Copyright Notice

This set of transparencies, hereinafter referred to as slides, is protected by copyright laws and provisions of International Treaties. The title and copyright regarding the slides (including, but not limited to, each and every image, photography, animation, video, audio, music and text) are property of the authors specified on page 1.

The slides may be reproduced and used freely by research institutes, schools and Universities for non-profit, institutional purposes. In such cases, no authorization is requested.

Any total or partial use or reproduction (including, but not limited to, reproduction on magnetic media, computer networks, and printed reproduction) is forbidden, unless explicitly authorized by the authors by means of written license.

Information included in these slides is deemed as accurate at the date of publication. Such information is supplied for merely educational purposes and may not be used in designing systems, products, networks, etc. In any case, these slides are subject to changes without any previous notice. The authors do not assume any responsibility for the contents of these slides (including, but not limited to, accuracy, completeness, enforceability, updated-ness of information hereinafter provided).

In any case, accordance with information hereinafter included must not be declared.

In any case, this copyright notice must never be removed and must be reported even in partial uses.
ping and DNS Resolution

Capture the traffic sent and received by a station executing the command

- `ping [name]`

- Make sure, prior to execution, that
  - the ARP cache is empty (use `arp` command)
  - the DNS cache is empty (use `ipconfig` command)

- Consider the following questions
  - How many ARP requests are generated? For which addresses?
  - Compare the Time To Live value associated to the name resolved in the DNS cache of the station and in the DNS response messages
traceroute and DNS Resolution

Capture the traffic sent and received by a station executing the command
- `tracert [name]` (Windows)
- `traceroute [name]` (Unix)

- Make sure, prior to execution, that
  - the ARP cache is empty (use `arp` command)
  - the DNS cache is empty (use `ipconfig` command)

- Consider the following questions
  - What is the source IP address of the packets generated by the command?
  - What is the destination IP address of the packets generated by the command?
  - What is the source IP address of the packets received by the command?
  - Does the destination IP address of the packets used by the command change over time?
  - Does the destination MAC address of the packets used by the command change over time?
  - How many DNS query/response sessions take place? What for?
    - How does the command handle cases in which the DNS query fails?
nslookup

- Execute the `nslookup` program in interactive mode (no parameters)
- Set DNS server to netgroup.polito.it (130.192.225.79)
- List (`ls` command) type A entries and aliases (non-canonical names) for domain ipv6.polito.it
  - Is netgroup.ipv6.polito.it a canonical name? If not, what is the canonical name of the host?
- Repeat same operations for domain polito.it; if they fail, explain why.
- Verify whether resolution requests (not using `ls`) for other domains (e.g., cisco.com, google.com) are successful
- Capture traffic when visualizing information (e.g., CPU, OS) stored in the DNS about hosts of domain ipv6.polito.it
  - Use type `ANY` requests
  - Which operations use TCP/UDP and why?
- Capture traffic when resolving `chebasti` and `didattica`.
  - Are both resolutions successful? Why?
  - What are the names actually resolved?
- Tip: check out `srchlist` option