in legacy IPv4
  - Denial of services at reassembly
  - Obfuscation of attacks to evade IPS and firewall
- Security devices can handle those attacks for IPv4 and IPv6
- New in IPv6: fragmented transport header
  - Stateful firewall can handle this
  - Stateless firewalls (ACL, RA-Guard) cannot handle this
  - Undetermined-transport (or equivalent) is your best friend
  - RFC 6980 should fix the RA-guard issue

APPLY

- **Learn** more about IPv6 and its security
  - In short: 99% as IPv4 ;-) except for fragments
- **Check** your security devices on how they handle IPv6 extension headers and fragmentation
- **Embrace IPv6**, you cannot avoid it

QUESTIONS AND ANSWERS?



#RSAC

RSA CONFERENCE EUROPE 2013

Thank you!

Eric Vyncke

Cisco

@evyncke

evyncke@cisco.com

www.cisco.com

#RSAC

RSA CONFERENCE EUROPE 2013