

Fundamentals of Network Security

APIGA / Seoul / 8-8-2017

Pablo Hinojosa

@lphinojosa

APNIC



The real questions

- If you ask...
 - “Is the Internet secure?”
 - “Can the Internet be secured?”
 - “Can society ever be safe?”
 - The truthful answer is “**No**”

- But if you ask...
 - “Can my services/networks/transactions be secured?”
 - “Can the Internet be used securely?”
 - “Can I stay safe?”
 - The answer is probably “**Yes**” (but with care!)

What can the attackers do?

- Eavesdropping – Listen in on communications
- Masquerading – Impersonating someone else
- Forgery – Invent or duplicate/replay information
- Trespass – Obtain unauthorised access
- Subversion – Modify data and messages in transit
- Destruction – Vandalise or delete important data
- Disruption – Disable or prevent access to services
- Infiltration – Hide out inside our machines
- Hijacking – “Own” and use machines for nefarious purposes

And why do they do it?

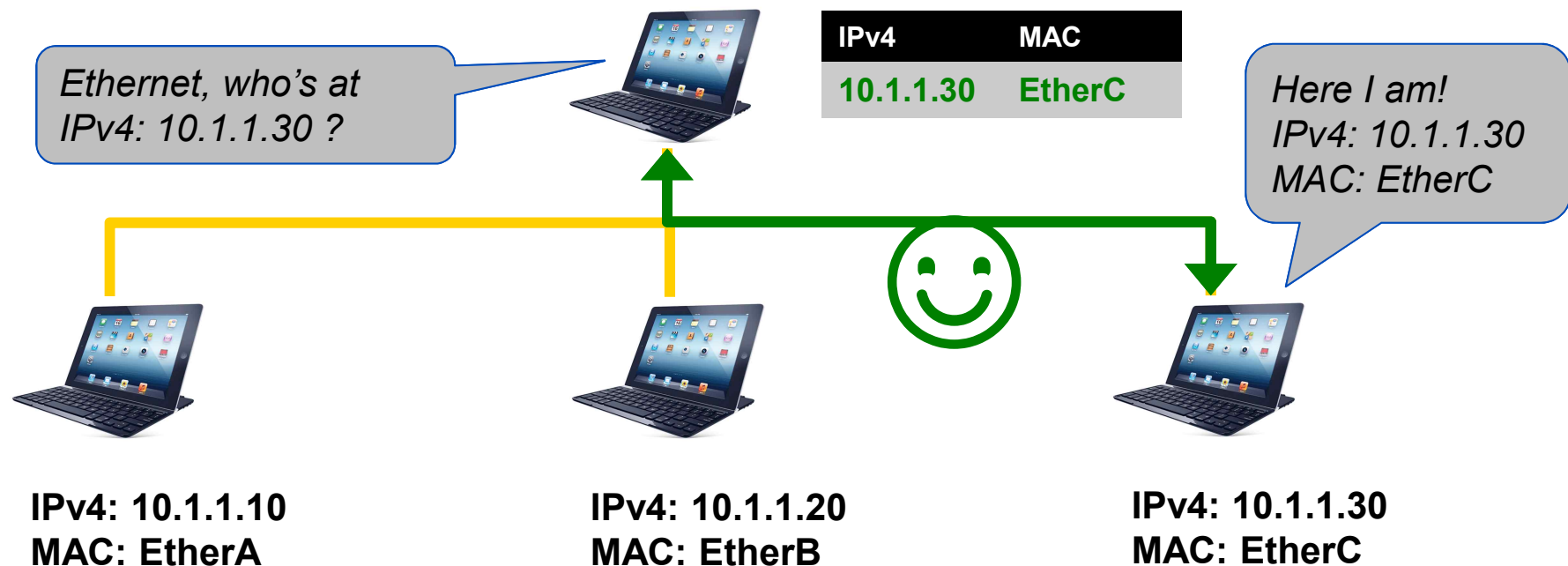
Motivation	Examples
Knowledge driven	<ul style="list-style-type: none">• Recreational• Research
Issue-based	<ul style="list-style-type: none">• Hacktivism• Patriotism
Antisocial	<ul style="list-style-type: none">• Revenge• Vandalism
Competitive	<ul style="list-style-type: none">• Theft of IP• Damage to competitors
Criminal	<ul style="list-style-type: none">• Theft of assets• Extortion
Strategic	<ul style="list-style-type: none">• Espionage• State-driven or sponsored

And, how do they do it?

- Social engineering attacks
 - Human beings – the weakest links
 - “Phishing”
 - Password attacks etc etc
- Masquerading
 - Address “spoofing”
- DNS attacks
 - Corruption and cache poisoning
- Denial of Service
 - DoS attacks
 - DDoS attacks

Masquerading example: ARP

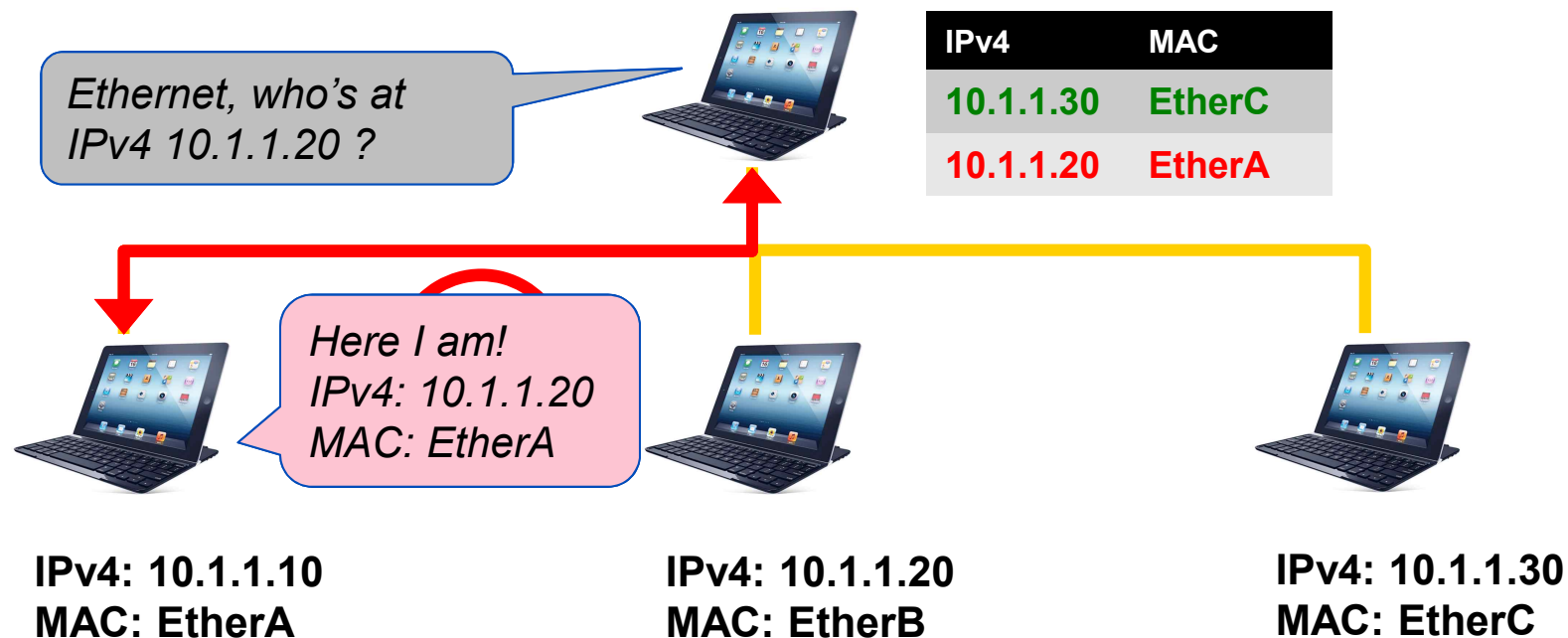
- Address Resolution Protocol (RFC 826, 1982)
 - Used by any TCP/IP device to discover the Layer 2 address of an IPv4 address that it wants to reach



*AKA "ARP spoofing"

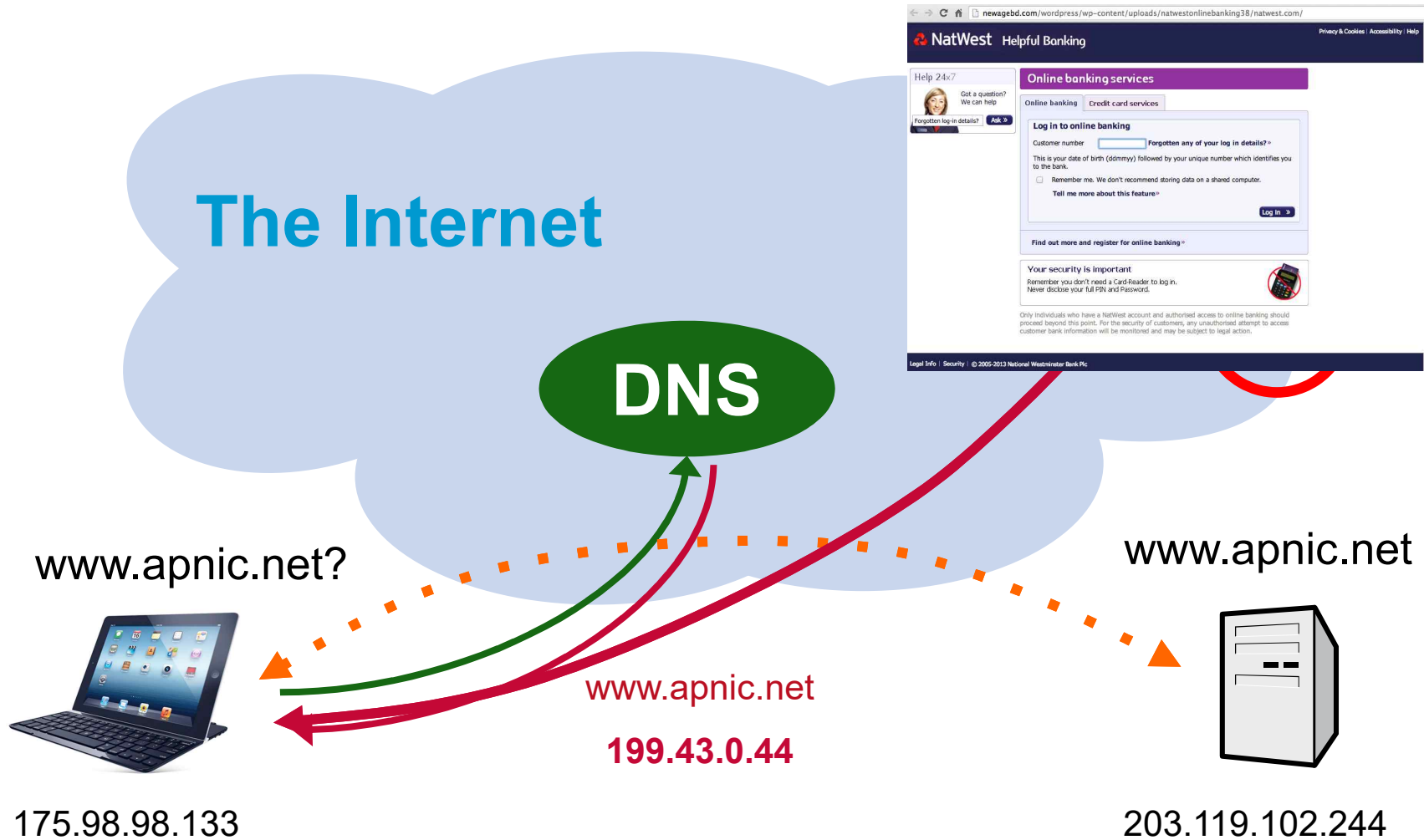
Masquerading example: ARP

- Address Resolution Protocol (RFC 826, 1982)
 - SEND: IPv6 SEcure Neighbour Discovery (RFC 3971, 2005)

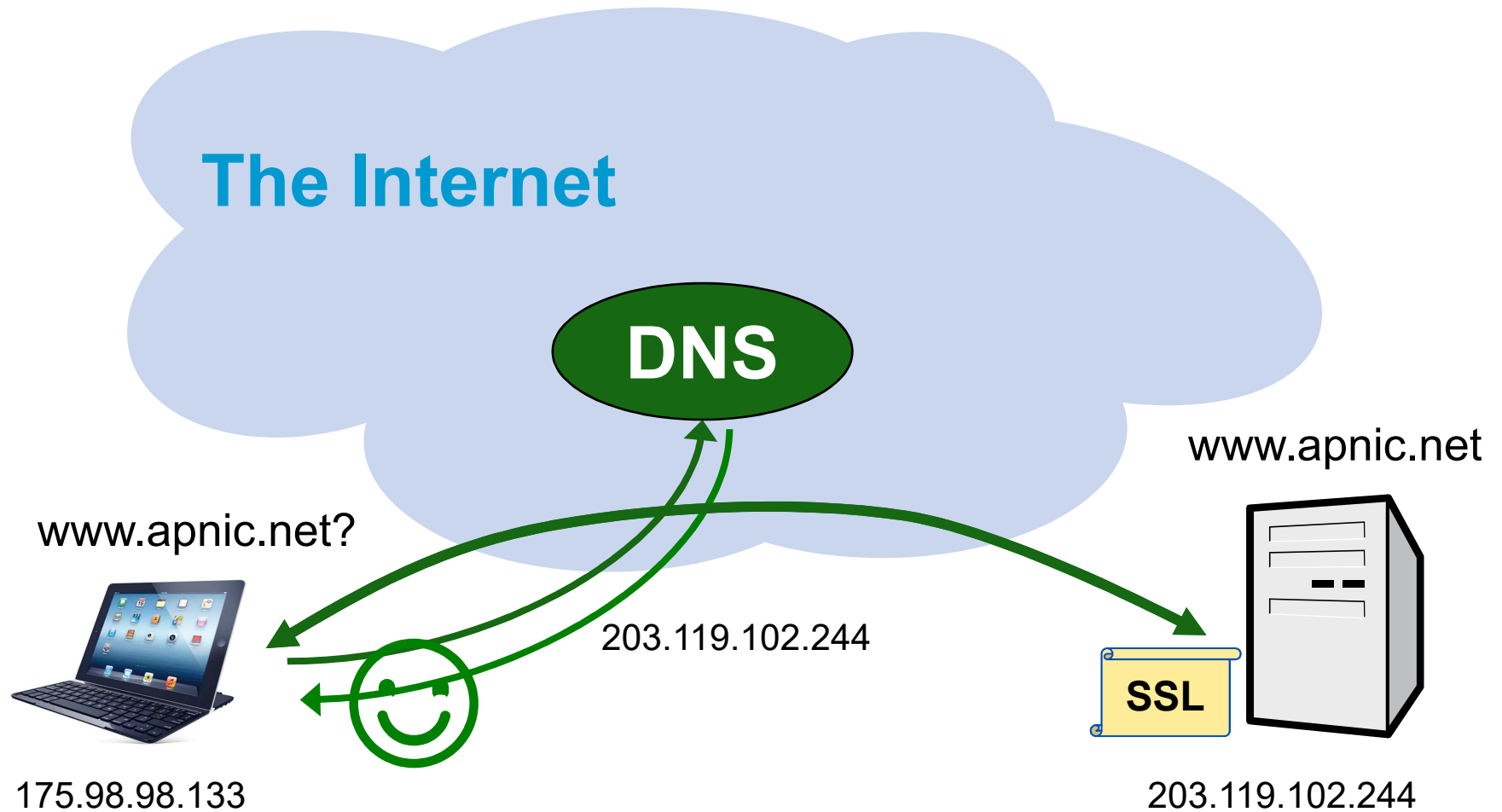


*AKA "ARP spoofing"

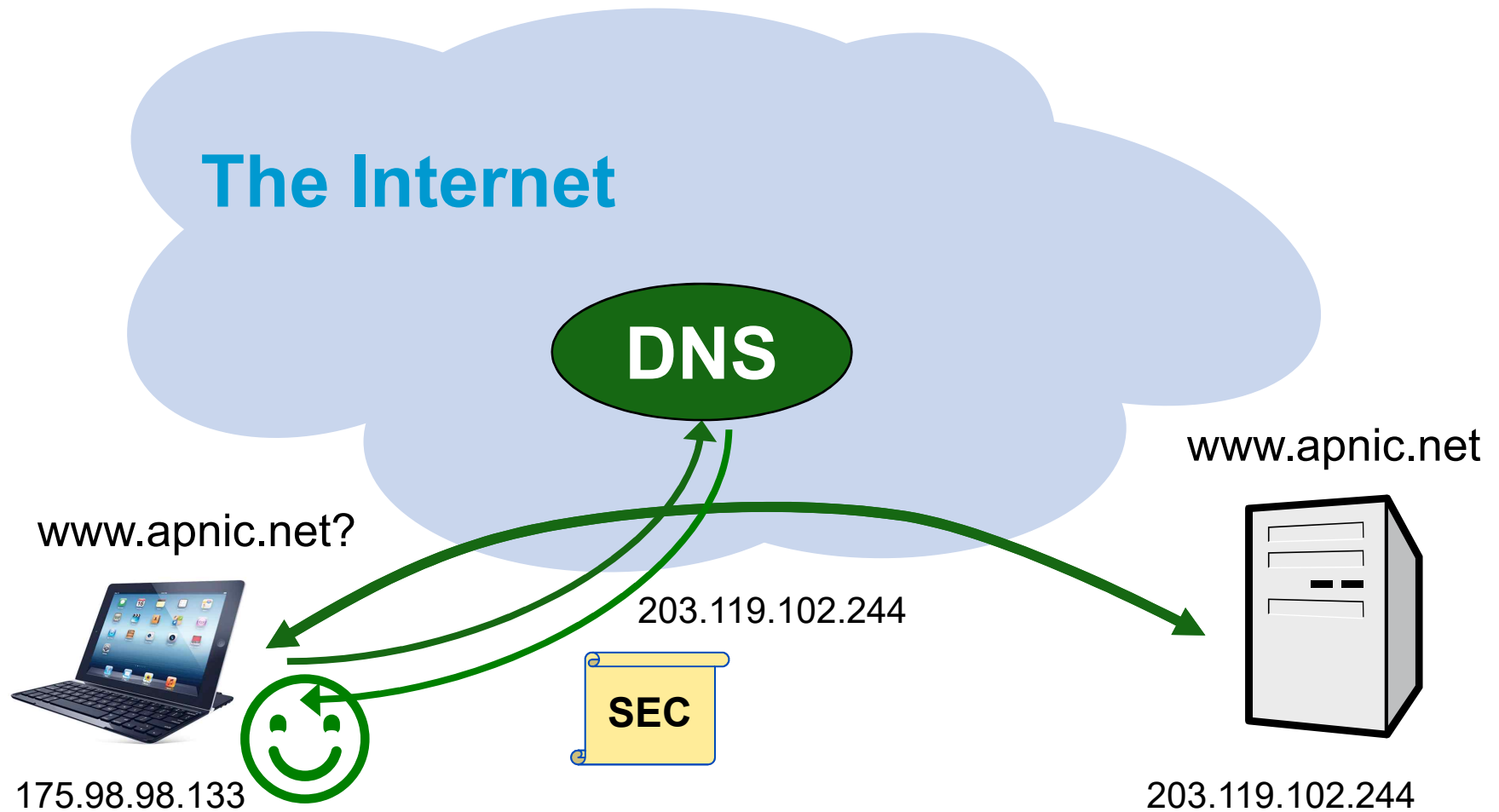
Attacking the DNS



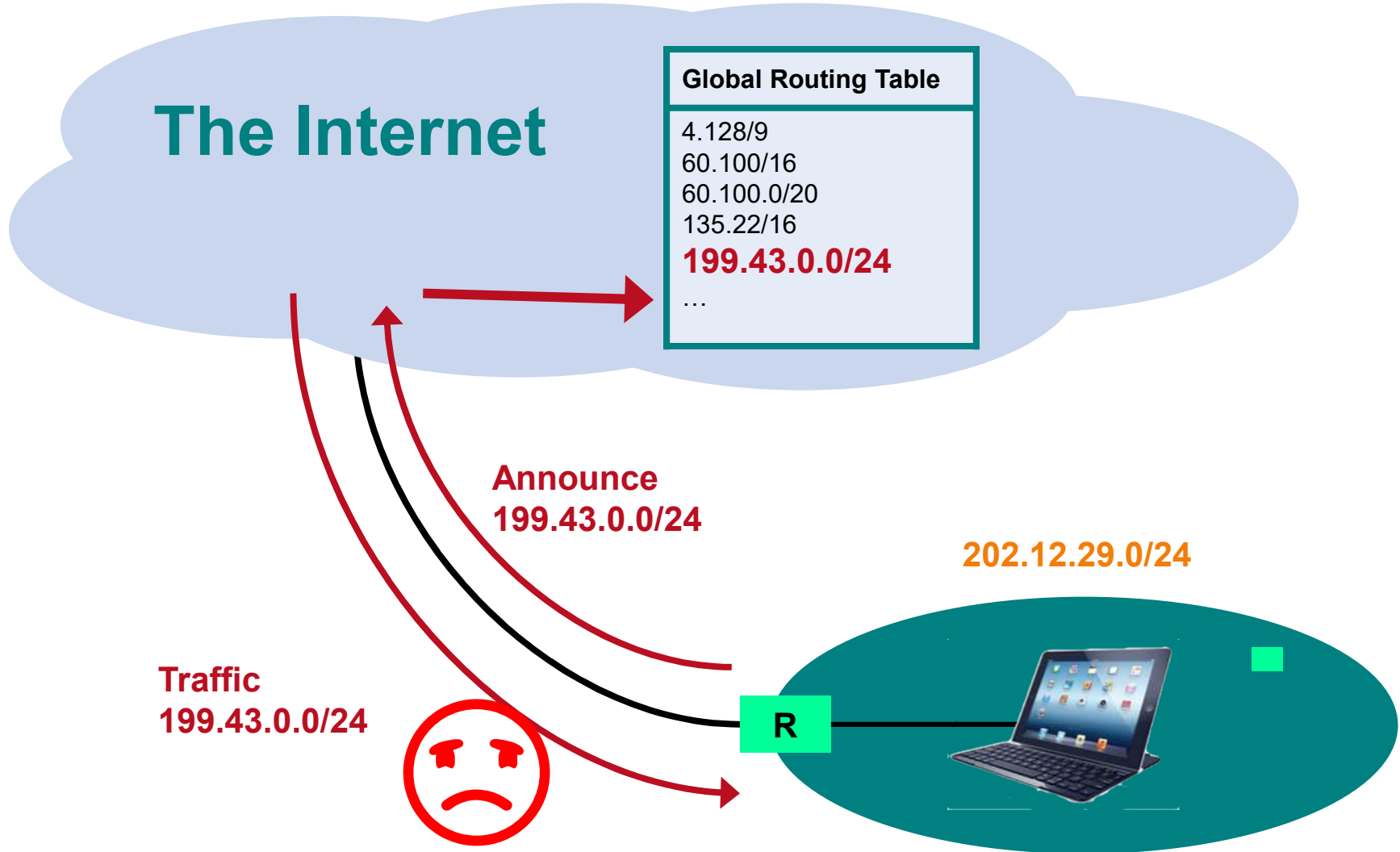
Securing websites – SSL certificates



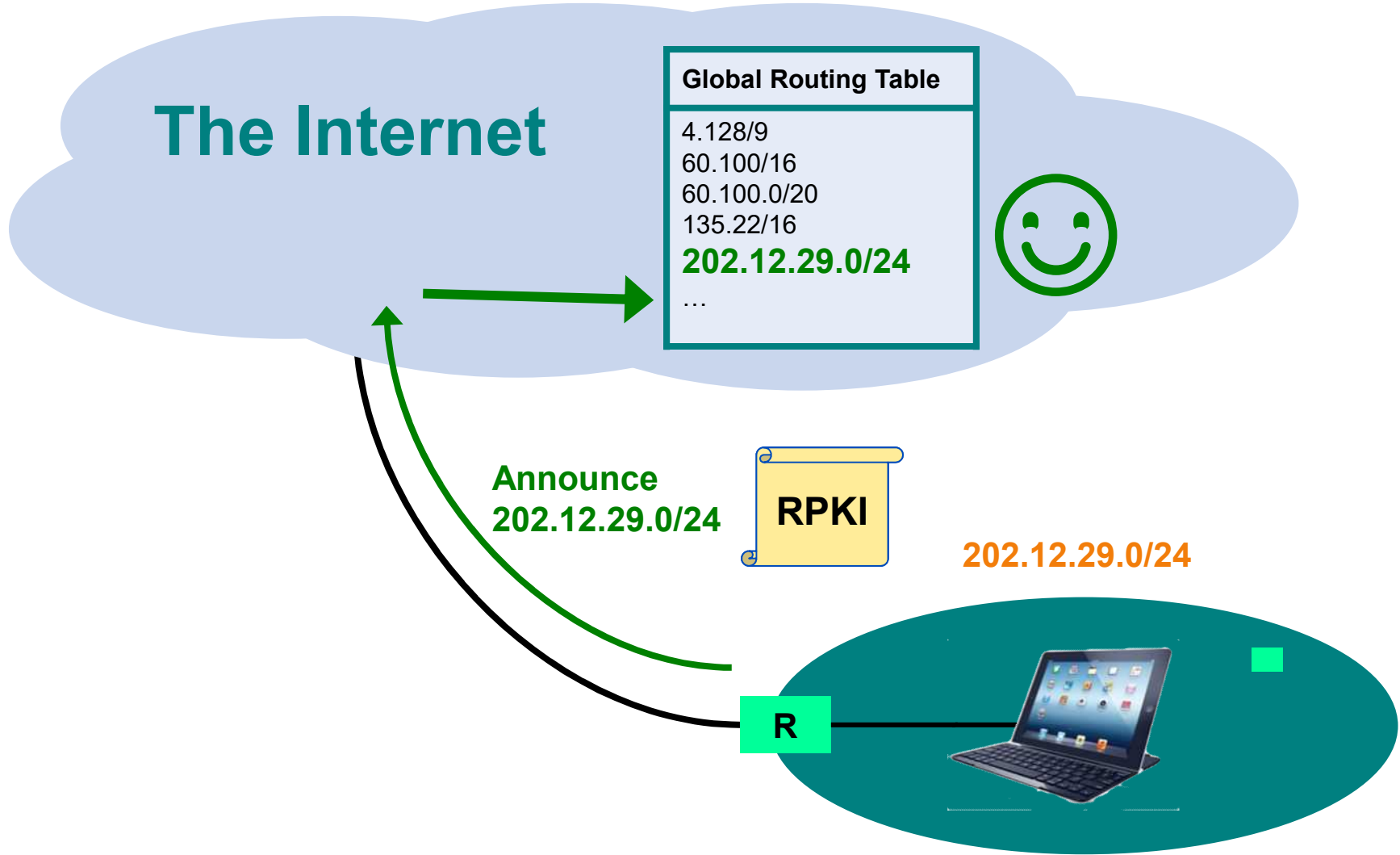
Securing DNS – DNSSEC



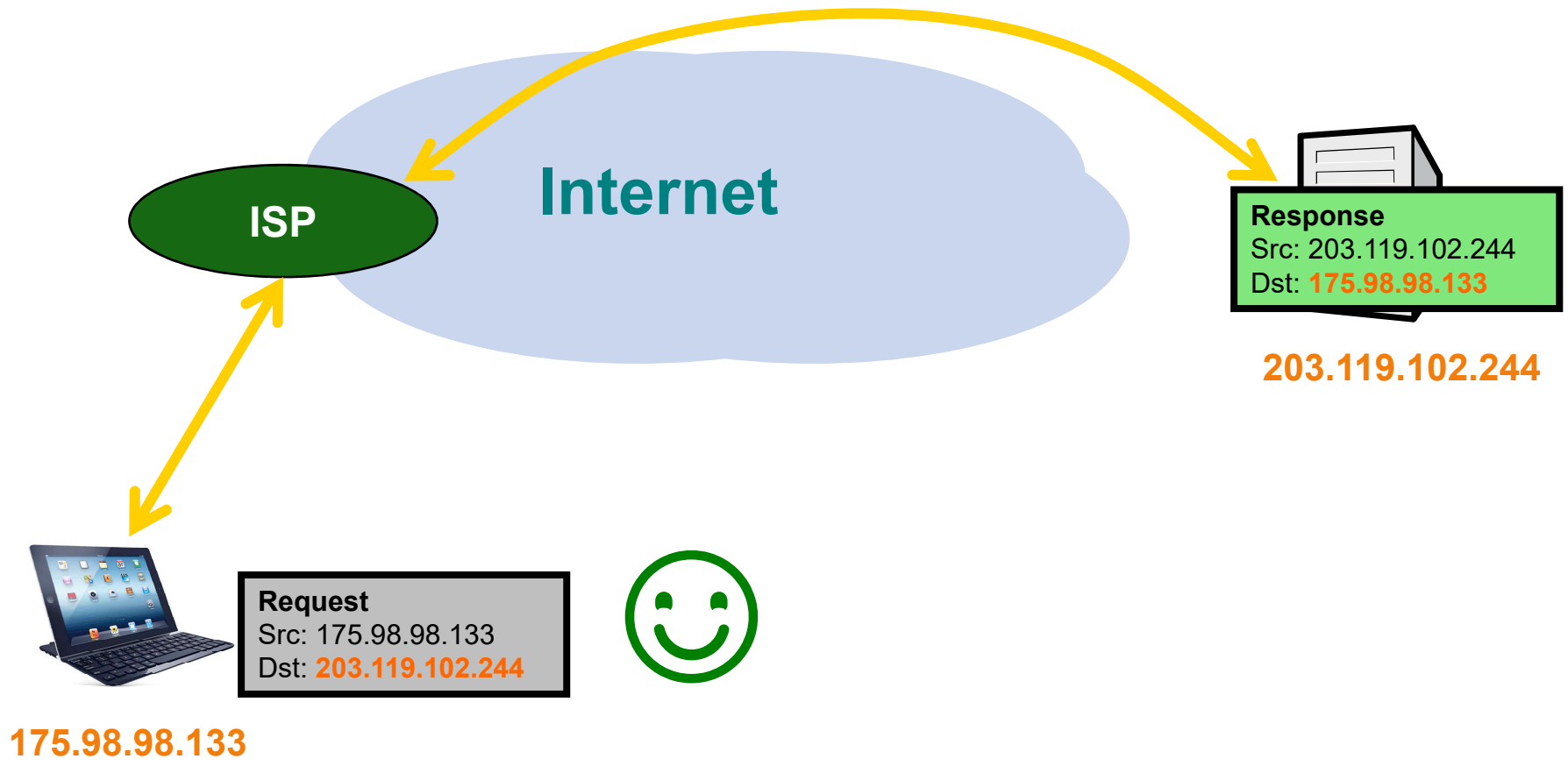
Misusing IP Addresses...



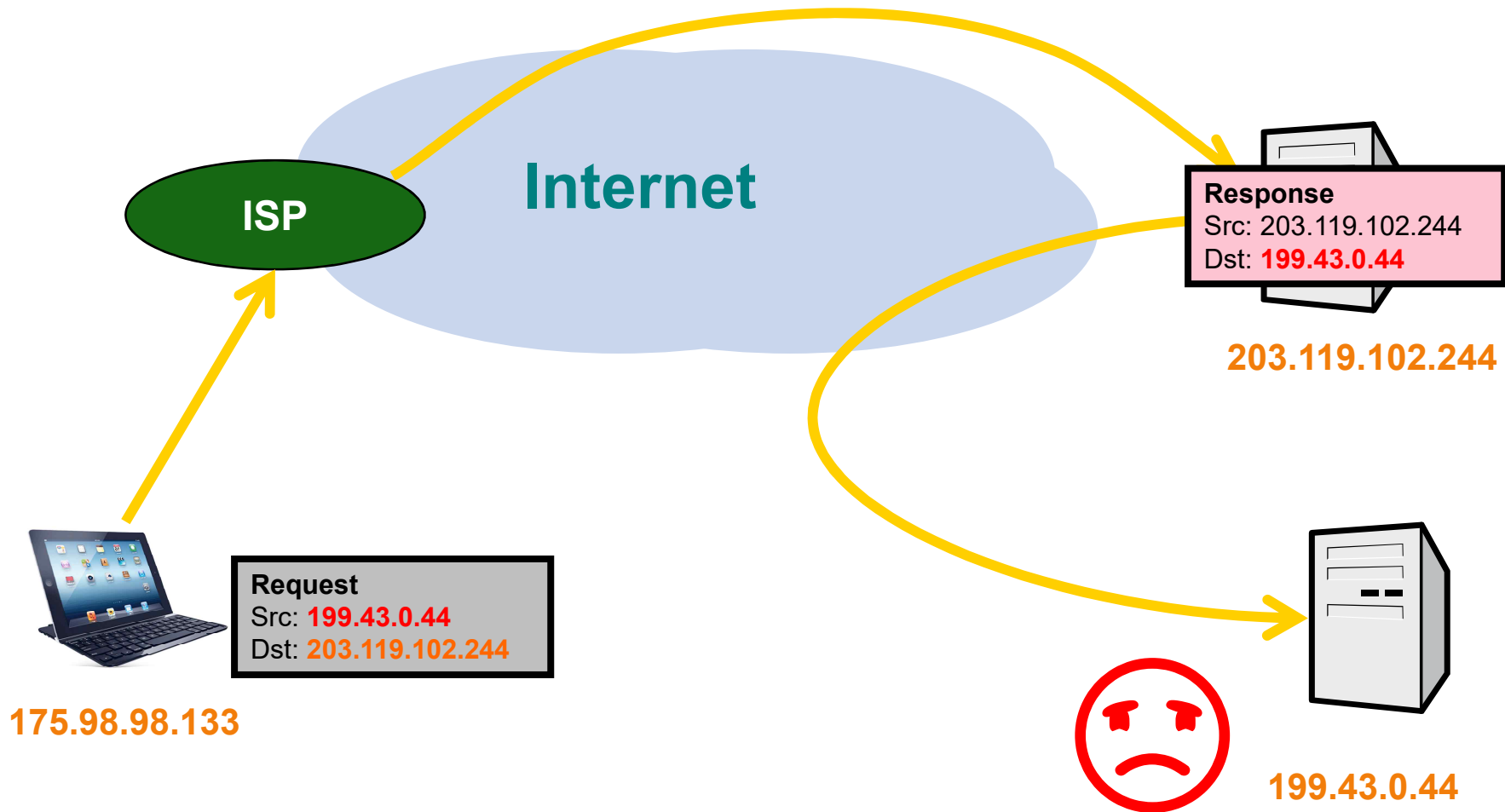
Misusing IP Addresses...



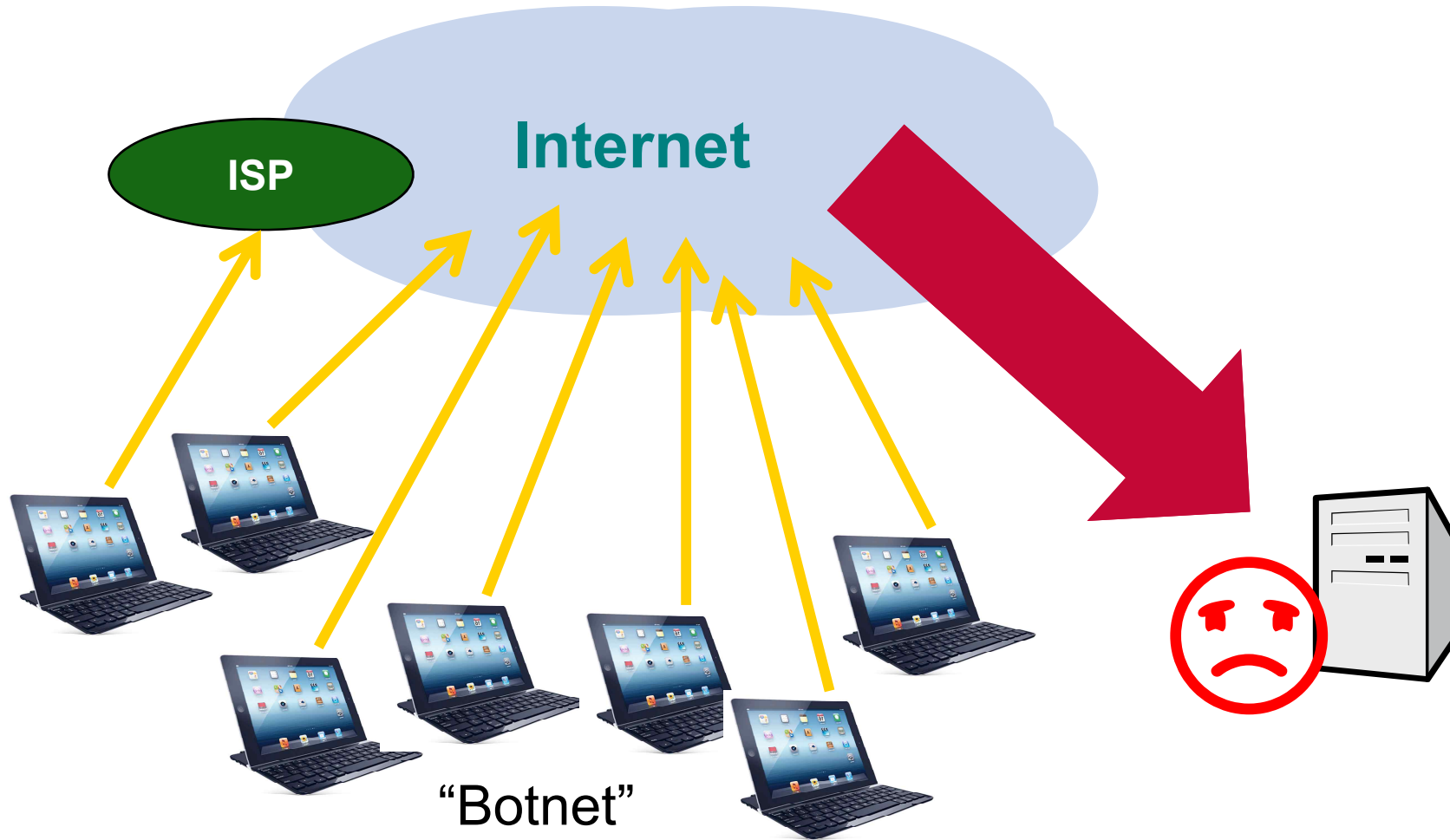
Masquerading again: IP spoofing



Masquerading again: IP spoofing



DDoS attack: Distributed DoS



<https://www.apnic.net/community/participate/maillinglists>

APNIC

CONTACT US MAKE A PAYMENT WHOIS & WEBSITE MyAPNIC
Advanced Whois search

Get IP Manage IP Training Events Research Community Blog About

Community

- ▶ Resource Policies
- ▼ Participation
 - ▶ Attend APNIC events
 - ▶ SIGs
 - ▼ Mailing lists
 - Mailing List Code of Conduct
 - ▶ Submit a policy proposal
 - ▶ Elections
 - ▶ Sponsor or host
 - ▶ Member & stakeholder feedback
 - ▶ APNIC Regional Meeting Program
- ▶ Community activities
- ▶ IANA transition
- ▶ Internet ecosystem
- ▶ Security@APNIC
- ▶ IPv6@APNIC
- ▶ Technical Assistance Service
- ▶ IPv4 post-exhaustion

Mailing lists

Like Share Tweet

APNIC hosts public forums to facilitate discussion on a range of topics related to Internet addressing and networking. The majority of the discussion occurs on mailing lists maintained by APNIC. This is complemented by publicly accessible face-to-face forums conducted at the twice-yearly APNIC Conferences.

Anyone with an interest is encouraged to attend or participate in any way. However, we please ask that you be mindful of the Code of Conduct that applies to the mailing lists.

+ APNIC Announce	Archives	Subscribe
+ APNIC Talk	Archives	Subscribe
+ APNIC Policy SIG	Archives	Subscribe
+ APNIC Transfers	Archives	Subscribe
+ APNIC Cooperation SIG	Archives	Subscribe
+ APNIC NIR SIG	Archives	Subscribe
+ IANA Transfer	Archives	Subscribe

[^ Top](#)

Related links

- ▶ APNIC SIGs
- ▶ APNIC Working Groups
- ▶ Policy development process

<https://conference.apnic.net/44>

APNIC 44

#apnic44



TAICHUNG, TAIWAN

7 - 14 September 2017

Questions?

Thank you

@lphinojosa

APNIC

