CAM Table & STP Attacks

CS 996 Pentest

`vikram@computer.org`

Polytechnic University

Introduction

- CAM table Attacks
- STP Attacks

Detailed information can be found at: http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/sfblu_wp.pdf

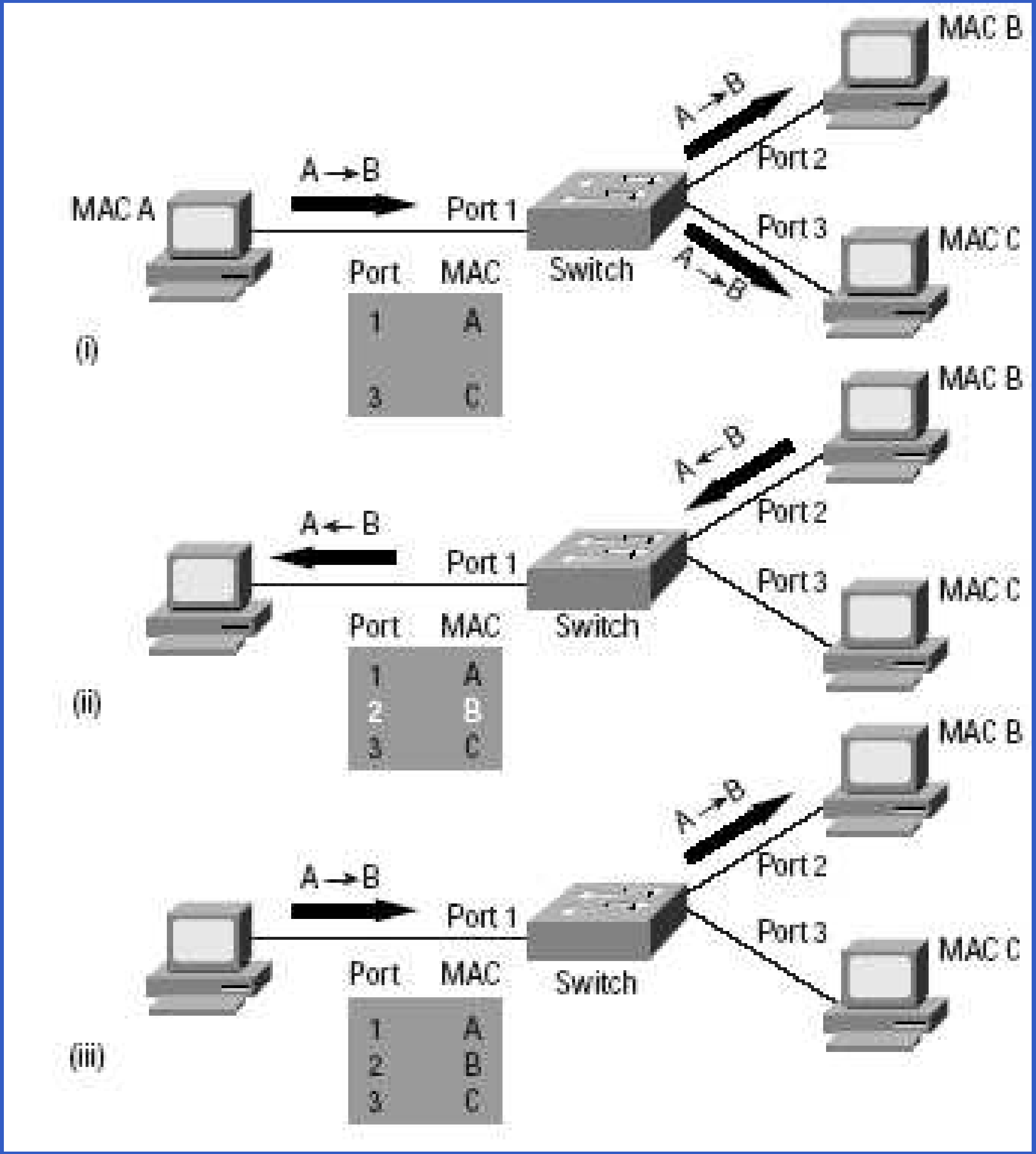
General Switch Operation

- Unlike a HUB, switch regulates traffic between ports.
- Switch creates a network between ports that contains only the device that are communication with each other.
- This network is created using the source and destination address contained within the data frame sent by the devices attached to the switch
- Switched Maintain Content-Addressable Memory(CAM) lookup tables to keep track of devices that are connected to each port

General Switch Operation

- CAM tables are populated by an address-learning process. The process associates the port and with source address by examining the frames sent by a device.
- If the switch receives a frame with a destination address that is not in the CAM table it broadcast the frame to all ports.
- Switch can be used to divide one physical networks into several logical networks through the use of Layer 2 traffic segmentation.
- CAM table in a switch contain information such as MAC address and their associated VLAN parameters, and the port the MAC address is associated to.

CAM Table Operation



(i)

Port	MAC
1	A
3	C

(ii)

Port	MAC
1	A
2	B
3	C

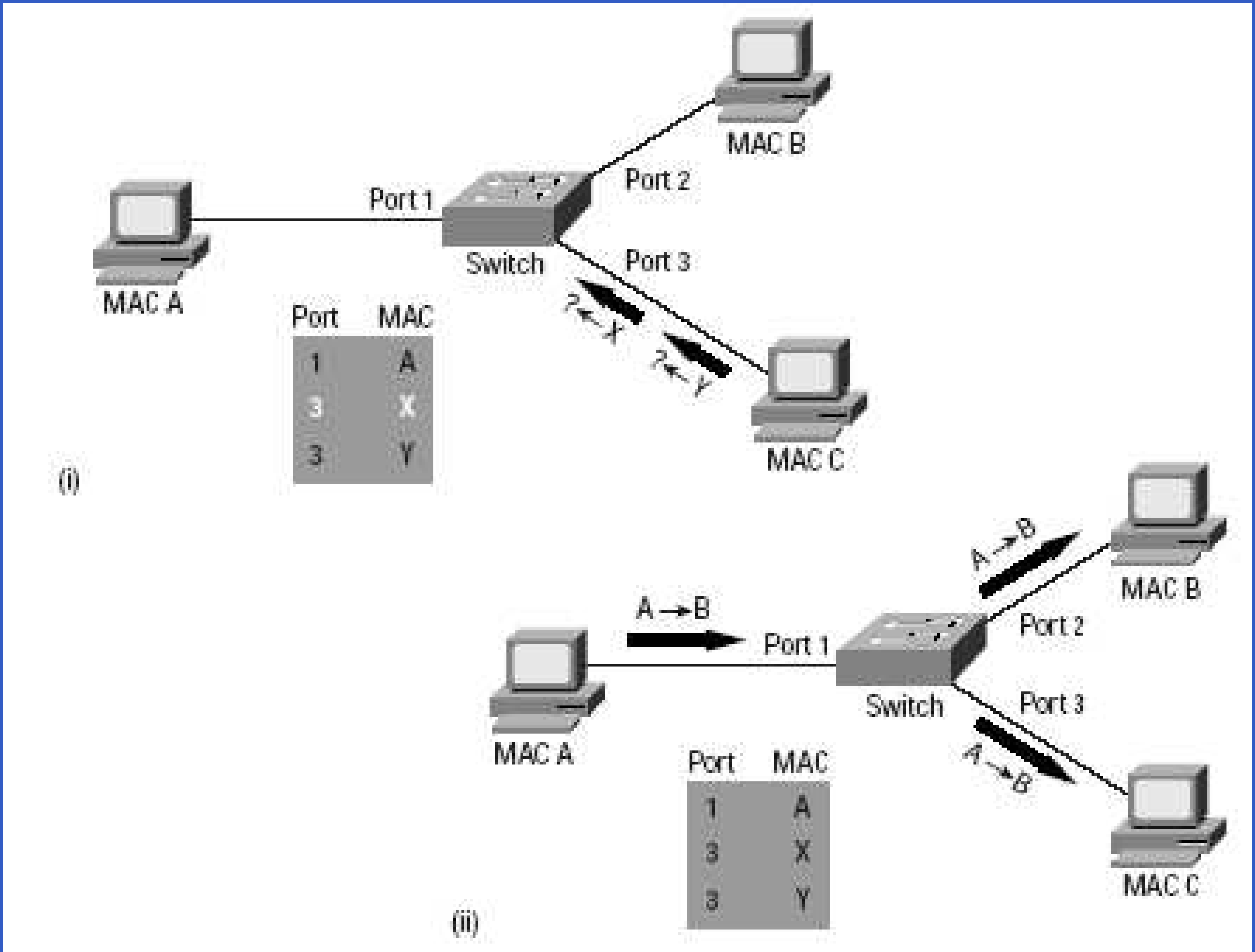
(iii)

Port	MAC
1	A
2	B
3	C

General Switch Operation

- CAM table have limited size, it will overflow if enough entries are entered before the old once expire.
- An adversary can overflow this thing by just generating a whole lot of fake mac address.

CAM Table Attack



(i)

Port	MAC
1	A
3	X
3	Y

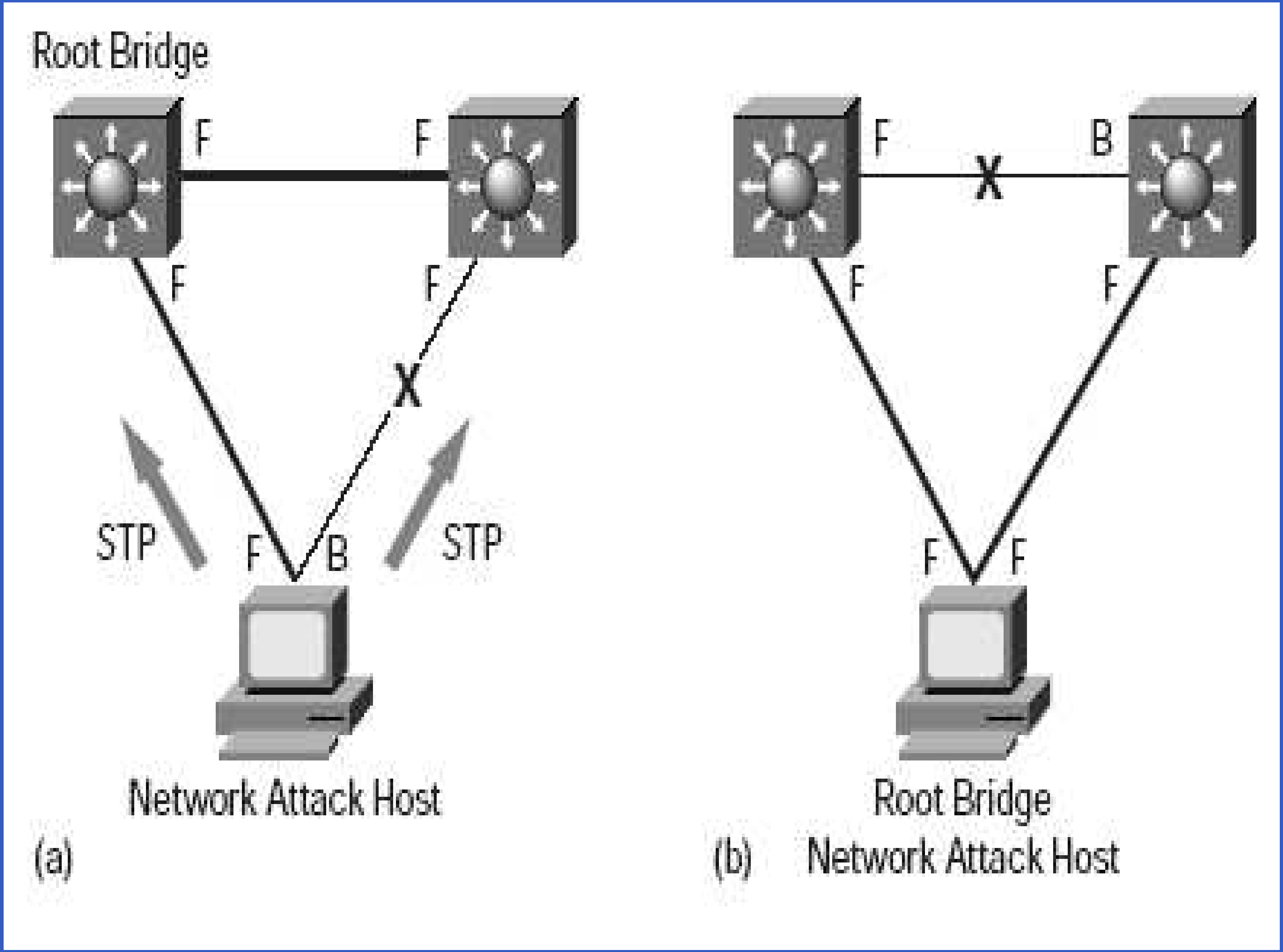
(ii)

Port	MAC
1	A
3	X
3	Y

Spanning-Tree Protocol (STP) Attacks

- STP is used in switched networks to prevent bridging loops by blocking redundant paths. STP function by broadcasting Bridge Protocol Data Unit (BDPU) to other switches to learn and block redundant paths.
- By attacking STP an adversary can force the switching network to pass through a particular switch or worse her node.

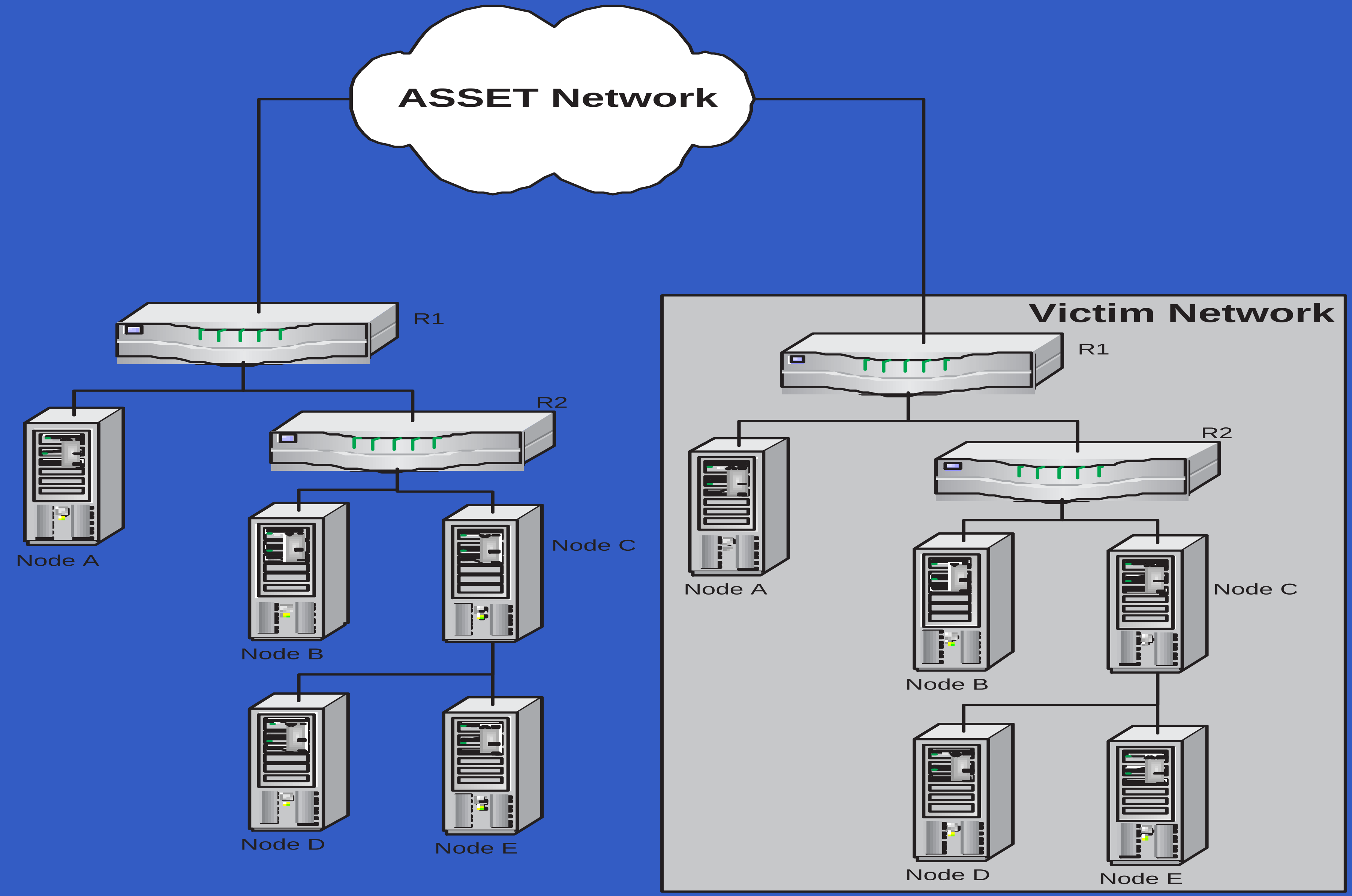
Spanning-Tree Protocol (STP) Attacks



Your Task

- Study:
  1. CAM table
  2. STP
  3. VLAN
- Verify if these attacks are possible in ISIS.

Your Network


ASSET Network
R1
R2
Node A
Node B
Node C
Node D
Node E
Victim Network
R1
R2
Node A
Node B
Node C
Node D
Node E