Fundamentals of Network Security

Asia Pacific Internet Leadership Program
Taipei, TW

26 July 2016

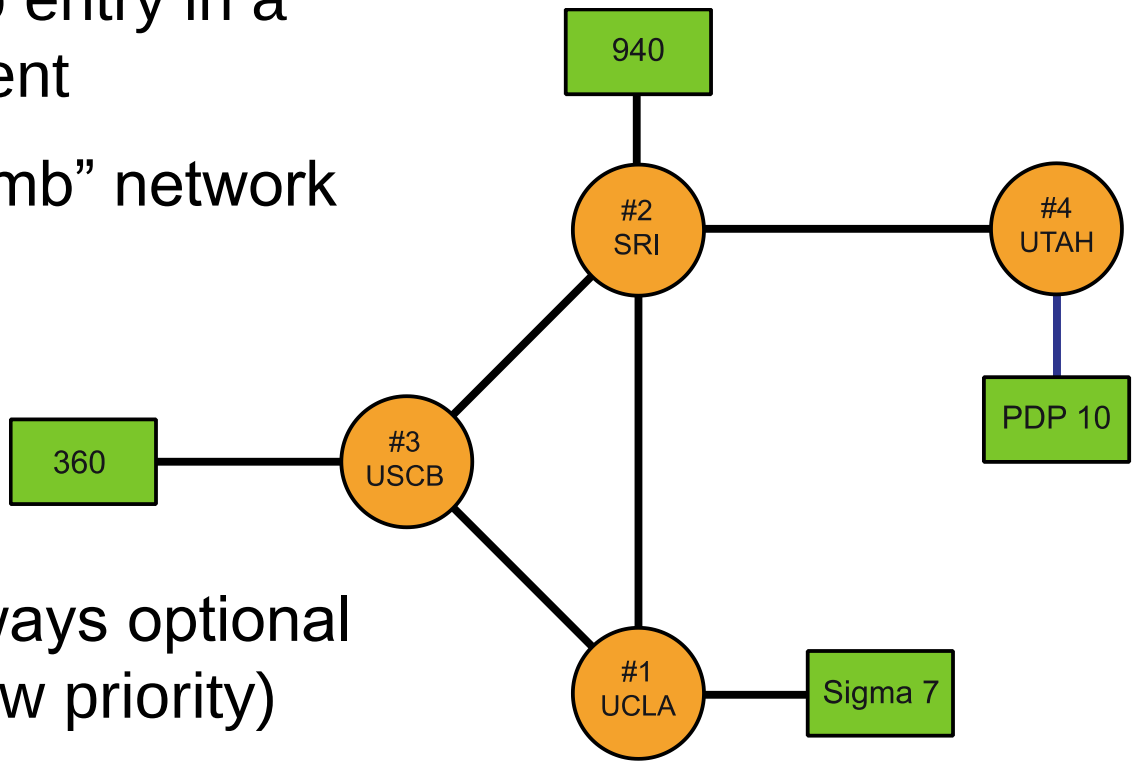
APNIC

What's coming up

- Is the Internet secure?
- Myths and Mysteries
- Evolution of security
- Security concepts and management
- Examples
- Developments: IPv6 and IoT
- The Internet security ecosystem

Is the Internet secure?

- The Internet was designed for open connectivity
- For low barriers to entry in a trusting environment
- A deliberately “dumb” network



- “Security” was always optional (and normally a low priority)

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!)

Myths and Mysteries

- Fiction: The Internet can be secured
- Fiction: Hackers are magicians
- Fiction: Security experts are the magicians
- Fiction: Computer viruses are like actual viruses

- Fact: The Internet can be used securely
- Fact: EVERY breach can be explained, and avoided
- Fact: The first bug was an actual moth

Some history…

- 1946: Grace Hopper, a US Naval Officer, tracks down a moth causing problems in an electromechanical computer; hence “**bug**”.
- 1960s: MIT model train group "**hacks**" their trains to make them perform better
- 1971: Joe Draper aka "Captain Crunch", uses cereal toy to generate 2600 Hz tone, “**phreaking**” the AT&T long distance system
- 1983: "War Games" film introduces public to the concept of hacking, and “**wardialing**”
- 1988: Cornell student Robert Morris Jr. releases self-replicating “**worm**” on ARPAnet, the first Internet-borne viral programme
- Late 1990s: Online sharing of automated tools. The first “**botnets**” – armies of virus-infected machines.

Terms: Breaking it down

- Threat
  - Any circumstance or factor with the potential to cause harm
  - *a motivated, capable adversary*
- Vulnerability
  - A weakness in a system; in procedures, design, or implementation that can be exploited
    - Software bugs, design flaws, operational mistakes
    - The human factor – “Social engineering”
- Risk = likelihood x consequence
  - The liklihood (probablility) that a particular vulnerability will occur
  - The severity (impact) of that occurrence

Authentication and Authorisation

- *Access control*
  - *The ability to permit or deny the use of a resource by a user, through three essential services…*
- Authentication
  - To reliably identify individual users
  - Users = people, processes, devices
- Authorisation
  - To control which users are allowed to do what with a resource
  - Representing trust, assuming reliable authentication

Security tradeoffs

- Services offered vs. security provided
  - Each service offers its own security risk
  - The more services, the less security
- Ease of use vs. security
  - Every security mechanism causes inconvenience
  - The more “plug n play”, the less security
- Risk of loss vs. Cost of security
  - Assets carry value and risk of loss
  - The higher the value, the higher the security cost
- These factors can be balanced in a comprehensive organisational security policy

An unexpected success…

1990s: Basic connectivity

2000s: Application-specific online content

2010s: Applications/data in the "cloud"

2020s: "IoT"

- Evolution of technology, usage and value
- Evolution of security problems and solutions
- Evolution never stops…

What is going on?

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
- DNS attacks
  - Corruption and cache poisoning
- Masquerading
  - Address “spoofing”
- Denial of Service
  - DoS attacks
  - DDoS attacks

“Phishing”

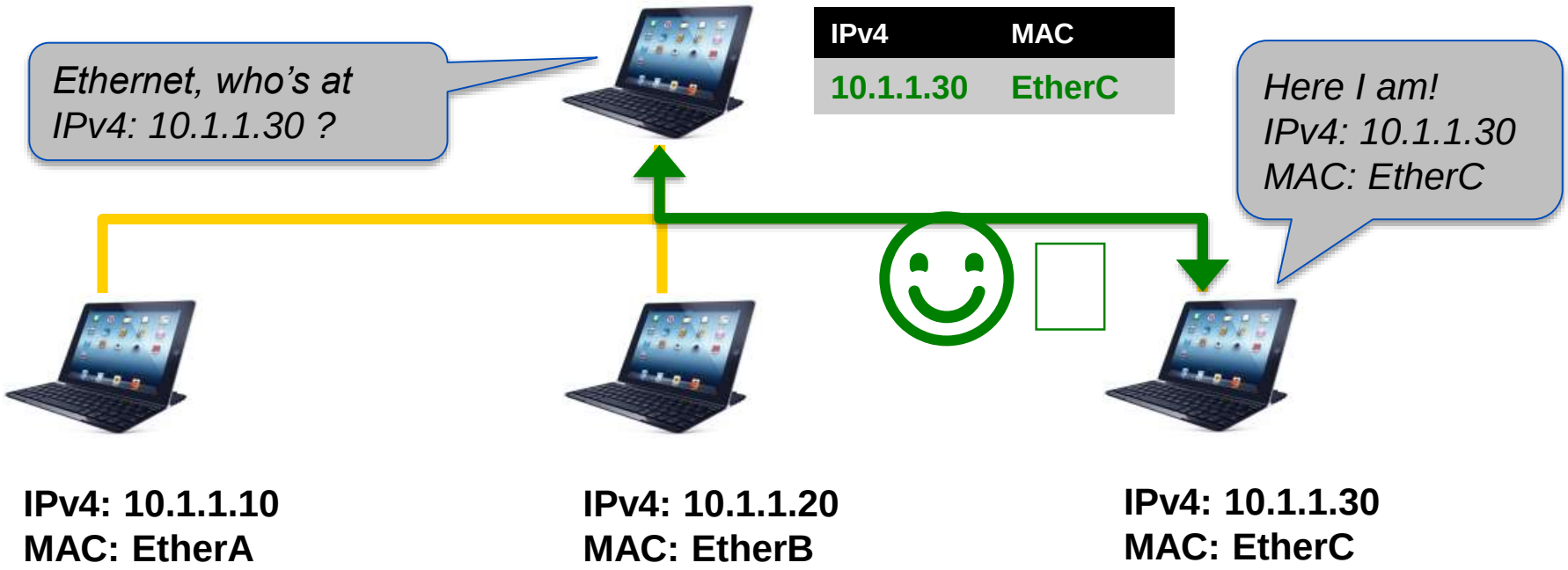
- “Fishing” for information such as usernames, passwords, credit card details, other personal information
- Forged emails apparently from legitimate enterprises, direct users to forged websites.

Other social engineering

- Password guessing or cracking
  - Hence need for “non-guessable” passwords
  - Use of different passwords for different services
- Email harvesting and “proof of life”
  - Misuse of collected personal information
  - Spam as a validation tool
    - embedded images – Turn them off!
    - unique URLs – Don’t click on anything!
- Short URLs
  - E.g. http://bit.ly/SGWjdif
  - We’re accustomed to clicking without checking where we go next

Masquerading example: ARP

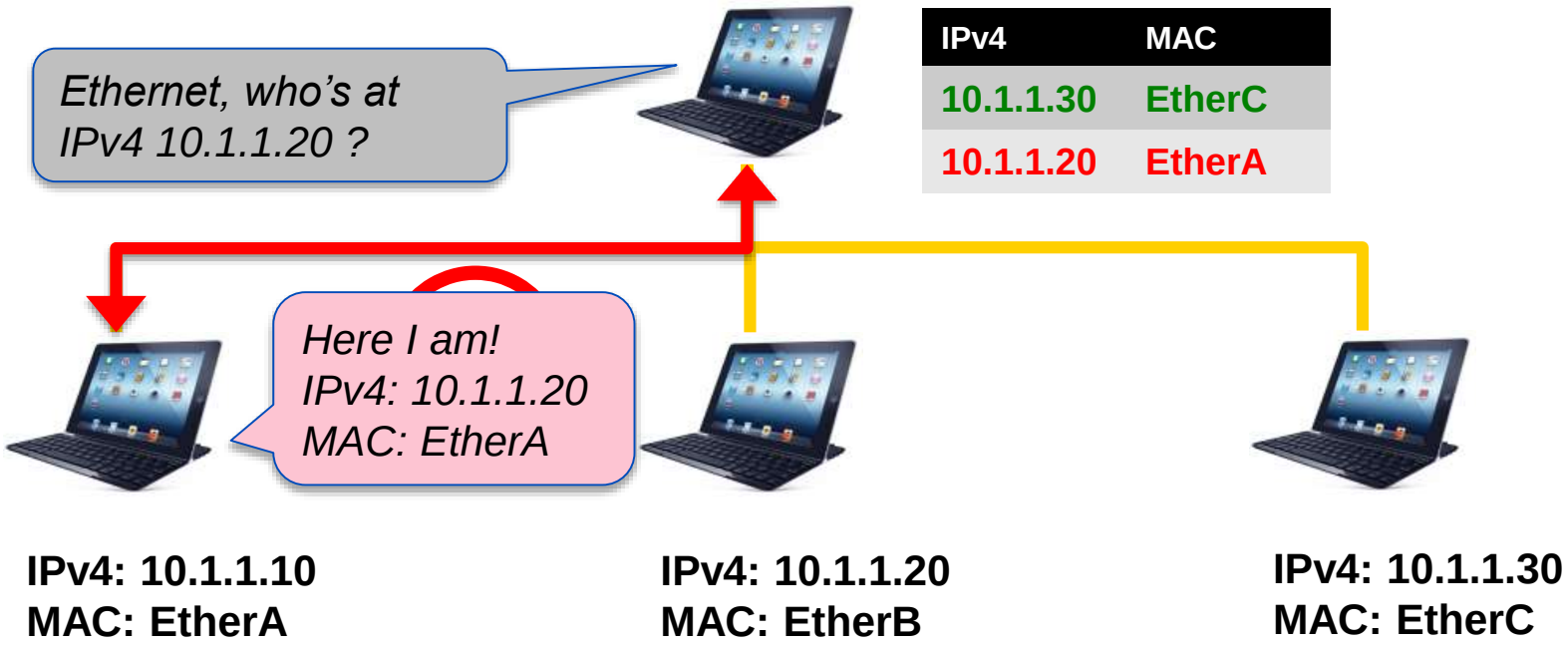
- Address Resolution Protocol (RFC 826, 1982)
  - Used by any TCP/IP device to discover the Layer 2 address of an IPv4 address that it wants to reach



*AKA "ARP spoofing"

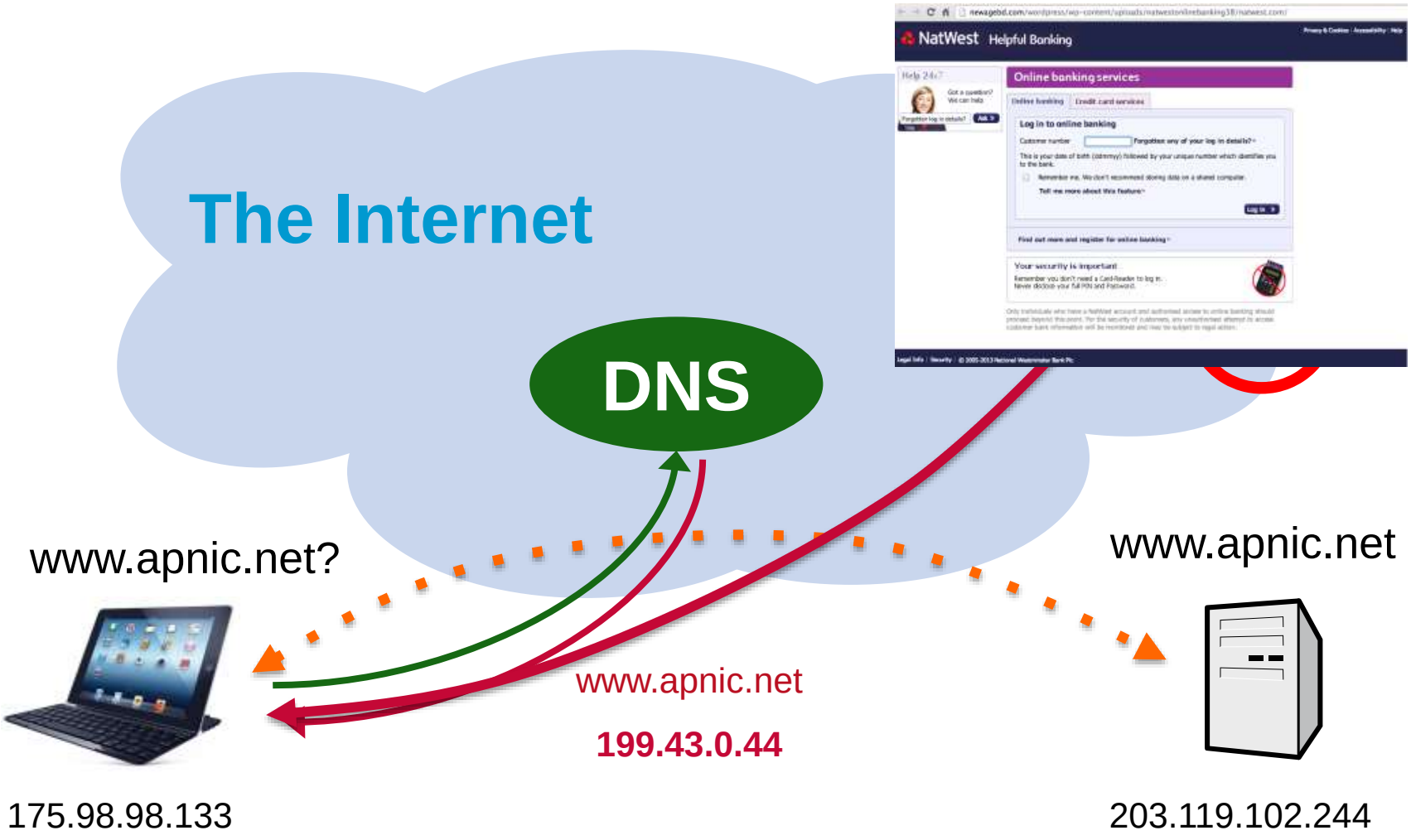
Masquerading example: ARP

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

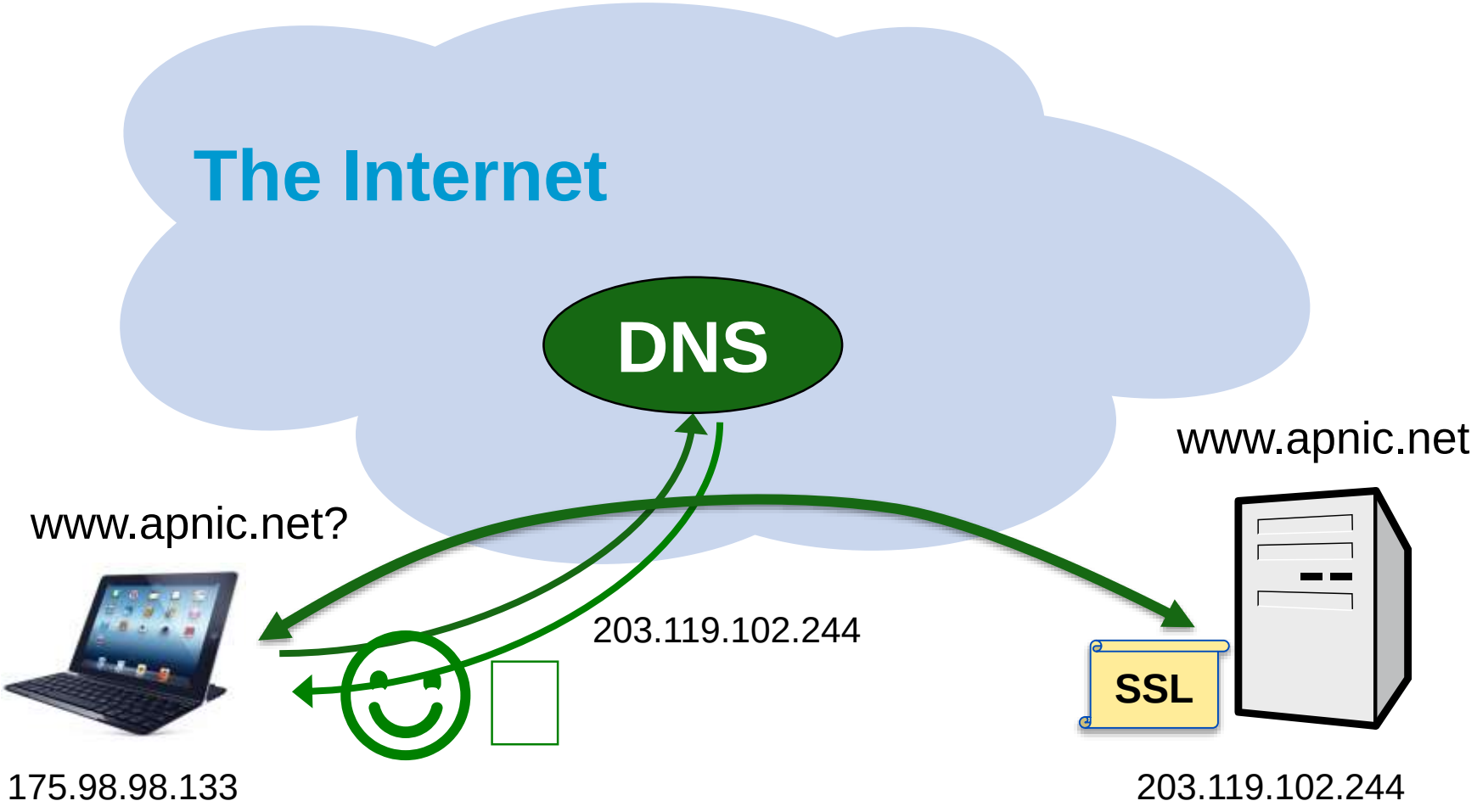


*AKA "ARP spoofing"

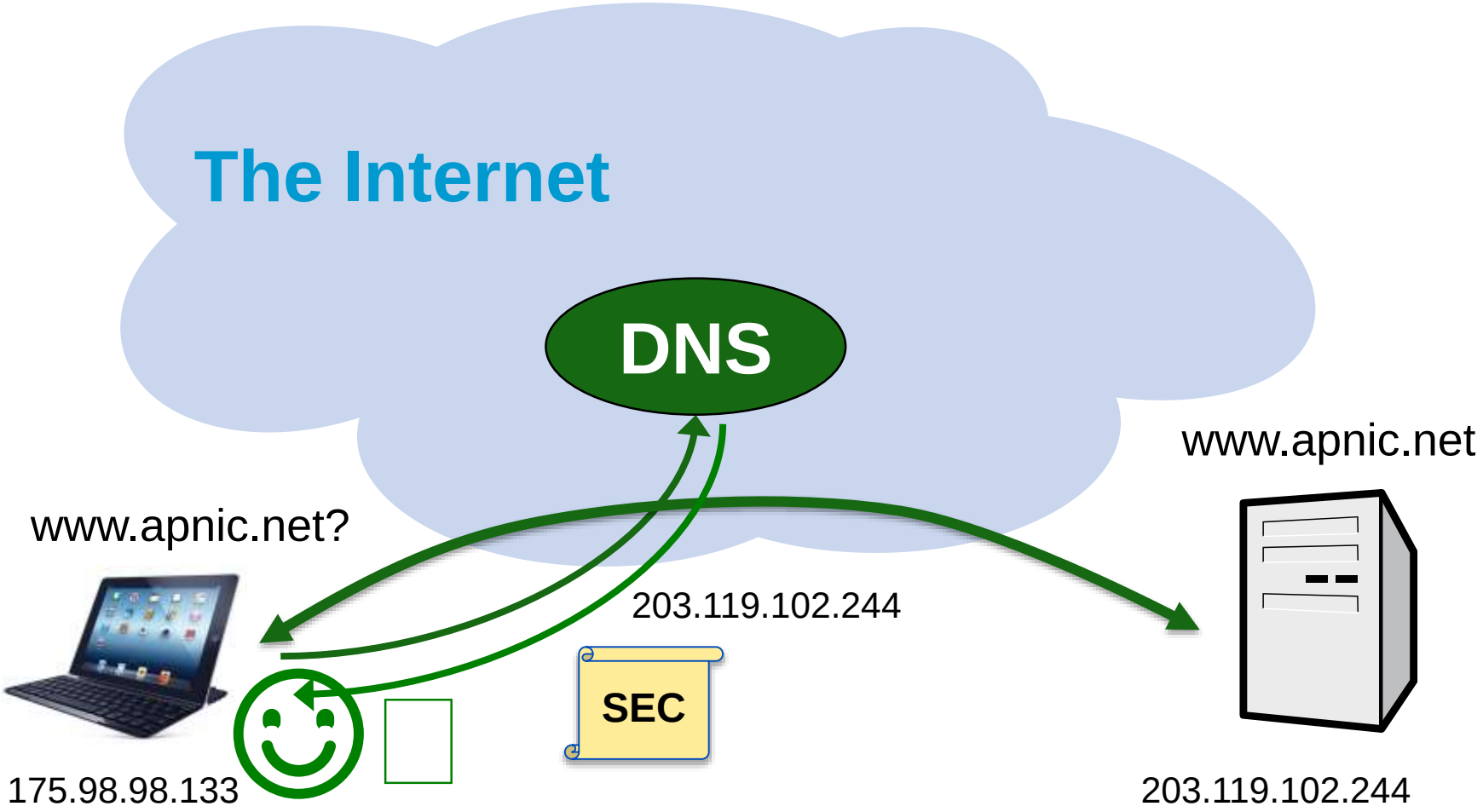
Attacking the DNS



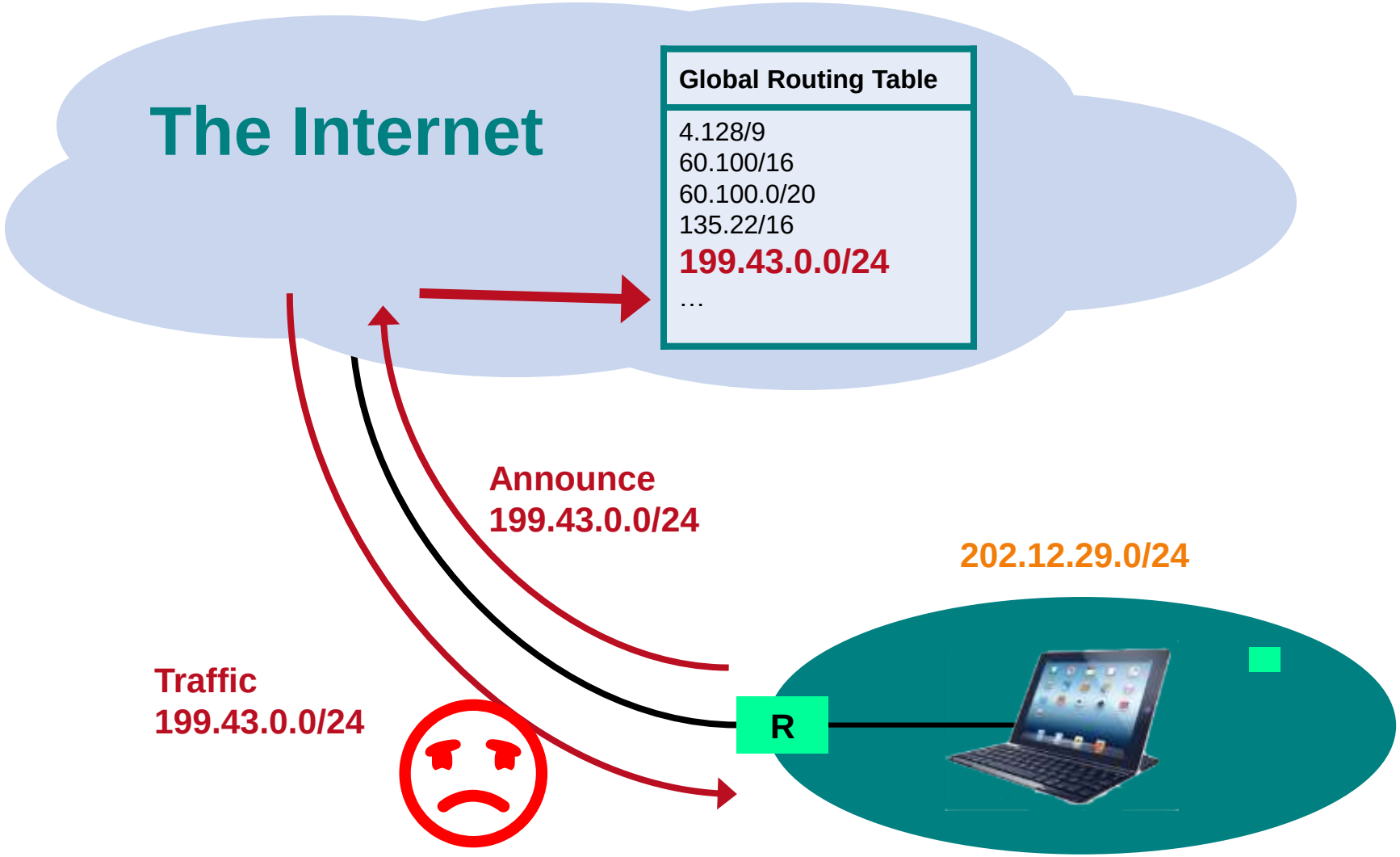
Securing websites – SSL certificates



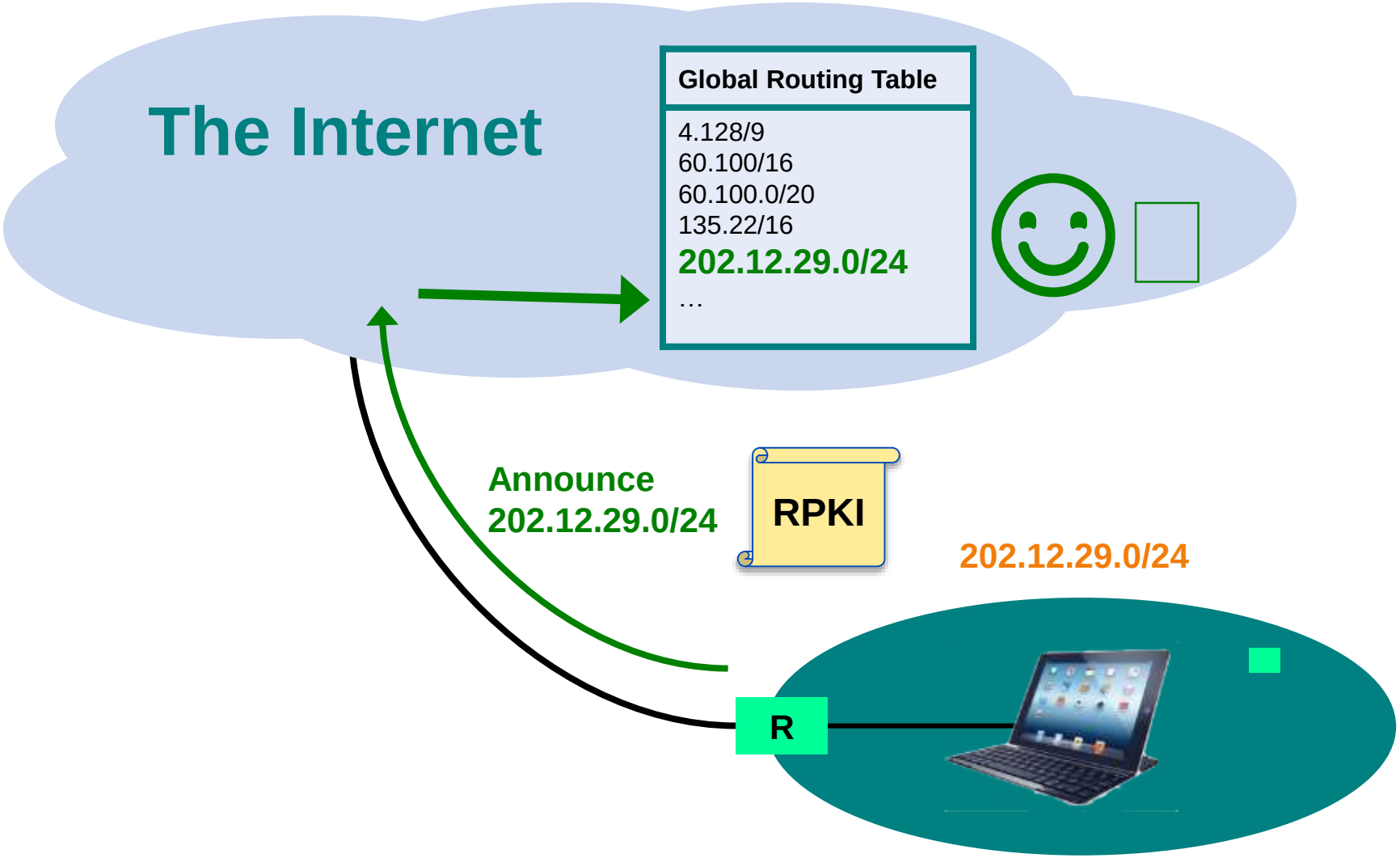
Securing DNS – DNSSEC



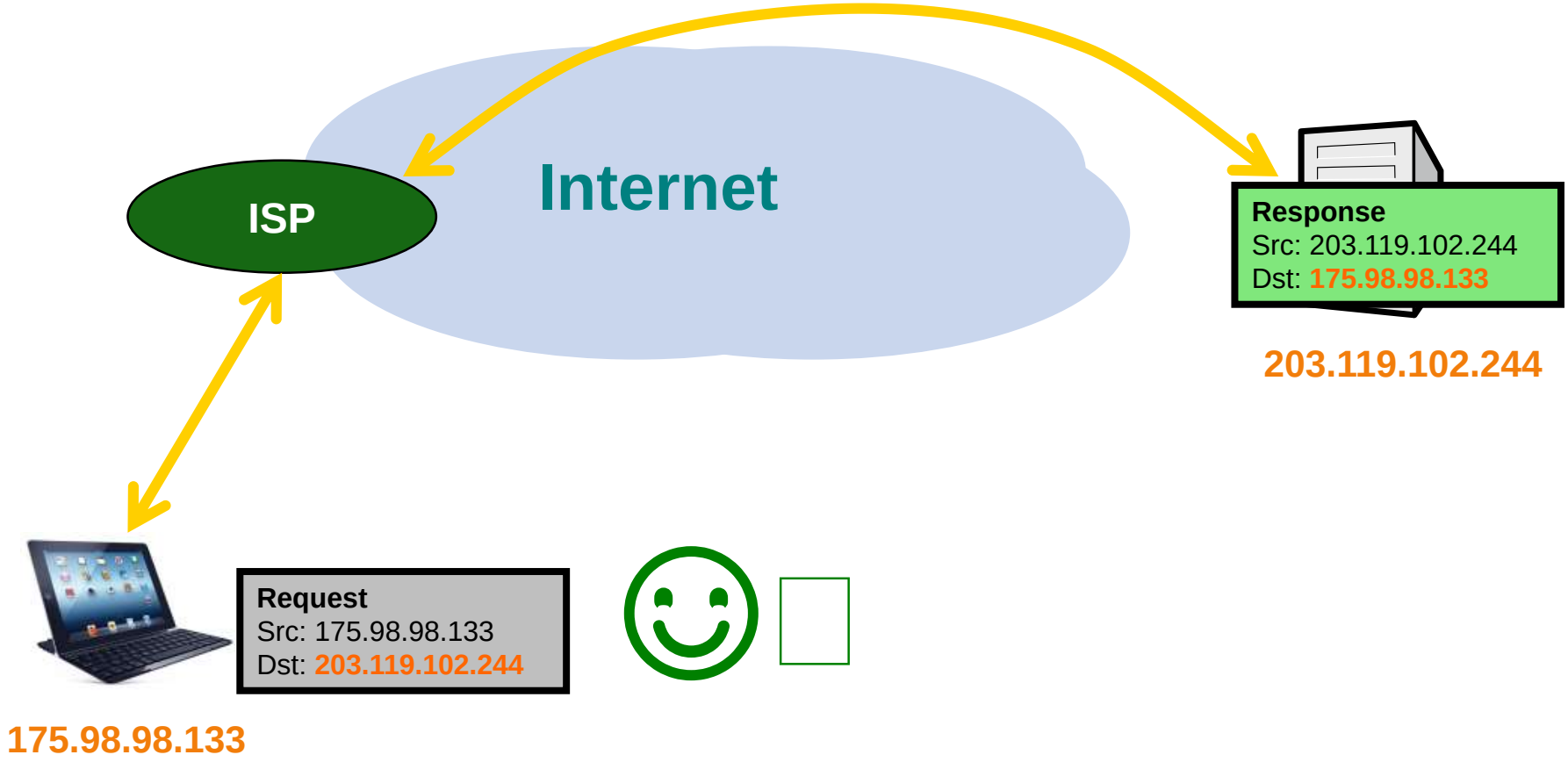
Misusing IP Addresses…



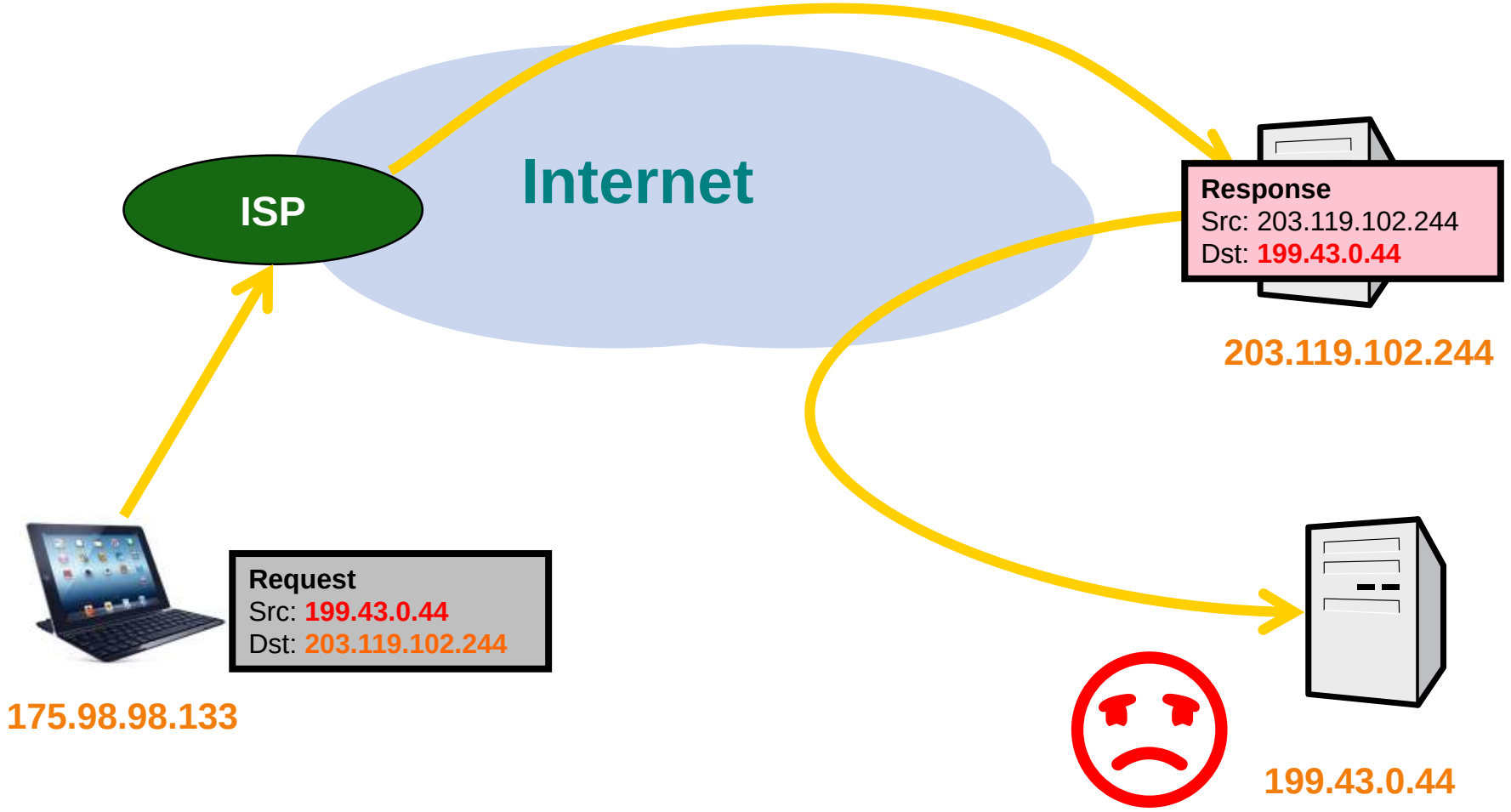
Misusing IP Addresses…



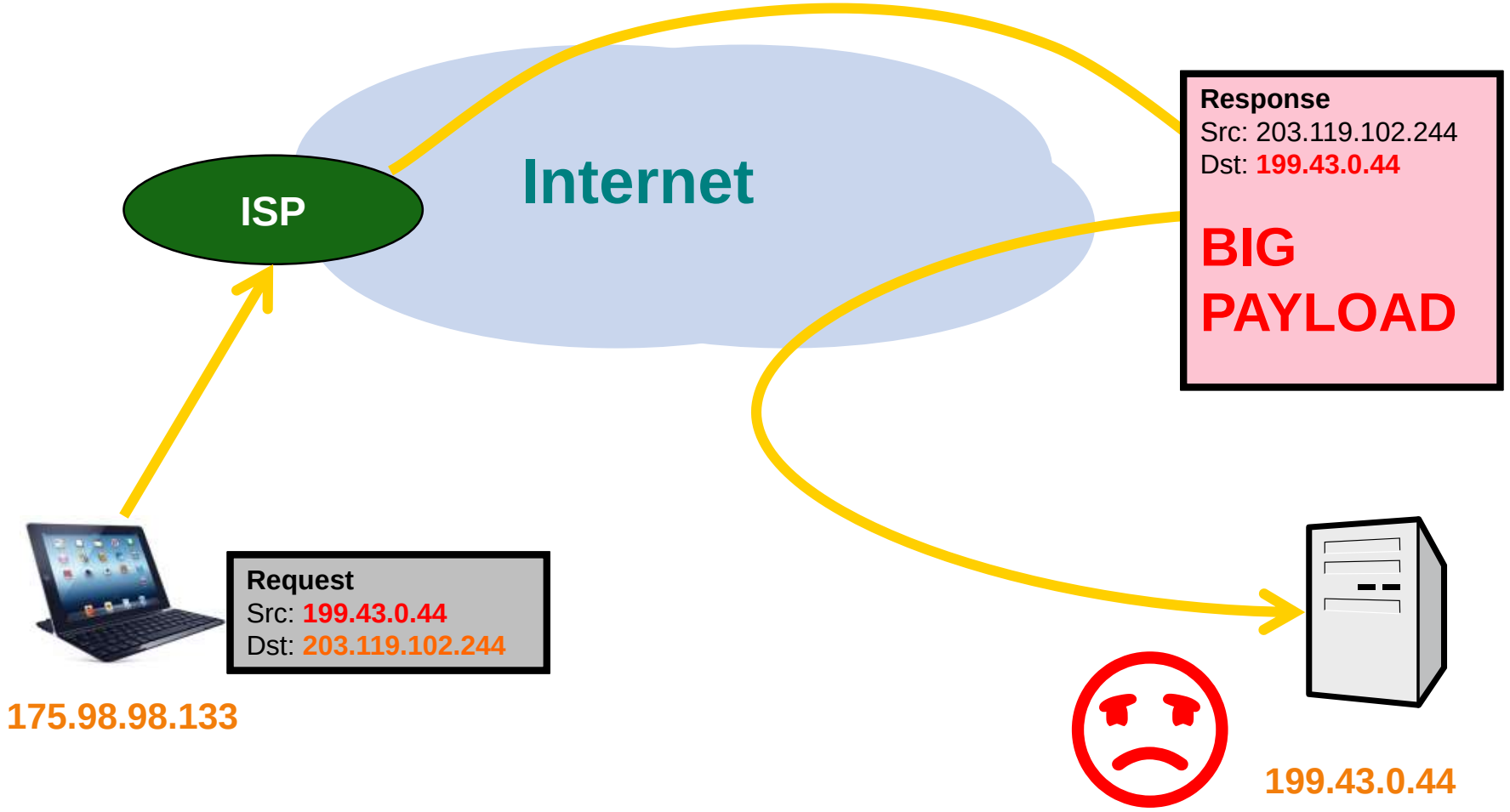
Masquerading again: IP spoofing



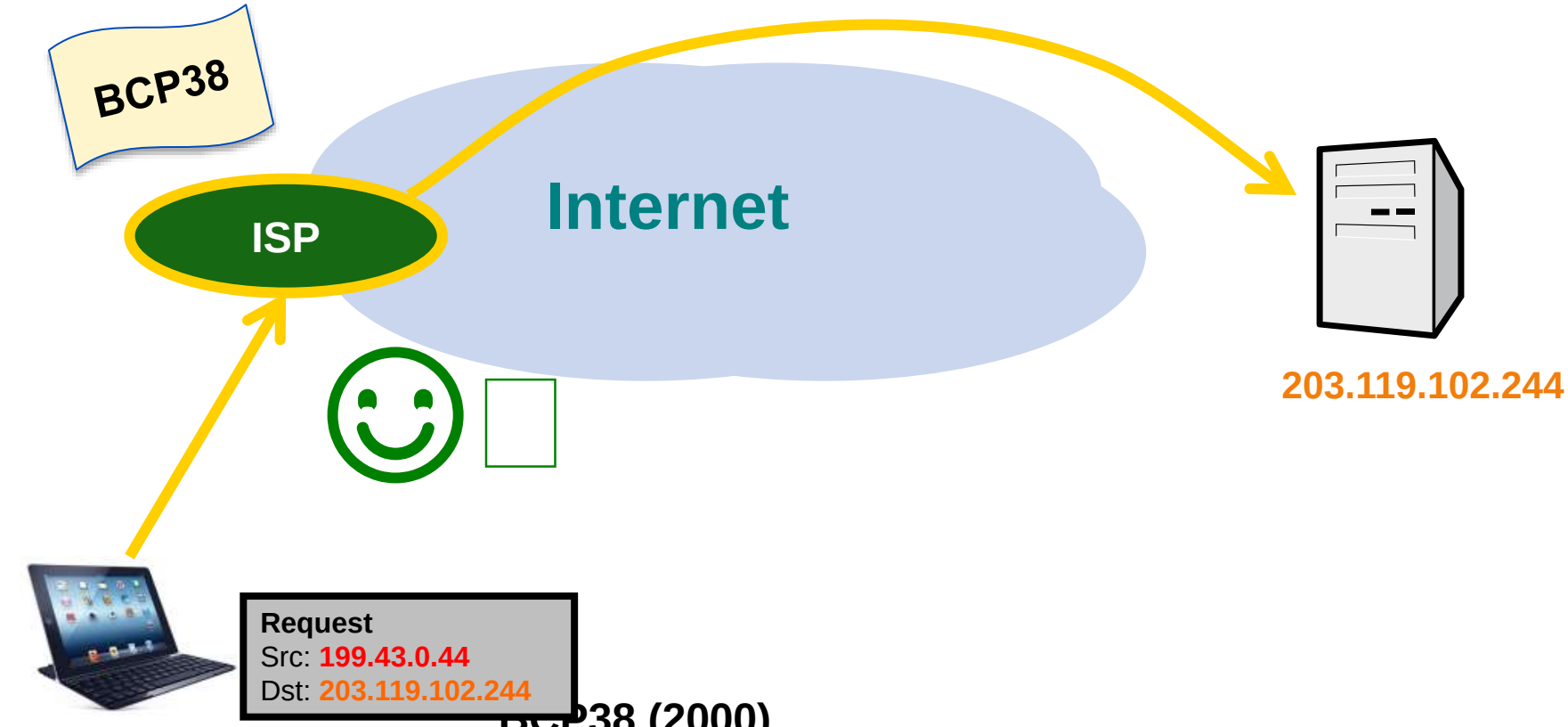
Masquerading again: IP spoofing



DoS attack: Amplification



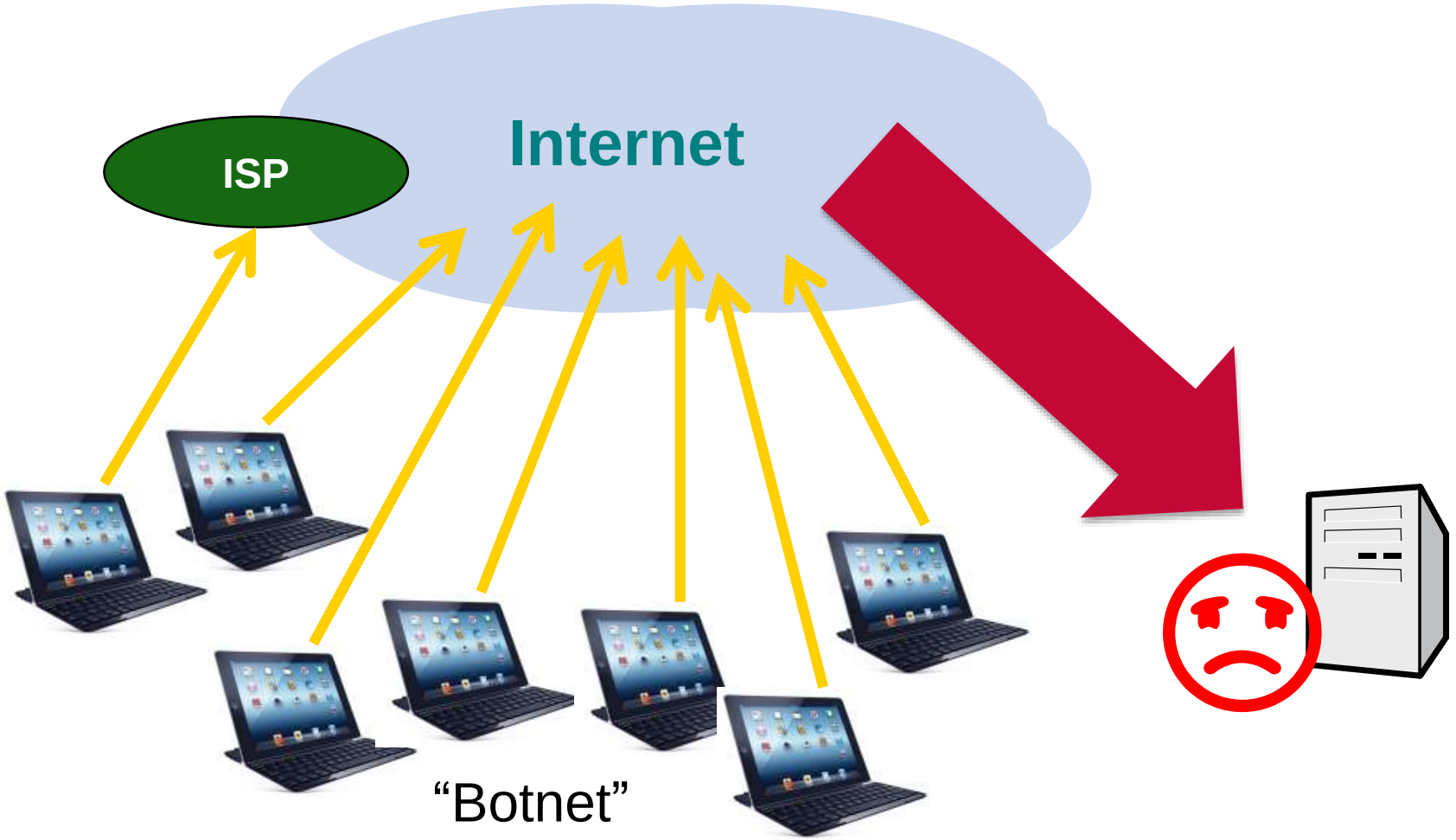
Defeating IP spoofing – BCP38



BCP38 (2000)

Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing

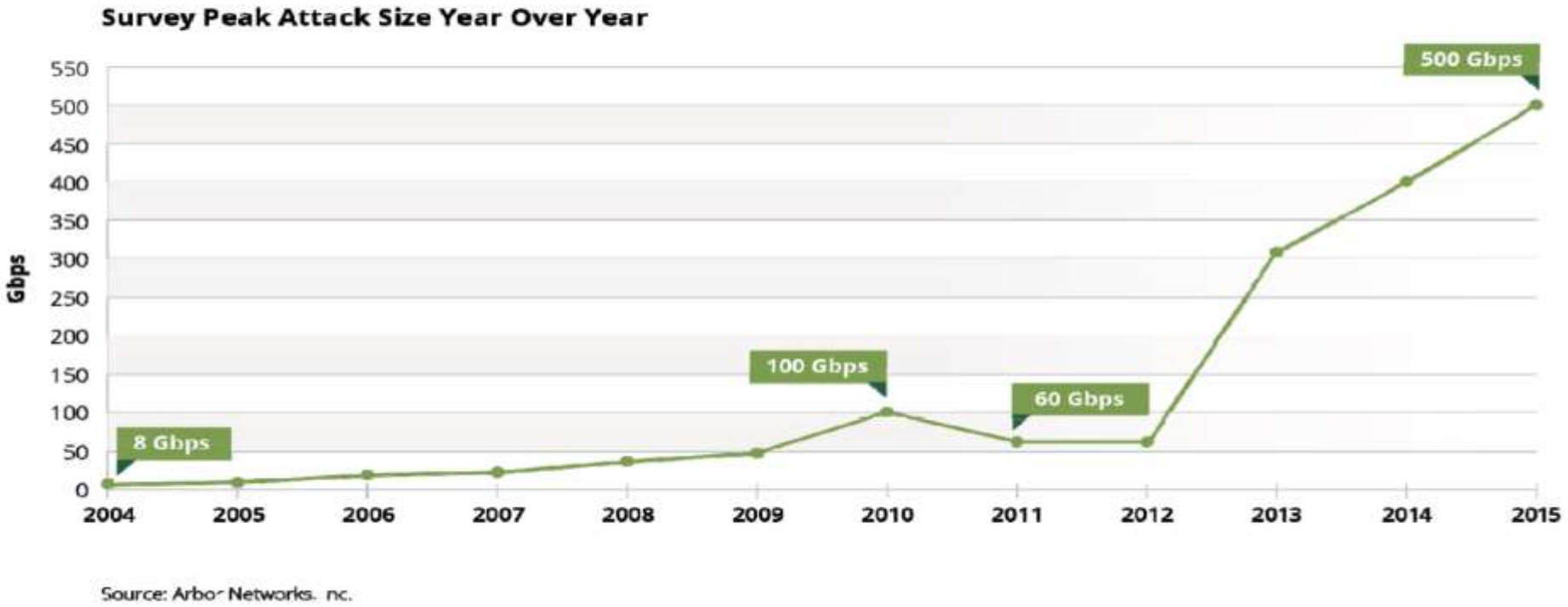
DDoS attack: Distributed DoS



DDoS attack: Distributed DoS

- Botnets for hire
  - Millions of virus-infected computers
  - Ready to be deployed by remote control
- Huge amplification
  - Target traffic volumes in 100s of Gbps
- Motivation
  - Various, but often extortion (requiring payment in BTC)
- Mitigation
  - Various approaches and services available
  - Often bandwidth is the best solution (using cloud-based services)

DDoS - Growth Continues



Source: Arbor Networks, Inc.

- Largest attack reported was 500 Gbps with other respondents reporting attacks of 450 Gbps, 425 Gbps, and 337 Gbps.

Source: Arbor Networks' WISR 2016 Survey

Security and IPv6

- “IPsec” is mandatory in IPv6 implementation
  - but this does not mean it must be used.
- No difference…
  - Traffic monitoring (Sniffing) – no change without IPsec
  - Application vulnerabilities – no change
  - Rogue devices, viruses etc
- Improvements…
  - IPsec available when needed (eg routing protocols)
  - Scanning address space for devices is much harder
- Threats
  - New expertise required, new implementations, less mature
  - Mistakes will be made

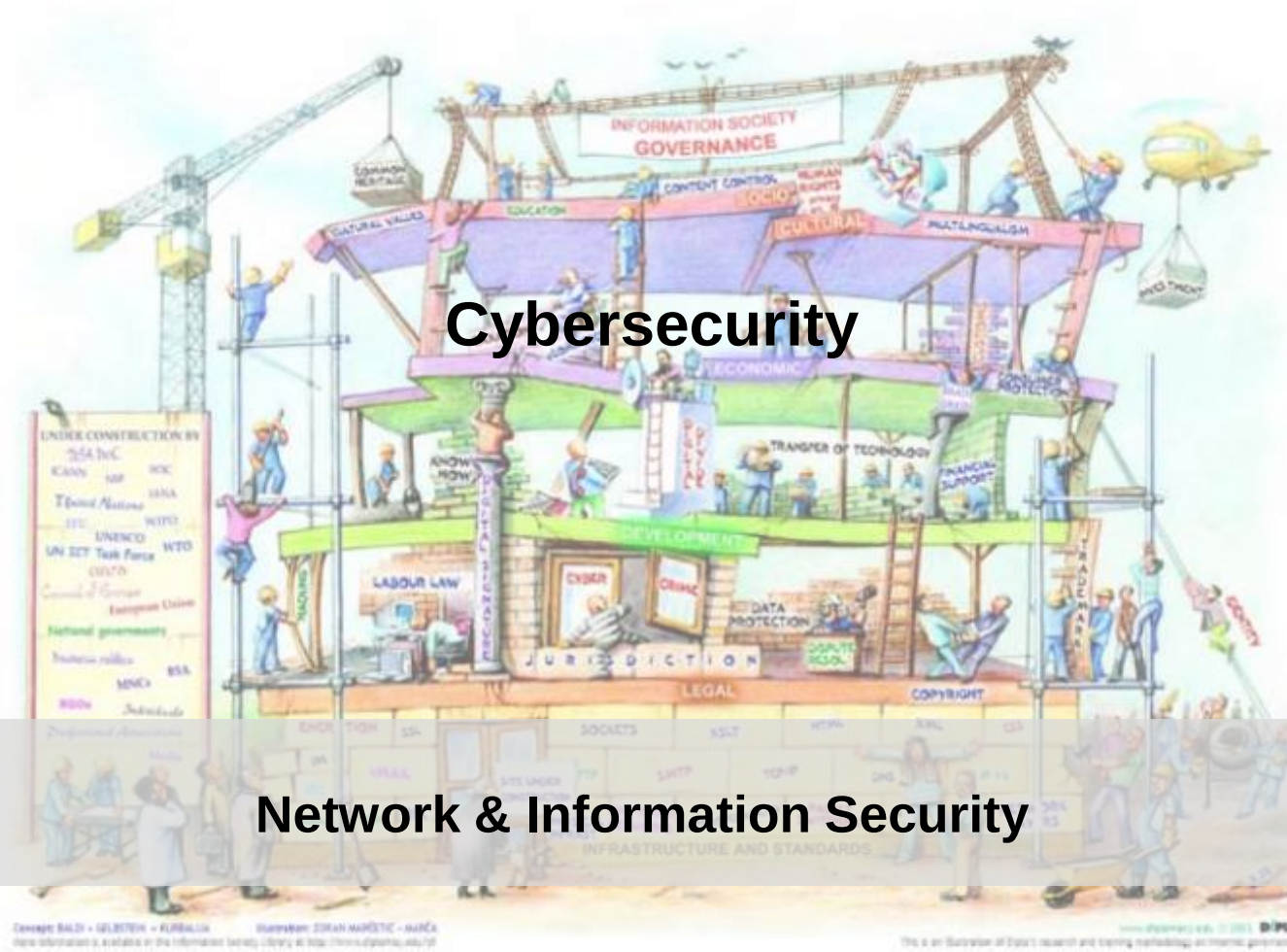
Security and IoT

- We have a long history of “things” on the Internet
  - In that sense, there is nothing fundamentally new with “IoT”
- However…
  - There will be huge increase in the variety of devices
  - Many new vendors will enter the market
  - Many vendors are not “Internet companies”
- Challenges
  - Implementation, Testing, Software upgrades, “EoL” management
- Reference: “Internet of stupid things”
  - Geoff Huston, APNIC

Internet Security Ecosystem

APNIC

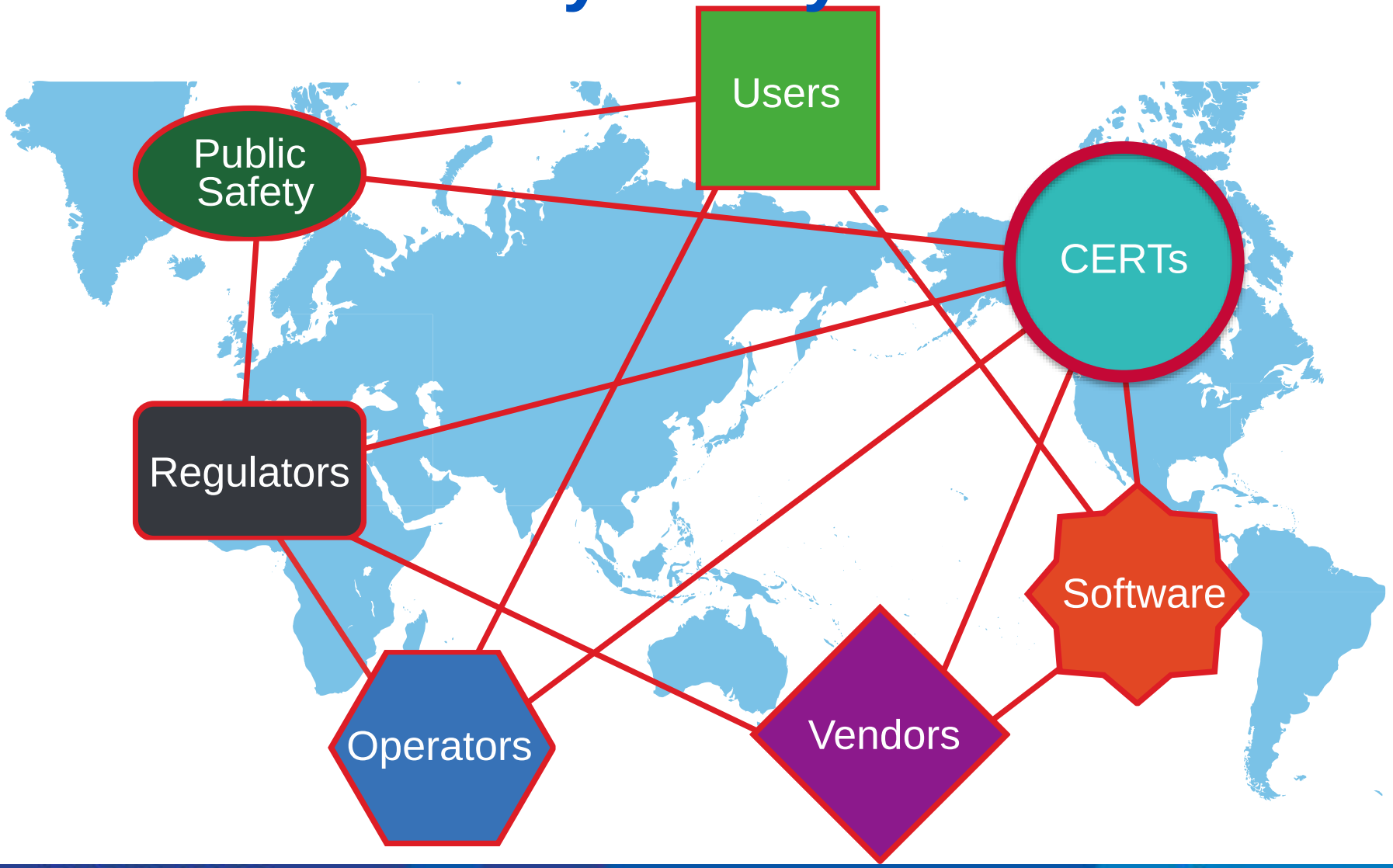
The Bigger Picture



Cybersecurity

Network & Information Security

Internet Security Ecosystem



Asia-Pacific CERTs

coordination

incident response

info sharing

Recap…

- Is the Internet secure?
- Myths and Mysteries
- Evolution of security
- Security concepts and management
- Examples
- Developments: IPv6 and IoT
- The Internet security ecosystem

Questions?

Thank you

dg@apnic.net

APNIC