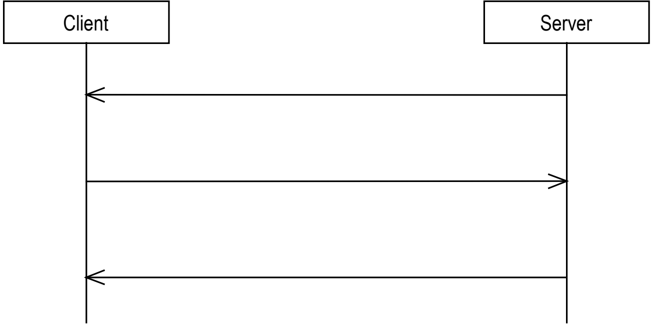
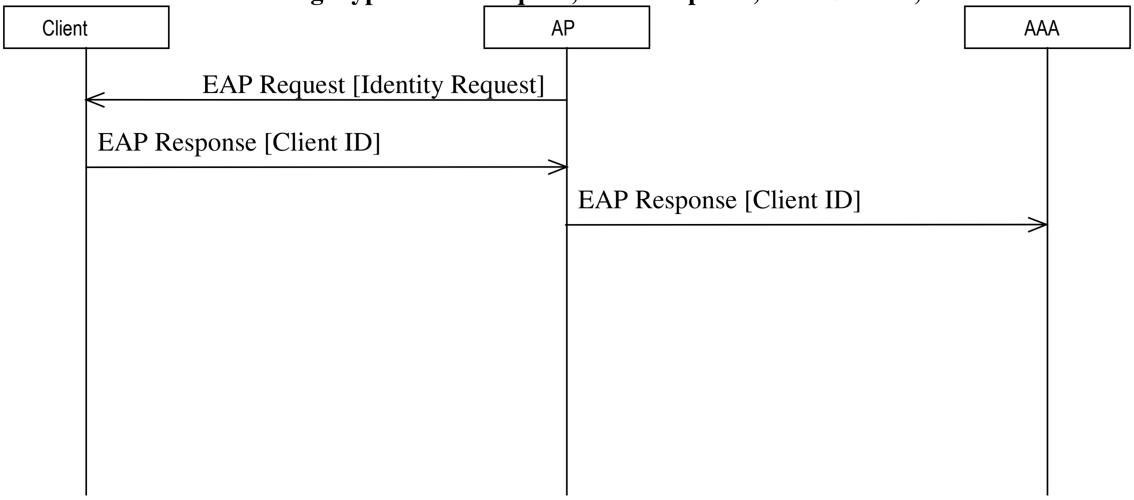
Corso di Network Security
a.a. 2012/2013

Collection of some exercises on the second part of the course

1) Specify the name of the CHAP messages exchanged between a Client e and a Server

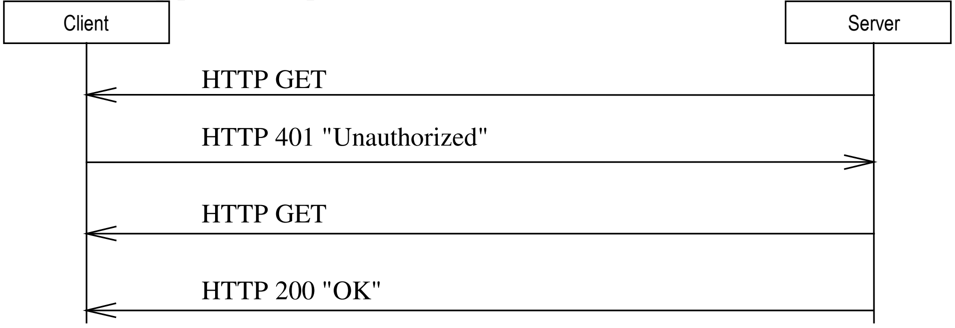


2) Let us consider a Wireless LAN with authentication and access control functionalities based on EAP/CHAP. Try to complete the following message exchange between: the client terminal (acting as EAP supplicant), the Access Point (acting as authenticator) and an AAA server acting as Back-end Authentication Server. Remember that EAP has 4 message types: EAP-Request, EAP-Response, EAP-Success, EAP-Failure.



3) In the following HTTP Client-Server interaction, specify which messages should separately include the following two HTTP header fields:

- **WWW-Authenticate: Digest realm="biloxi.com", qop="auth,auth-int", nonce="dcd98b7102dd2f0e8b11d0f6"**
- **Authorization: Digest username="bob", realm="biloxi.com", nonce=" dcd98b7102dd2f0e8b11d0f6", uri="/dir/index.html", qop=auth, response="6629fae49393a05397450978507c4ef1"**

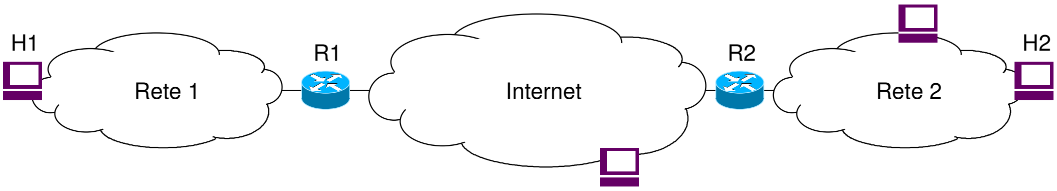


4) Let us consider the network scenario shown in figure, where two sub-networks are interconnected by means of a IPSec VPN established between the two access routers R1 and R2 connected to the external Internet.

If the IPSec VPN uses both ESP and AH protocols (with AH protecting also the ESP data), and if the encapsulation combination mode (transport/tunnel) with minimum overhead is chosen, you are requested to:

i) show the format of the packets in the external network, sent by H1 to H2 (indicate the sequence of all headers and payloads);

ii) for each possible IP header, specify the source address (SA) and destination address (DA) (use the name of the node as node address).

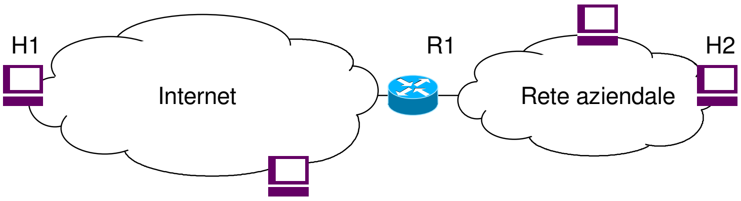


5) Let us consider the road-warrior scenario shown in figure, where a user terminal H1 is interconnected through IPSec to the access router R1 of its remote company network.

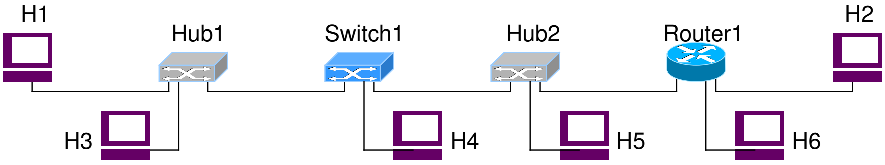
If ESP is used for protecting information between H1 and R1, if H1 further protects the communication with a remote terminal H2 by means of ESP, and if the encapsulation combination mode (transport/tunnel) with minimum overhead is chosen, you are requested to:

iii) show the format of the packets in the external network, sent by H1 to H2 (indicate the sequence of all headers and payloads);

iv) for each possible IP header, specify the source address (SA) and destination address (DA) (use the name of the node as address).

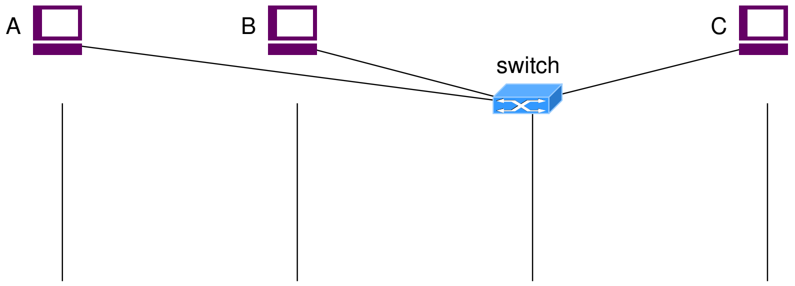


**6) In the following IP over Ethernet network scheme, which nodes are able to eavesdrop all the traffic exchanged between H1 and H2?
Which nodes are able to launch a Man In The Middle (MITM) attack, based on their position, without the need of using ICMP or ARP spoofing?**

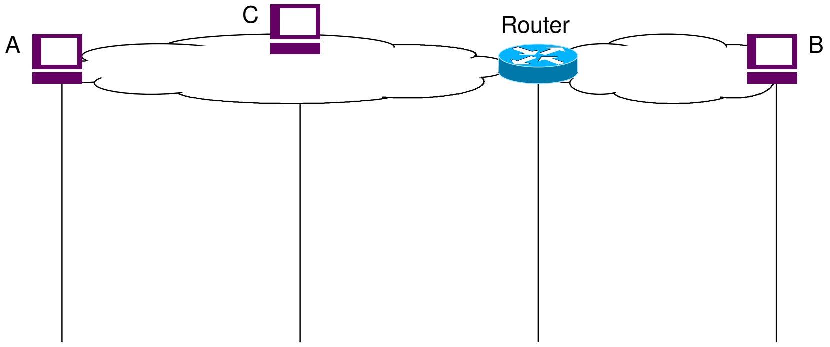


7) Considering the following network scheme, specify a possible message flow for a an ARP spoofing attack (also referred to as ARP poisoning attack) launched by a node C (attacker) against a node A (victim), where B is the spoofed node.

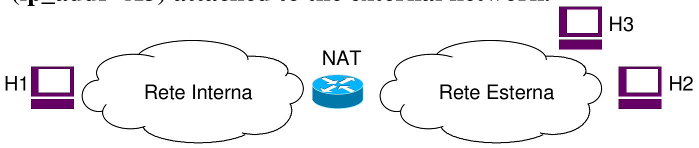
If ipA, macA, ipB, macB, ipC, macC are the IP and MAC addresses of the three nodes, specify the ARP tables of A and C after the attack.



8) Considering the following network scheme, specify a possible message flow for a an ICMP spoofing attack of type “redirect”, launched by a node C (attacker) trying to become Man In The Middle between nodes A (victim) and B. Particularly, consider the case in which A and B want to exchange the following 4 IP packets: pkt1:A→B, pkt2:B→A, pkt3:A→B, pkt4:B→A, and the attack starts when the first packet (pkt1) is sent.



9) Let us consider a network scenario in which a NAT node is used for interconnecting an internal network to an external network as in figure. Let us consider a node H1 (ip_addr=A1) attached to the internal network, and nodes H2 (ip_addr=A2) and H3 (ip_addr=A3) attached to the external network.



If H1 sends to H2 an UDP datagram (pkt1) addressed as: A1:p1→A2:p2, and if the NAT changes the packet into pkt1’ addressed as A10:p10→A2:p2,
Which of the following packets sent from H2 and H3 to H1 will reach H1, assuming that NAT works as “restricted cone NAT”?

pkt2=A2:p2→A1:p1

pkt3=A2:p4→A1:p1

pkt4=A3:p3→A1:p1

pkt5=A2:p2→A10:p10

pkt6=A2:p4→A10:p10

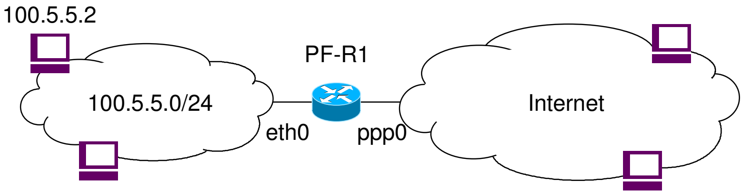
pkt7=A3:p3→A10:p10

10) **Let us consider the following network scheme, where in the node 100.5.5.2 there is a HTTP web server (TCP port 80) and a SMTP mail server (TCP port 25); you are requested to configure the filtering table of the router R1 so that:**

i) **it is possible to access to the internal server web (in the node 100.5.5.2) from external clients;**

ii) **it is possible to access any external web server (limited to the server TCP port 80) from any internal client;**

iii) **it is possible the communication, established by both sides, between the internal SMTP mail server and possible external i SMTP servers; that is: internal client → external server (TCP port 25), and internal server (TCP port 25) ← external client.**



FORWARD								
Matching								action
in_int	out_int	s_addr	d_addr	proto	s_port	d_port	Altro	ACCEPT/ DROP

11) **Let us consider the following company network formed by an internal network and a DMZ separated by a screening router R1, and connected to the external public network (Internet) through the screening router R2, as shown in figure.**

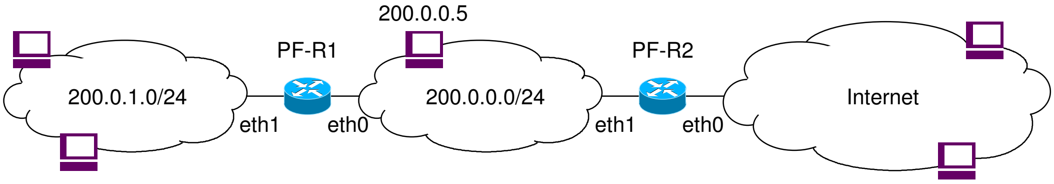
You are requested to configure the filtering table of R2 so that:

a) **it is possible to establish application level client-server communications (through any transport protocol) from any DMZ node toany external node;**

b) **it is blocked any attempt to establish a client/server communication from the external network to the DMZ;**

c) **it is blocked any communication between the internal and the external networks;**

d) **it is possible to establish TCP connections from the external network to the node 200.0.0.5 TCP port 80 (HTTP).**



FORWARD								
Matching								action
in_int	out_int	s_addr	d_addr	proto	s_port	d_port	Altro	ACCEPT/ DROP

12) **Let us consider the network of the previous exercise. You are requested to configure the filtering table of R2 so that:**

   e) **it is possible to establish application level client-server communications (through any transport protocol) from any node of the internal network (network address 200.0.1.0/24) to the DMZ;**

   f) **it is blocked any attempt to establish a client/server communication from the DMZ to the internal network;**

   g) **it is blocked any communication between the internal and external network.**

FORWARD								
matching								action
in_int	out_int	s_addr	d_addr	proto	s_port	d_port	altro	ACCEPT/ DROP

13) **Let us consider an anonymizing network formed by high-latency anonymizing *Mix* nodes. Le us consider the case in which a node *A* wants to send a message *m* to a node *B* by means of three intermediate *Mix* nodes *X*, *Y*, and *Z*. Assume that K^{+}_{i} and K^{-}_{i} are respectively the public and private keys of node *i* (*i*=*x*,*y*,*z*).**
Indicate the format of the message composed by *A* and sent to the first node *X*.