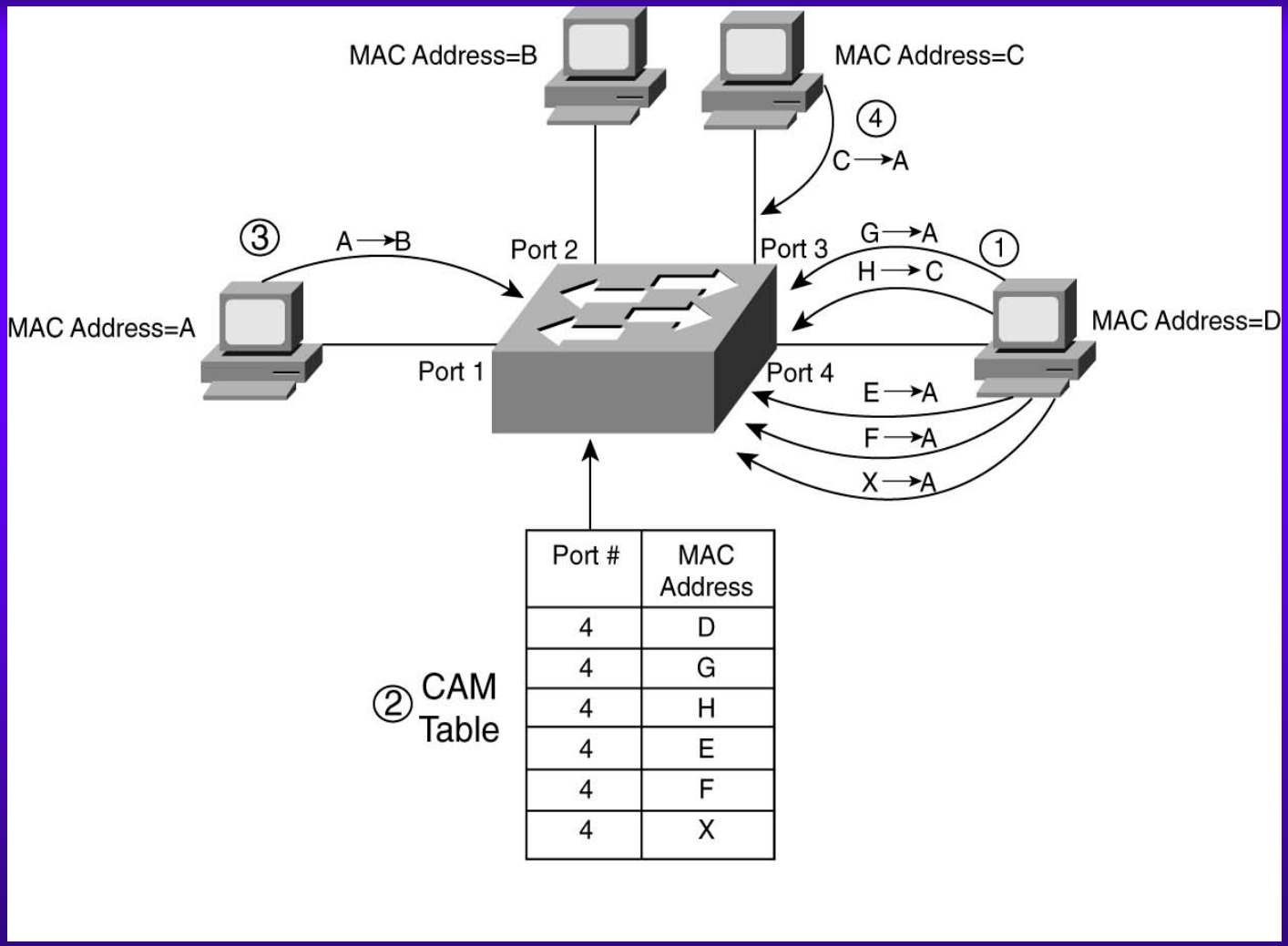
Chapter 5
Secure LAN Switching



- MAC Address Flooding Causing CAM Overflow and Subsequent DOS and Traffic Analysis Attacks

Port Security

- Example
  - Set port security 2/1 enable
  - Set port security 2/1 00-90-2b-03-34-08
  - Set port security 3/2 maximum 1

Restricting Access to a Switch via IP Permit List

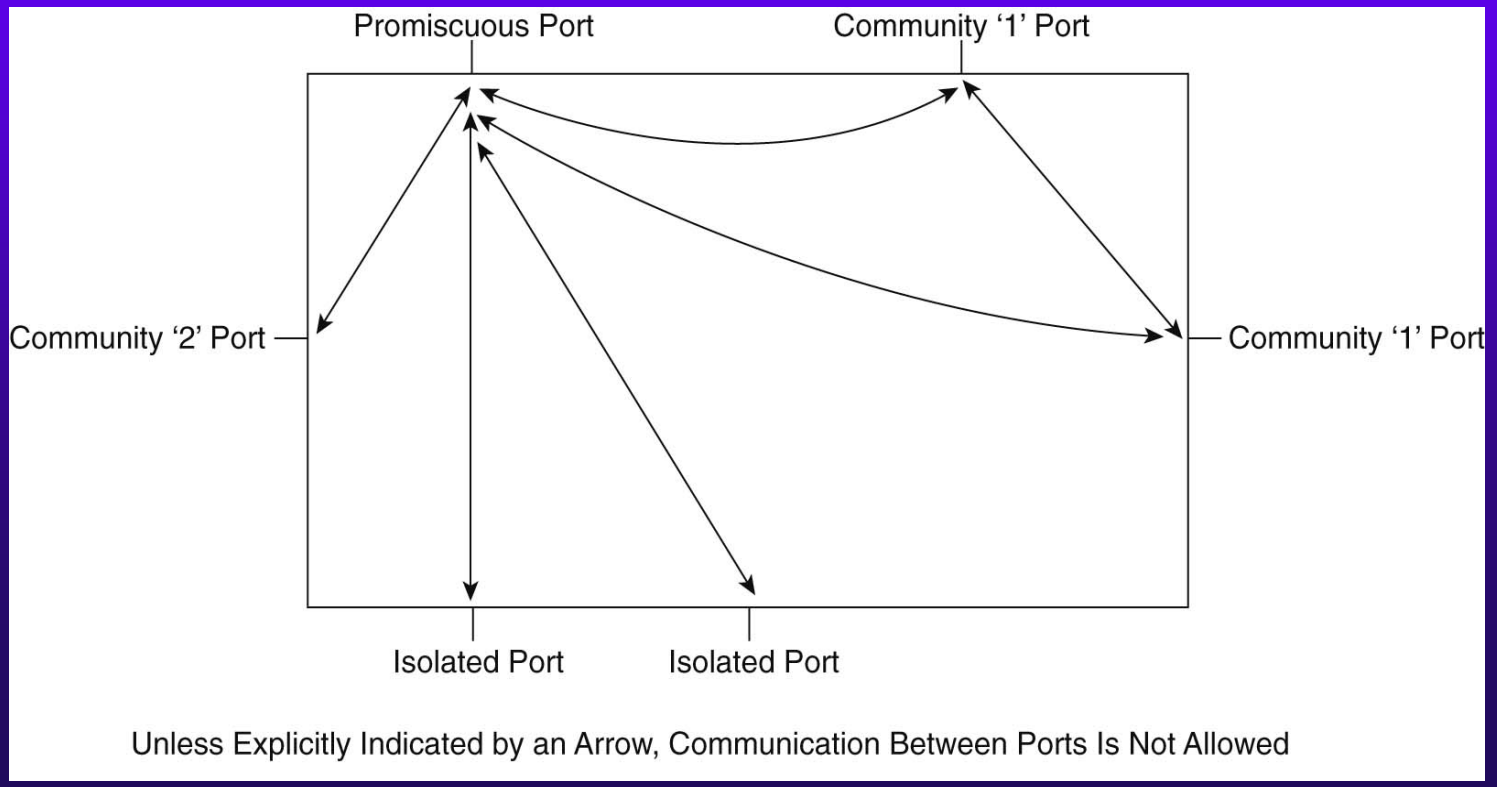
- Example
  - Set ip permit enable
  - Set ip permit 172.16.0.0 255.255.0.0 telnet
  - Set ip permit 172.20.52.2 255.255.255.255 snmp
  - Set ip permit 172.20.52.3 all

Controlling LAN Floods

- Example
  - Set port broadcast 2/1-6 75%

Private VLANs on the Catalyst 6000

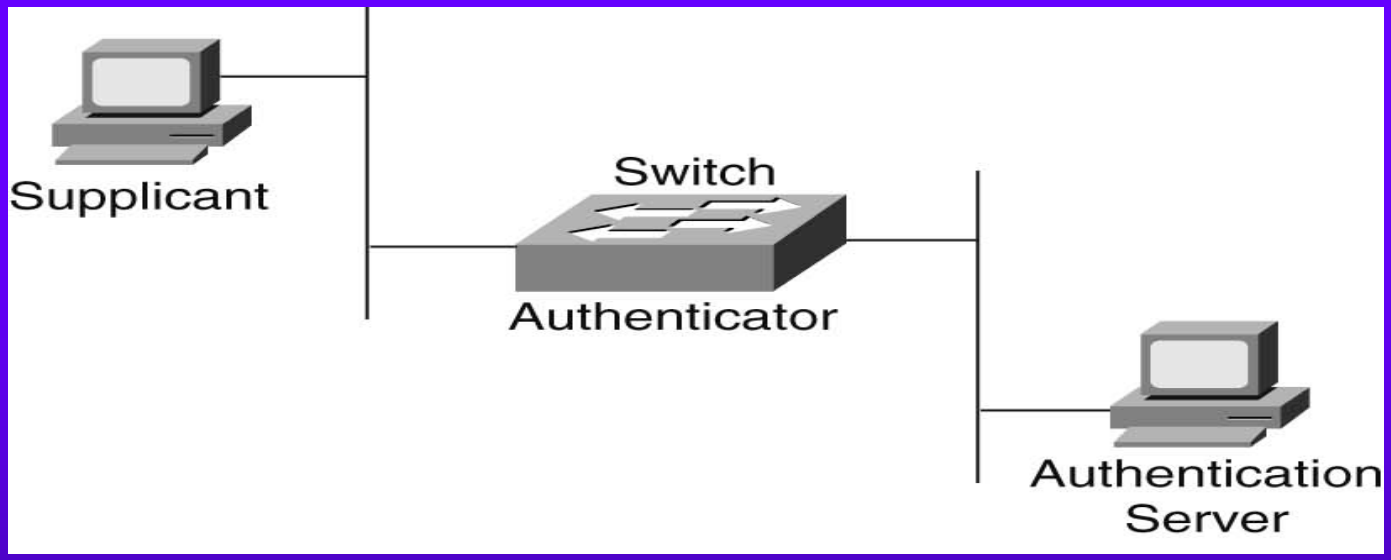
- Restricts intra VLAN traffic on a per port basis
- Solves ARP spoofing



IEEE 802.1x Standard

- Provides authentication of devices connecting to a physical port on a layer 2 switch or a logical port on a wireless access point

802.1x Entities



- Supplicant: a device (eg. Laptop) that needs to access the LAN
- Authenticator: a device that initiates the authentication process between the supplicant and the authentication server
- Authentication server: a device (eg. Cisco ACS) that can authenticate a user on behalf of an authenticator

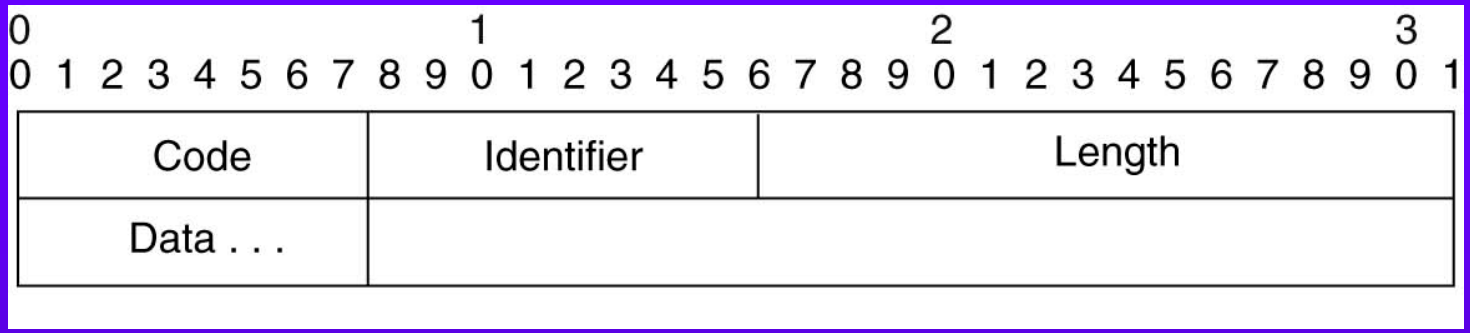
802.1x Communication

- Uses Extensible Authentication Protocol (EAP) described in RFC 3748
- Authentication data is transmitted in EAP packets
  - encapsulated in EAPOL frames between supplicant and authenticator
  - encapsulated TACACS+ or RADIUS packets between authenticator and authentication server

Extensible Authentication Protocol (EAP)

- Carries authentication data between two entities that wish to set up an authenticated channel for communication
- Supports one-time password, MD5 hashed username and password, and transport layer security

EAP Packet Format (RFC 2284)

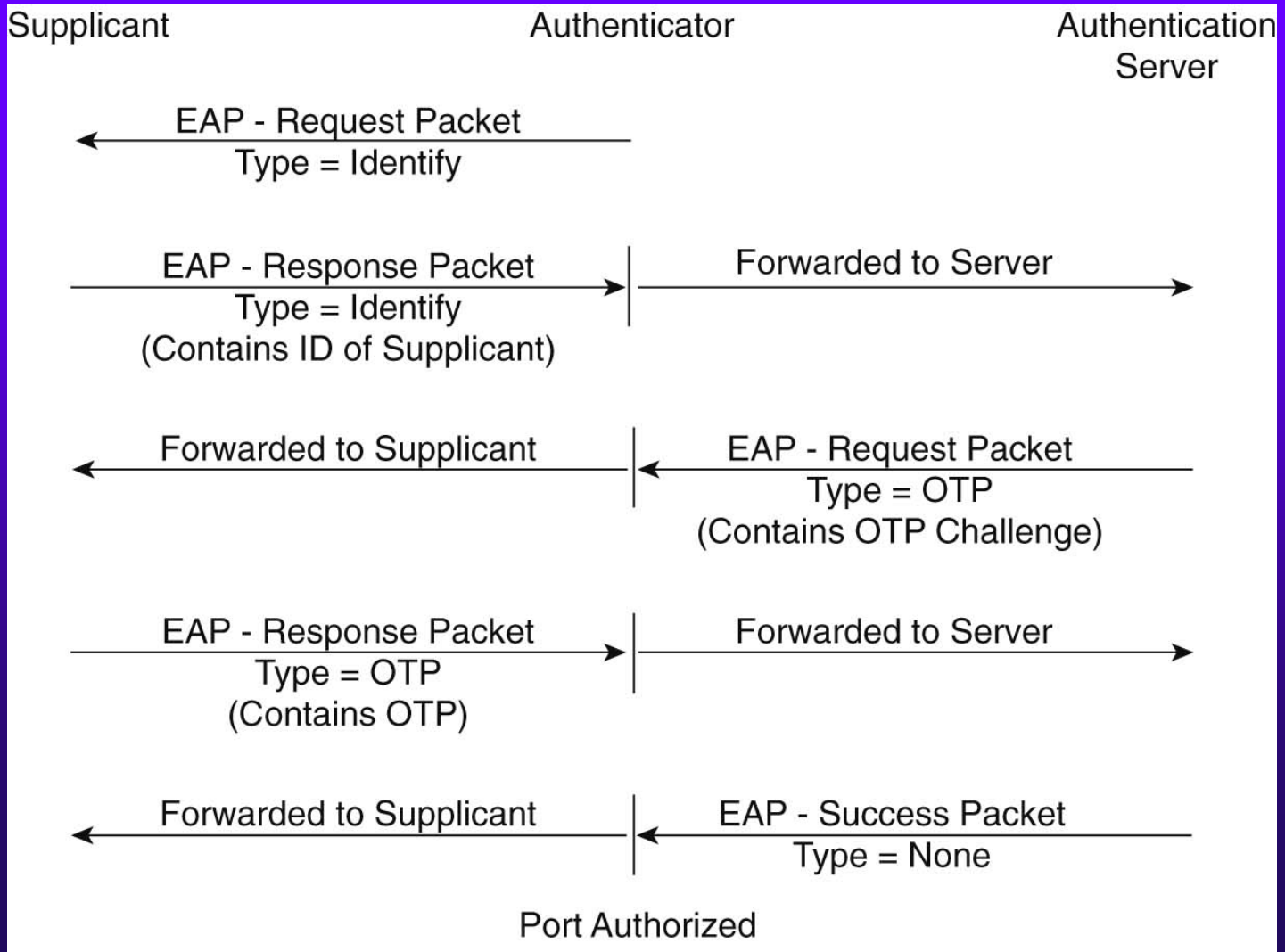


- Code: identifies EAP packet type such as request, response, success, or failure
- Identifier: used to match responses with requests
- Length: length of EAP packet

Types of EAP Request/Response messages

- Identity message
- Notification message
- NAK message
- MD-5 challenge message
- One-time password message
- Transport-Layer Security (TLS) message

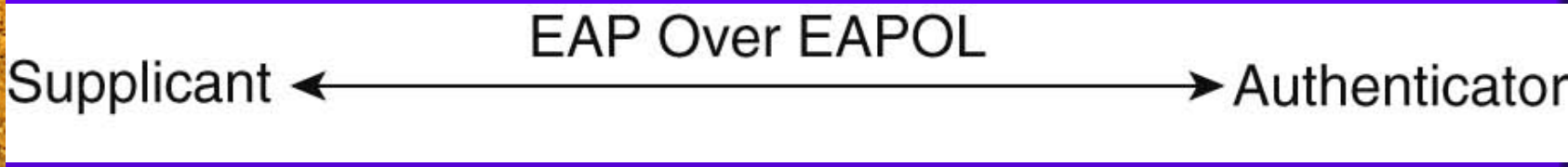
EAP Exchange Involving Successful OTP Authentication

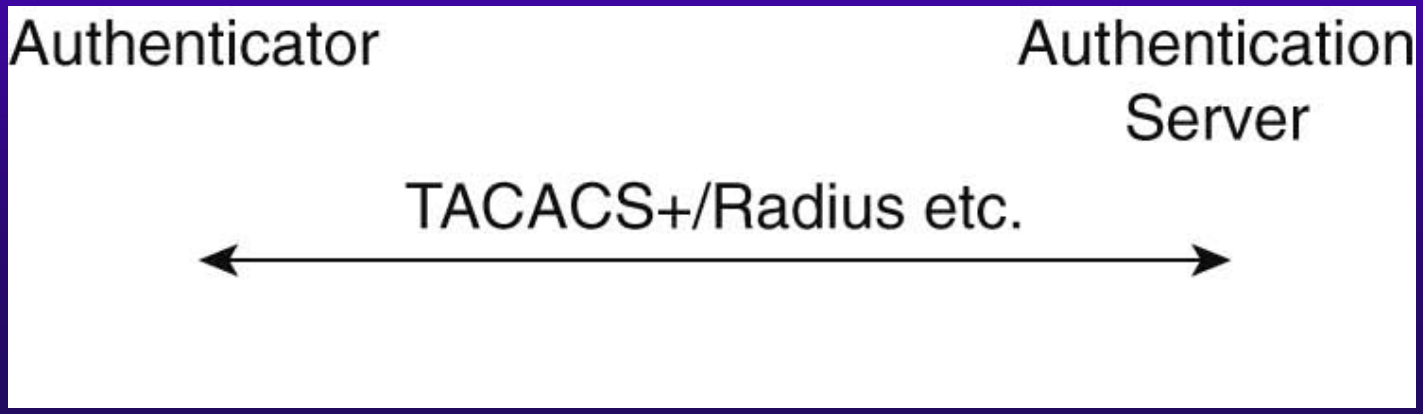


Frame Format for EAPOL Using Ethernet 802.3

PAE Ethernet Type = 88-8E
Protocol Version = 0000 0001
Packet Type EAP Packet or EAP-OL Start or EAPOL - Logoff or EAPOL-Key or EAPOL-Encapsulated-ASF-Alert
Packet Body Length = Length of Body Field in Octets
Packet Body (Only present if EAP-Packet, EAPOL-key or EAPOL-Encapsulated- ASF-Alert)

Relationship between Supplicant, Authenticator, Authentication server, EAPOL, and TACACS+/Radius





802.1x Architecture and Flow using EAP over EAPOL and EAP over TACACS+/RADIUS