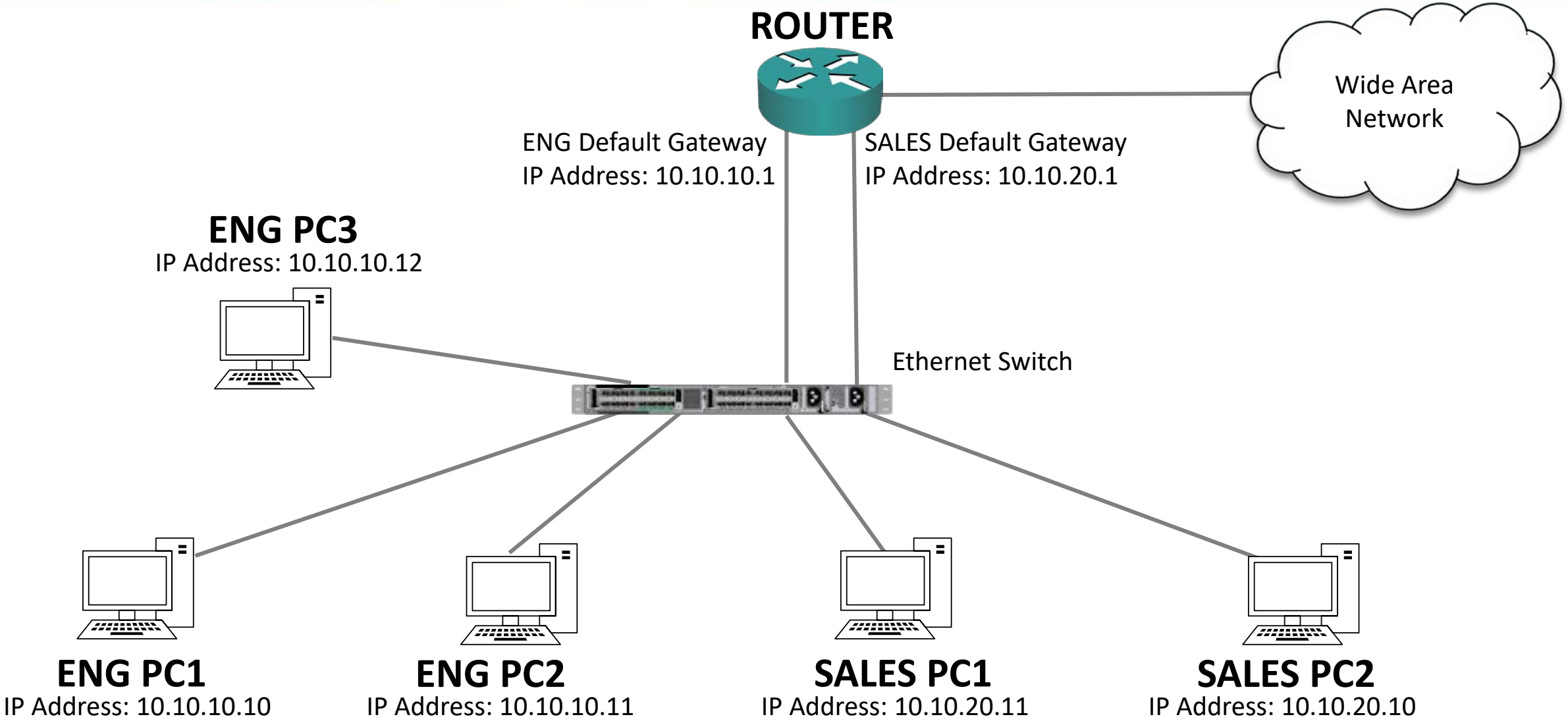
Router Operations

- Routers operate at Layer 3 of the OSI stack
- Hosts in separate IP subnets must send traffic via a router to communicate
- Security rules on routers or firewalls can be used to easily control what traffic is allowed between different IP subnets at Layer 3
- Routers do not forward broadcast traffic by default
- They provide performance and security by splitting networks into smaller domains at Layer 3

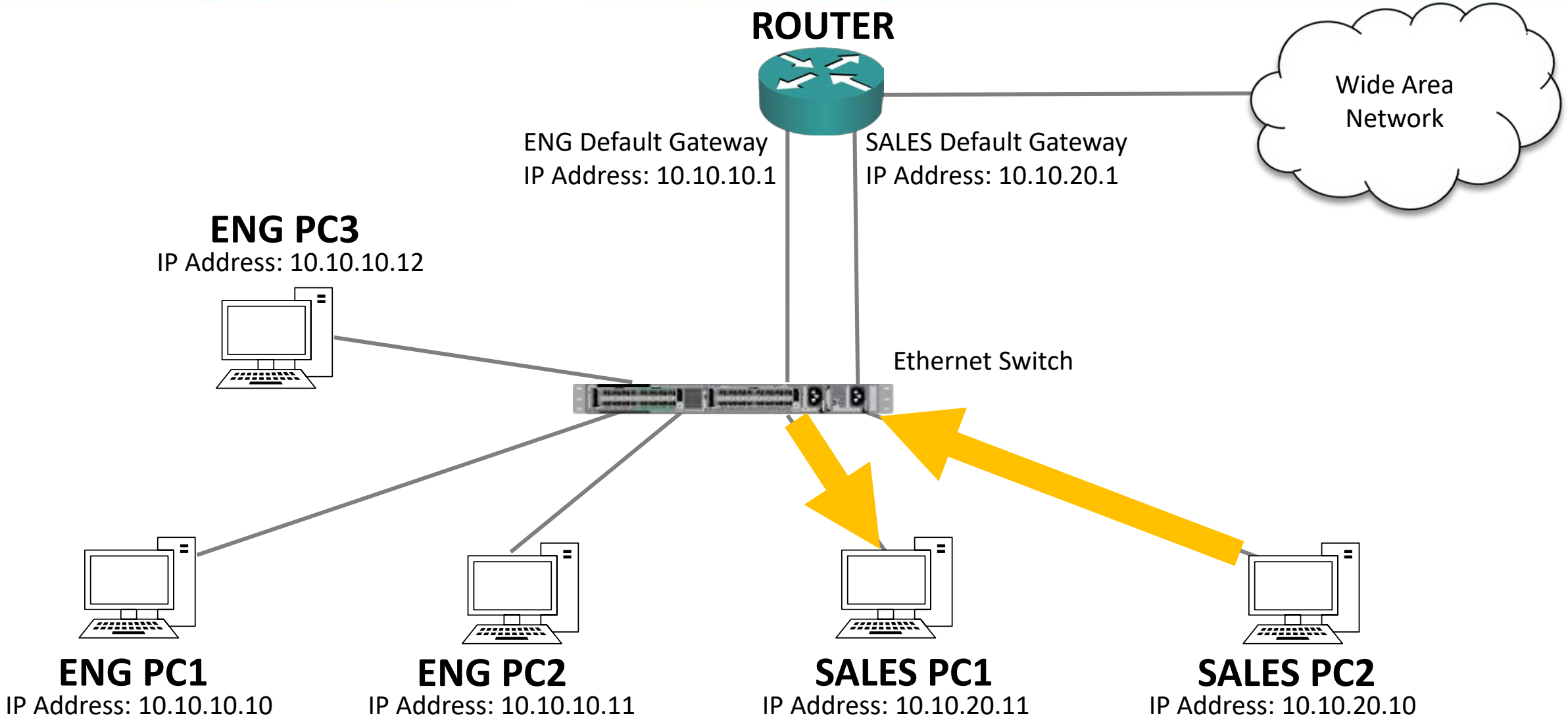
Switch Operations

- Switches operate at Layer 2 of the OSI stack
- They **do** forward broadcast traffic by default
- By default a campus switched network is one large broadcast domain
- Switches flood broadcast traffic everywhere, including between different IP subnets
- This raises performance and security concerns

LAN Networks

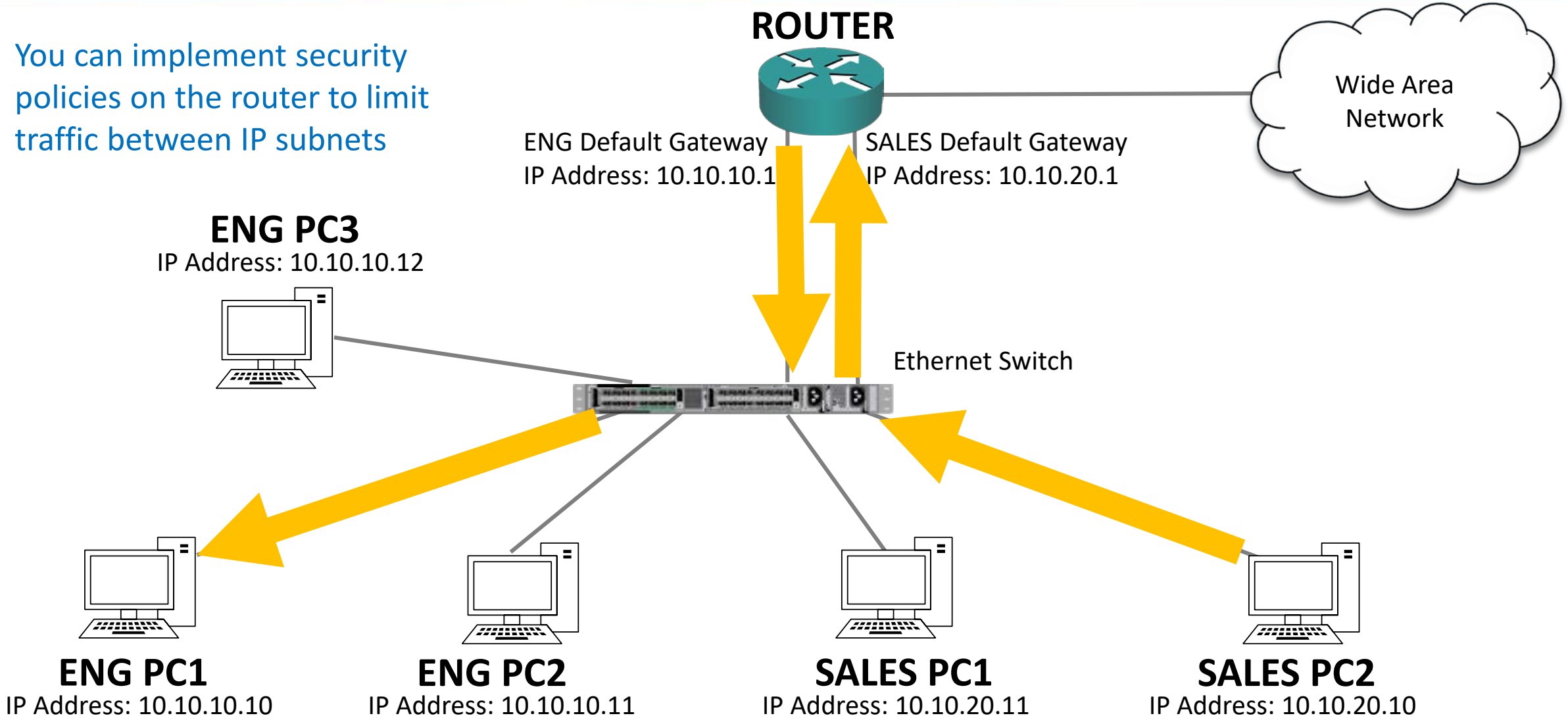


Unicast Traffic within same IP subnet

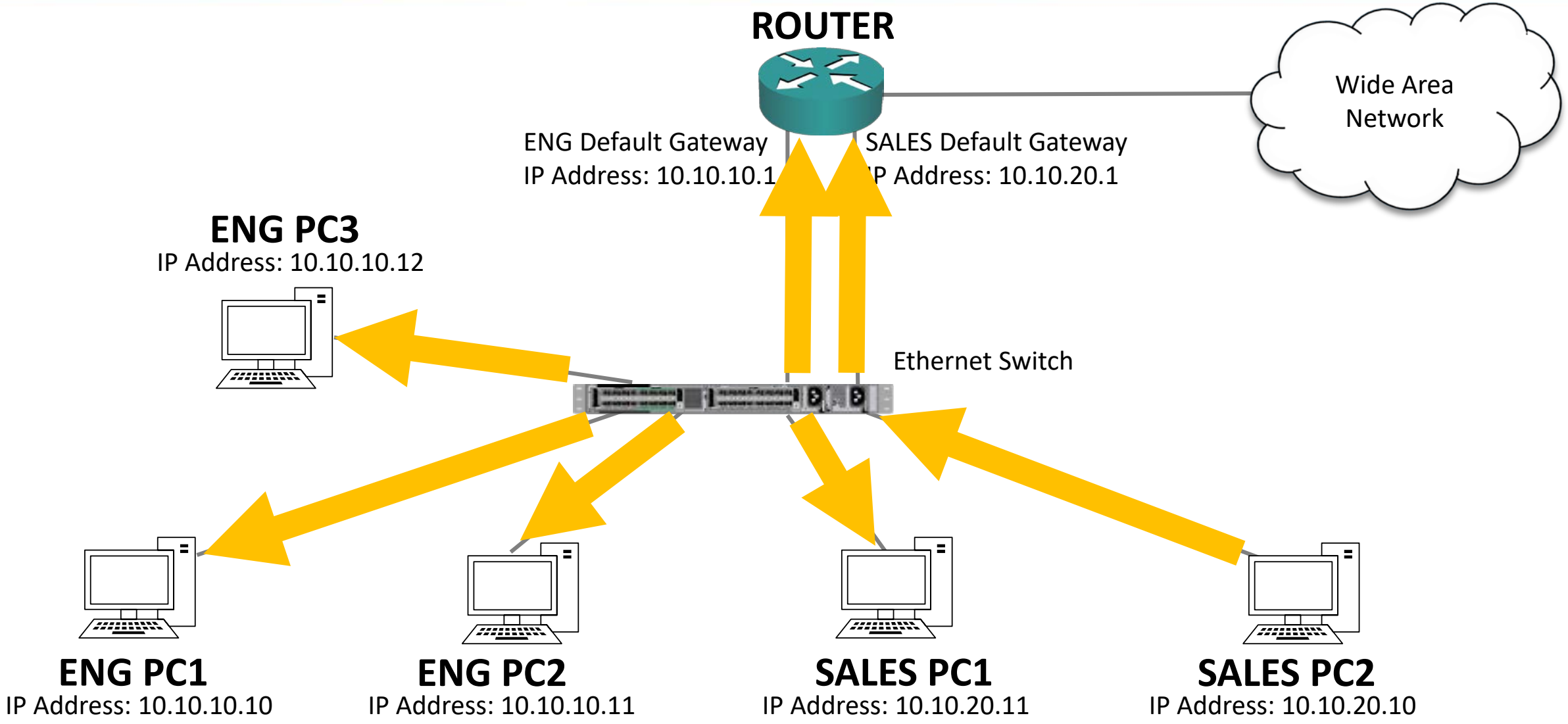


Unicast Traffic between different IP subnets

You can implement security policies on the router to limit traffic between IP subnets



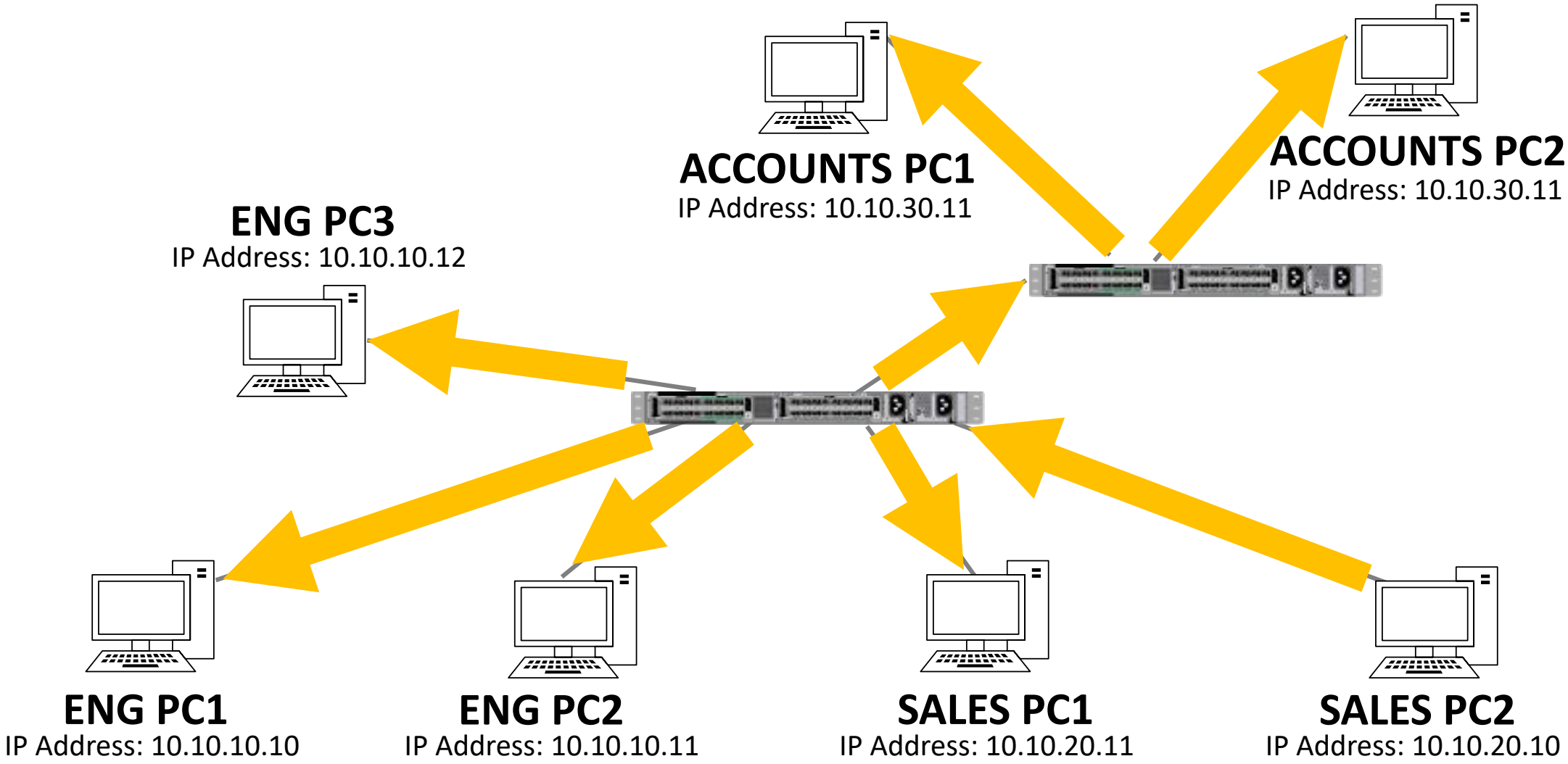
Broadcast Traffic



The Problem

- Switches flood broadcast traffic everywhere, including between different IP subnets
- This affects security because the traffic bypasses router or firewall Layer 3 security policies
- It affects performance because every end host has to process the traffic
- It also affects performance by using bandwidth on links where the traffic is not required

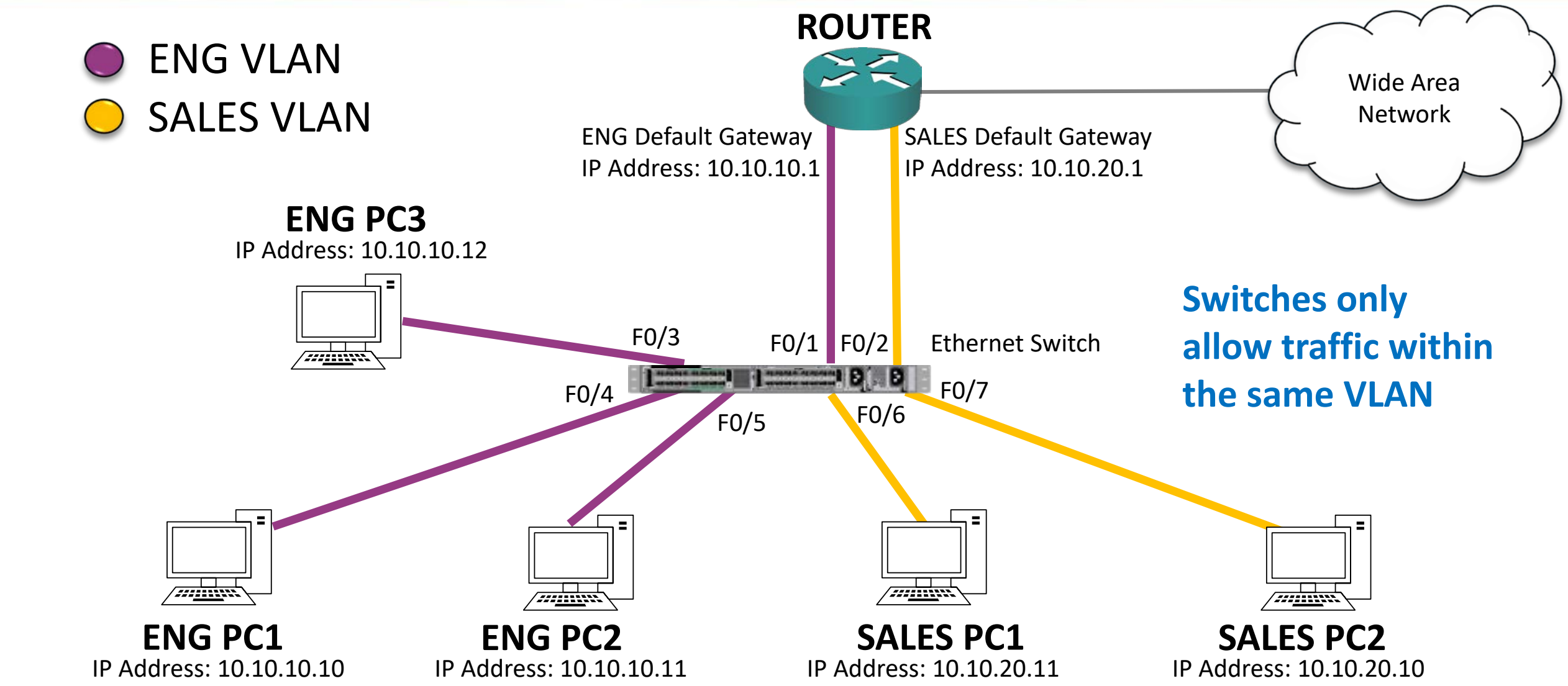
Broadcast Traffic



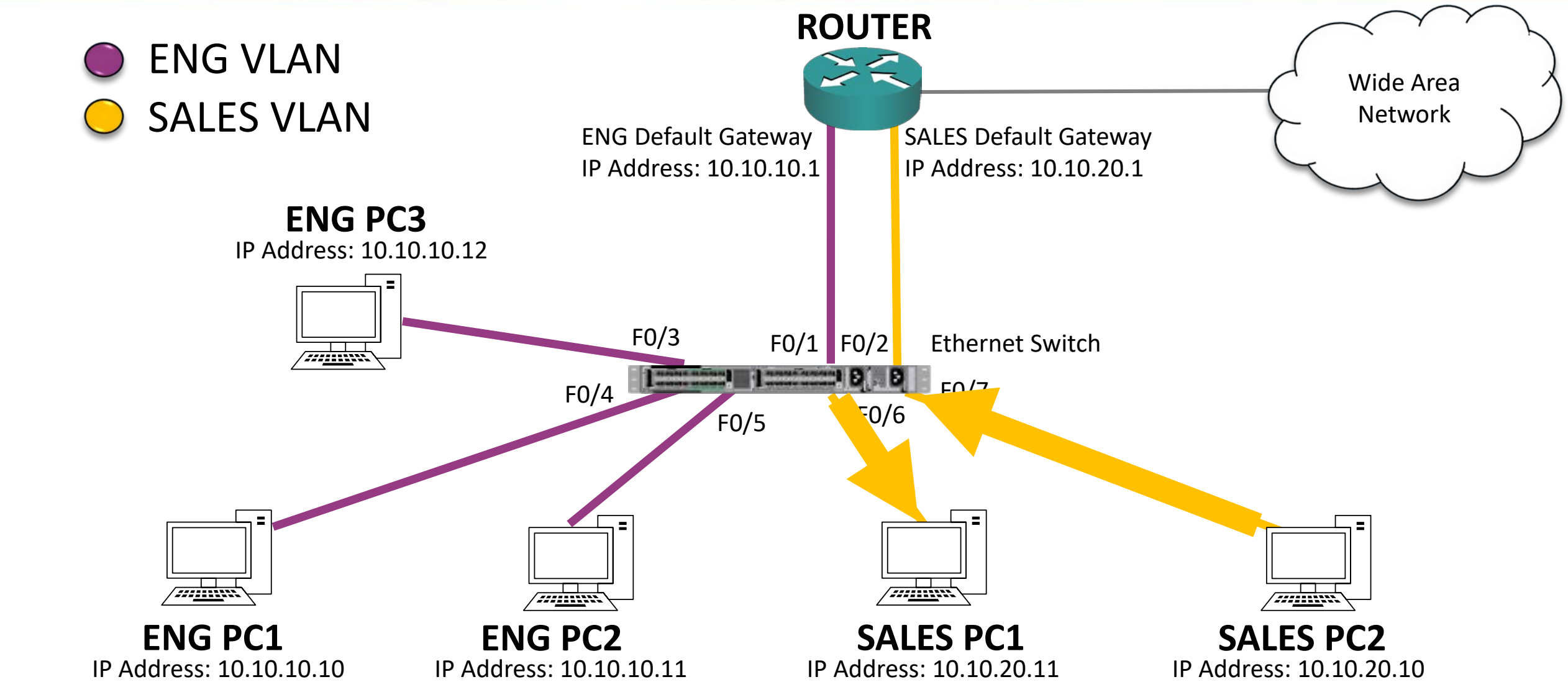
VLAN Virtual Local Area Networks

- We can increase performance and security in the LAN by implementing VLANs on our switches
- VLANs segment the LAN into separate broadcast domains at Layer 2
- There is typically a one-to-one relationship between an IP subnet and a VLAN

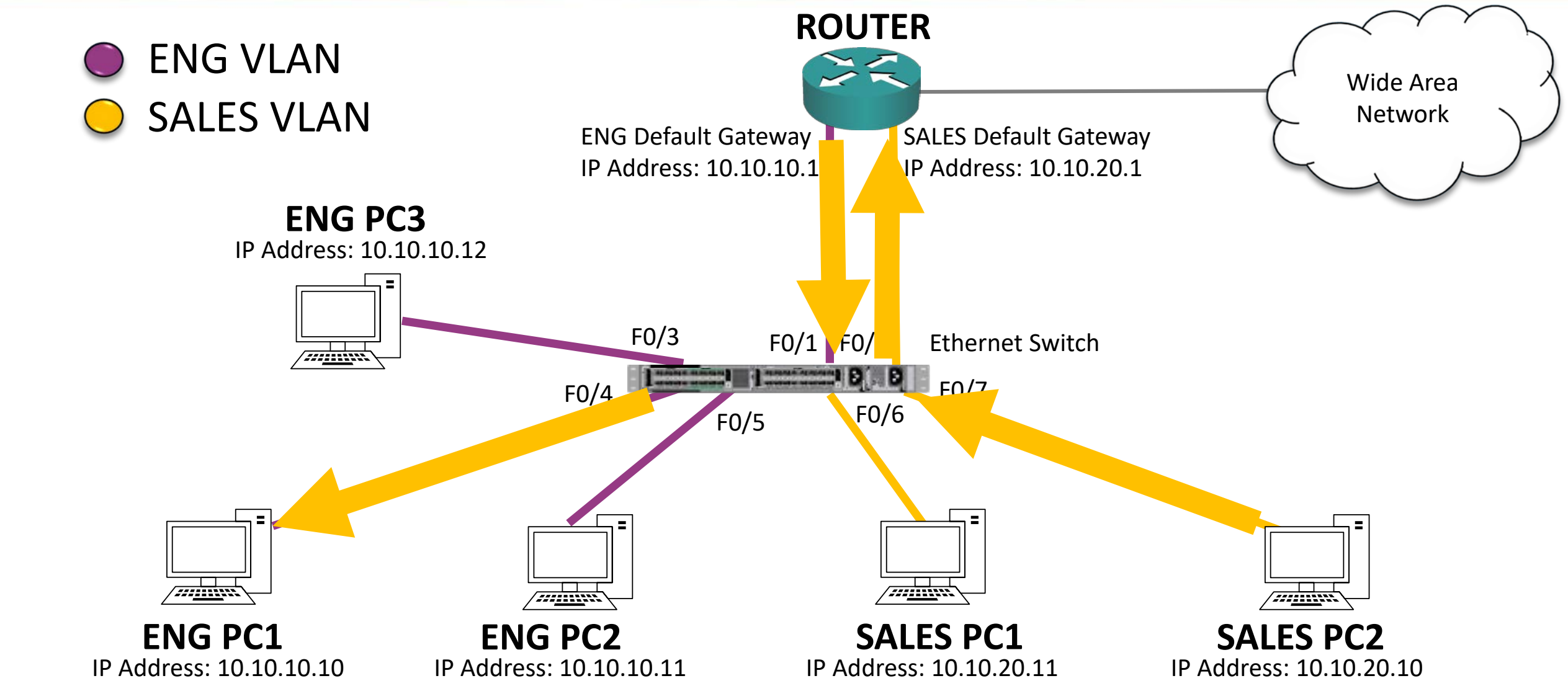
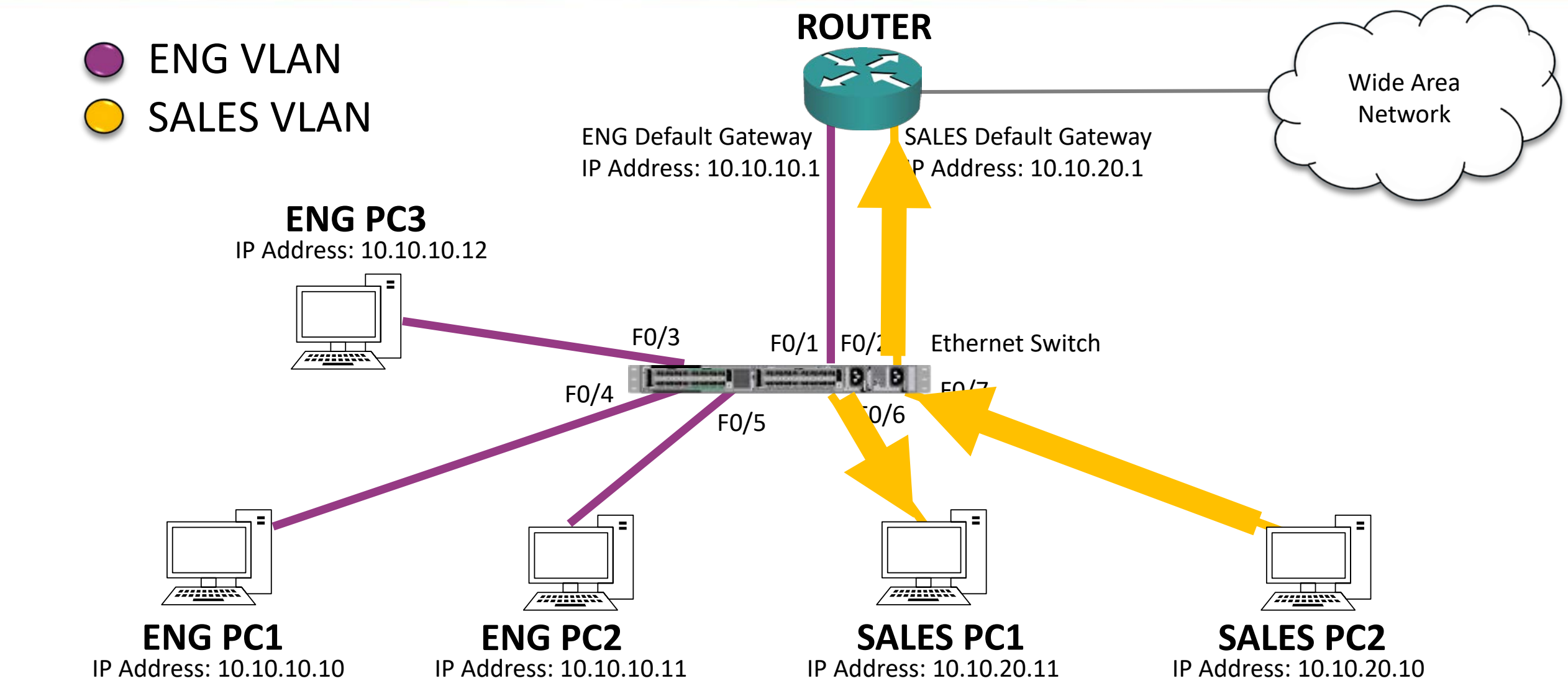
VLAN Virtual Local Area Networks



Unicast Traffic within same IP subnet



Unicast Traffic between different IP subnets



Broadcast Traffic