## MAC Flooding

1. PC o adresie MAC yy:yy:yy:… chce wysłać ramkę do urządzenia o adresie xx:xx:xx:
2. Switch otrzymuje tą ramkę na porcie Fa0/1, odczytuje z niej adres źródłowy i wpisuje do tablicy CAM, że na porcie FA0/1 jest yy:yy:yy:…
3. Po otrzymaniu ramki przełącznik szuka adresu MAC odbiorcy w tablicy skojarzeń, jeżeli adres nie występuje w niej, to ramka wysyłana jest na wszystkie porty z wyjątkiem źródłowego, gdy jest znany, to tylko na port określony w tablicy skojarzeń.

## ARP

1. Komputer wysyła żądanie adresu ip, wysyłając je do adresu ff:ff:ff:… w treści tutaj yy:yy:: kto ma xx:xx
2. Ramka trafia do każdego urządzenia z wyłączeniem nadawcy, urządzenie analizuje kontent ramki i jeśli w niej jest jego adres ip wysyła w odpowiedzi swój adress mac
3. Komputer zna adress mac docelowy urządzenia

### ATAK MAC FLOODING

1. Aatakujacy wysyla do przelacznika tysiące ramek ze sfałszowanymi adresami MAC
2. Tablica MAC przepełnia się
3. Uzytkownik XYZ przesyła ramkę do użytkownika ZYX
4. Switch zalewa ramką wszystkie urządzenia w sieci

Atakujący jest snifferem

### DHCP

Jeżeli switch warstwy 2 ma przy pomocy serwera LINUX-owego przydzielać adresy IP, wówczas w konfiguracji wpisujemy interface vlan …. Ip helper-address ip\_serwera\_z\_dhcp

### Bridging loop

1. Komputer generuje ramkę broadcastową i wysyła ją do sieci. Switch odbiera ją na swoim porcie, i wysyła na wszystkie inne podłączone porty
2. Następny przełącznik otrzyma tę ramkę na obu portach, i ponownie przekąże je na wszystkie swoje porty

### VLAN TAG

16 bitów= (3 definiujące CoS , 1 bit Canonical Format Indicator czy jest obecne pole RIF, 12- bitowy VLAN ID)

### Q-inQ Tag

16-bitów=3 bity CoS,1 b Drop Eligibility Identifier- markowanie klientów niskiego poziomy,12-bitowy VLAN Tunnel ID

### STP

Funkcja root bridge otrzymuje urządzenie posiadające najniższą wartość BID (Bridge ID)

BID (KOD Priorytetu(4bity konfigurowalne, numer vlanu),MAC)