Fundamentals of Network Security

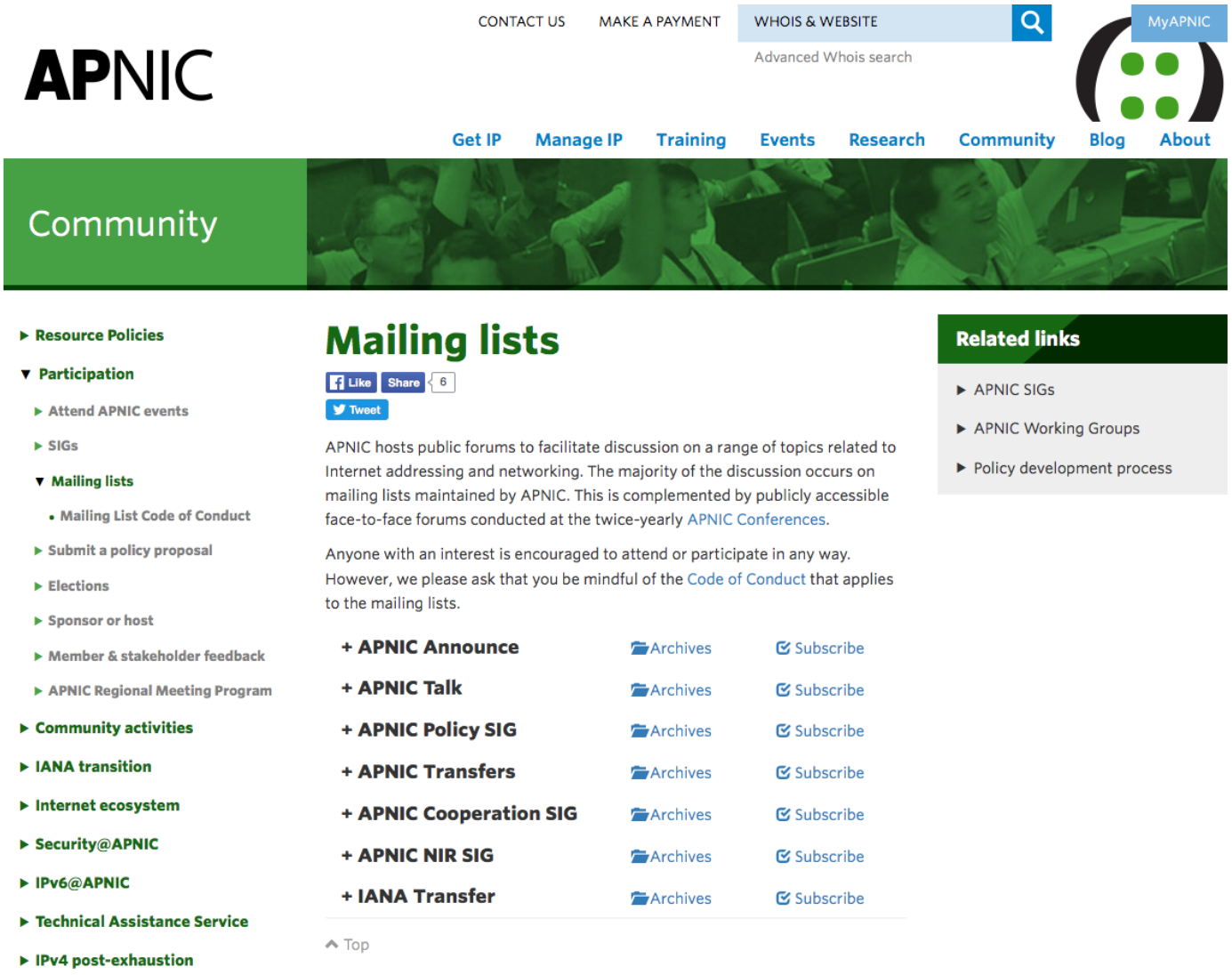
APIGA / Seoul / 9-8-2016

Pablo Hinojosa

@lphinojosa

APNIC

https://www.apnic.net/community/participate/mailinglists



https://conference.apnic.net/42

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?

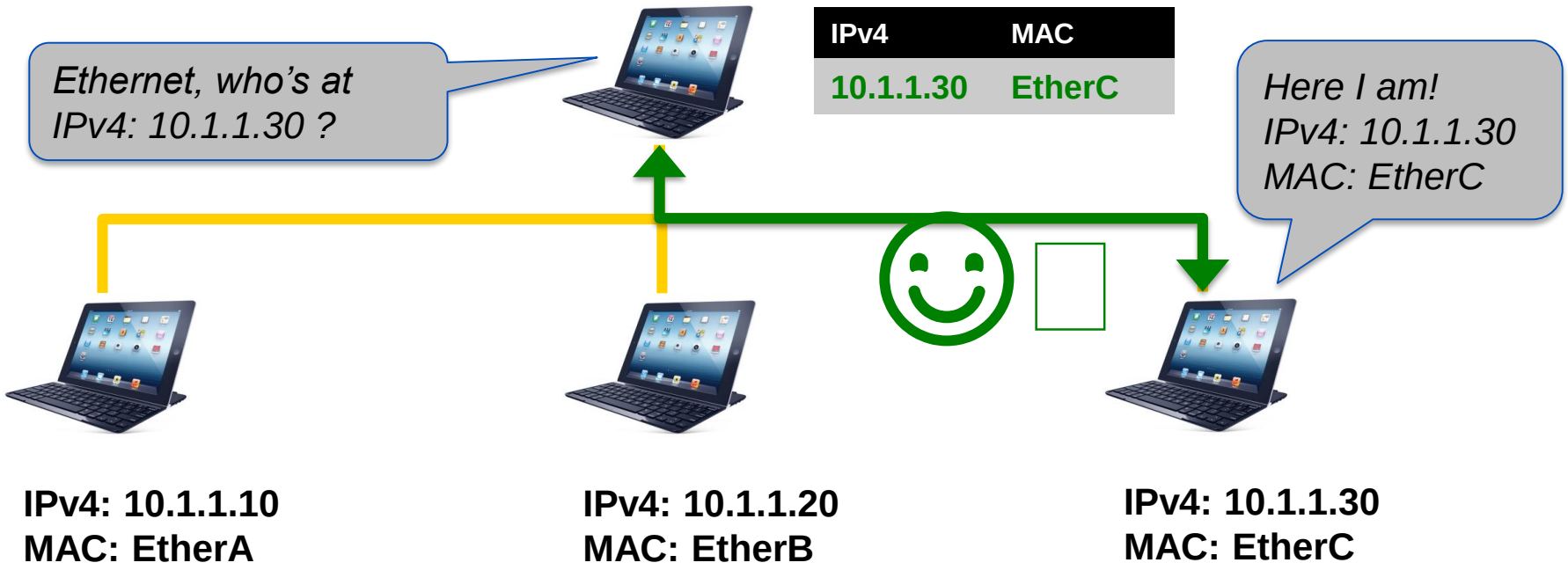
Motivation	Examples
Knowledge driven	• Recreational • Research
Issue-based	• Hacktivism • Patriotism
Antisocial	• Revenge • Vandalism
Competitive	• Theft of IP • Damage to competitors
Criminal	• Theft of assets • Extortion
Strategic	• Espionage • State-driven or sponsored

And, how to 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

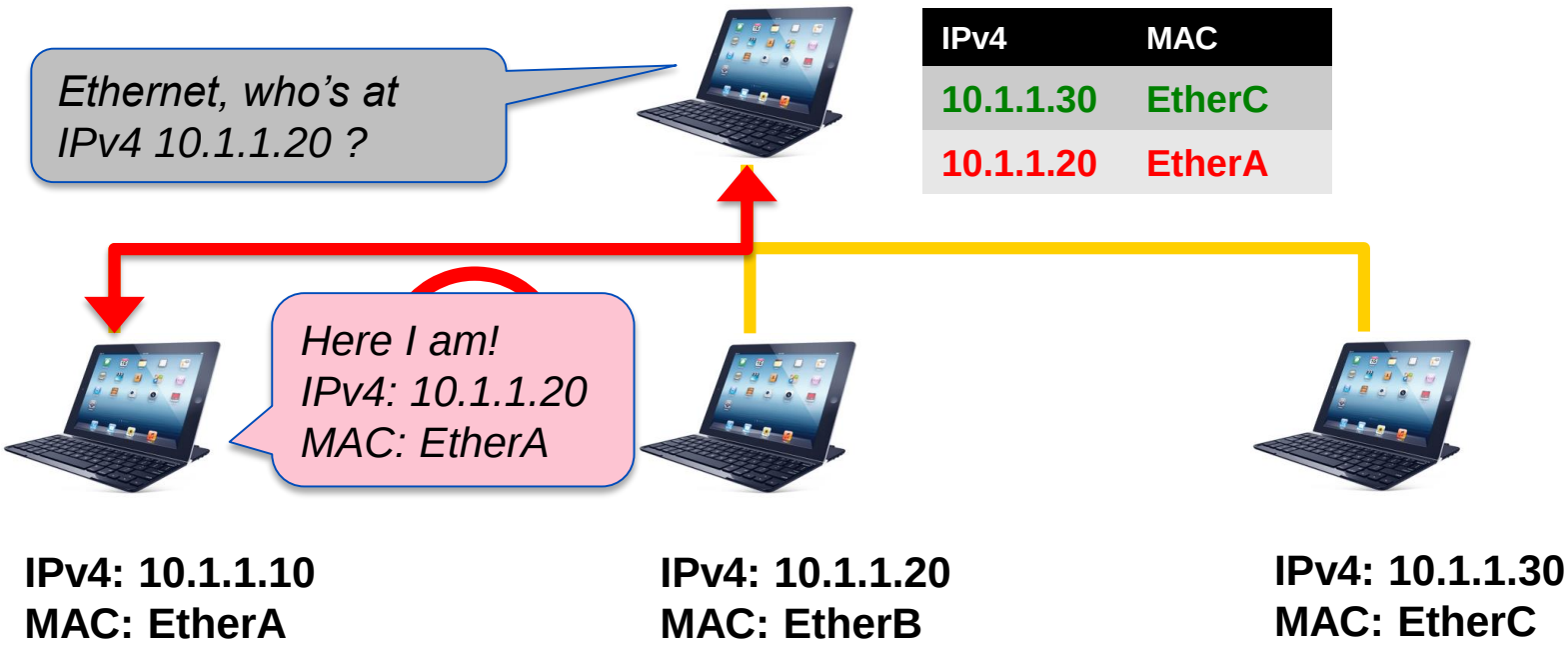
- Address Resolution Protocol (RFC 826, 1982)
  - Used by any TCP/IP device to discover the Layer 2 address of an IPv4 address that it wants to reach



*AKA "ARP spoofing"

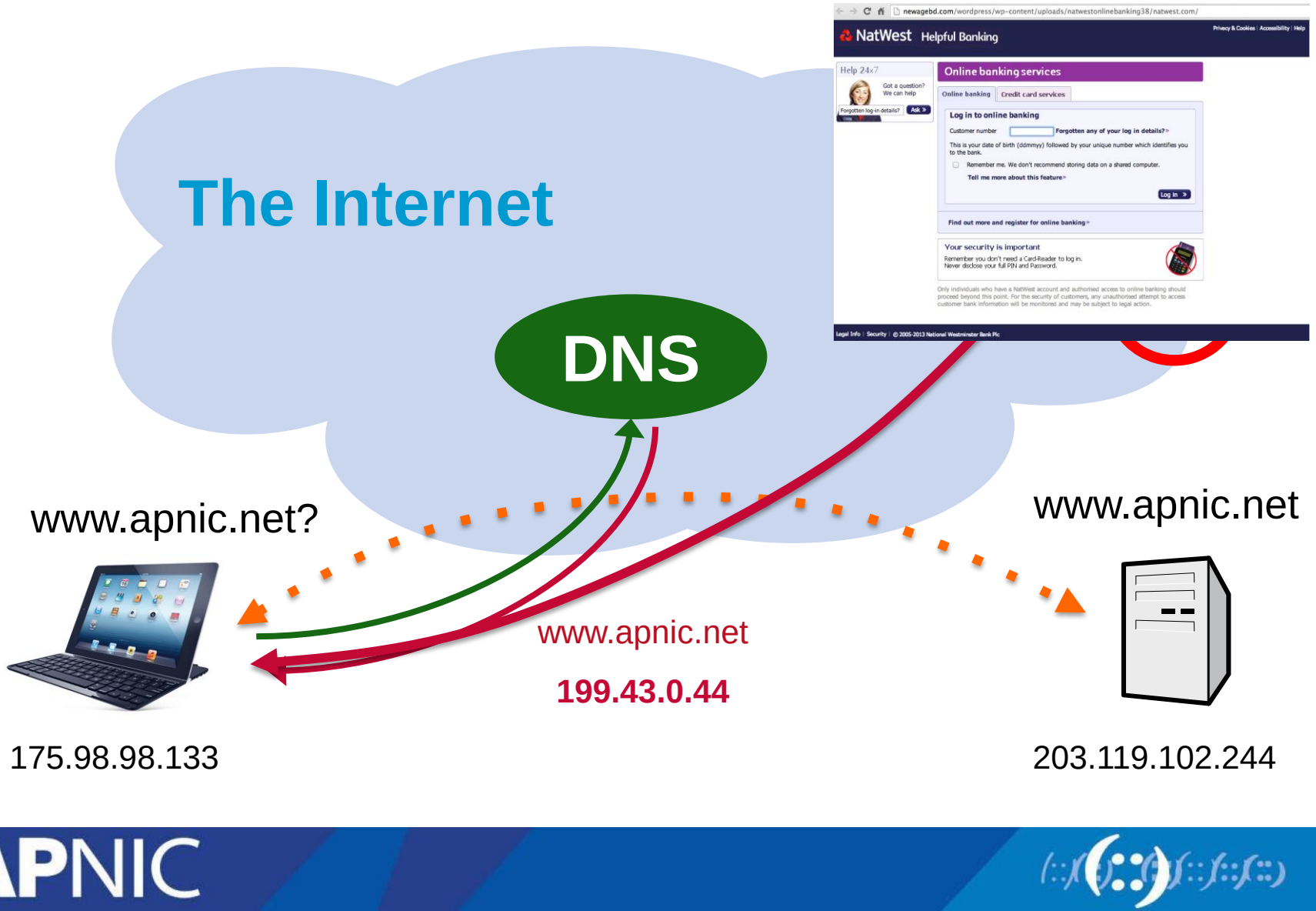
Masquerading example: ARP

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

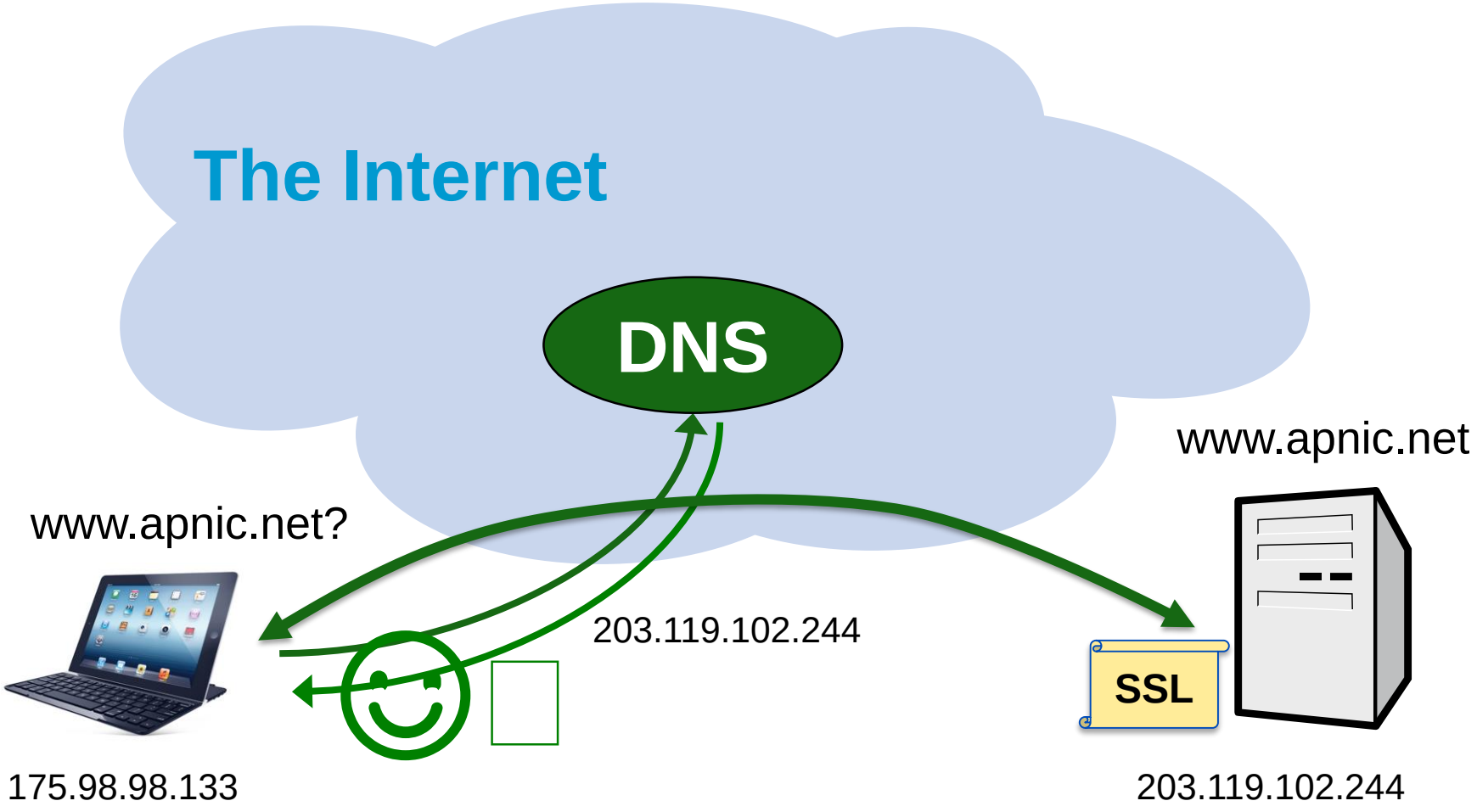


*AKA "ARP spoofing"

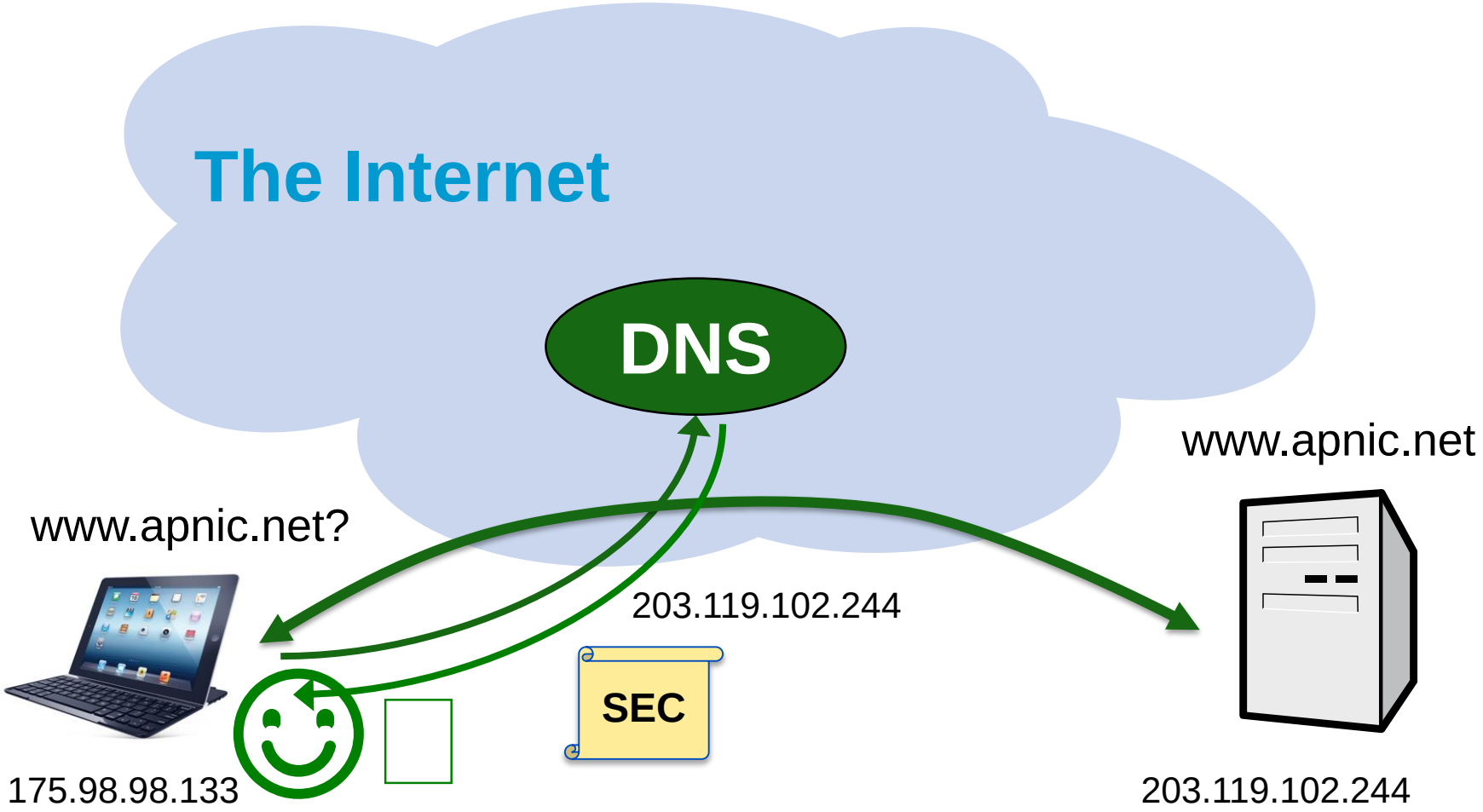
Attacking the DNS



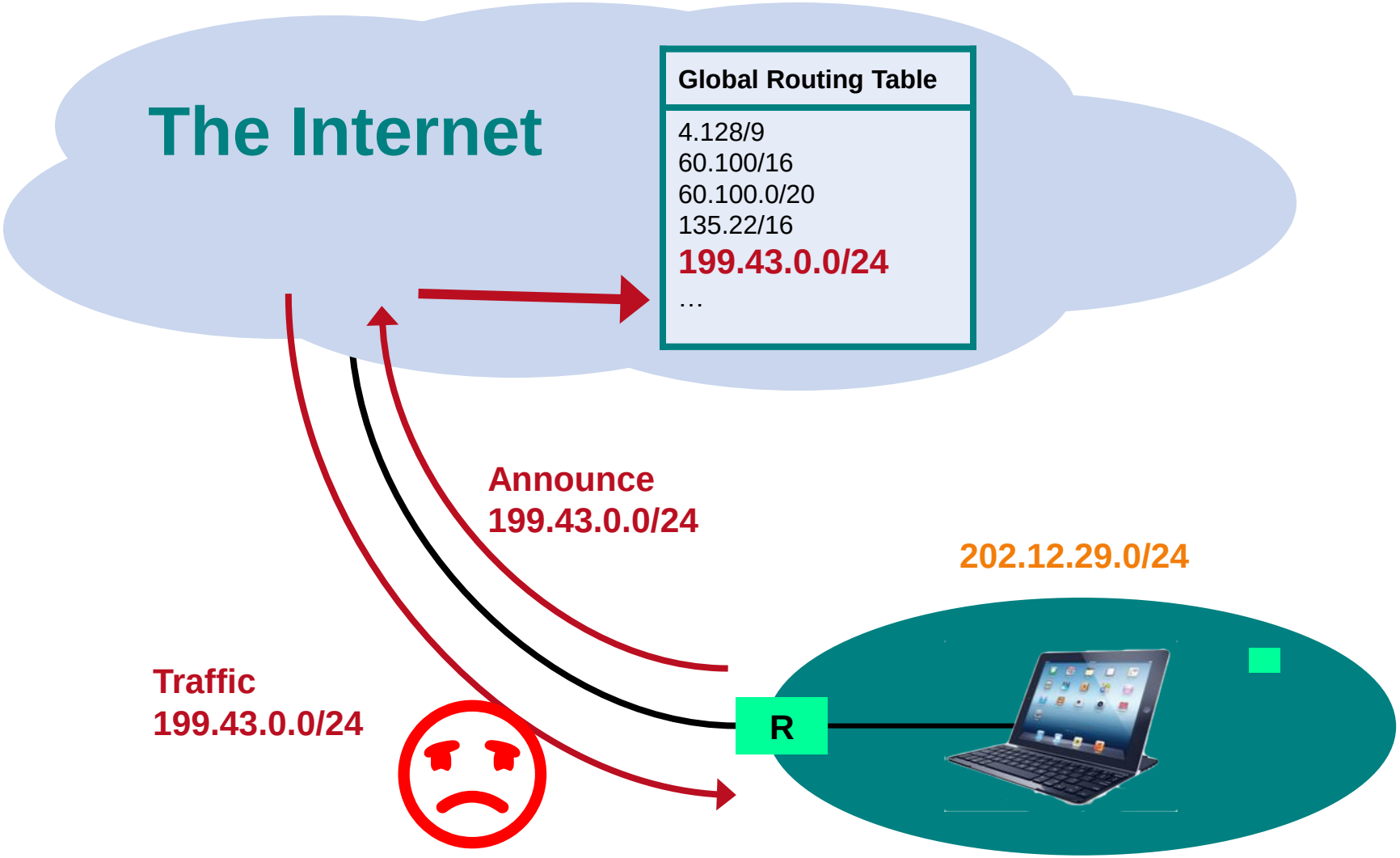
Securing websites – SSL certificates



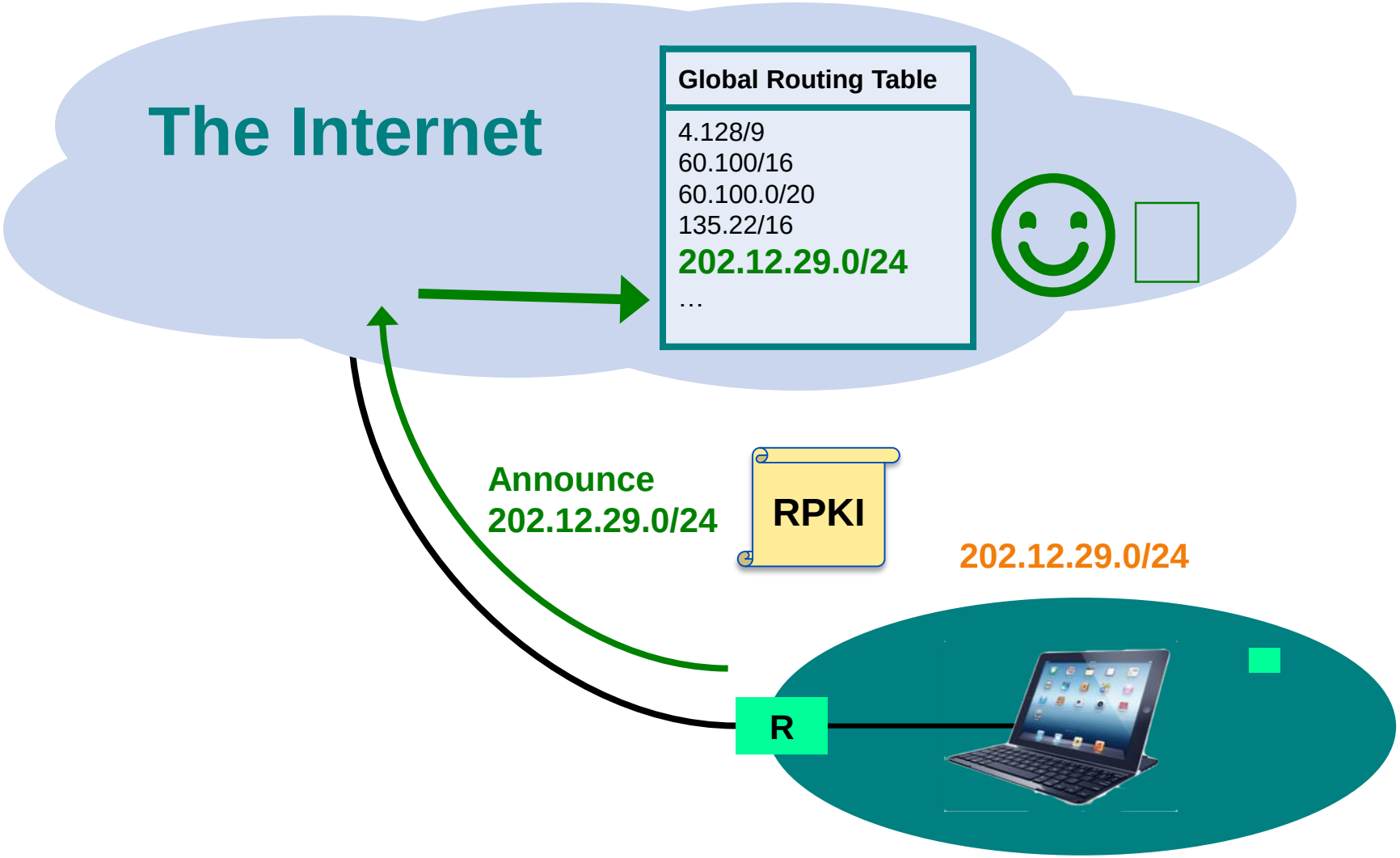
Securing DNS – DNSSEC



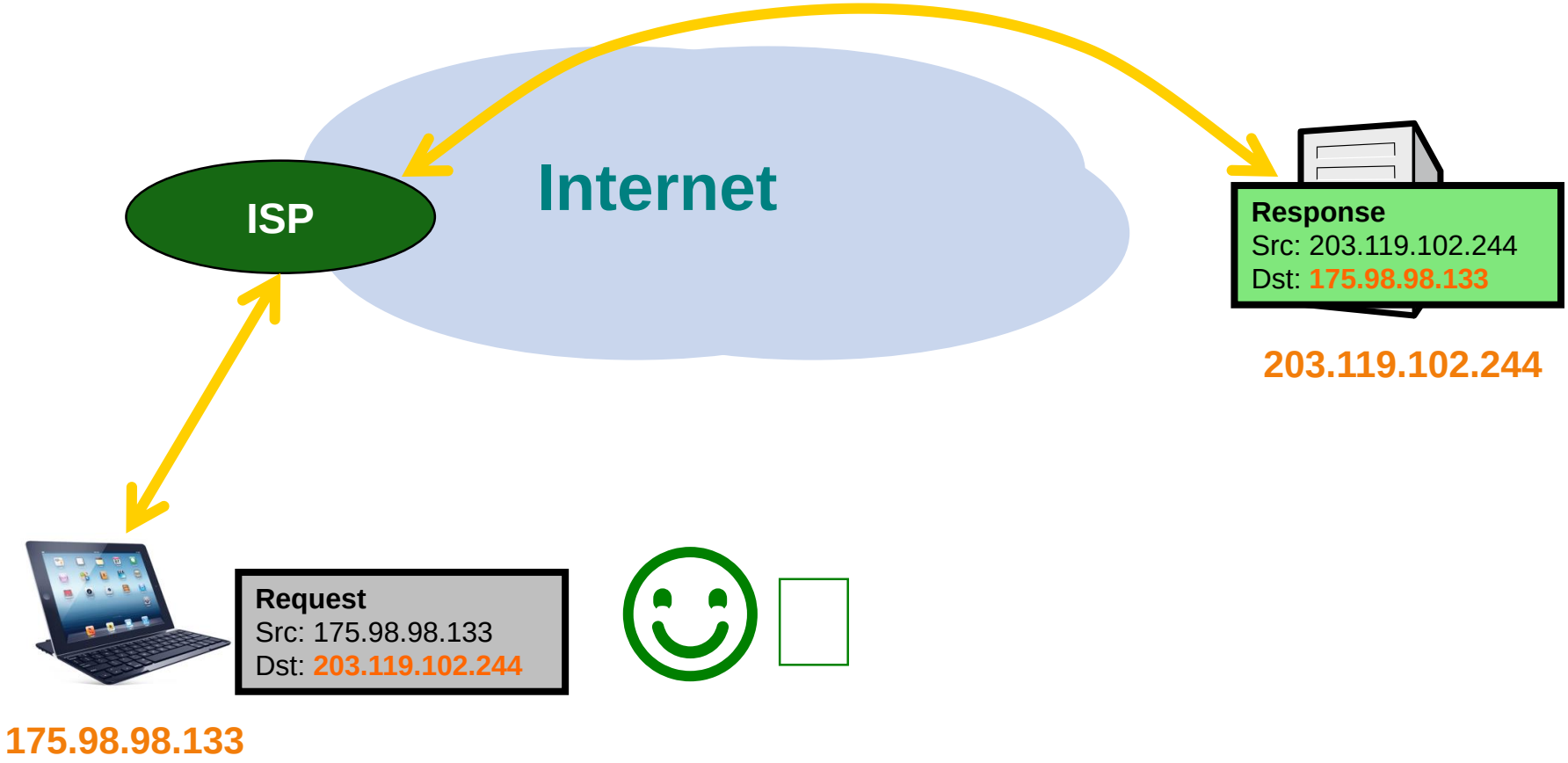
Misusing IP Addresses…



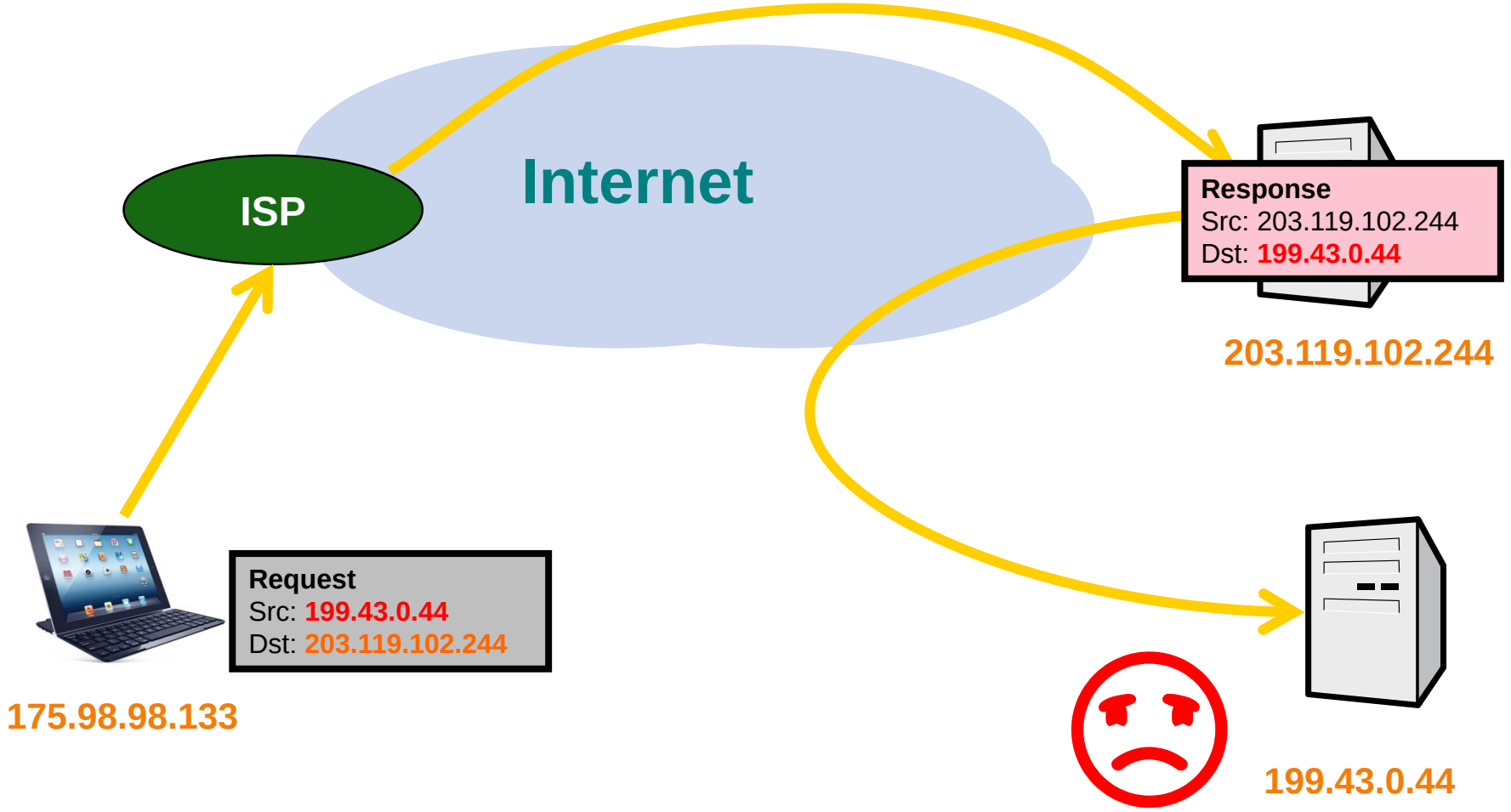
Misusing IP Addresses…



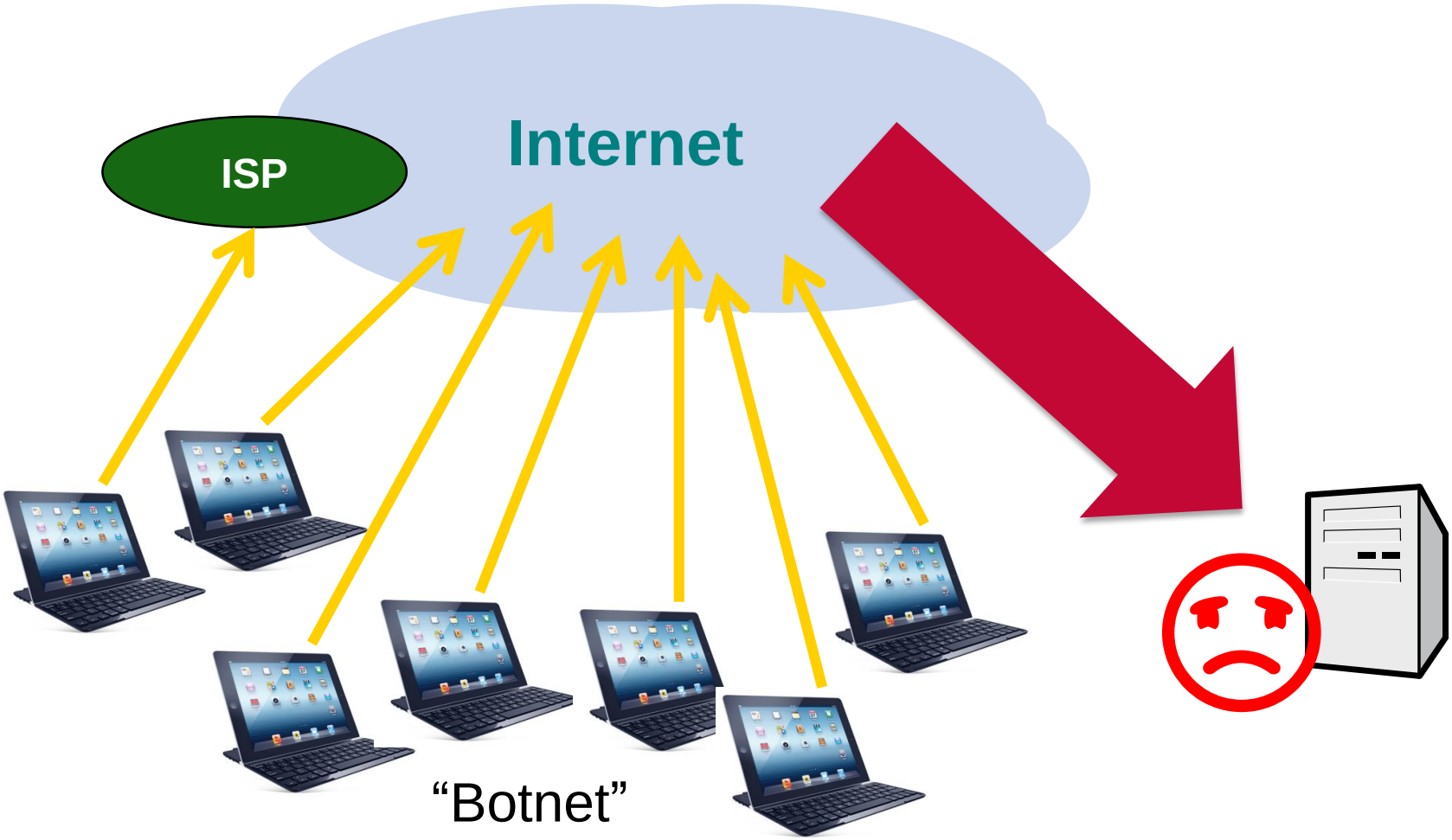
Masquerading again: IP spoofing



Masquerading again: IP spoofing



DDoS attack: Distributed DoS



Questions?

Thank you

@Iphinojosa

APNIC