CS 547: Foundation of Computer Security

S. Tripathy
IIT Patna

Previous Class

- Security in Networks
  - Threats in Networks
    - Layer 2,

Characteristics of the Internet

- Different types of nodes
  - Server, laptop, router, UNIX, Windows,…
- Different types of communication links
  - Wireless vs. wired

- No single entity that controls the Internet
- Traffic from a source to a destination likely flows through nodes controlled by different, unrelated entities
- End nodes cannot control through which nodes traffic flows
  - Worse, all traffic is split up into individuals packets, and each packet could be routed along a different path

Attacks on MAC Layer

- MAC Layer:
  - Responsible for moving pkts from 1 NIC to another via a shared channel
- CAM Table
  - poisoning
  - **MAC Flooding:**

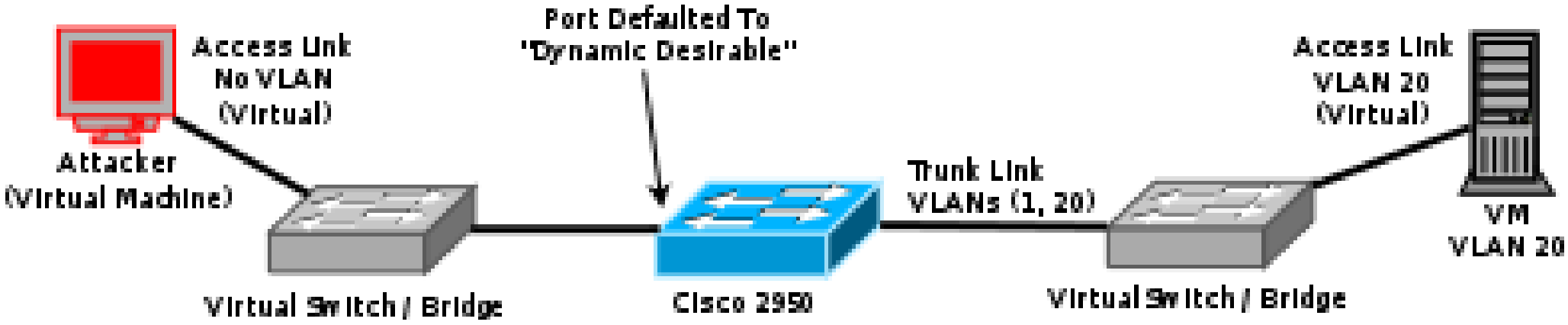
PORT	MAC
1	00:00:01:01:01:01
2	00:00:02:02:02:02
....	.....
....	.....

  - overflows the switch MAC address table (CAM) forcing the switch to forward frames to all ports on a VLAN (much like a hub)
  - Catalyst CAM Table 16000 entries with 8 buckets (uses hash function)
  - MACOF tool generates random MAC/IP address combinations in order to overflow the CAM table
    - 155,000 MAC entries per minute

VLAN Hopping Attack

- VLAN Hopping Attack:
  - Attack used to gain unauthorized access to another Virtual LAN on a packet switched network
  - Attacker sends frames from one VLAN to another that would otherwise be inaccessible
  - Two methods:
    - Switch Spoofing
    - Double Tagging
      - send Dynamic Trunk protocol (DTP) packet

Switch Spoofing

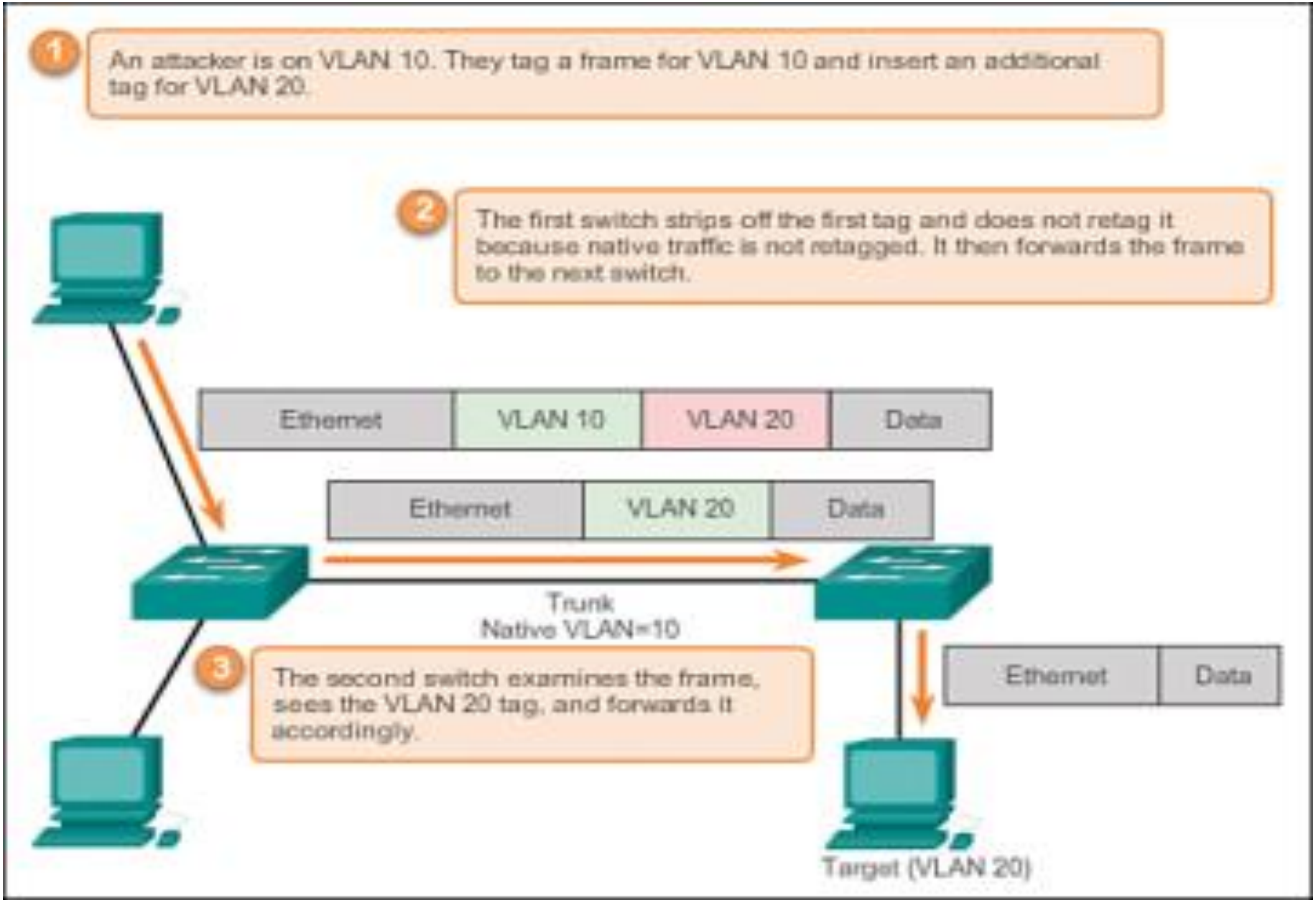


By tricking a switch into thinking that another switch is attempting to form a trunk,

Attacker generates frames for any VLAN supported by the trunk connection

Attacker can gain access to all VLANs allowed on the trunk port.

Double Tagging



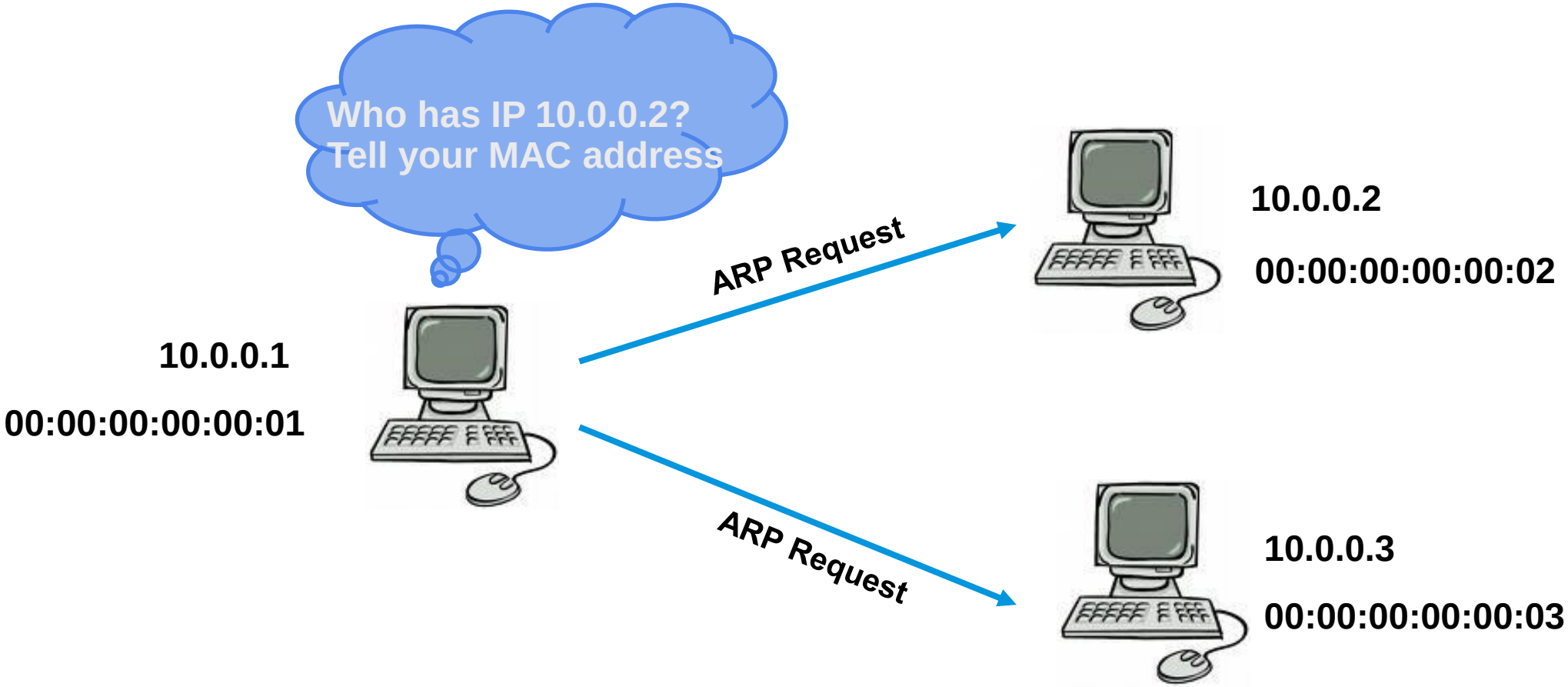
ARP Poisoning Attack

- ARP (Address Resolution Protocol) maps IP address to MAC address

IP	MAC	TYPE
10.0.0.2	00:00:00:00:00:02	dynamic

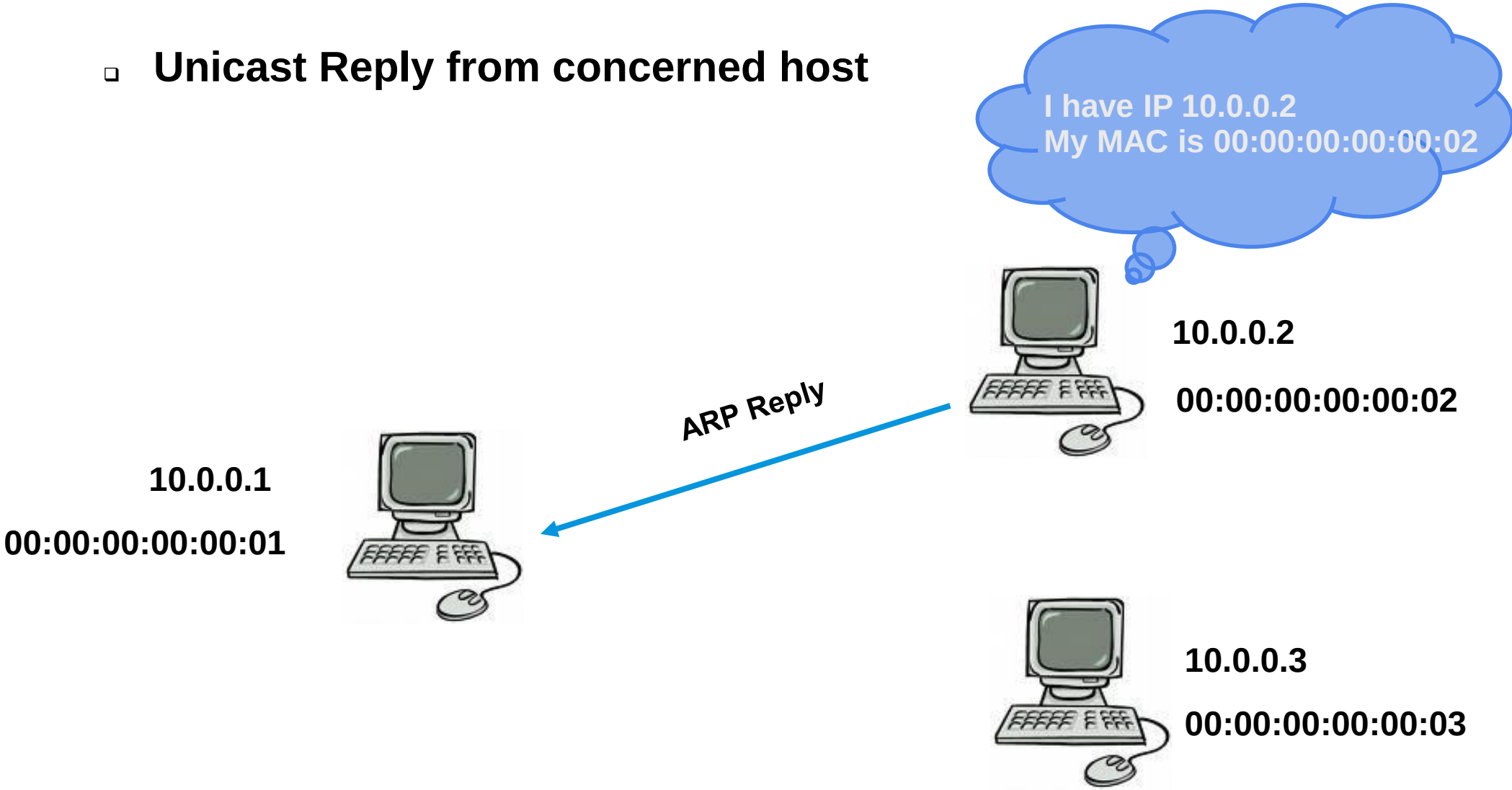
How ARP Works?

- ARP Request is Broadcast to all the hosts in LAN



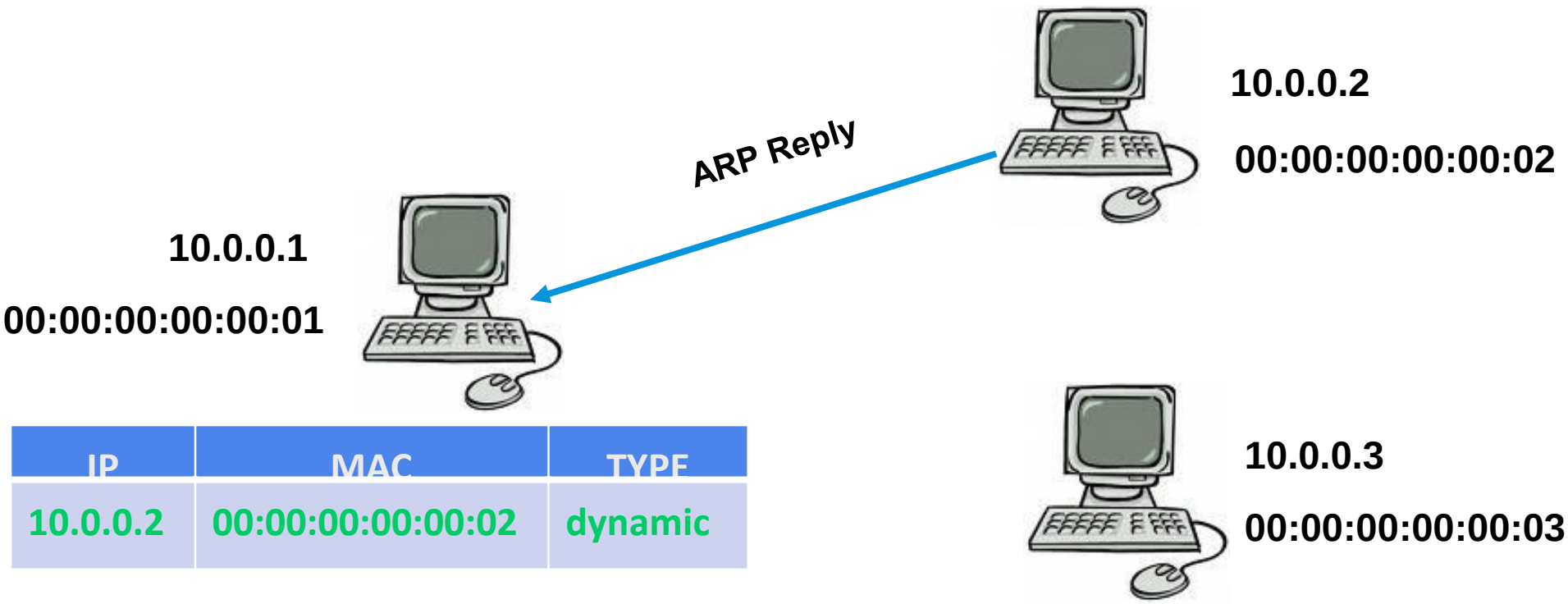
How ARP Works?

- **Unicast Reply from concerned host**



ARP Cache Stores IP-MAC Pairs

- **ARP cache : updated**



IP	MAC	TYPE
10.0.0.2	00:00:00:00:00:02	dynamic

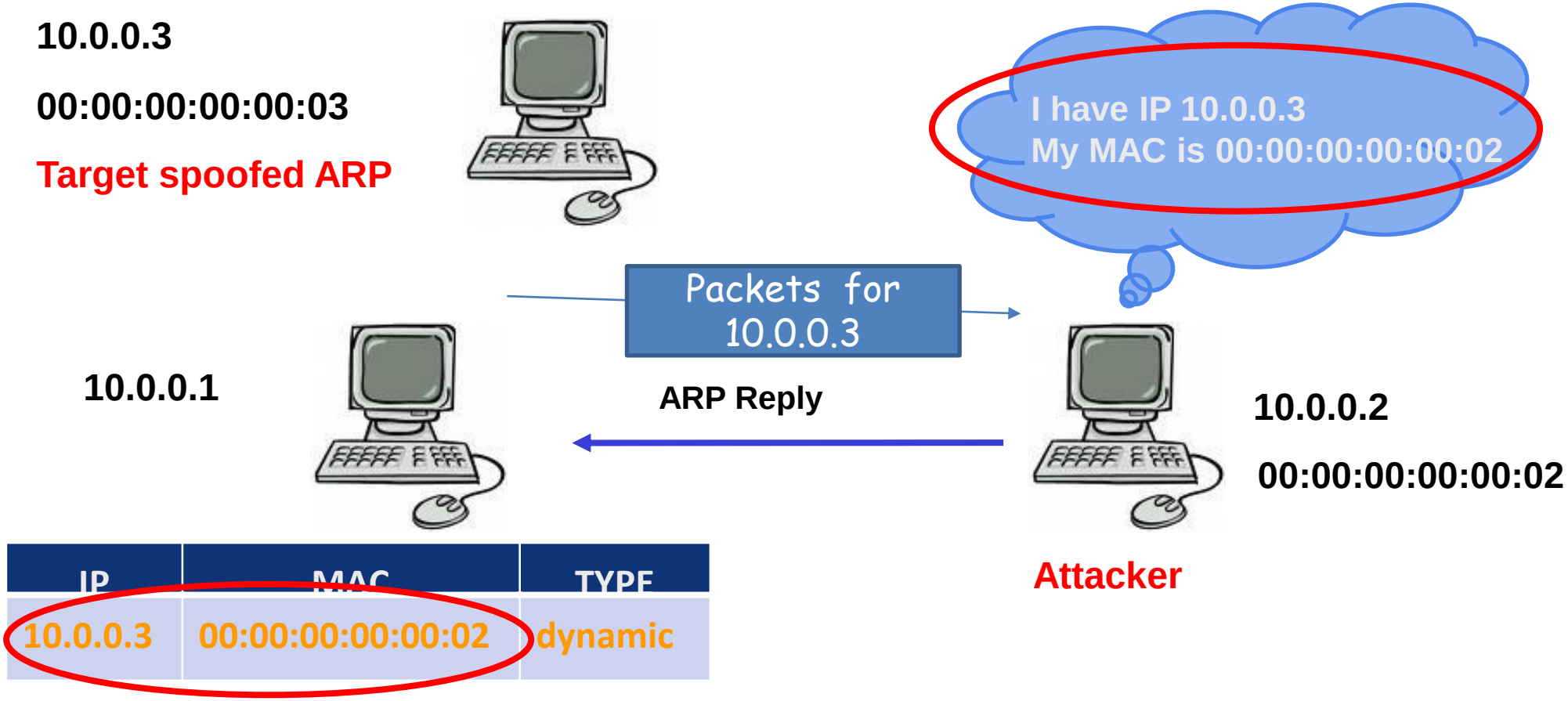
Why is ARP Vulnerable?

- **ARP is a stateless protocol**
  - **Hosts cache all ARP replies sent to them even if they had not sent an explicit ARP request for it.**
- **No mechanism to authenticate their peer**
  - Known Attacks Against ARP
  - ARP Spoofing
    - Man-in-the-Middle Attack
    - Denial-of-Service Attack
    - MAC Flooding (on Switch)
    - DoS by spurious ARP packets

ARP Spoofing Attacks

- ARP Poisoning
  - It is used to alter ARP entries in a switch and on hosts

❑ **Attacker sends forged ARP packets to the victim**



IP	MAC	TYPE
10.0.0.3	00:00:00:00:00:02	dynamic

Consequences

- Results in
  - Redirection of Traffic
  - Man-in-the-Middle Attack Allows Third Party to Read Private Data
  - Denial of Service Stops Legitimate Communication

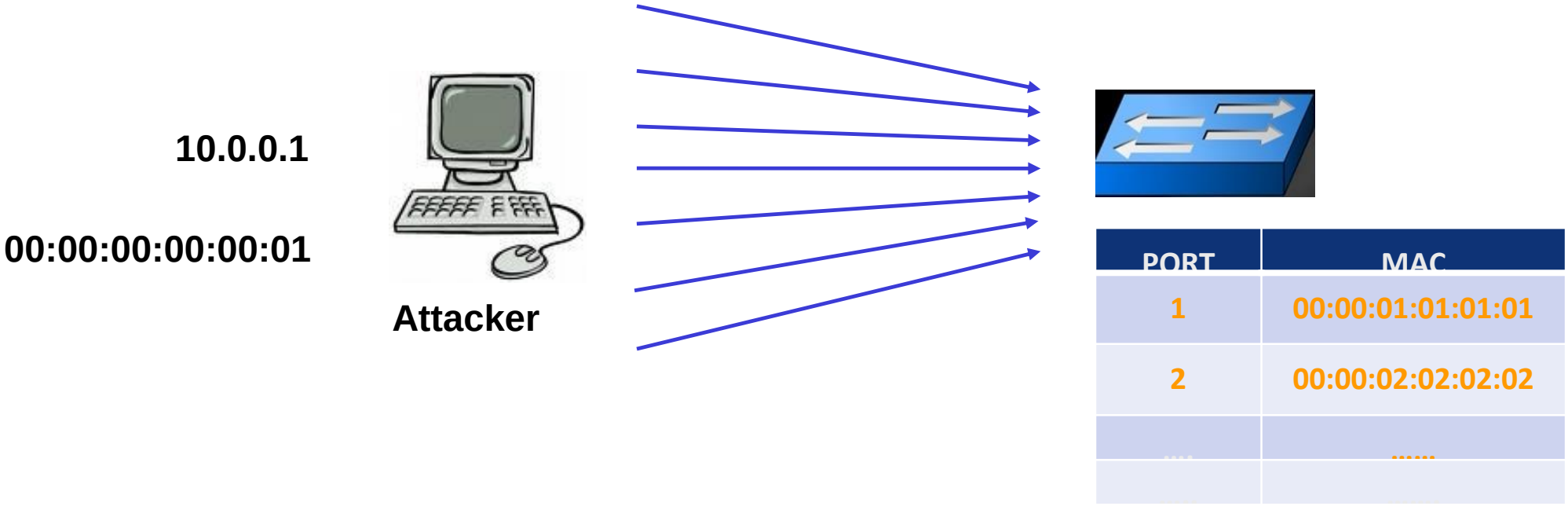
IP	MAC	TYPE
10.0.0.3	00:00:00:00:00:01	dynamic

IP	MAC	TYPE
10.0.0.4	XX:XX:XX:XX:XX:XX	dynamic

IP	MAC	TYPE
10.0.0.2	00:00:00:00:00:01	dynamic

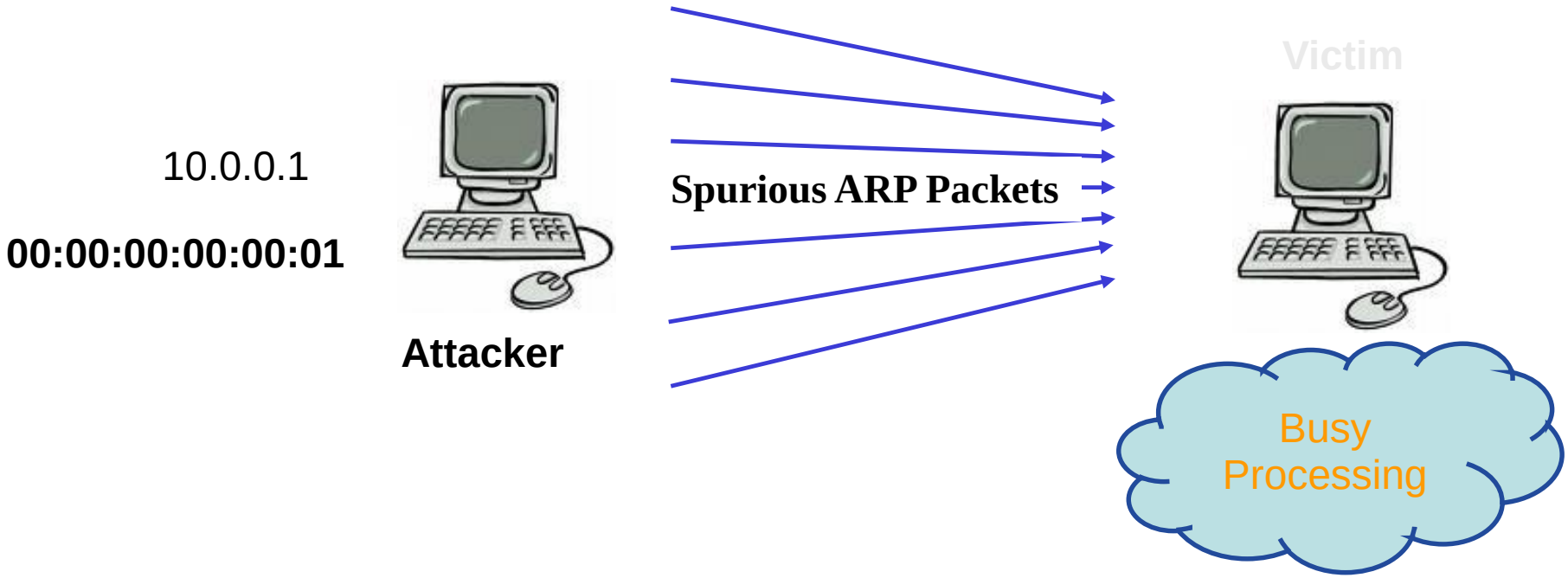
MAC Flooding Degrades Network Performance

- **Attacker bombards the switch with numerous forged ARP packets at an extremely rapid rate such that its CAM table overflows**



DoS by Spurious ARP Packets

- Attacker sends numerous spurious ARP packets at the victim such that it gets engaged in processing these packets
- Makes the Victim busy and might lead to Denial of Service



Detection and Mitigation Techniques

- Static ARP Cache entries—Fixed IP-MAC pairs
- ARPWATCH /COLOSOFT CAPSA/ARP-Guard- Maintains a database with IP-MAC mappings and any change detected is reported to administrator
- Count the imbalance in number of requests and responses
  - Evaded
- Cryptographic Techniques:
  - Secure ARP – use cryptographic algorithms to authenticate
  - TARP- ticket based