Basic Traffic Analysis
Exercises

Mario Baldi
Politecnico di Torino
(Technical University of Turin)
http://www.baldime
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.
Exercise 2: IP Header

Using the capture of the previous exercise (or a new one)

- Do all the captured Ethernet frames contain IP packets?
  - How can we know whether a captured frame contains an IP packet?

- Observe the header and all of the fields of a few IP packets
  - What is the version of the protocol?
  - What is the destination address?
  - What is the source address?
  - How is the protocol of the packet carried in the payload field identified?
  - What is the value of the TTL field?
  - What is the value of the ToS field?
  - Is there any fragmented packet?
Exercize 3: Ping

Capture the traffic resulting from a station executing the command

- ping [address]

where [address] is the IP address of another PC in the lab.

- Make sure, prior to execution, that the ARP cache is empty (use \texttt{arp} command)
  - In case of access privilege issues in flushing the ARP cache, use the \texttt{arp2} command rather than the stock \texttt{arp} command

- Use an address (e.g., 10.2.1.3), not a name (www.polito.it)

- Consider the following questions
  - What is the purpose of the first two packets in the capture (related to the execution of the command) explaining to which systems the source and destination MAC address belong?
  - Is the source MAC address in the ARP response the same as the destination MAC address of the first IP packet? Why is that the case?
  - What is the Destination IP Address in the first IP packet? What does it mean/is it used for?
  - What is the source IP address of the packets used by ping?
  - What is the destination IP address of the packets used by ping?
  - Does the MAC destination address of the first packet belong to the host targeted with the ping command?
Exercise 4: Ping

Capture the traffic resulting from a station executing the command

- ping 130.192.182.33

- Make sure, prior to execution, that the ARP cache is empty (use `arp` command)
  - In case of access privilege issues in flushing the ARP cache, use the `arp2` command rather than the stock `arp` command
- Use an address (e.g., 10.2.1.3), not a name (`www.polito.it`)
- Consider the following questions
  - What is the purpose of the first two packets in the capture (related to the execution of the command) explaining to which systems the source and destination MAC address belong?
  - Is the source MAC address in the ARP response the same as the destination MAC address of the first IP packet? Why is that the case?
  - What is the Destination IP Address in the first IP packet? What does it mean/is it used for?
  - What is the source IP address of the packets used by ping?
  - What is the destination IP address of the packets used by ping?
  - Does the MAC destination address of the first packet belong to the host targeted with the ping command?
Exercise 5: Traceroute

Capture the traffic resulting from a station executing the command

- `tracert -d 130.192.182.33` *(Windows)*
- `traceroute -n 130.192.182.33` *(Unix)*

- Make sure, prior to execution, that the ARP cache is empty *(use `arp` 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?
Exercise 3: Encapsulation

Start a capture, execute the following command, and then stop the capture:

- `ping 130.192.182.33`

- What is the source IP address of the packets used by ping?
- What is the destination IP address of the packets used by ping?
- Does the MAC source address of a frame carrying an IP packet belong to the host whose IP address is in the IP source address field?
  - Identify the MAC address of your host by looking at the network interface configuration of the host
- Does the MAC destination address of a frame carrying an IP packet belong to the host whose IP address is in the IP destination address field?