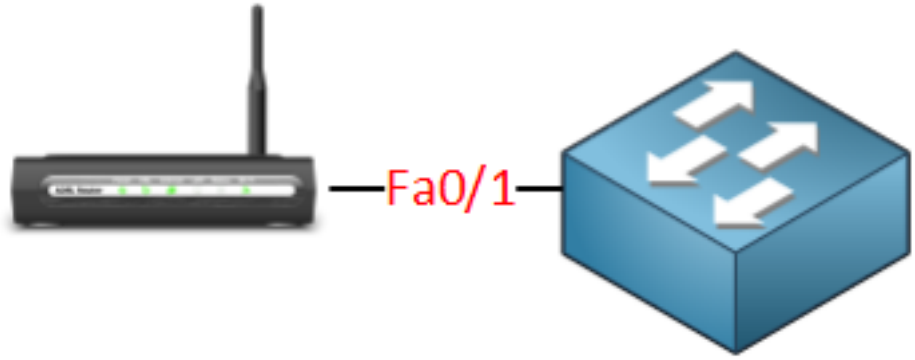
AAA and 802.1X Authentication

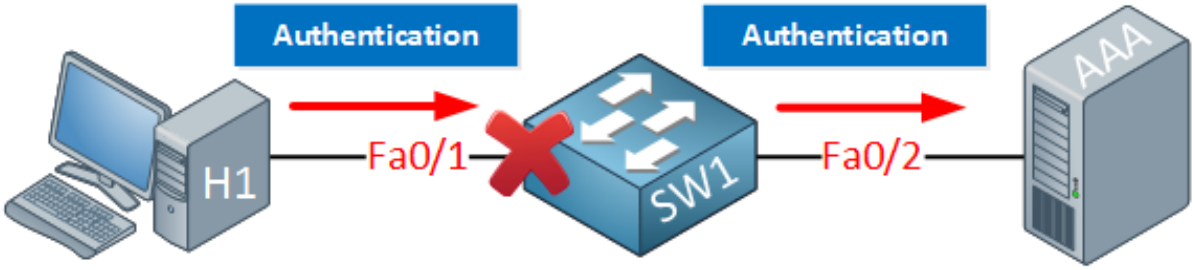
When it comes to securing the network, AAA and 802.1X authentication are two powerful tools we can use. Let me show you an example why you might want this for your switches:



Network users might bring their own wireless router from home and connect it to the switch so they can share wireless internet with all their colleagues. An access point like this is called a **rogue access point** and this is something you DON'T want to see on your network. It's hard to detect because on the switch you'll only see one MAC address. The router is doing NAT so you will only see one IP address, this is something you can't prevent with port security.
One way of dealing with issues like this is to use **AAA**.

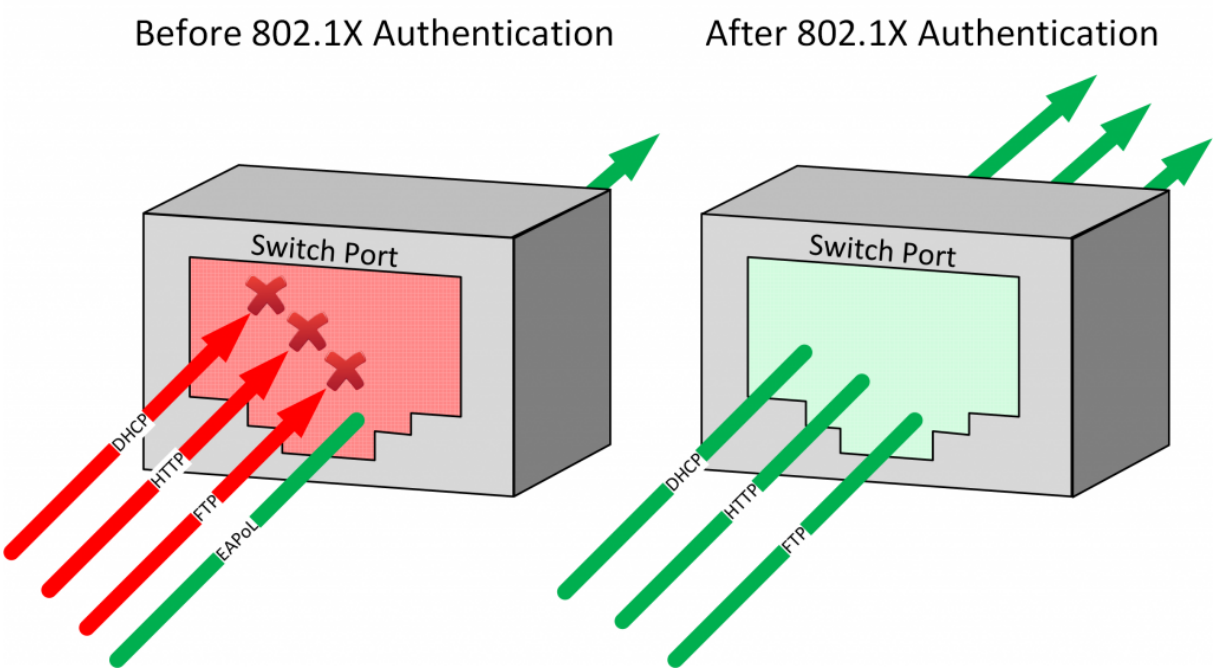
AAA stands for **Authentication**, **Authorization** and **Accounting**:

- **Authentication**: Verify the identity of the user, who are you?
- **Authorization**: What is the user allowed to do? what resources can he/she access?
- **Accounting**: Used for billing and auditing.



The idea behind AAA is that a user has to authenticate before getting access to the network. The fa0/1 interface on SW1 will be blocked and you are not even getting an IP address. The only thing the user is allowed to do is send his/her credentials which will be forwarded to the AAA server. If your credentials are OK the port will be unblocked and you will be granted access to the network.

AAA and 802.1X Authentication



802.1X is the mechanism that will **block** or **unblock** the interface. It's called **port-based control.** In the picture above an unknown user plugged in a cable to the switch.