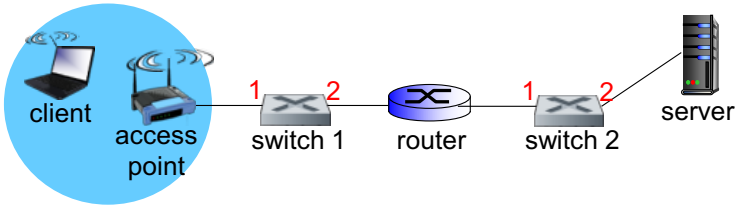
IK1203
Networks and Communication

Recitation 4 – Data link layer, wireless networks, and network security

1. A network has two Ethernet switches, an access point, and a router. See the figure below. There is a client and a server connected to the network. The client sends a web request to the server, which responds with a web page (the client and the server know each other's IP addresses). As usual, assume that the network has recently been brought into operation and all tables are empty.



a) Specify the content in the switch tables (MAC address tables, learning tables, …) in switch 1 and 2 after the web transaction. Use suitable names for the MAC addresses that appear in the tables.

b) In the network, there are also ARP tables. Specify where the ARP tables are, and give their contents after the web transaction. Use suitable names for the addresses in the tables here as well.

2. Alice wants to encrypt a file and give it to Bob. It is a large file and for performance reasons, Alice wants to use symmetric encryption. The problem is that Alice and Bob do not share a symmetric key. To make matters worse, Bob is offline and does not have network access. Therefore, Alice plans to put the encrypted file on a memory stick and give it to Bob. She also wants to digitally sign the file. The idea is that Bob by using the content on the memory stick should be able to decrypt the file, verify that it comes from Alice, and that it is intact and has not been tampered with.

How does Alice achieve this? Explain the different steps involved, and in which order they are made. For the cryptographic operations that Alice does, explain what operations are performed on the data, and what key (if any) is used.

Assume that Alice and Bob have agreed in advance on what cryptographic algorithms to use, and that they know each other's public keys.