โพรโทคอลต้นไม้แบบทอดข้าม

Spanning Tree Protocol

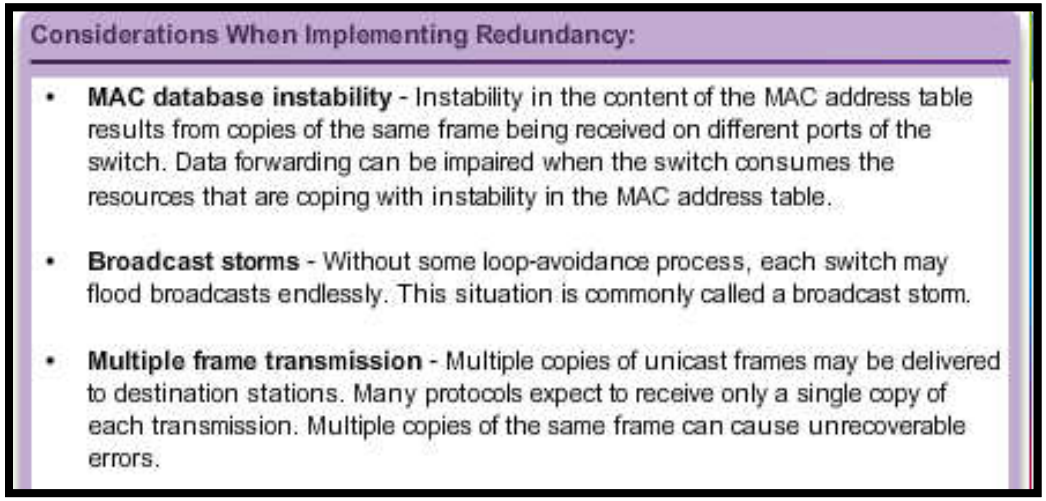
วัตถุประสงค์การเรียนรู้

- อธิบายปัญหาการใช้เส้นทางในเครือข่ายมากกว่า 1 เส้นทางได้ (redundant network)
- อธิบายการดำเนินการของ IEEE 802.1D STP
- อธิบายความแตกต่างของ spanning tree แต่ละชนิดได้
- อธิบายการดำเนินการของ PVST+ ใน LAN switched ได้
- อธิบายการดำเนินการของ Rapid PVST+ ใน LAN switched ได้
- สามารถตั้งค่า PVST+ ใน LAN switched ได้
- สามารถตั้งค่า Rapid PVST+ ใน LAN switched ได้
- สามารถแก้ปัญหาการตั้งค่า STP ได้

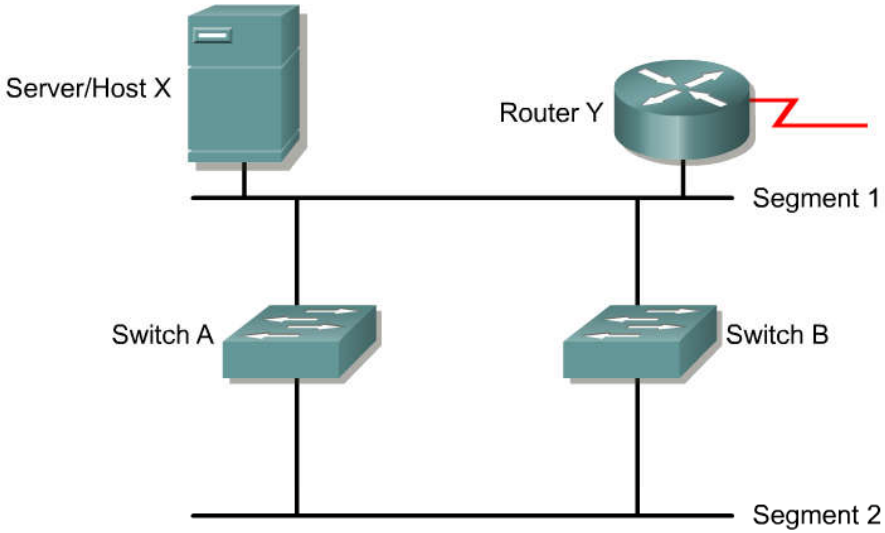
ปัญหาการซ้ำซ้อนใน OSI Layers 1 และ 2

การเชื่อมต่อเส้นทางหลายเส้นทางในสวิทซ์:

- ช่วยให้การการเชื่อมต่อซ้ำซ้อนทางกายภาพในเครือข่ายสวิทซ์
- เพิ่มความน่าเชื่อถือและเส้นทางสำรองในเครือข่าย
- ทำให้ผู้ใช้เข้าถึงทรัพยากรในเครือข่ายได้ แม้จะมีบางเส้นทางหยุดชะงัก

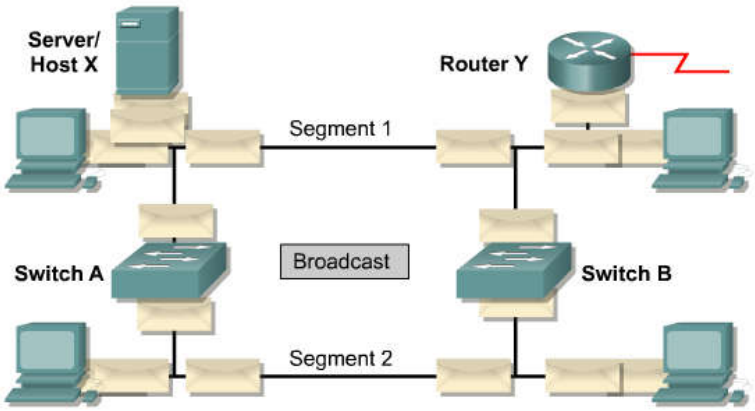


Redundant switched topologies



- สวิทซ์เรียนรู้ MAC addresses ของอุปกรณ์จากข้อมูลพอร์ตที่ส่งต่อปลายทางได้อย่างถูกต้อง
- สวิทซ์จะฟลัดเฟรมเมื่อไม่รู้ปลายทางจะกระทั่งสามารถเรียนรู้ MAC addresses ของอุปกรณ์
- Broadcasts และ multicasts ต่างใช้วิธีฟลัด (ยกเว้นในกรณีที่สวิทช์จะทำสอดแนม multicasts หรือ IGMP)
- การเชื่อมต่อมากกว่า 1 เส้นทางของสวิทซ์ ***อาจ*** (STP disabled) ทำให้เกิดปัญหา broadcast storms, multiple frame และ MAC address table instability

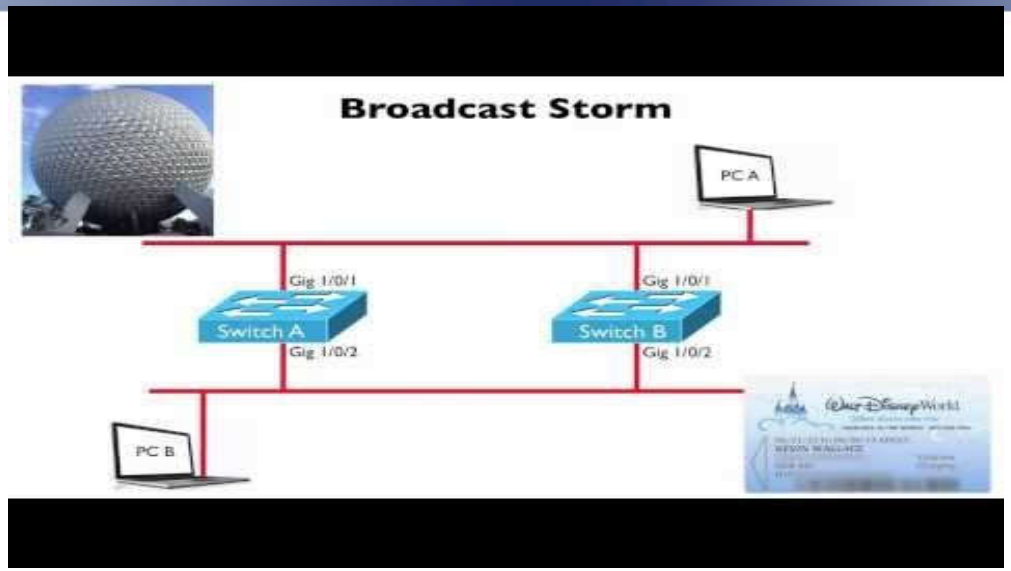
Broadcast Storm

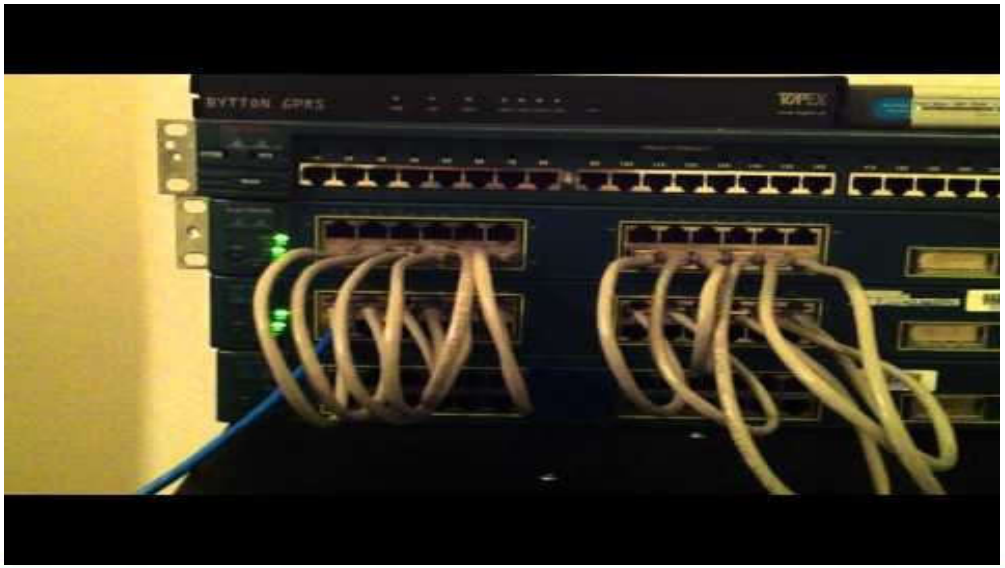


A state in which a message that has been broadcast across a networkresults in even more responses, and each response results in still more responses in a snowball effect. www.webopedia.com

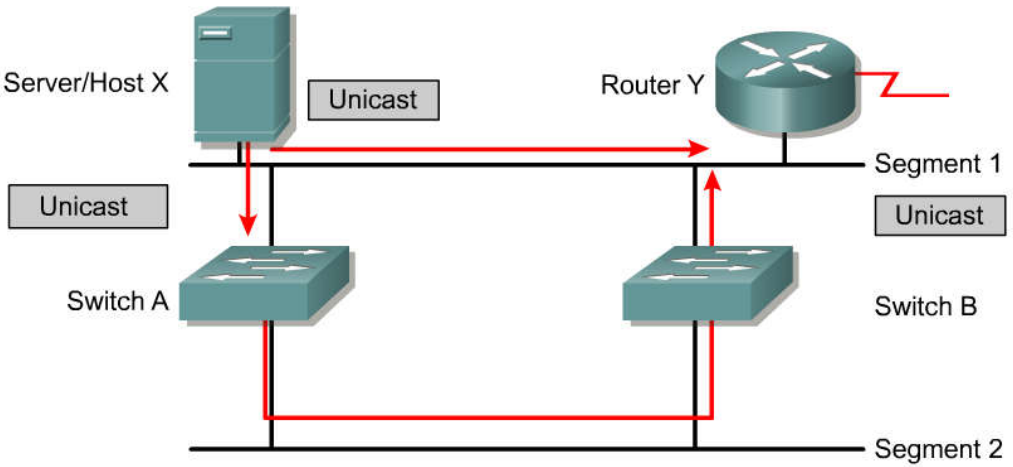
- Broadcasts และ multicasts สามารถทำให้เกิดปัญหาในเครือข่าย
- ถ้า Host X ส่ง บรอดคาสต์ (broadcast) เช่น ส่ง ARP request เพื่อหาที่อยู่ใน Layer 2 ของเราเตอร์ แล้ว Switch A ส่งต่อบรอดคาสต์ออกไปทุกพอร์ต
- Switch B ที่อยู่ในเซกเมนต์เดียวกัน ก็ส่งต่อบรอดคาสต์ออกไป
- Switch B เห็นบรอดคาสต์ของ Switch A ที่ส่งมา และ Switch A เห็นบรอดคาสต์ของ Switch B ที่ส่งมา
- Switch A เห็นบรอดคาสต์และทำการส่งต่อ
- Switch B เห็นบรอดคาสต์และทำการส่งต่อ
- สวิทช์ยังคงเผยแพร่ทราฟฟิกซ์บรอดคาสต์ออกไปเรื่อยๆ เรียกว่า **Broadcast storm**

ตัวอย่าง Broadcast Storm



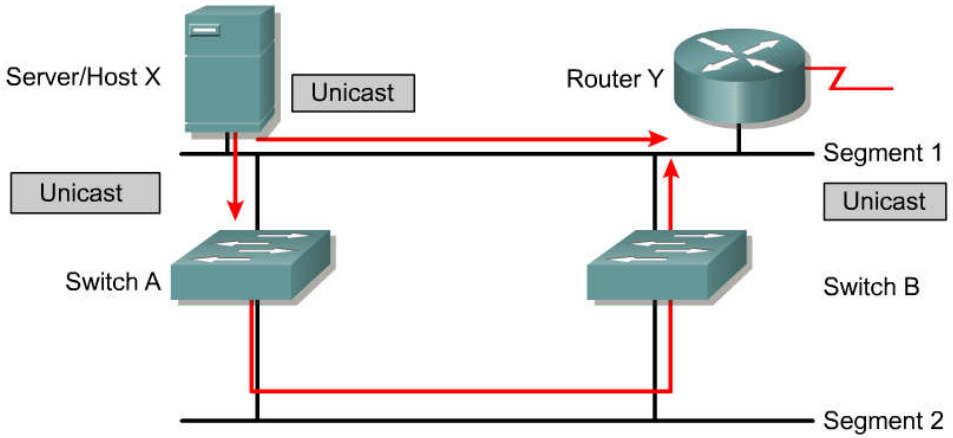


Multiple frame transmissions



- การเชื่อมต่อมากกว่า 1 เส้นทางของสวิทซ์ อาจให้เกิดอุปกรณ์ที่รับข้อมูลได้รับเฟรมที่ซ้ำซ้อนกันได้
- สมมุติว่า MAC address ของ Router Y หมดเวลา ในสวิทซ์ทั้งคู่
- สมมุติว่า โฮสต์ X ยังคงมีที่อยู่ MAC ของเราเตอร์ Y ใน ARP Cache และส่ง unicast frame ไปยัง router Y

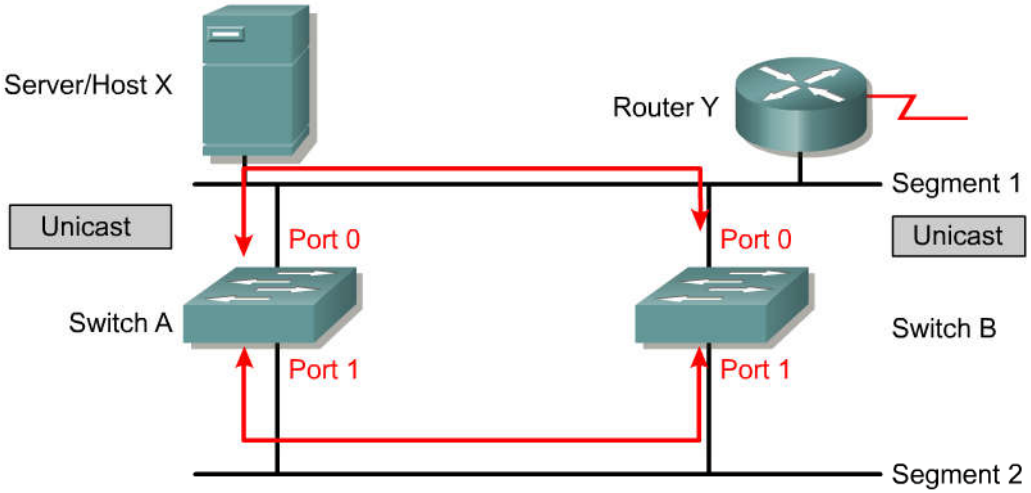
Multiple frame transmissions



(Some changes to curriculum)

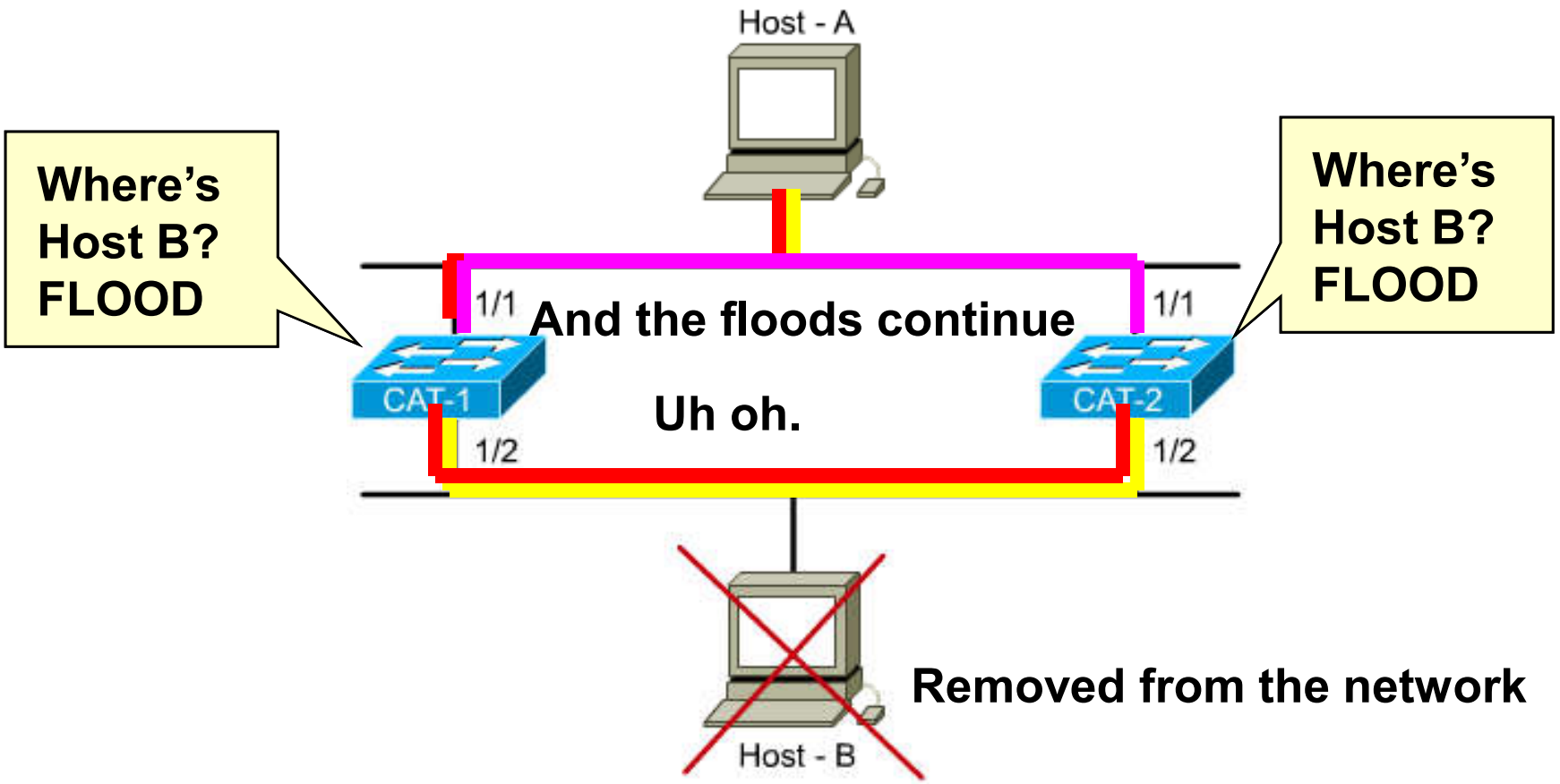
- The router receives the frame because it is on the same segment as Host X.
- Switch A does not have the MAC address of the Router Y and will therefore flood the frame out its ports. (Segment 2)
- Switch B also does not know which port Router Y is on.
- Note: Switch B will forward the the unicast onto Segment 2, creating multiple frames on that segment.
- After Switch B receives the frame from Switch A , it then floods the frame it received causing Router Y to receive multiple copies of the same frame.
- This is a causes of unnecessary processing in all devices.

Media access control database instability



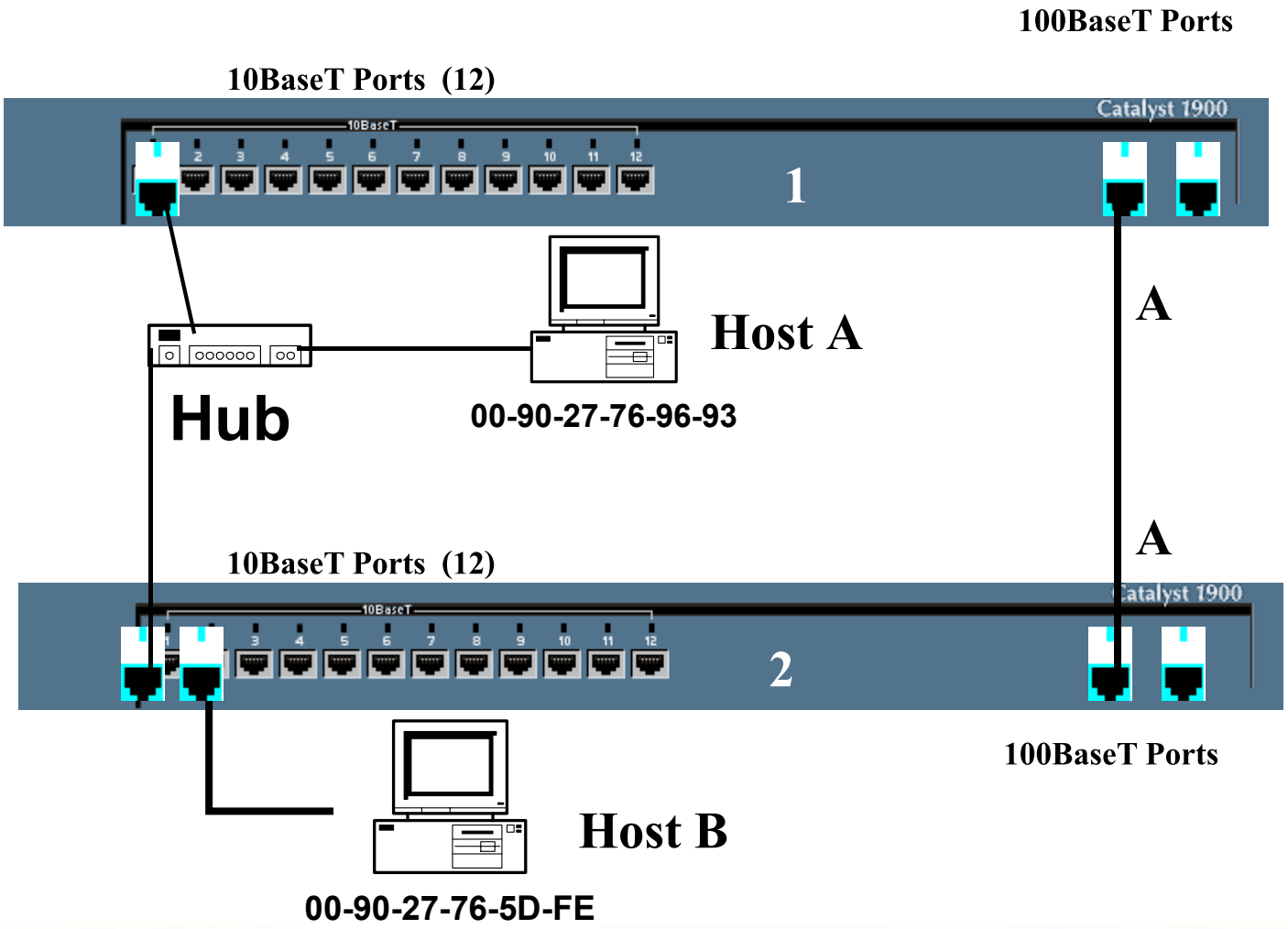
- In a redundant switched network it is possible for switches to learn the wrong information.
- A switch can incorrectly learn that a MAC address is on one port, when it is actually on a different port.
- Host X sends a frame directed to Router Y.
- Switches A and B learn the MAC address of Host X on port 0.
- The frame to Router Y is flooded on port 1 of both switches.
- Switches A and B see this information on port 1 and incorrectly learn the MAC address of Host X on port 1.

Layer 2 Loops - Flooded unicast frames



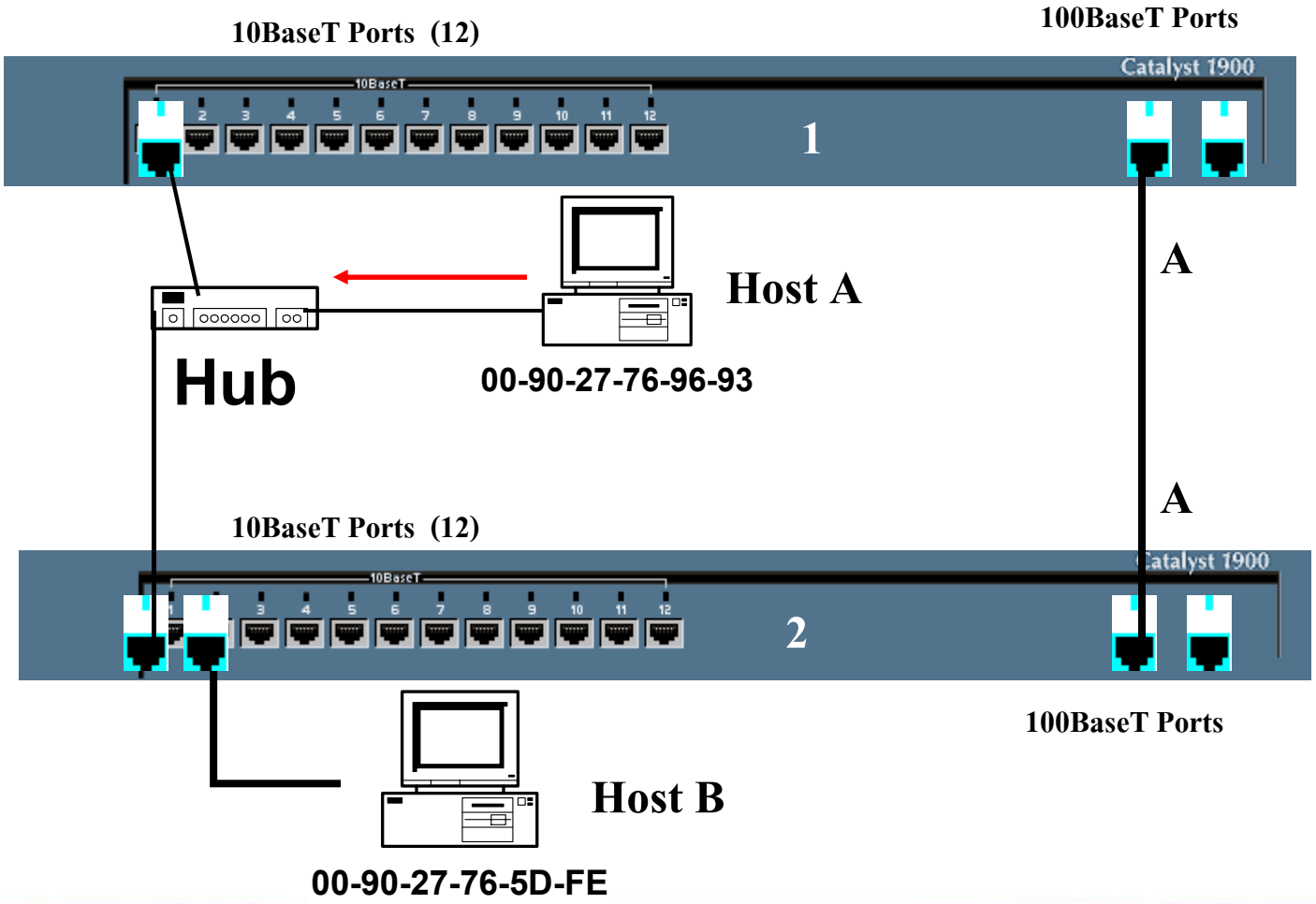
Redundant Paths and No Spanning Tree

Another problem, incorrect MAC Address Tables



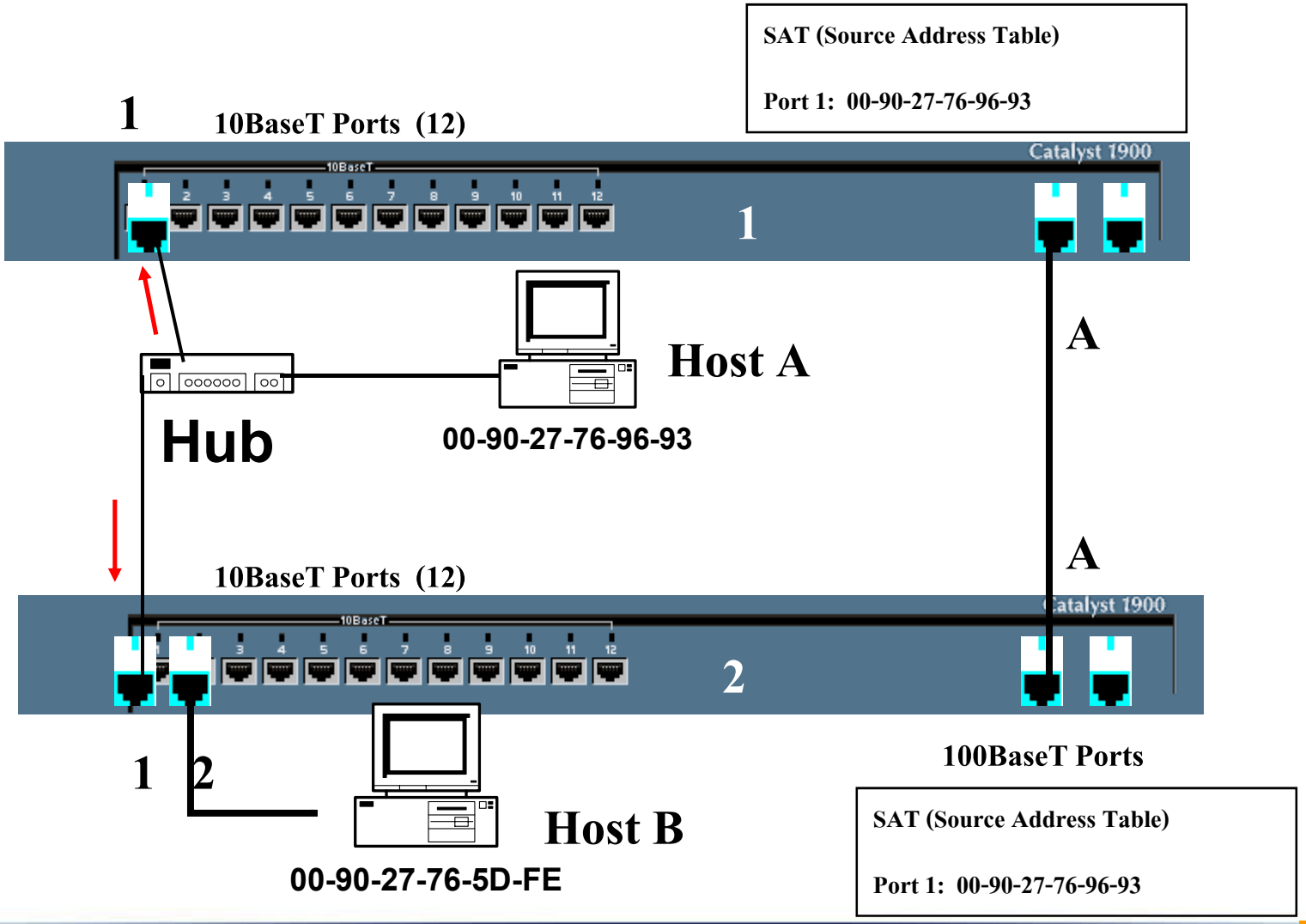
Redundant Paths and No Spanning Tree

Host A ส่ง Ethernet frame ไป Host B ทั้ง Switch 1 และ Switch 2 เห็นเฟรม และบันทึก Mac Address ของ Host A ใน switching tables.



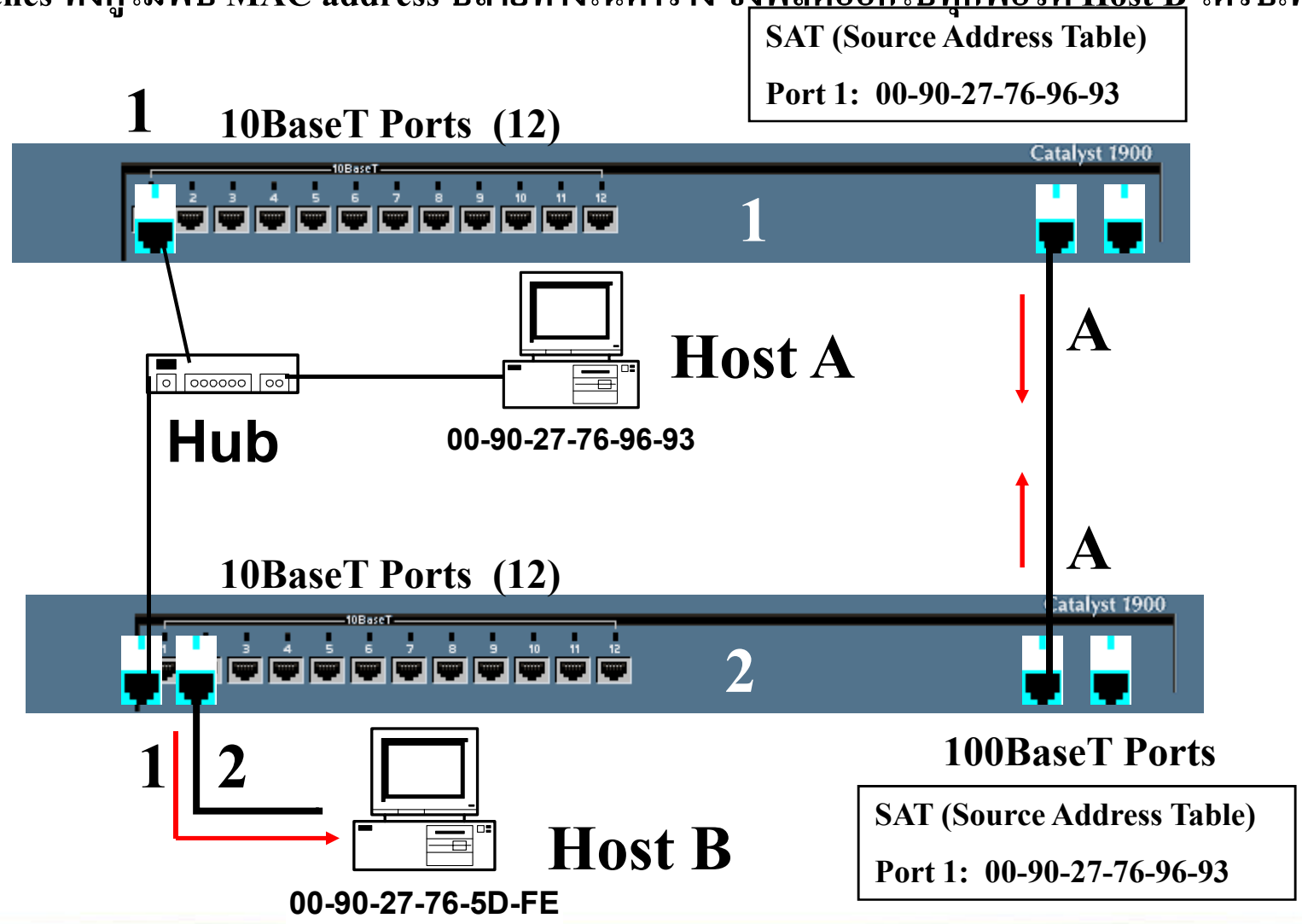
Redundant Paths and No Spanning Tree

ทั้ง Switch 1 และ Switch 2 เห็นเฟรม บันทึก Mac Address ของ Host A ลงใน switching tables ของตัวเอง



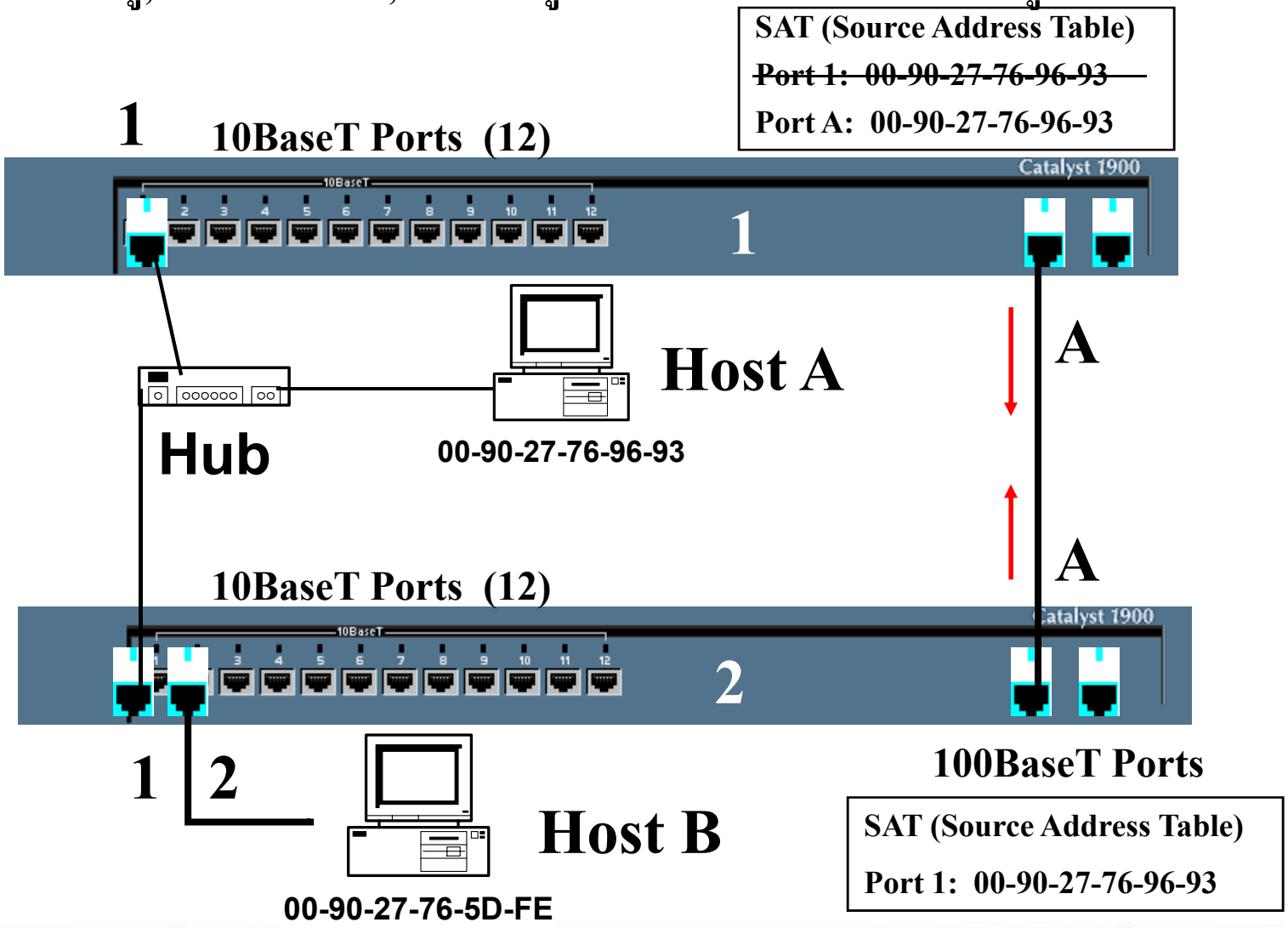
Redundant Paths and No Spanning Tree

Switches ทั้งคู่ไม่พบ MAC address ปลายทางในตาราง จึงฟลัดออกไปทุกพอร์ต Host B ได้รับเฟรม)



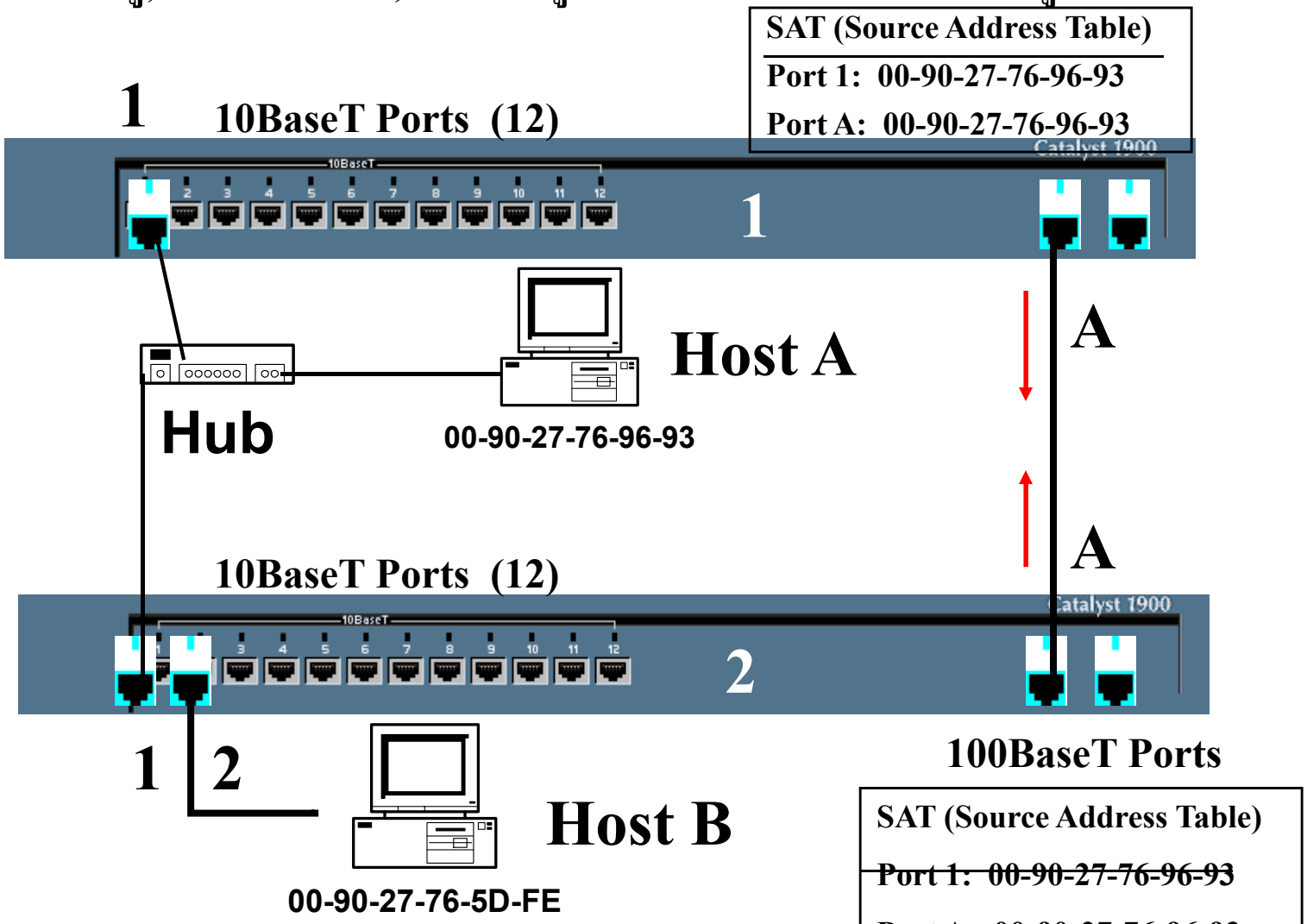
Redundant Paths and No Spanning Tree

Switch 1 เรียนรู้, พบข้อผิดพลาด, เพราะที่อยู่ต้นทางคือ 00-90-27-76-96-93 อยู่ Port A.



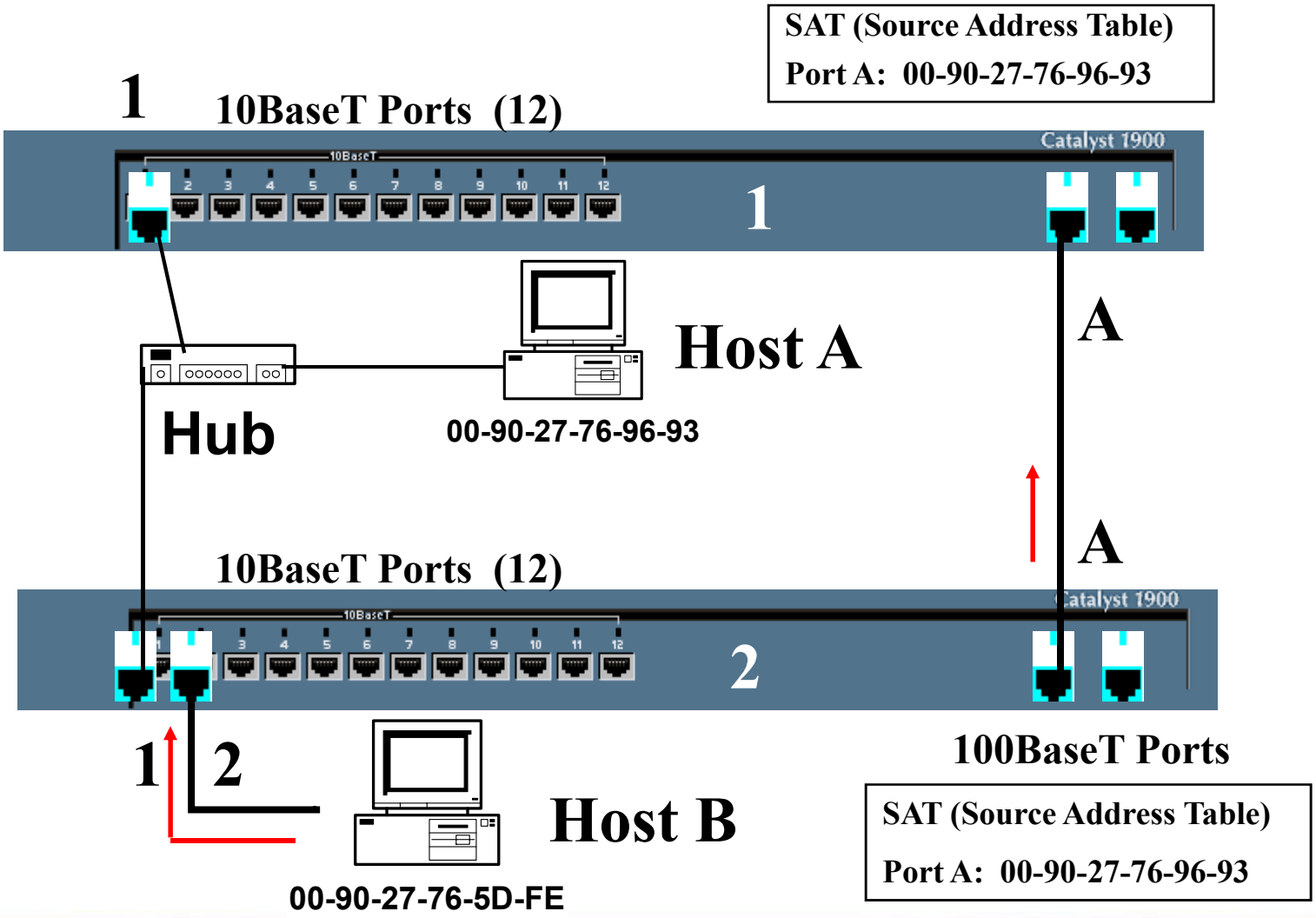
Redundant Paths and No Spanning Tree

Switch 2 เรียนรู้, พบข้อผิดพลาด, เพราะที่อยู่ต้นทางคือ 00-90-27-76-96-93 อยู่ Port A.



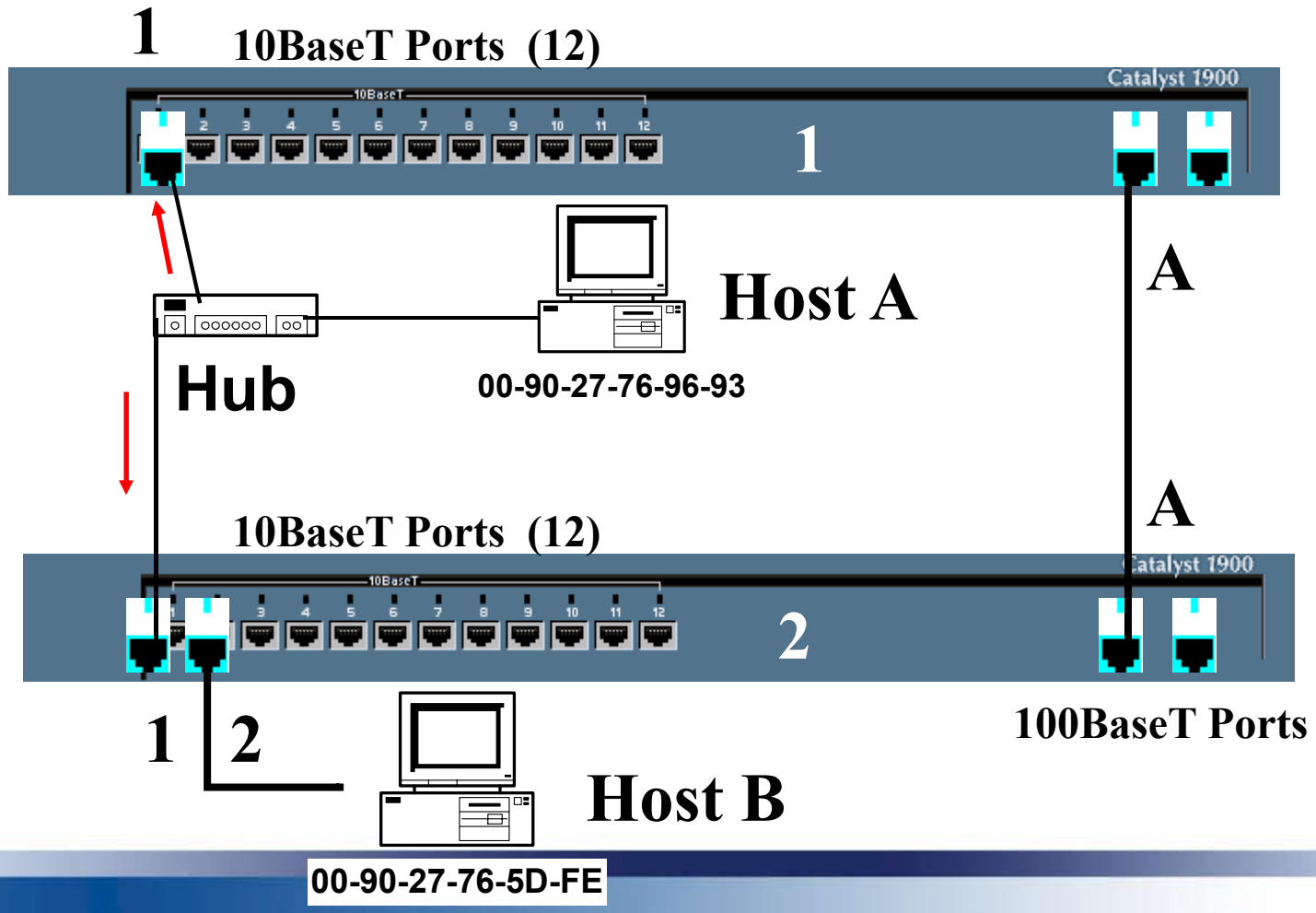
Redundant Paths and No Spanning Tree

ในเวลาเดียวกัน เมื่อ Host B ส่งเฟรมไป Host A จะส่งข้อมูลผ่านทาง port A ของ Switch 2



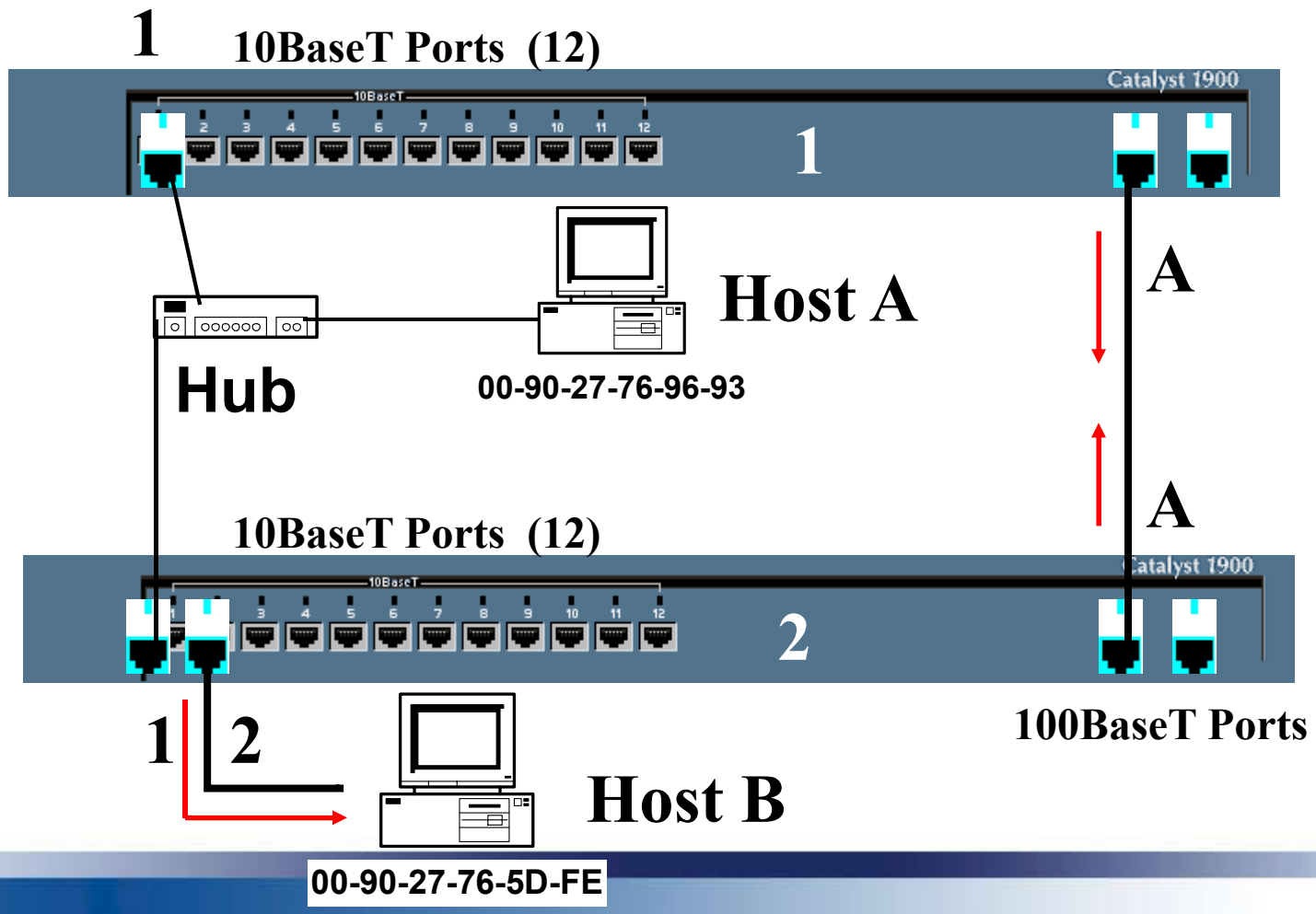
Broadcasts and No Spanning Tree

Lets, leave the switching tables alone and just look at what happens with the frames. Host A sends out a layer 2 broadcast frame, like an ARP Request.



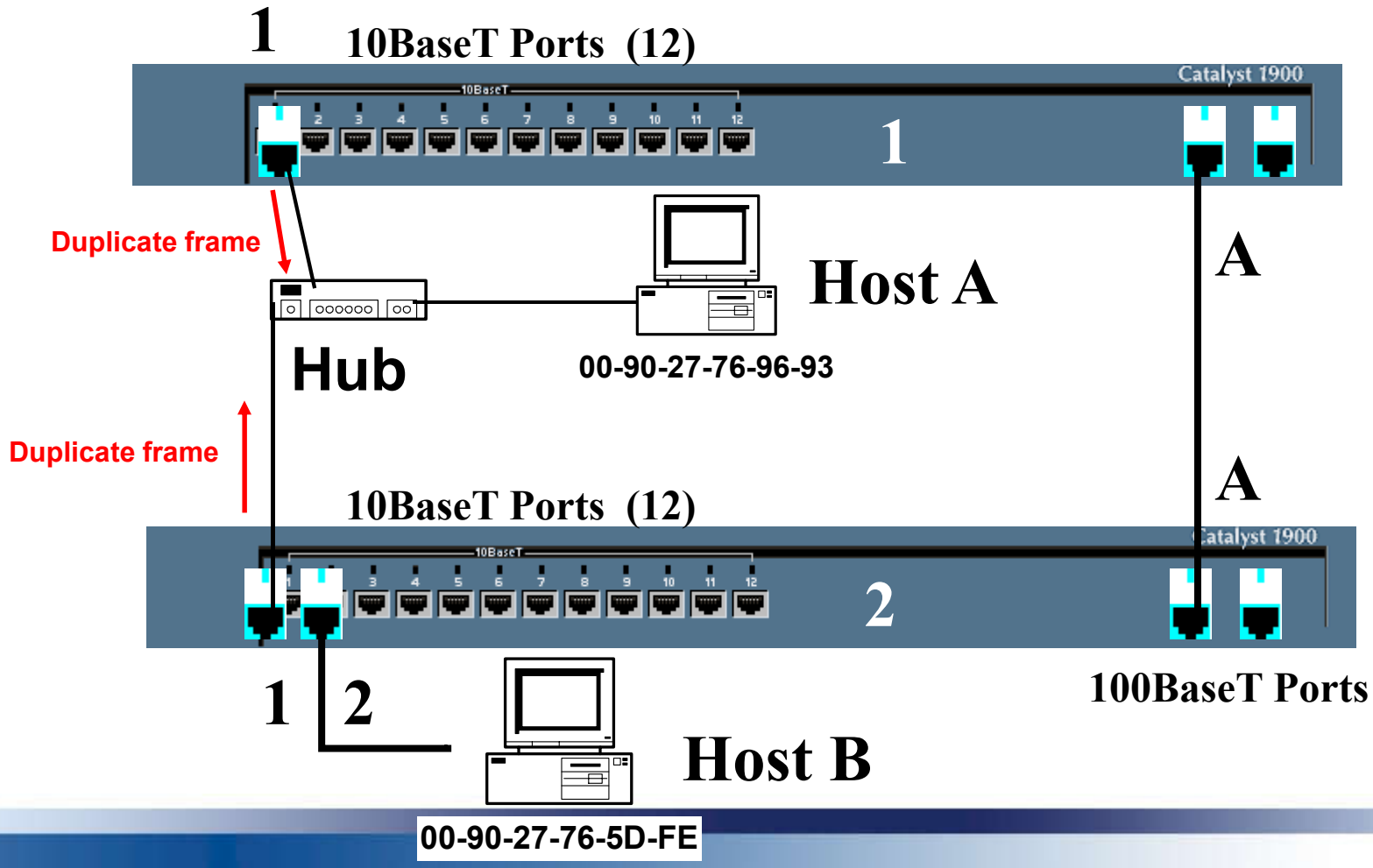
Broadcasts and No Spanning Tree

Because it is a layer 2 broadcast frame, both switches, 1 and 2 , flood the frame out all ports, including their port A's.



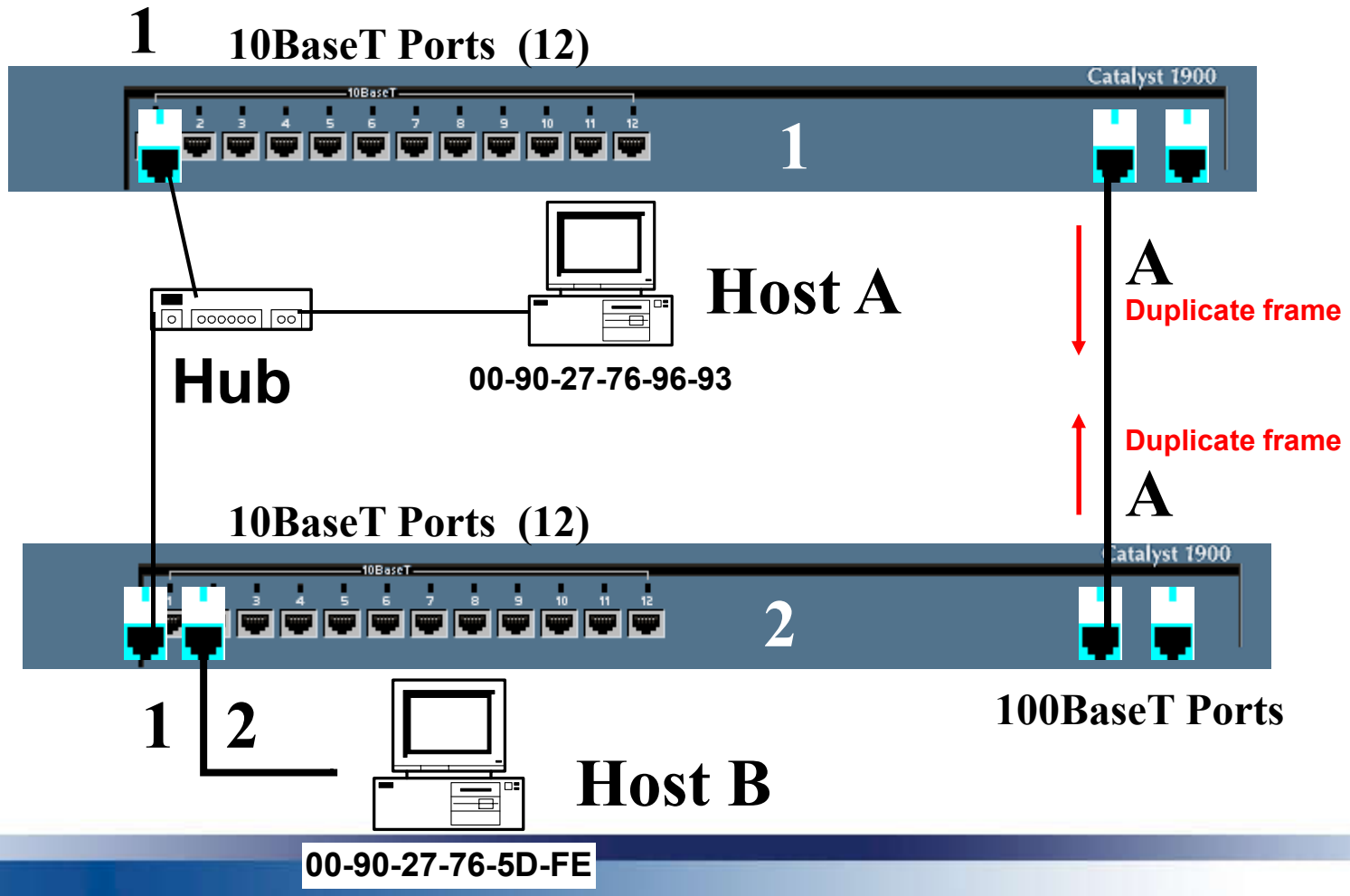
Broadcasts and No Spanning Tree

Both switches receive the same broadcast, but on a different port. Doing what switches do, both switches flood the duplicate broadcast frame out their other ports.



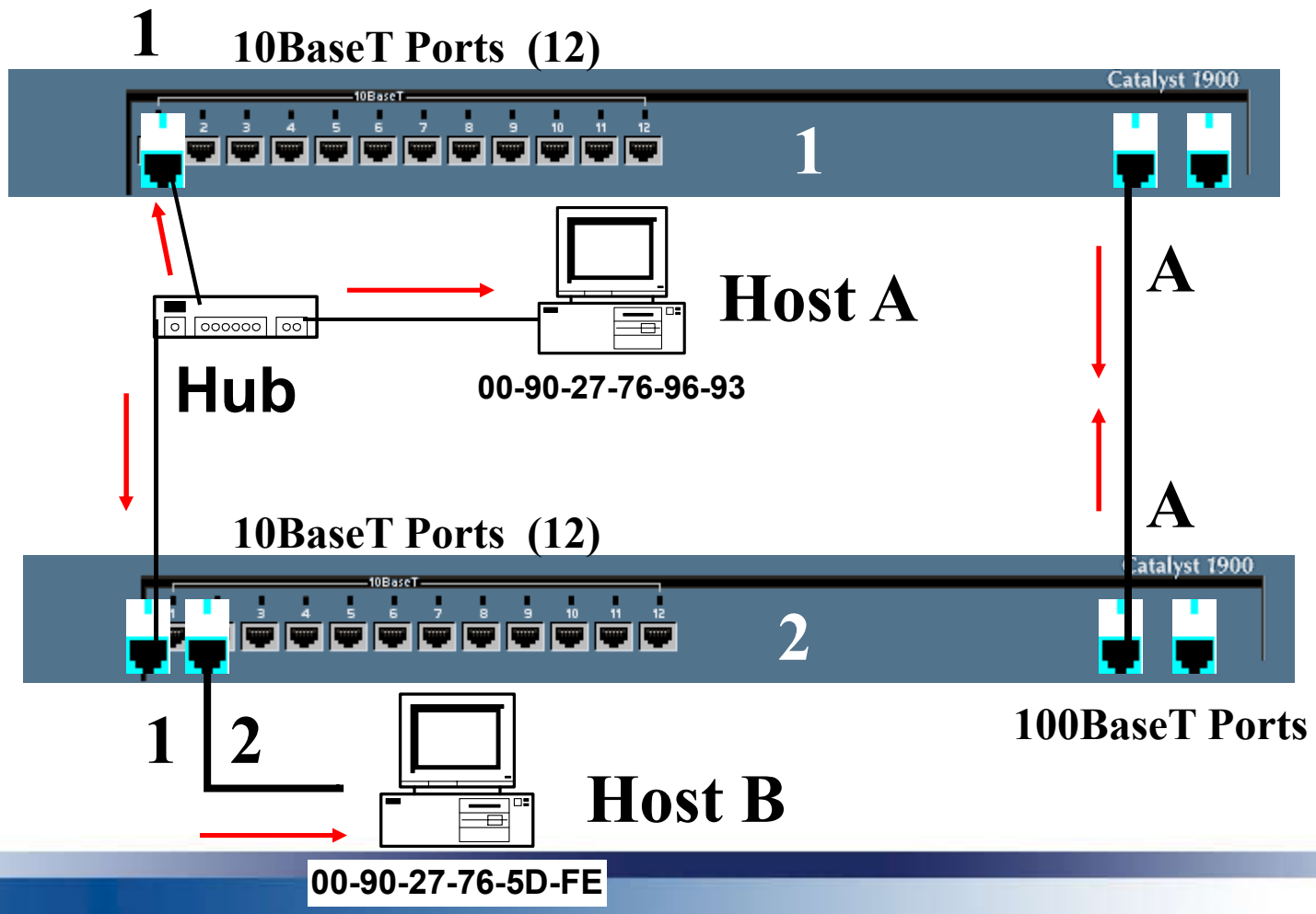
Broadcasts and No Spanning Tree

Here we go again, with the switches flooding the same broadcast again out its other ports. This results in duplicate frames, known as a *broadcast storm*!



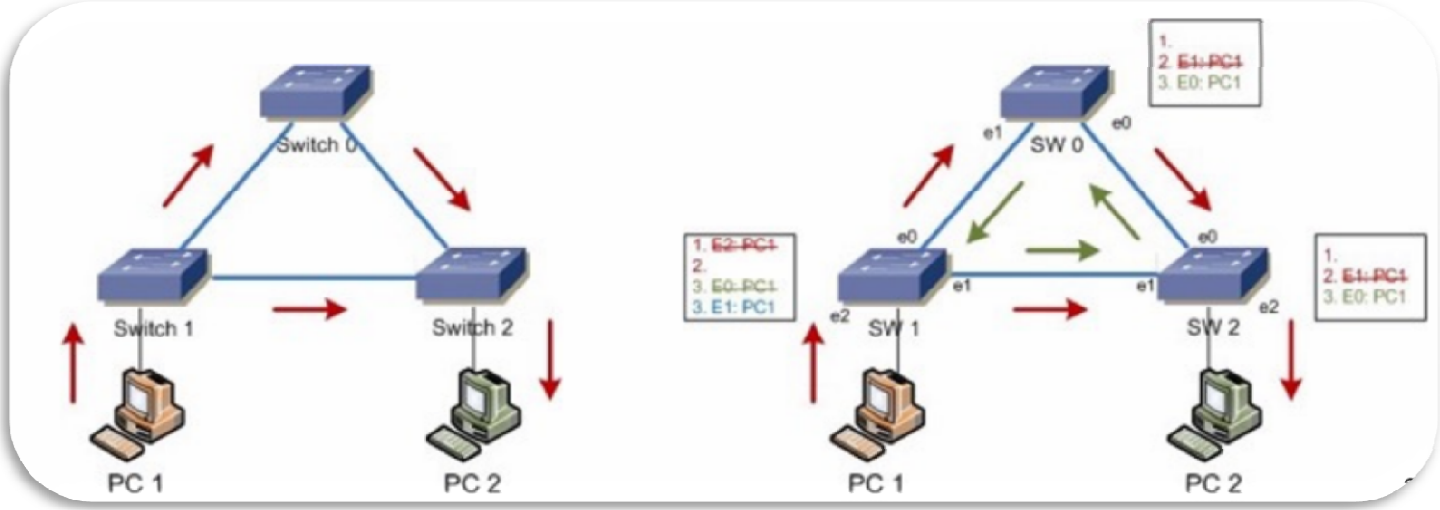
Broadcasts and No Spanning Tree

Remember, that layer 2 broadcasts not only take up network bandwidth, but must be processed by each host. This can severely impact a network, to the point of making it unusable.



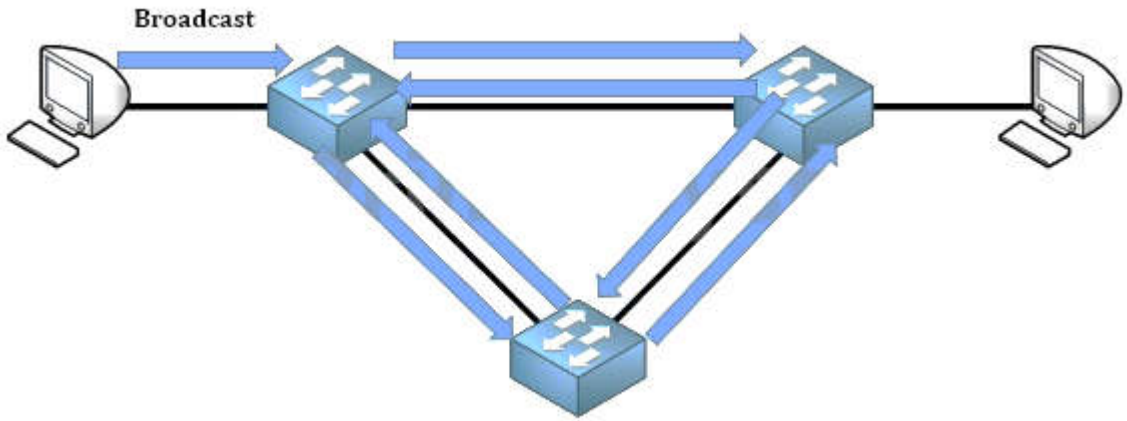
โพรโทคอลต้นไม้แบบทอดข้าม(Spanning tree Protocol :STP)

- Spanning Tree protocol (IEEE 802.1d) เป็น Protocol ที่ช่วยในเรื่องการหาเส้นทางในหมู่ Switch ที่ "Active" เพียงเส้นทางเดียวเท่านั้น
- เนื่องจาก หากเรามีเส้นทางสำรองในสวิทซ์ในการเข้าถึง Host ที่อยู่ในสวิทซ์ปลายทางมากกว่า 1 เส้นทาง อาจเกิดปัญหา Switching Loop



เมื่อมี Loop จะทำให้เกิดปัญหา ที่เกิดขึ้นตามมา 3 อย่างหลักๆ คือ

- Broadcast Storm โดยปกติบน Layer 2 เอง Switch จะมีการ Broadcast อยู่แล้ว คือ flood ออกทุกพอร์ต ดังนั้น เมื่อเกิด Loop ขึ้น broadcast traffic จะถูกส่งต่อวนไปเรื่อยๆ แบบไม่มีที่สิ้นสุด เกิดเป็นพายุ broadcast ขึ้น ทำให้ CPU ของ Switch นั้นพุ่งขึ้นสูงและทำงานไม่ได้ในที่สุด

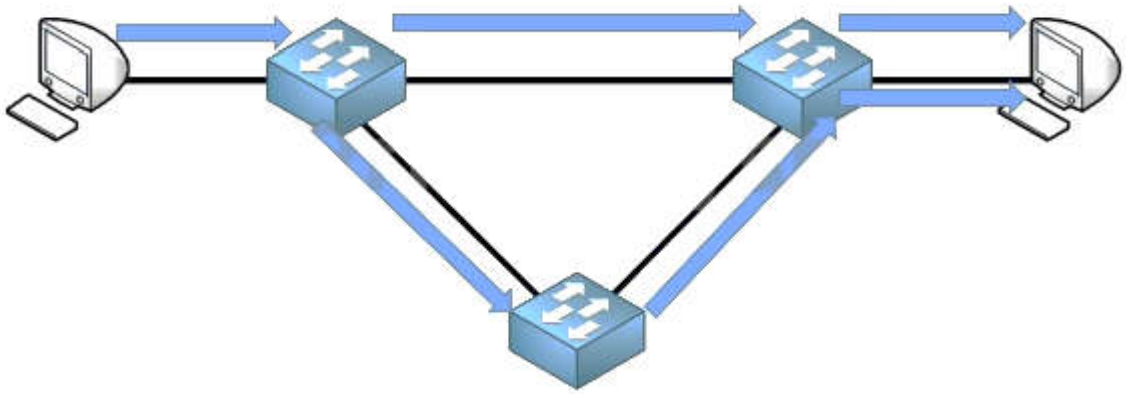


Broadcast Storms

- หลักการของสวิทซ์ ในการส่งเฟรมไปยังโฮสต์ที่มันไม่รู้จักหรือไม่มี MAC Address ในตารางของสวิทซ์ตัวนั้นๆ ก็คือ Flood เฟรมออกไปยังทุกๆ พอร์ตที่มันมีอยู่ ยกเว้นพอร์ตที่มันได้รับเฟรมเข้ามา
- broadcast storm เกิดขึ้นเมื่อมี broadcast เฟรมจำนวนมากติดลูปอยู่ในเลเยอร์ 2 แบนด์วิดธ์ที่มีอยู่จะถูกใช้ทั้งหมด ปัญหานี้ยังเป็นที่รู้จักในชื่อ การปฏิเสธการให้บริการ (denial of service)
- broadcast storm เป็นสิ่งที่หลีกเลี่ยงไม่ได้บนเครือข่ายที่มีลูป
  - เมื่อมีหลายอุปกรณ์ส่ง broadcast ผ่านเครือข่าย การจราจรในเครือข่ายจะติดขัดภายในลูป จึงมีการใช้ทรัพยากรมากขึ้น
  - ทำให้เกิด broadcast storm จนทำให้เกิดเครือข่ายล่ม

Duplicate Unicast Frames

- เป็นเรื่องของ Frame ไปถึงจุดปลายทาง 2 อัน คือ ข้อมูลชุดเดียวกันไปถึงจุดหมายปลายทาง 2 ครั้ง ที่เครื่องปลายทางได้รับข้อมูล (frame) เข้ามาซ้ำ ทำให้เสียเวลาในการประมวลผลไปอีก

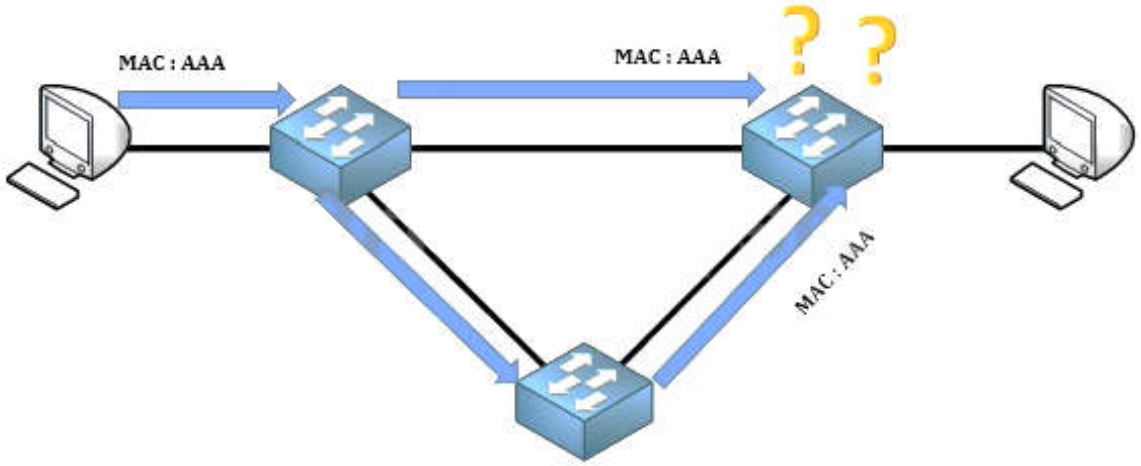


Duplicate Unicast Frames

- Unicast เฟรมที่ถูกส่งไปยังเครือข่ายที่มีลูป ส่งผลให้เกิดเฟรมซ้ำส่งไปยังอุปกรณ์ปลายทาง
- Upper layer protocols ส่วนใหญ่จะไม่ได้ออกแบบมาเพื่อรับรู้ หรือ รับมือกับการส่งแบบซ้ำซ้อน
- Layer 2 LAN protocols เช่น Ethernet ไม่มีกลไกในการรับรู้และขจัดเฟรมที่วนลูปไม่รู้จบ

MAC Database Instability

- ความไม่แน่นอนของ Mac Address table ถ้าเกิดข้อมูลในตาราง Mac Address เปลี่ยนอยู่ตลอดเวลา จะเกิดการสับสนข้อมูลอาจหาย
- เมื่อเกิด Loop ทำให้ Switch ได้รับ MAC address ของอุปกรณ์เดียว เข้ามาหลายทาง ทำให้ Switch เกิดการเรียนรู้ MAC address ที่ผิดเพี้ยนไปในการส่งต่อ



- ซึ่งบน Layer 3 จะมีค่า TTL เพื่อไว้ป้องกัน Loop ได้ แต่บน Layer 2 ไม่มีค่า TTL เหมือน Layer 3 จึงต้องมี protocol เข้ามาช่วยในการป้องกัน Loop ที่เกิดขึ้นบน Layer 2 นั่นคือ Spanning-Tree Protocol (STP)

MAC Database Instability

- Ethernet เฟรมจะไม่มีคุณลักษณะ time to live (TTL)
  - เฟรมยังจะคงวิ่งไประหว่างสวิตช์อย่างไม่มีที่สิ้นสุด หรือจนกว่าจะตัดการเชื่อมต่อและตัดลูปออก
  - ทำให้ฐานข้อมูล MAC Address เกิดความไม่แน่นอน
  - สามารถทำให้เกิดการส่งต่อ broadcast เฟรม
- ถ้ามีมากกว่า 1 เส้นทางในการส่งต่อเฟรมออกไป จะส่งผลให้ติดลูปแบบไม่มีที่สิ้นสุด
  - เมื่อเกิดลูป ตาราง MAC Address ในสวิทช์จะมีการเปลี่ยนแปลงตลอดเวลาที่มีการปรับปรุงจาก broadcast เฟรม ทำให้ฐานข้อมูล MAC เกิดความไม่แน่นอน

Spanning Tree Protocol (STP)

- การแก้ไขปัญหา Loop นั้นของระบบ Network เพื่อไม่ให้เกิดข้อมูลที่วนอยู่ในระบบ มีวิธีหนึ่งที่เรียกว่า Spanning Tree Protocol(STP)
- ซึ่งเป็นการแก้ไขปัญหาการเกิด Loop ได้ โดยตัวโปรโตคอลนั้นจะทำการท่องไปยัง Node ต่างๆของระบบ Network เพื่อค้นหาว่าเส้นทางใดมีการวนมาพบกันหรือไม่ หากมีการวนก็จะทำการตัดเส้นทางเพื่อให้เกิดเป็น Unique Distance หรือ เส้นทางเดียวในการท่องไปยัง Node นั่นเอง
- โดยตัวโปรโตคอลจะดูจากระยะทางใกล้จาก Root Node มากสุด หรือมีการเดินทางผ่าน Node ของ Ethernet น้อยที่สุด แล้วจะทำการตัดเส้นทางที่ไกลออกไป เพื่อให้เกิดประสิทธิภาพในการทำงานของระบบไม่ให้เกิดการวนของข้อมูลในระบบได้

Spanning-Tree Protocol (STP)

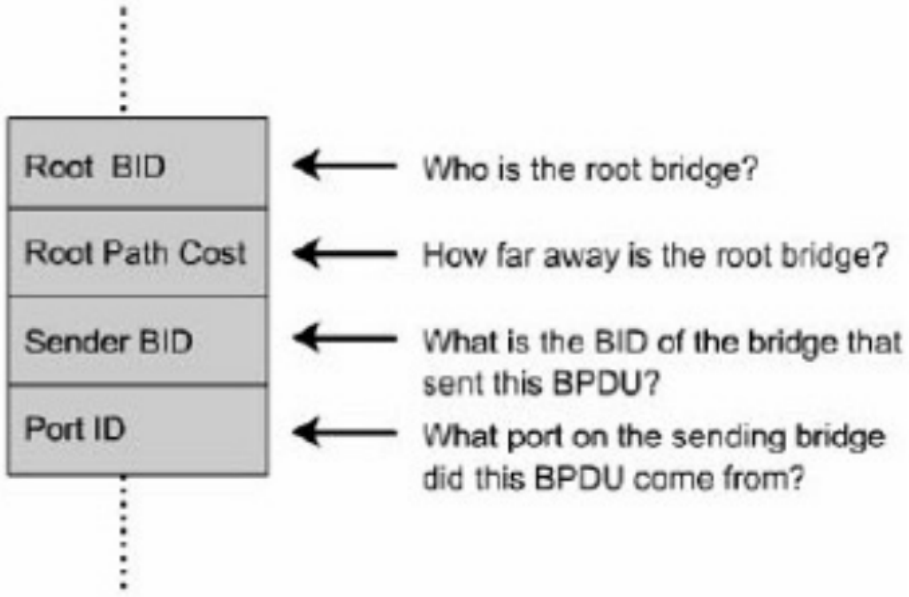
- เป็น protocol ที่ใช้ป้องกัน Loop บน Layer 2 ตามมาตรฐานกลาง IEEE 802.1D
- โดยจะทำการเปลี่ยนสถานะของ port นึง ให้เป็น blocking เพื่อไม่ให้รับส่งข้อมูลได้ชั่วคราว
- จนกว่าเส้นทางหลักที่ใช้งานจะมีปัญหา port blocking ไว้ ก็จะกลับขึ้นมาใช้งานและส่งข้อมูลได้นั่นเองครับ !!!

- แนวคิดของ STP จะมีมาตั้งแต่สมัยที่ยังไม่มี Switch โดยจะอ้างอิงถึงระบบที่ใช้สาย Coaxial Cable ที่วิ่งอยู่บนมาตรฐาน 10Base5
- แต่ละวงสามารถต่อ Repeater ได้ไม่เกิน 4 ตัวเท่านั้น และได้ระยะทางสูงสุดที่ 2.5 km ใน 1 ระบบ
- แต่ละระบบสามารถแยกออกจากกันด้วยอุปกรณ์ที่ชื่อว่า Bridge ซึ่ง Bridge จะทำหน้าที่แบ่ง collision domain หรือ Lan Segment ออกจากกัน เพราะใน Lan Segment ใดๆเมื่อมีการส่งข้อมูลจะเห็นถึงกันทุกตัว
- ซึ่ง Bridge จะเป็นตัวขั้นเพื่อไม่ให้ Package จาก Lan Segment แรกไปวิ่งอยู่ใน Lan Segment ที่สองนั้นเอง

Spanning tree Protocol (STP)

- โดยจะยอมให้มีเส้นทางเพียงเส้นทางเดียวในหมู่ Switch ที่สามารถส่ง Frame ออกไปได้ (Forwarding States)
- ในหมู่ Switch ด้วยกันนั้นจะมีการ "เลือก" Root Bridge เพื่อเป็น Root Tree ของ Switch ใน Domain นั้นๆ
  - Bridge ID (คำนวณจาก **priority** + MAC Address ที่ต่ำที่สุด โดยที่ priority ใน Cisco Catalyst Switch จะเท่ากับ **32768**)
  - Switch ทุกตัว จะส่ง Message ตัวหนึ่ง คือ BPDU เพื่ออ้างตนเองว่า ตนนั้นเป็น Root Bridge

Spanning tree Protocol (STP)



- เมื่อ Switch ทุกตัวได้รับ BPDU มันจะเปรียบเทียบกับตนเอง หากว่ามันได้รับ BPDU ที่ดีกว่า มันก็จะ update ตาม BPDU นั้นๆ
- ซึ่งระยะความถี่ในการส่งของ BPDU นั้นคือ ทุกๆ 2 วินาที
- เมื่อการเลือกตั้ง Root Bridge จบลง ก็จะได้ Root Bridge มา 1ตัว
- ซึ่ง Port ทุกๆ Port บน Root Bridge นั้นๆ เราจะเรียกว่า "Designated Port“ ซึ่งสามารถทำการ Forward Frame ได้

ศัพท์ที่เกี่ยวข้องกับ STP

- Bridge Priority คือ ค่าลำดับความสำคัญ ของ Switch นั้นเมื่อเทียบกับ Switch ตัวอื่น (มีค่าตั้งแต่ 0 - 65,535) by default คือ 32,768
- Mac address คือ Mac address ประจำตัว Switch เองขึ้นกับ Switch แต่ละโมเดล ซึ่งจะ Hard code ไว้ภายใน Switch มาจากโรงงาน และไม่สามารถเปลี่ยนโดยผู้ใช้ได้
- Bridge ID คือ เป็นค่าตัวเลข 8 byte ที่ประกอบด้วยฟิลด์ Bridge Priority (2 byte) + Mac address (6 byte) ซึ่งจะอยู่ใน BPDU

ศัพท์ที่เกี่ยวข้องกับ STP

- Forwarding State คือ สถานะที่สามารถ รับ-ส่ง เฟรมได้
- Blocking State คือ สถานะที่ไม่สามารถ รับ-ส่ง เฟรมได้
- Root Bridge คือ Switch ที่ถูกเลือกให้ทำหน้าที่เป็นศูนย์กลางหลักของ Network
- Root Port คือ Port ที่มี Path Cost ไปยัง Root Bridge น้อยที่สุดเมื่อเทียบกับ Port อื่นๆ บน Switch ตัวเดียวกัน
- Designated Port คือ Port ที่มี Path Cost ไปยัง Root Bridge น้อยที่สุดเมื่อเทียบกับ Port ของ Switch ตัวอื่นที่เชื่อมต่ออยู่ในเซกเมนต์เดียวกัน

Path Cost

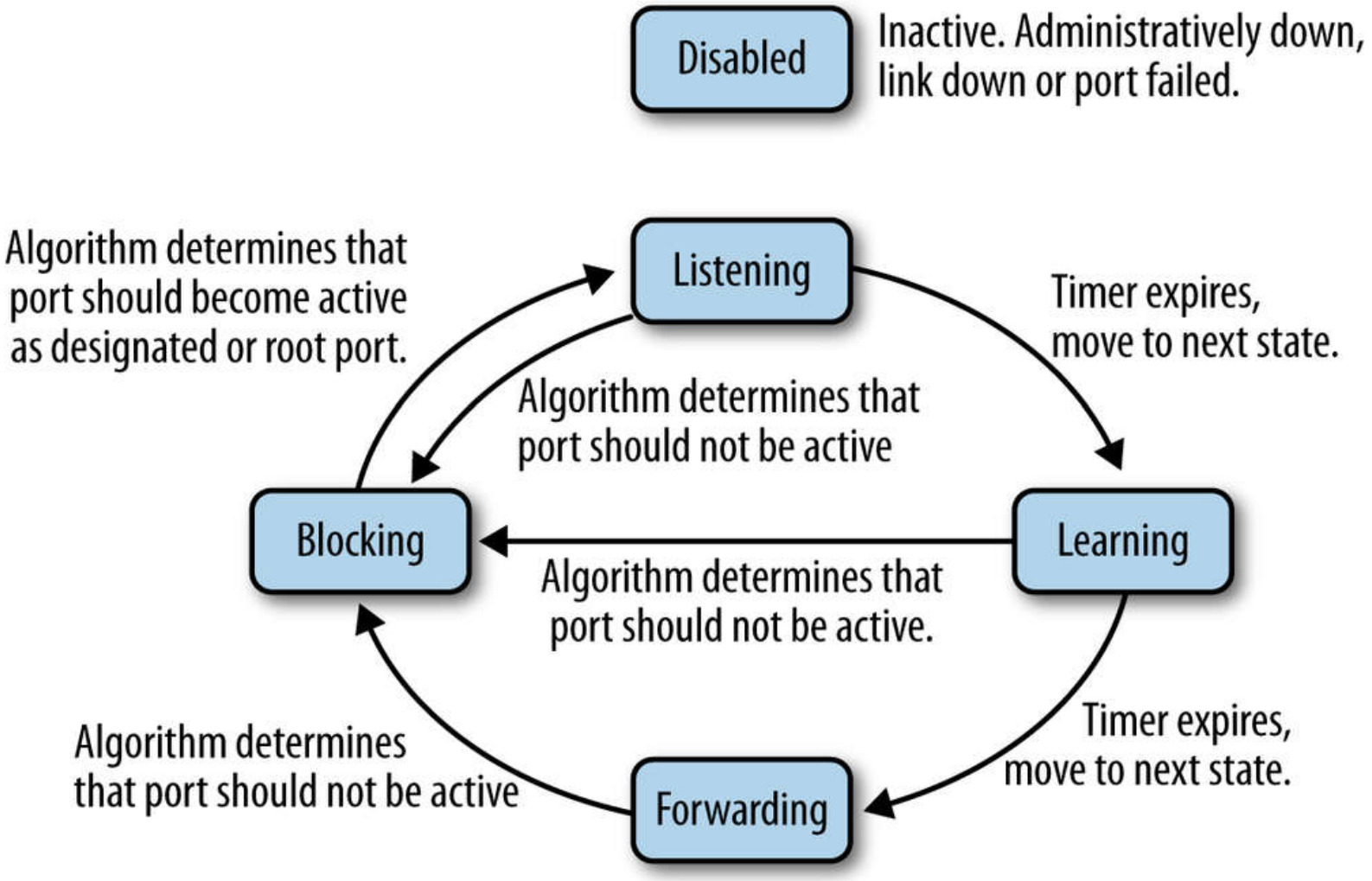
- คือ ค่าที่ใช้เปรียบเทียบในการหา Root Port และ Designated Port โดยเปรียบเทียบกับค่า Bandwidth โดยแต่ละ Bandwidth จะมีค่า Path Cost ดังนี้

Data rate	STP Cost (802.1D-1998)	RSTP Cost (802.1W-2001)
4 Mbit/s	250	5,000,000
10 Mbit/s	100	2,000,000
16 Mbit/s	62	1,250,000
100 Mbit/s	19	200,000
1 Gbit/s	4	20,000
2 Gbit/s	3	10,000
10 Gbit/s	2	2,000

Mode การทำงานของ Spanning-Tree

- ถ้า Switch ตรวจสอบพบว่ามีการเปลี่ยนแปลงเกิดขึ้นภายใน Switch และถ้ามีค่า cost พอที่จะเปลี่ยนสถานะมาเป็น Designated port มันก็จะทำการเปลี่ยนสถานะจาก Blocking ไปจนถึง Forward port ตามสถานการณ์นั้นๆ
  - Blocking มันจะไม่ส่ง user ของมันออกไป แต่จะมีการส่ง BPDU ส่งไปให้ port ที่ Block ก็คือว่า Blocking นั้นเป็นสถานะที่ไม่สามารถส่งข้อมูลได้ แต่มันสามารถรับ BPDU ได้ ถ้าข้อมูลของ user หายไปหรือเริ่มมีการผิดปกติมันก็จะเปลี่ยนสถานะไปสู่สถานะ Listening มันจะใช้เวลาประมาณ 20 วินาที
  - Listening มันจะเริ่มเชื่อม link ขึ้นมา (Enable Link) มันจะรอฟังว่ามันจะได้เป็น Designate port หรือเปล่าจะใช้เวลารอประมาณ 15 วินาที
  - Learning มันก็จะเรียนรู้ Mac Address จากที่อื่นๆ และก็ดูว่ามีอะไรเกิดขึ้น ข้อมูลที่ถูกส่งเข้ามามันก็จะเก็บที่ Mac Table ทันทีเพื่อเก็บเป็นข้อมูลตั้งต้นใช้เวลาประมาณ15 วินาที
  - Forwarding มันจะส่งข้อมูล User ได้ตามปกติ

Spanning tree port states



IEEE802.1D

- STP ใช้เงื่อนไขต่อไปนี้ในการพิจารณาว่าพอร์ตใดอยู่ในสถานะ Forwarding หรือ Blocking

  ขั้นที่ 1 ทำการตั้ง Root Bridge

  ขั้นที่ 2 เลือก Root Port ใน switch อื่นๆที่ไม่ใช่ Root Bridge

  ขั้นที่ 3 เลือก Designated Ports

IEEE802.1D

- 1 root bridge / network (root bridge ==> bridge id น้อยสุด ==> bridge id = priority + mac
- 1 root port / non root bridge (designated bridge(RVST) (port ที่ forward frame ไปหา root bridge ค่า cost น้อยสุด ถ้าค่า cost เท่ากันให้ดูที่ ค่า Bridge ID))
- 1 designated port/ 1 segment
- 1 Non designated port คือ พอร์ตที่ไม่ได้ใช้ (Block port, alternated port) (path Cost มากสุด)

ขั้นที่ 1 ทำการ Root Bridge

- โดย Switch แต่ละตัวจะอ้างว่าตัวเองคือ Root Bridge จะทำการเปลี่ยน Bridge Protocol Data Unit(BPDU) ซึ่งหาก Switch ตัวใดมีค่า Bridge ID น้อยสุดก็จะได้เป็น Root Bridge
- ใน Bridge ID ประกอบด้วย Bridge Priority และ VLAN มีค่าเท่ากับ 2 Byte (มีค่าตั้งแต่ 0-65535 โดยดีฟอร์ตจะมีค่าเท่ากับ 32768 แต่สามารถตั้งค่าผ่าน Config)

Switch(config)#spanning-tree vlan <vlan id> Priority <ค่าBridge Priority>

หรือ Switch(config)#spanning-tree vlan <vlan id> root primary

ขั้นที่ 2 เลือก Root Port ใน switch อื่นๆที่ไม่ใช่Root Bridge

- Switch อื่นๆที่ไม่ใช่ Root Bridge จะมีการเลือกพอร์ตที่มีค่า Cost จากพอร์ตนั้นๆไปยัง Root Bridge ที่มีค่าต่ำสุด เพื่อให้เป็น Root Port
- โดย Switch 1 ตัวจะมี Root Port 1 พอร์ตและจะทำการ set เป็น Forwarding State

ขั้นที่ 3 เลือก Designated Ports

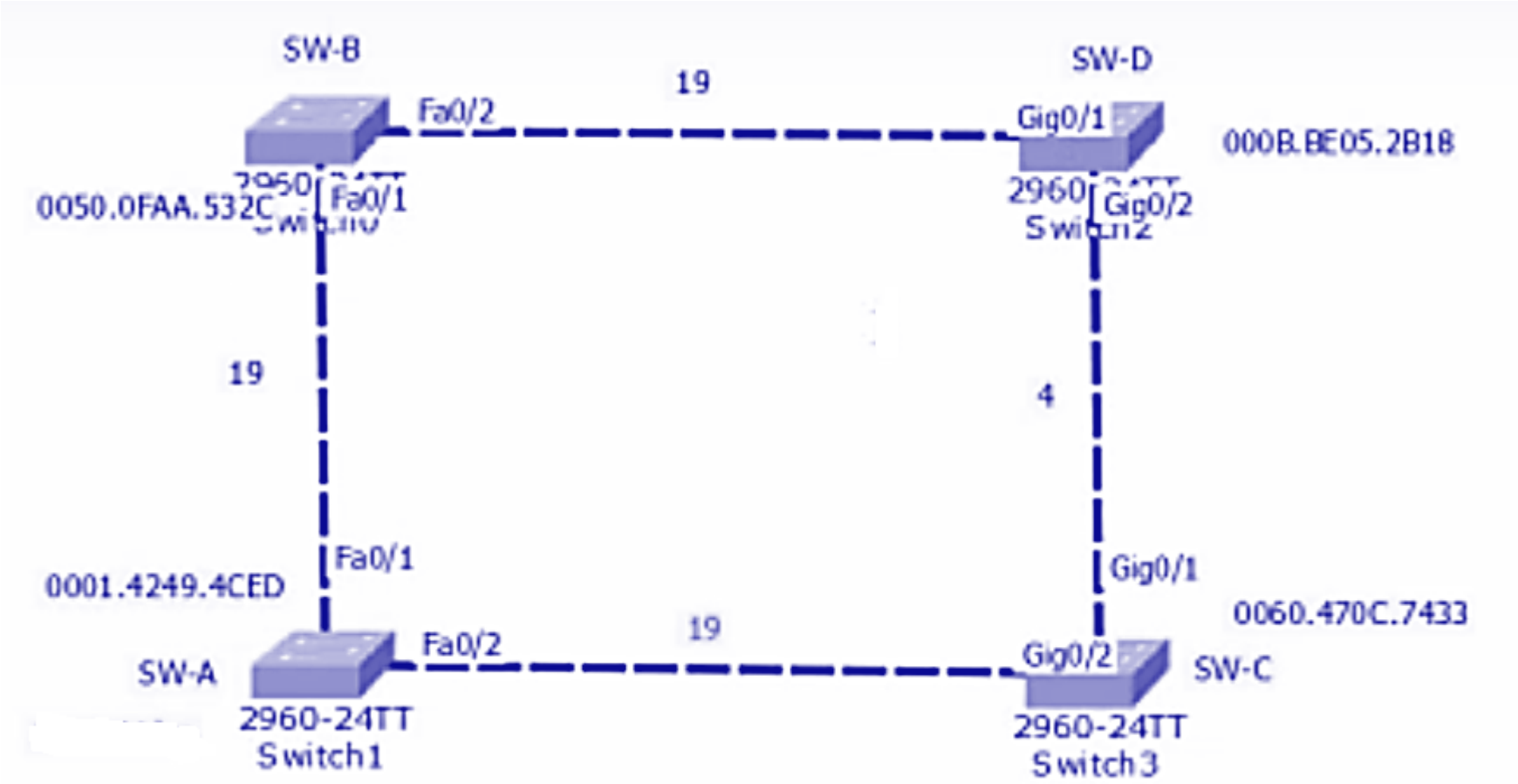
เป็นการพิจารณาว่าพอร์ตไหนมี Root Path Cost ต่ำสุดโดยมีเงื่อนไขการเลือกดังนี้

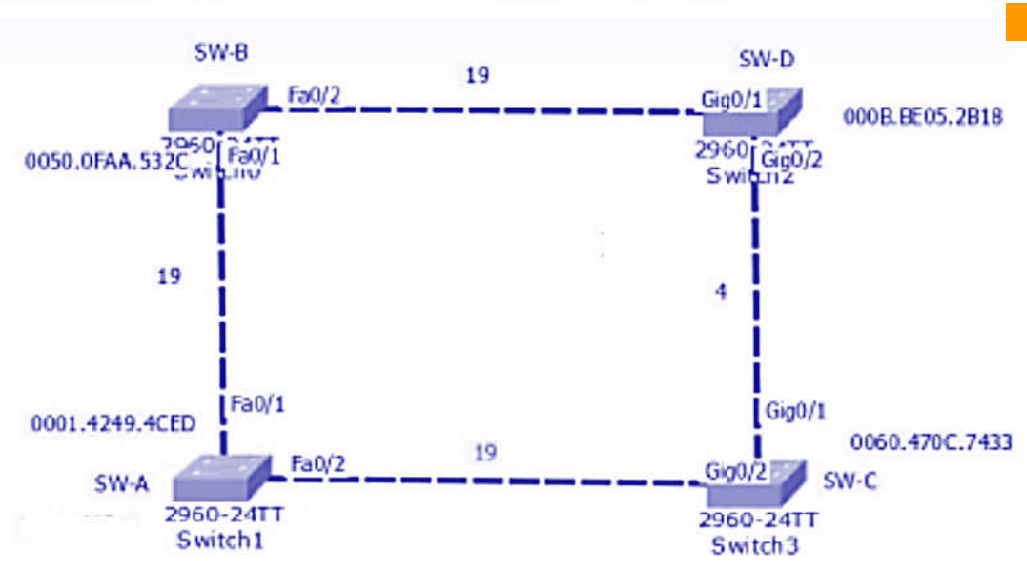
1. เลือกพอร์ตที่มี Cost ต่ำสุดก่อน ถ้าเท่ากันพิจารณาขั้นถัดไป

2. สำหรับ Designated Port ระหว่าง Switch มากกว่า 1 ตัว ให้เลือกพอร์ตที่มี Bridge ID ต่ำสุด

3. ถ้า Bridge ID เท่ากันอีก ให้เลือกพอร์ตที่มีค่า Port ID ต่ำสุด

ฉะนั้นพอร์ตที่เป็น Designated Ports จะกลายเป็นสถานะ Forwarding ส่วนพอร์ตที่เหลือจะกลายมาเป็นสถานะ Blocking


SW-B
SW-D
19
Fa0/2
Gig0/1
000B.BE05.2B18
0050.0FAA.532C
Fa0/1
Gig0/2
19
4
Fa0/1
Gig0/1
0001.4249.4CED
0060.470C.7433
SW-A
Fa0/2
19
Gig0/2
SW-C
2960-24TT
Switch1
2960-24TT
Switch3



Root Bridge

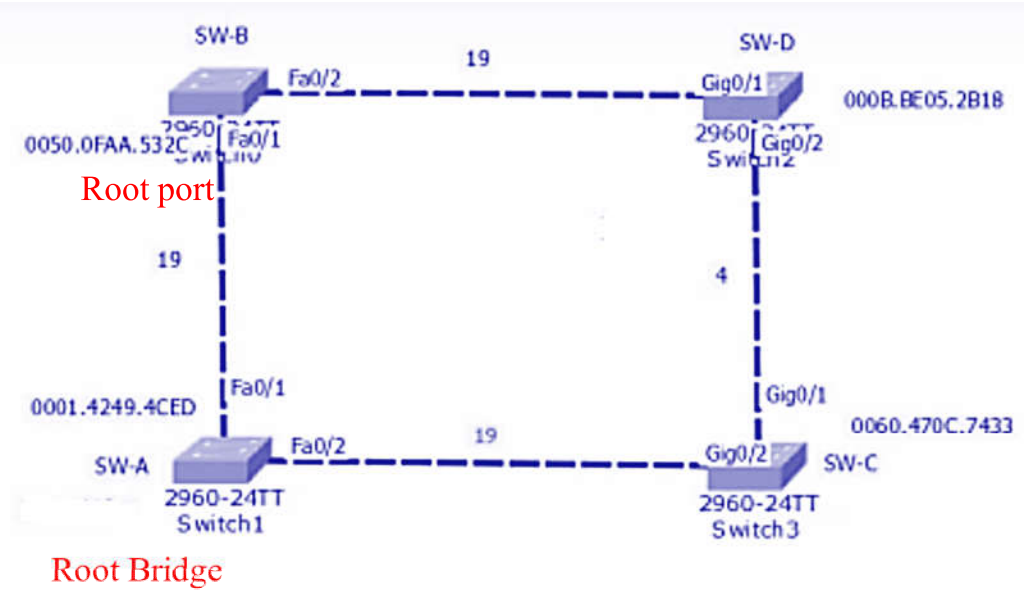
ขั้นที่ 1 ทำการหา Root Bridge

- โดยการดูที่ค่า Priority ก่อน
- ถ้าค่า Priority เท่ากัน ให้ไปเปรียบเทียบที่ค่า Mac-address ว่า Switch ตัวไหนมีค่า Mac-address น้อยที่สุด Switch ตัวนั้นก็จะเป็น Root Bridge
- จากรูป Switch SW-A ก็จะเป็น Root Bridge

ขั้นตอนที่ 2 หา root port

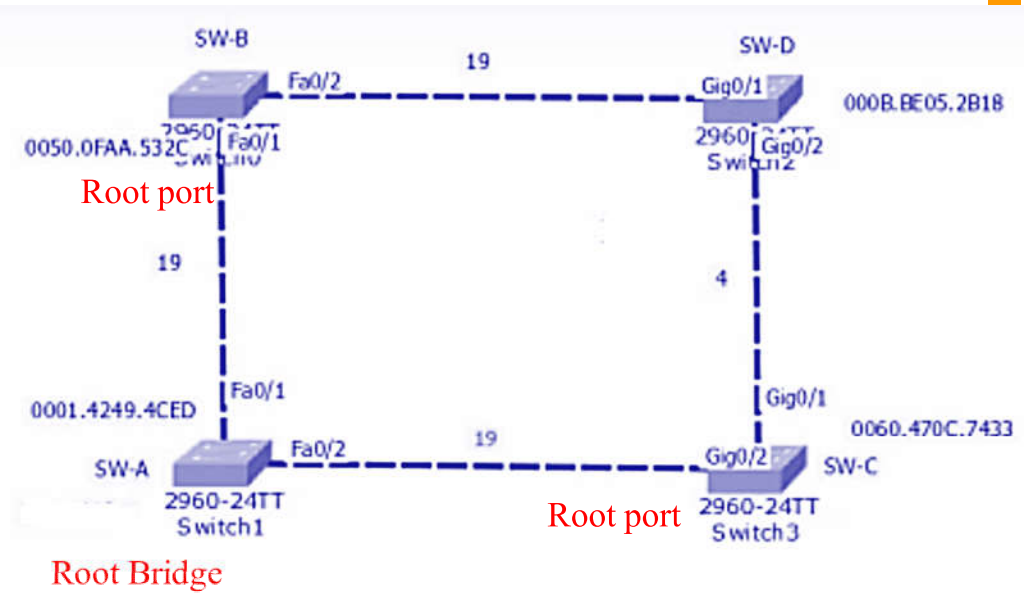
- หา Port ที่ดีที่สุดที่เดินทางไปยัง Root Bridge โดย Switch แต่ละตัว จะมี Root Port ได้แค่ 1 Port เท่านั้น
  - เลือกจากค่า Path Cost
  - ถ้าค่า Path Cost เท่ากัน ก็จะเปรียบเทียบที่ Bridge ID
  - ถ้า Bridge ID ยังเท่ากันอีก ก็จะทำการเปรียบเทียบที่ Port ID (Port ID ก็คือ ชื่อของ Interface ที่เชื่อมต่ออยู่ เช่น F0/1 กับ F0/2 ซึ่ง F0/1 มีค่าน้อยกว่า จึงทำให้ Port F0/1 ได้เป็น Root Port ในที่สุด)

ตัวอย่างการหา root port



- SW-B จะมีการต่อสู้กันเพื่อจะเป็น Root Port อยู่ 2 เส้นทาง
  - ทางที่ 1 มีค่า Path Cost เท่ากับ 19
  - ทางที่ 2 มีค่า Path Cost เท่ากับ 23 (19+4 +19)
  - ดังนั้นที่สวิทซ์ SW-B พอร์ตที่ต่อกับทางที่ 1 ซึ่งมีค่า Path Cost ที่น้อยที่สุด คือ 19 จะได้เป็น Root Port

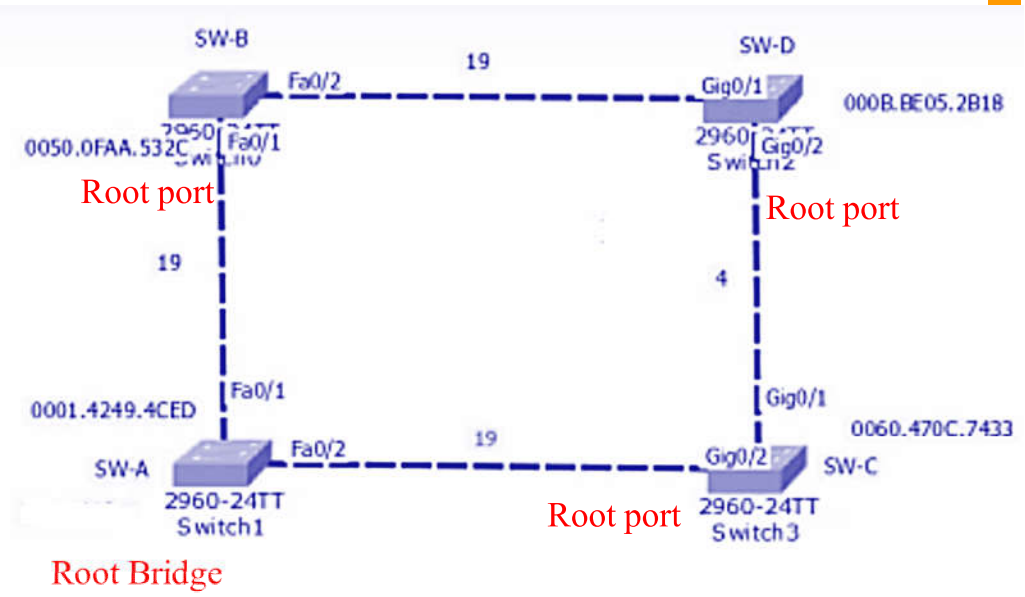
ตัวอย่างการหา root port(ต่อ)



Switch SW-C จะมีการต่อสู้กันเพื่อจะเป็น Root Port อยู่ 2 เส้นทาง

- ทางที่ 1 มีค่า Path Cost เท่ากับ 19
- ทางที่ 2 มีค่า Path Cost เท่ากับ 42 (19+19+4)
- ดังนั้นที่ Switch SW-C ที่ต่อกับทางที่ 1 ซึ่งมีค่า Path Cost ที่น้อยที่สุดคือ 19 จะได้เป็น Root Port

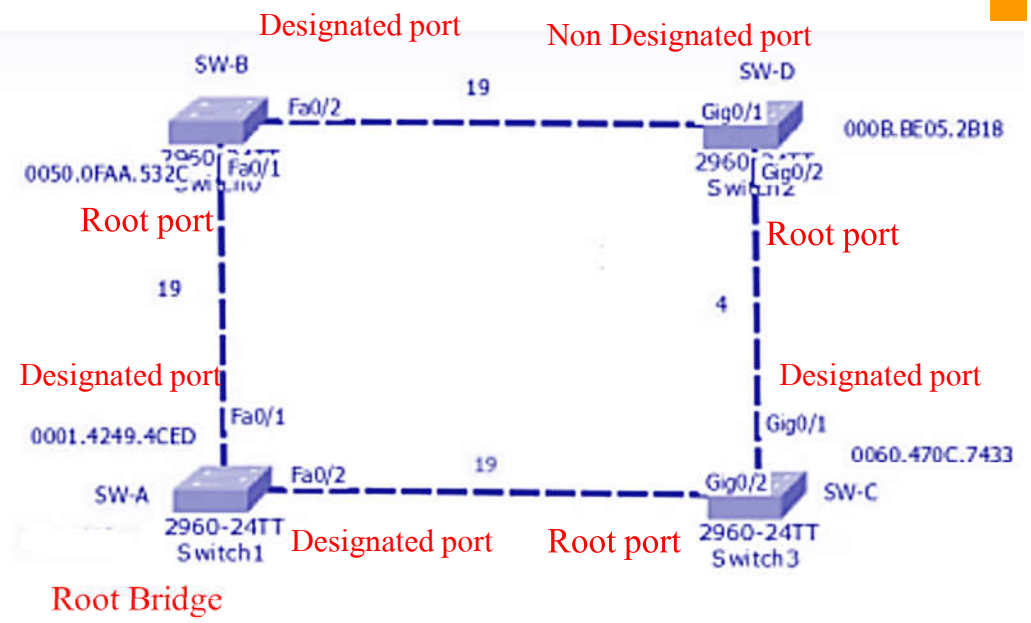
ตัวอย่างการหา root port(ต่อ)



Switch SW-D จะมีการต่อสู้กันเพื่อจะเป็น Root Port อยู่ 2 เส้นทาง

- ทางที่ 1 มีค่า Path Cost เท่ากับ 23 (19+4)
- ทางที่ 2 มีค่า Path Cost เท่ากับ 38 (19+19)
- ดังนั้นที่ Switch SW-D ที่ต่อกับทางที่ 1 ซึ่งมีค่า Path Cost ที่น้อยที่สุดคือ 23 จะได้เป็น Root Port

ขั้นที่ 3 หา Designated Port



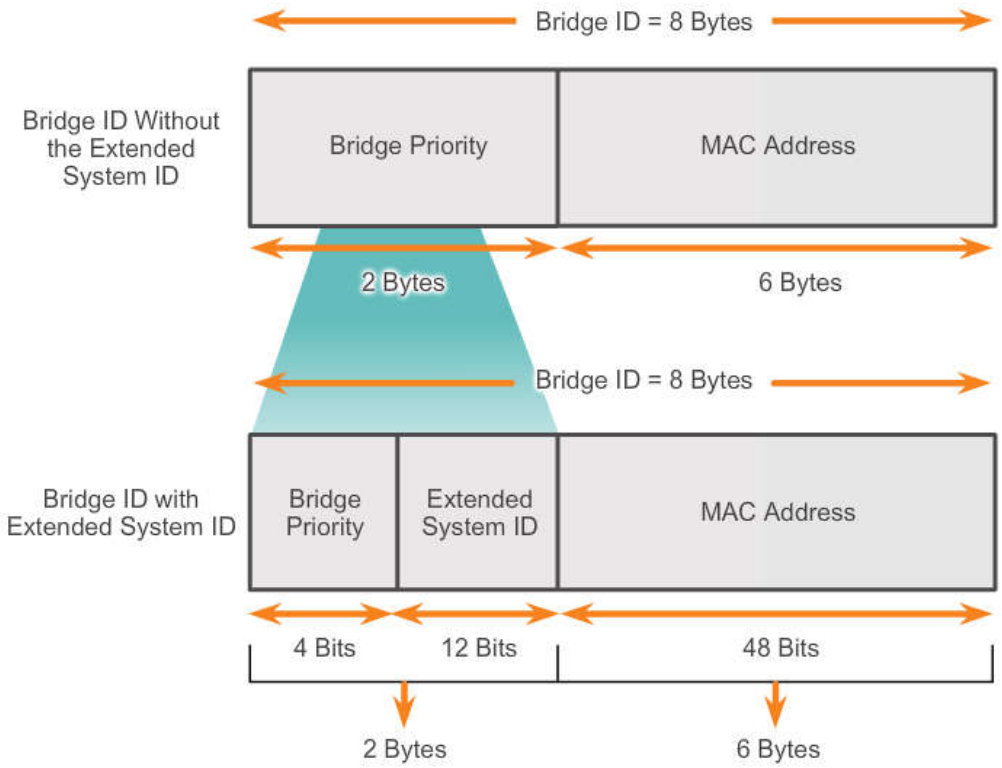
การหา Designated Port

- Port ทุก Port ที่อยู่บน Switch ที่เป็น Root Bridge จะเป็น Designated Port ทั้งหมด
- Port ของ Switch ที่เชื่อมต่อกัน ฝั่งใดฝั่งหนึ่งเป็น Root Port ไปแล้ว อีกฝั่งก็จะเป็น Designated Port ทันที
- หา Non Designated Port จากพอร์ตที่มีเส้นทางไกลจาก Root Bridge ที่สุด

Spanning Tree and VLAN

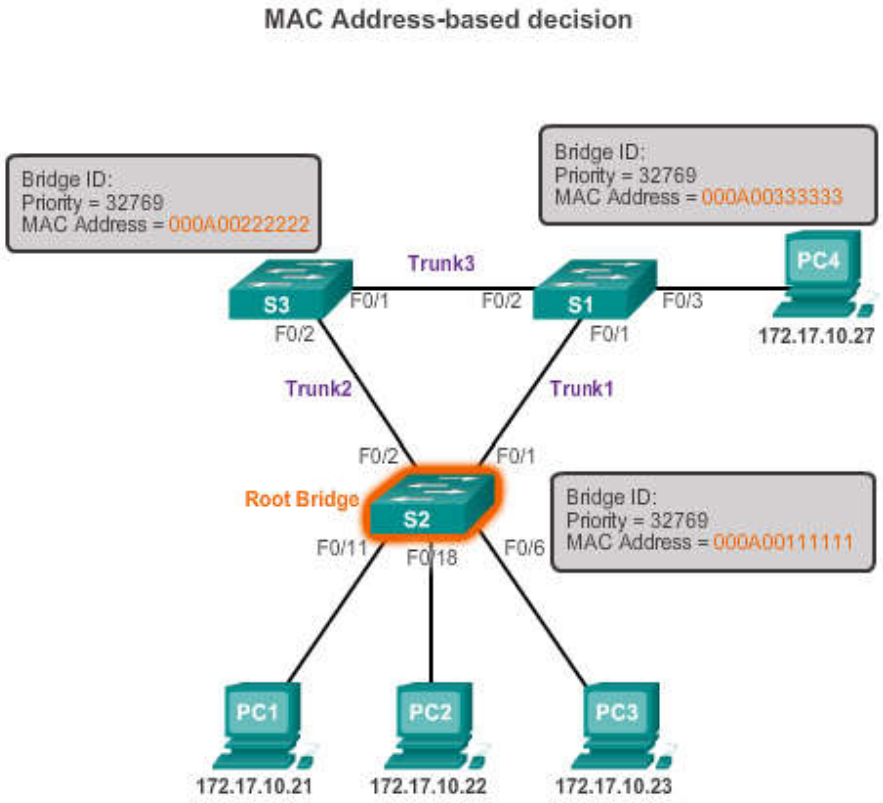
- เนื่องจากมาตรฐานของ Spanning Tree(802.1D) นั้นได้ตั้งขึ้นมาก่อน VLAN ดังนั้นการทำ VLAN ใน Network จะมีมากกว่า 1 Spanning Tree ไม่ได้
- ทุกๆ VLAN จะต้องมี Spanning Tree เดียว ซึ่งถ้าทำ VLAN แบบ ง่ายๆจะไม่มีปัญหา แต่บางครั้งถ้าเรามีการทำ Filter ของ Trunk Port อาจจะทำให้บาง VLAN หลุดจาก Spanning Tree ได้
- Cisco ได้เพิ่มส่วนของ Protocol ของ Spanning Tree ที่ทำให้สามารถมี Spanning Tree แยกสำหรับแต่ละ VLAN ได้ แต่ก็ใช้ได้กับ Switch ของ Cisco เท่านั้น
- มาตรฐานใหม่ของ IEEE คือ IEEE 802.1s ซึ่งเป็นมาตรฐานสำหรับ Multiple Spanning Tree(MST) จะยอมให้มีหลาย Spanning Tree ได้

Extended System ID



STP ได้รับการปรับปรุงเพื่อรวมถึงการสนับสนุน VLANs จำเป็นต้องมี VLAN ID ที่จะรวมอยู่เฟรม BPDU ผ่านการใช้งานของ extended system ID

Extended System ID



ในตัวอย่าง ค่าลำดับความสำคัญของสวิทซ์ทุกตัวคือ 32769 ค่าพื้นฐานคือ 32768 เป็นค่าลำดับความสำคัญ เริ่มต้น และ VLAN 1 ถูกกำหนดให้แต่ละสวิทซ์ที่เกี่ยวข้อง (32768+1)

Varieties of Spanning Tree Protocols

ชนิดของ Spanning Tree Protocols

- STP or IEEE 802.1D-1998
- PVST+
- IEEE 802.1D-2004
- Rapid Spanning Tree Protocol (RSTP) or IEEE 802.1w
- Rapid PVST+
- Multiple Spanning Tree Protocol (MSTP) or IEEE 802.1s

Characteristics of the Spanning Tree Protocols

Protocol	Standard	Resources Needed	Convergence	Tree Calculation
STP	802.1D	Low	Slow	All VLANs
PVST+	Cisco	High	Slow	Per VLAN
RSTP	802.1w	Medium	Fast	All VLANs
Rapid PVST+	Cisco	Very high	Fast	Per VLAN
MSTP	802.1s Cisco	Medium or high	Fast	Per Instance

เปรียบเทียบ 802.1D กับ 802.1W

802.1D State	802.1w State	Default Port Operational Status	Port in Active Topology?	Port Learning MAC Addresses?
Disabled	Discarding	Enabled	No	No
Blocking	Discarding	Enabled	No	No
Listening	Discarding	Enabled	Yes	No
Learning	Learning	Enabled	Yes	Yes
Forwarding	Forwarding	Enabled	Yes	Yes

Per VLAN Spanning Tree (PVST)

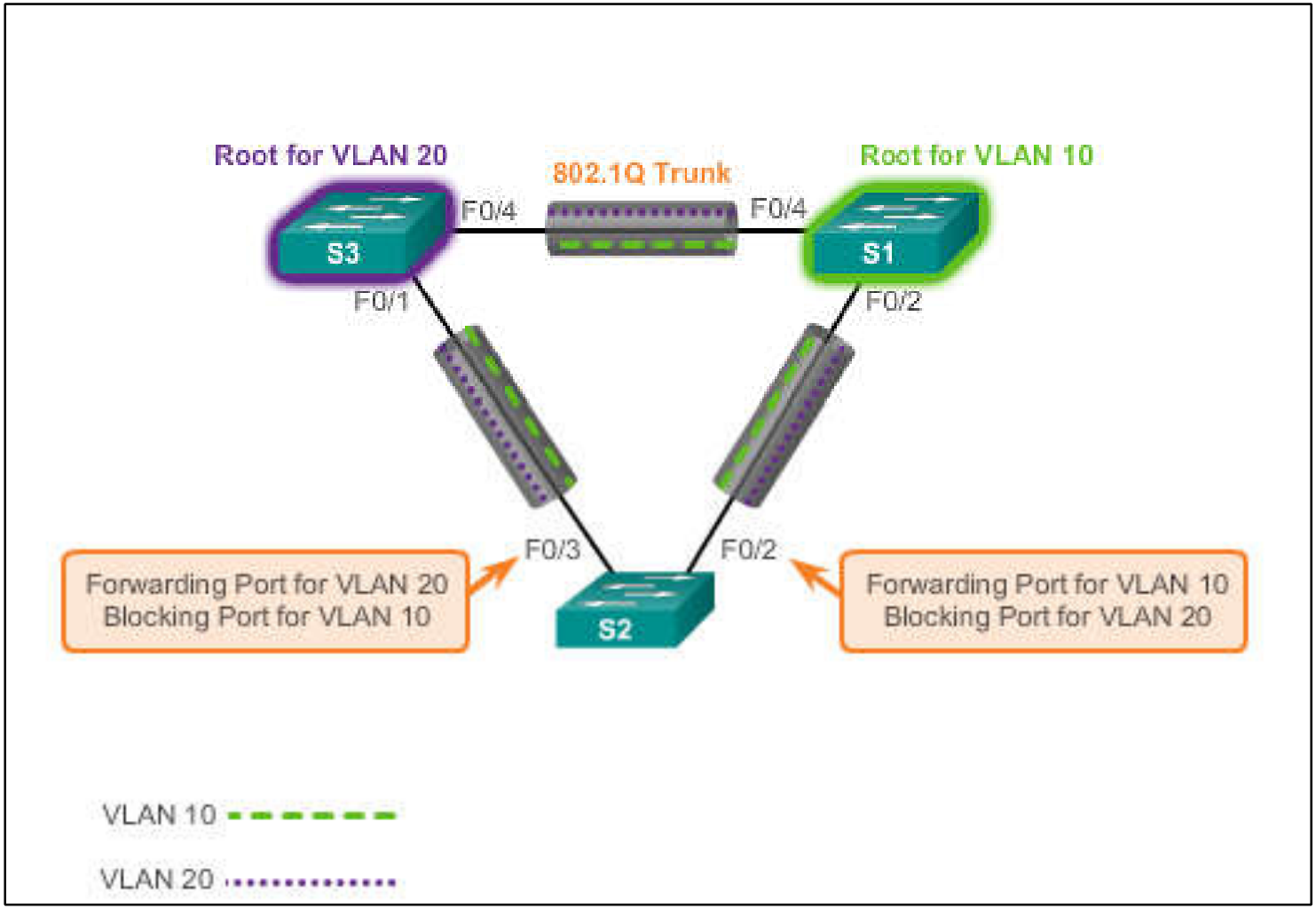
- การทำ STP ทำให้ทุกๆ VLAN จะมีการใช้งาน STP เพียงชุดเดียว ทำให้ Traffic ของ VLAN จะวิ่งผ่านค่อนข้างแออัดในเส้นทางใดเส้นทางหนึ่ง โดย Traffic ทุกๆ VLAN จะพุ่งไปยัง Root Bridge
- การทำ PVST นั้นเป็นการเพิ่มความสามารถให้แต่ละ VLAN ให้มี STP เป็นของตนเอง กล่าวคือ VLAN นั้นๆจะมีเส้นที่แตกต่างกันในแต่ละ VLAN ที่เราได้ตั้งค่าไว้
- ยังมี PVST+ ที่สามารถทำงานร่วมกับ STP แบบเก่าได้อีกด้วย

Overview of PVST+

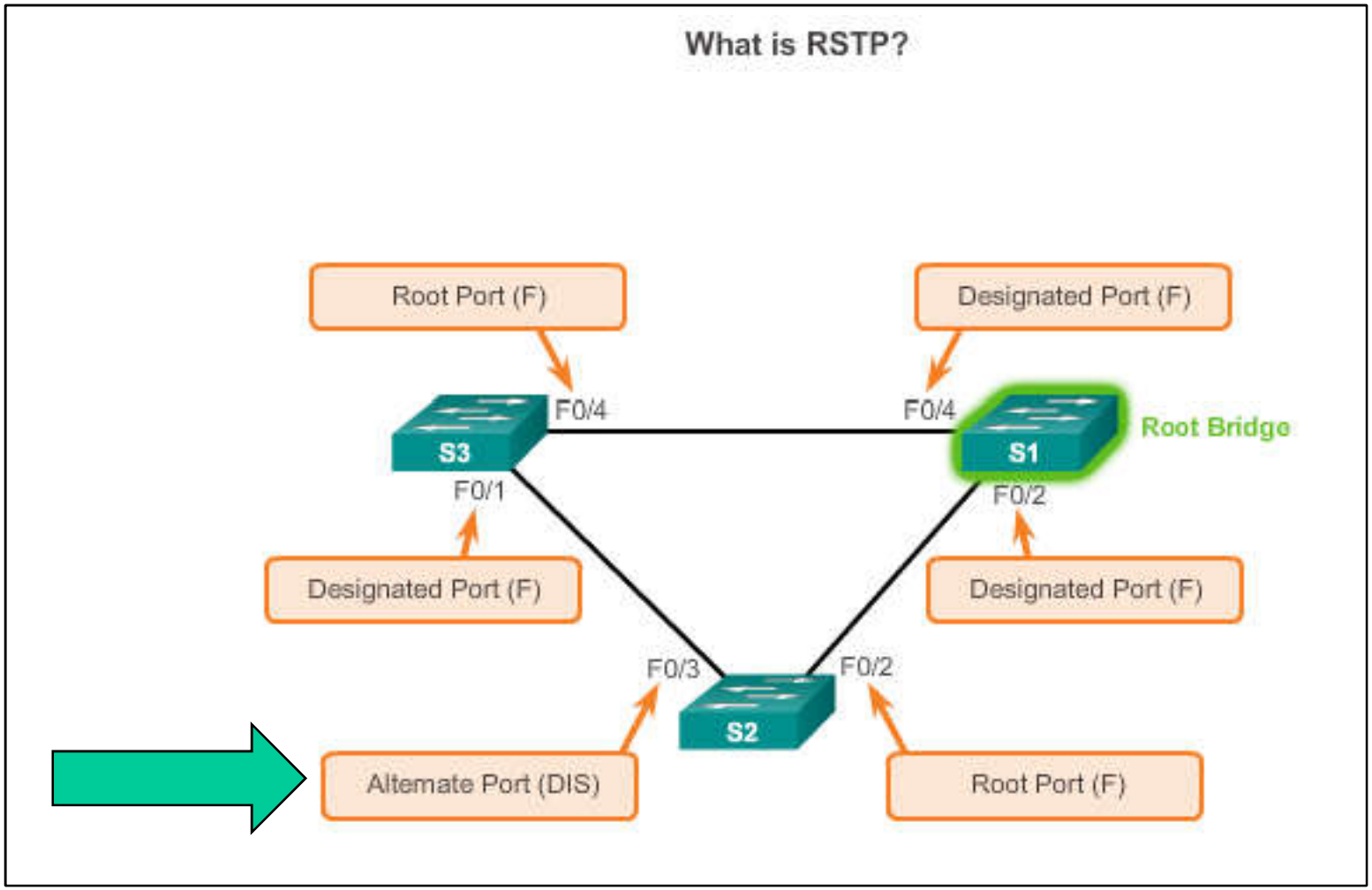
Per VLAN Spanning Tree (PVST)

- เป็นการทำ STP ทำให้ทุกๆ VLAN จะมีการใช้งาน STP เพียงชุดเดียว ทำให้ Traffic ของ VLAN จะวิ่งผ่านค่อนข้างแออัดในเส้นทางใดเส้นทางหนึ่ง โดย Traffic ทุกๆ VLAN จะพุ่งไปยัง Root Bridge
- การทำ PVST นั้นเป็นการเพิ่มความสามารถใจแต่ละ VLAN ให้มี STP เป็นของตนเอง กล่าวคือ VLAN นั้นๆจะมีเส้นที่แตกต่างกันในแต่ละ VLAN ที่เราได้ตั้งค่าไว้
- PVST+ สามารถทำงานร่วมกับ STP แบบเก่าได้อีกด้วย

Overview of PVST+



Overview of Rapid PVST+



Port States and PVST+ Operation

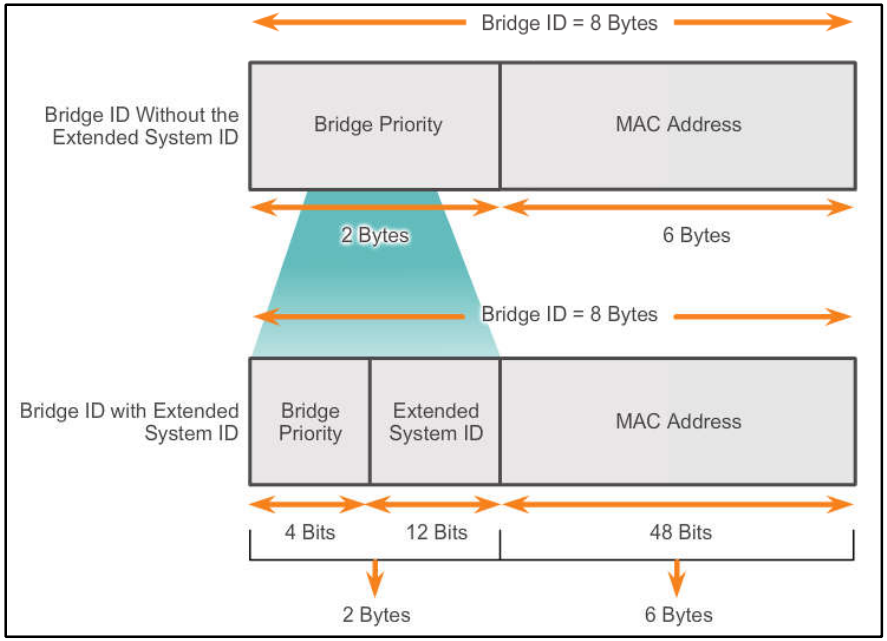
STP introduces the five port states:

Port States

Processes	Blocking	Listening	Learning	Forwarding	Disabled
Processes received BPDUs	YES	YES	YES	YES	NO
Forward data frames received on interface	NO	NO	NO	YES	NO
Forward data frames switched from another interface	NO	NO	NO	YES	NO
Learn MAC addresses	NO	NO	YES	YES	NO

Extended System ID and PVST+ Operation

- ในสภาพแวดล้อมที่ PVST+ extended switch ID เพื่อให้แน่ใจว่าแต่ละสวิทซ์มี BID ที่ไม่ซ้ำกันในแต่ละ VLAN
- ยกตัวอย่างเช่น VLAN 2 ค่า BID เริ่มต้นจะเป็น 32770 ลำดับความสำคัญเป็น 32768 รวมทั้ง extended system ID ของ 2



Overview of Rapid PVST+

- Rapid PVST เรียกอีกชื่อว่า IEEE802.1W
- เมื่อทำการ Enable แล้วจะได้ฟีเจอร์ต่างๆเทียบเท่ากับการทำ Port Fast , Uplink Fast , Backbone Fast ในทันที
- โดยโปรโตคอลนี้จะใช้เวลาเพียง 6 วินาทีในการเข้าสู่สถานะ Forwarding State เมื่อเส้นทางหลักเกิด Down ลงไป

IEEE802.1W - Rapid STP

- เมื่อทำการ Enable แล้วจะได้ฟีเจอร์ต่างๆเทียบเท่ากับการทำ Port Fast , Uplink Fast , Backbone Fast ในทันที
- โปรโตคอลนี้จะใช้เวลาเพียง 6 วินาทีในการเข้าสู่สถานะ Forwarding State เมื่อเส้นทางหลักเกิด Down ลงไป
- ต่างจากเทคโนโลยี Spanning Tree Protocol มาตรฐานเดิม คือ IEEE 802.1d ใช้เวลาในการ Recovery เส้นทางสำรองขึ้นมาใช้งานถึงประมาณ 30-40 วินาที หลังจากเส้นทางหลักขัดข้อง

RSTP BPDU

RSTP Version 2 BPDU

Field	Byte Length
Protocol ID=0x0000	2
Protocol Version ID=0x02	1
BPDU Type=0X02	1
Flags	1
Root ID	8
Root Path Cost	4
Bridge ID	8
Port ID	2
Message Age	2
Max Age	2
Hello Time	2
Forward Delay	2

Flag Field

Field Bit	Bit
Topology Change	0
Proposal	1
Port Role Unknown Port Alternate or Backup Port Root Port Designated Port	2-3 00 01 10 11
Learning	4
Forwarding	5
Agreement	6
Topology Change Acknowledgment	7

IEEE802.1S - Multiple Spanning Tree Protocol (MSTP)

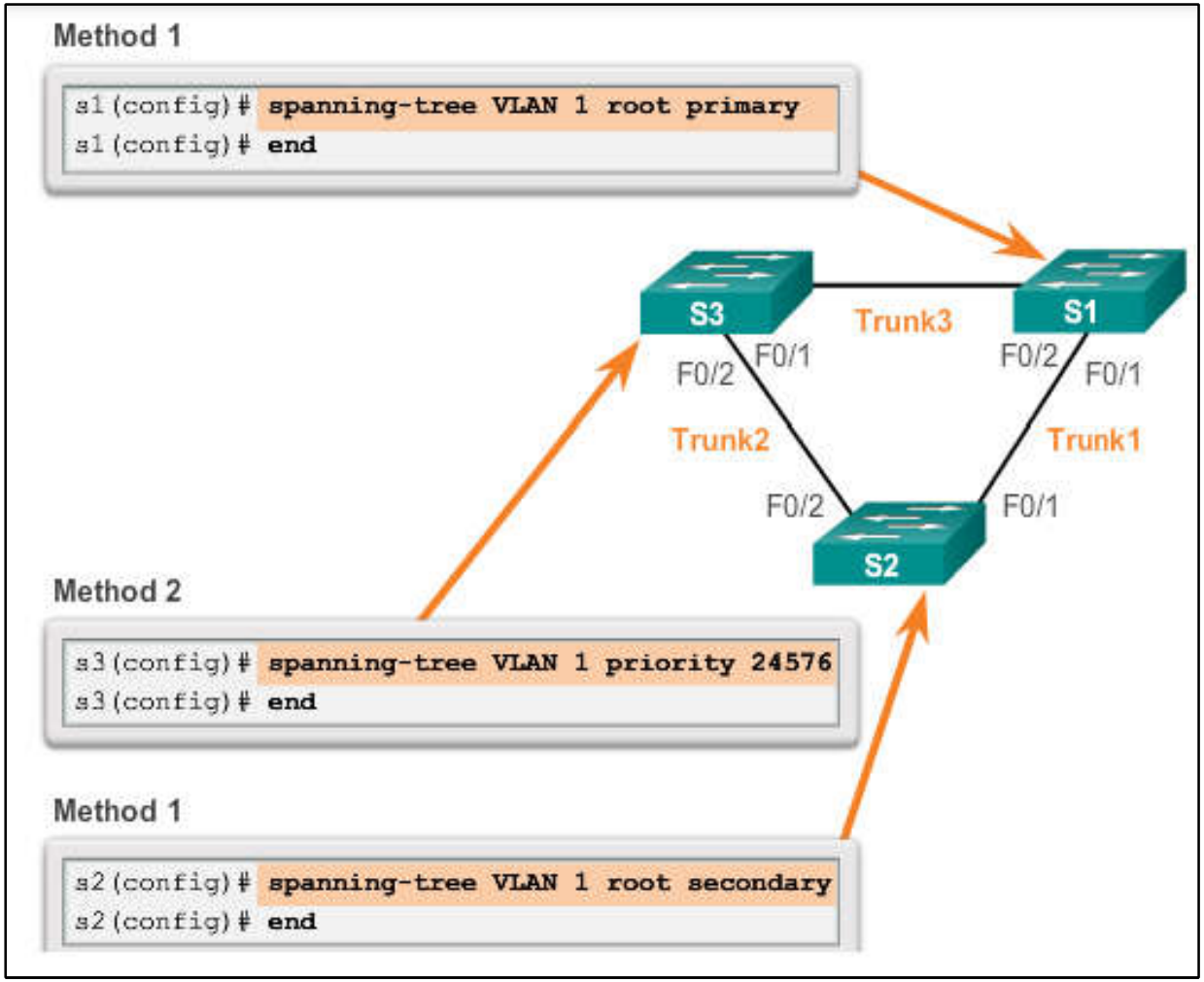
- MSTP เป็น open standard ที่พัฒนาต่อเนื่องมาจาก RSTP มาคนละสายกับ PVST)
- อนุญาตให้สร้าง spanning tree ได้หลาย tree แต่ไม่ถึงขนาดต้อง 1 tree ต่อ 1 VLAN
- โดยพิจารณาก่อนว่าในระบบน่าจะมี tree แบบไหนบ้างถึงจะเหมาะสมและครอบคลุม แล้วก็จัดว่า VLAN ไหนบ้างที่ควรจะใช้ topology ของ tree อันไหน
- ทำการ map VLAN เหล่านั้นเข้ากับ tree ที่เหมาะสมกับมัน (Cisco ก็มี proprietary protocol ที่ชื่อว่า MISTP (Multiple Instance STP)

Spanning Tree Configuration

Catalyst 2960 Default Configuration

Feature	Default Setting
Enable state	Enabled on VLAN 1
Spanning-tree mode	PVST+ (Rapid PVST+ and MSTP are disabled.)
Switch priority	32768
Spanning-tree port priority (configurable on a per-interface basis)	128
Spanning-tree port cost (configurable on a per-interface basis)	1000 Mb/s: 4 100 Mb/s: 19 10 Mb/s: 100
Spanning-tree VLAN port priority (configurable on a per-VLAN basis)	128
Spanning-tree VLAN port cost (configurable on a per-VLAN basis)	1000 Mb/s: 4 100 Mb/s: 19 10 Mb/s: 100
Spanning-tree timers	Hello time: 2 seconds Forward-delay time: 15 seconds Maximum-aging time: 20 seconds Transmit hold count: 6 BPDUs

Configuring and Verifying the Bridge ID

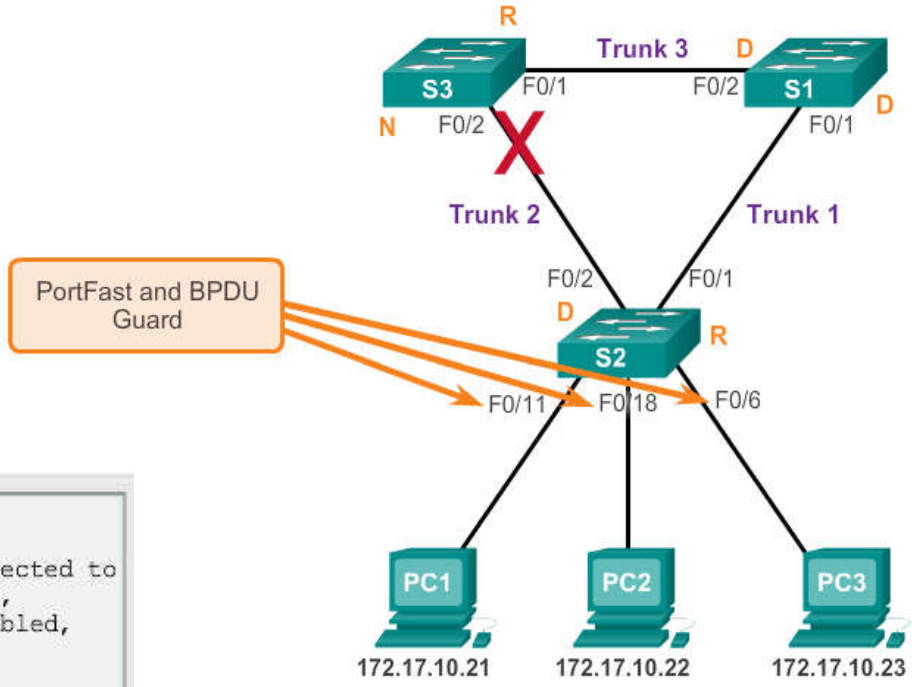


Configuring and Verifying the Bridge ID

```
S3# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     00A.0033.3333
              This bridge is the root
              Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
  Bridge ID   Priority    24577  (priority  24576  sys-id-ext  1)
              Address     000A.0033.3333
              Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
              Aging Time  300

Interface      Role    Sts    Cost      Prio.Nbr       Type
-------------  -----   ----   -----     ----------     ------
Fa0/1          Desg    FWD    4         128.1          p2p
Fa0/2          Desg    FWD    4         128.2          p2p
S3#
```

PortFast and BPDU Guard

- เมื่อพอร์ตสวิตช์มีการกำหนดค่า PortFast พอร์ตนั้นที่เปลี่ยนสถานะจากการบล็อกไปยังสถานะการส่งต่อทันที
- BPDU Guard จะทำให้พอร์ตในสถานะปิดการใช้งานเกิดข้อผิดพลาด จากการรับของ BPDU

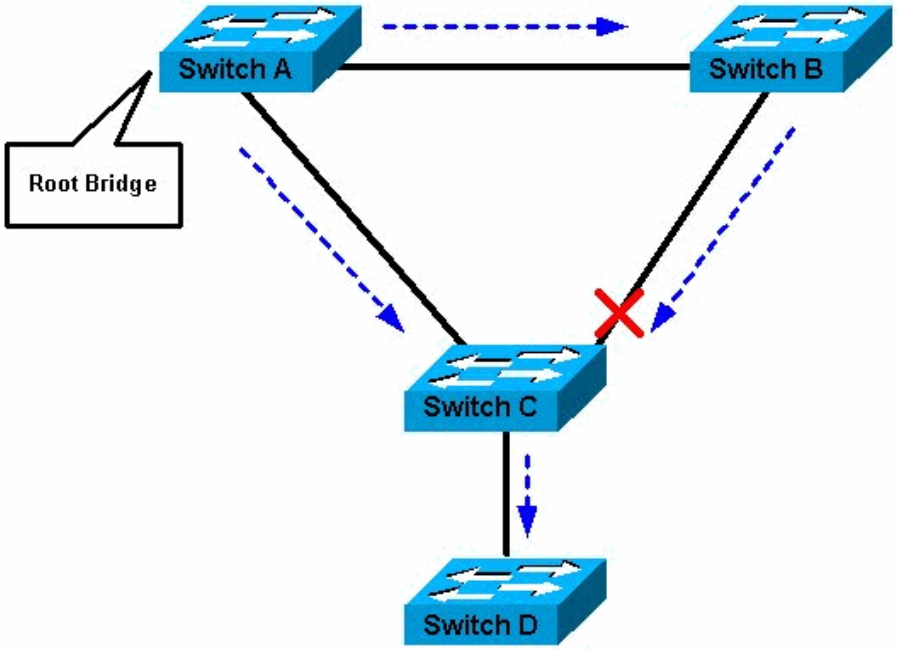


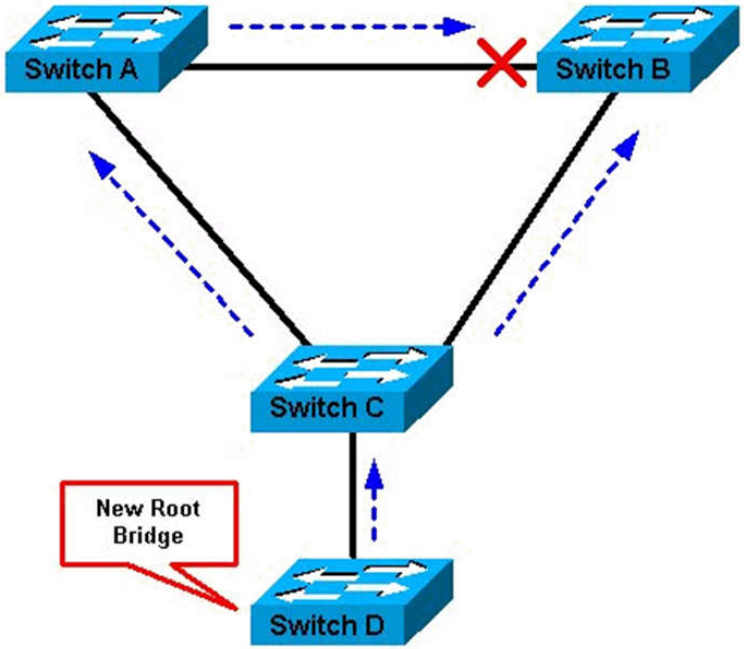

```
S2(config)# interface FastEthernet 0/11
S2(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to
a single host. Connecting hubs, concentrators, switches,
bridges, etc... to this interface  when portfast is enabled,
can cause temporary bridging loops.
 Use with CAUTION

%Portfast has been configured on FastEthernet0/11 but will only
 have effect when the interface is in a non-trunking mode.
S2(config-if)# spanning-tree bpduguard enable
S2(config-if)# end
```

Root Guard (Spanning Tree Protocol Root Guard Enhancement)

- Root Guard เป็นฟังก์ชันของ Switch ที่ใช้ป้องกันไม่ให้ Switch ตัวอื่นมาเป็น Root Bridge แทนตัวเดิมที่ตั้งค่าไว้อยู่แล้ว
- โดยปกติในระบบที่เราใช้งาน เราก็จะทำการตั้งค่า Root Bridge ไว้ที่ Core Switch เพื่อให้เกิดการเลือก STP ที่เหมาะสม
- แต่ถ้ามี Access Switch ถูก config ให้มีค่า Bridge Priority ต่ำกว่า Root Bridge จะทำให้ Access Switch ตัวนั้นกลายเป็น Root Bridge ไป
- สามารถป้องกันได้ด้วย config Bridge Priority ของ Root Bridge ให้เป็นมีค่า 0 จะทำให้ Switch ตัวนั้นมีค่า Bridge ID ต่ำสุดและการันตีความเป็น Root Bridge แน่นอน
  - *Switch(config)#spanning-tree vlan 1 priority 0*

- แต่ถ้ามี Switch ตัวใด config Bridge Priority เป็น 0 เหมือนกัน
- ตามกฎการเลือก Root Bridge เมื่อ Priority เท่ากัน ให้ไปดูที่ MAC Address ต่อ แล้วถ้าเกิด Switch ตัวใหม่นี้เกิดมี MAC Address ต่ำกว่า Root Bridge ตัวเดิม ก็กลายเป็น Root Bridge ทันที ดังนั้นควรใช้ Root Guard เข้ามาช่วย
- Root Guard จะ enable บน designated port เพื่อป้องกันไม่ให้ designated port กลายเป็น root port หรือ block port
- ถ้า port ที่ enable Root Guard ได้รับ Superior BPDU (BPDU ที่มีค่า BridgeID ต่ำกว่า) เข้ามา port นั้นจะเข้าสู่ root-inconsistent (blocked) state.



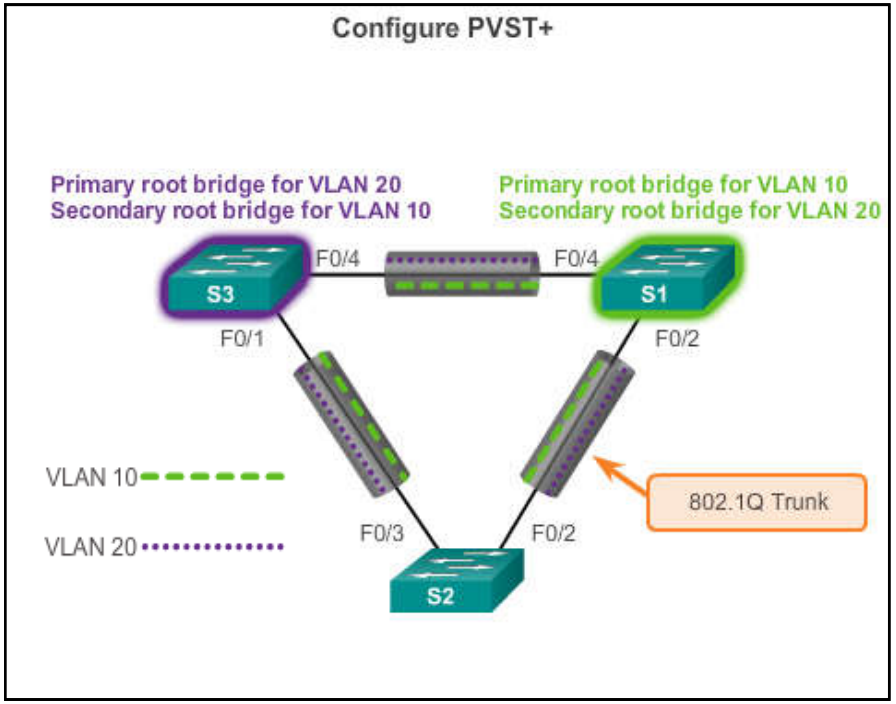


- Switch A เป็น Root Bridge และมีการทำงานปกติตามกลไลของ STP
- แต่เมื่อ Switch D มีค่า Bridge ID ต่ำกว่าในระบบ จะทำให้ Switch D กลายเป็น New Root Bridge ทันที

การ enable Root Guard

- กำหนดไว้บน port ของ Switch C ที่เชื่อมต่อไปหา Switch D
  - SwitchC(config)#interface fa0/3
  - SwitchC(config-if)#spanning-tree guard root
- เมื่อใดที่ Switch D มี Bridge ID ต่ำกว่าในระบบ แล้วส่ง Superior BPDU ออกไปให้ Switch C จะทำการ block port นั้นทันที โดยจะมี message แสดงขึ้นมา
  - %SPANTREE-2-ROOTGUARD_BLOCK: Root guard blocking port FastEthernet0/3 on VLAN0001.
  - %SPANTREE-2-ROOTGUARDBLOCK: Port 0/3 tried to become non-designated in VLAN 1. Moved to root-inconsistent state
- และ port จะเข้าสู่ root-inconsistent (blocked) state ทันที

PVST+ Load Balancing



Configure PVST+

```
S3(config)# spanning-tree vlan 20 root primary
```

This command forces S3 to be the primary root for VLAN 20.

```
S3(config)# spanning-tree vlan 10 root secondary
```

This command forces S3 to be the secondary root for VLAN 10.

```
S1(config)# spanning-tree vlan 10 root primary
```

This command forces S1 to be the primary root for VLAN 10.

```
S1(config)# spanning-tree vlan 20 root secondary
```

This command forces S1 to be the secondary root for VLAN 20.

PVST+ Load Balancing

- วิธีการหนึ่งในการระบุ root bridge ก็คือการตั้งค่าลำดับความสำคัญของต้นไม้ทอดข้ามในแต่ละสวิทซ์ไปที่ค่าต่ำสุด เพื่อให้สวิทช์ถูกเลือกเป็นบริดจ์หลักสำหรับ VLAN ที่เกี่ยวข้อง

Configure PVST+

```
S3(config)# spanning-tree vlan 20 priority 4096
```

This command sets the priority for S3 to be the lowest possible, making it most likely that S3 will be the primary root for VLAN 20..

```
S1(config)# spanning-tree vlan 10 priority 4096
```

This command sets the priority for S1 to be the lowest possible, making it most likely that S1 will be the primary root for VLAN 10.

PVST+ Load Balancing

- การดูและตรวจสอบรายละเอียด spanning tree configuration

Configure PVST+

```
S3# show spanning-tree active

<output omitted>

VLAN0010
   Spanning tree enabled protocol ieee
   Root ID     Priority    4106
               Address     0019.aa9e.b000
               This bridge is the root
               Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
   Bridge ID   Priority    4106  (priority  4096  sys-id-ext  10)
               Address     0019.aa9e.b000
               Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
               Aging Time  300

Interface       Role    Sts    Cost      Prio.Nbr      Type
------------    -----   ----   -----     ----------    ------
Fa0/2           Desg    FWD    19         128.2         p2p
Fa0/4           Desg    FWD    19         128.4         p2p

<output omitted>
```

PVST+ Load Balancing

Configure PVST+

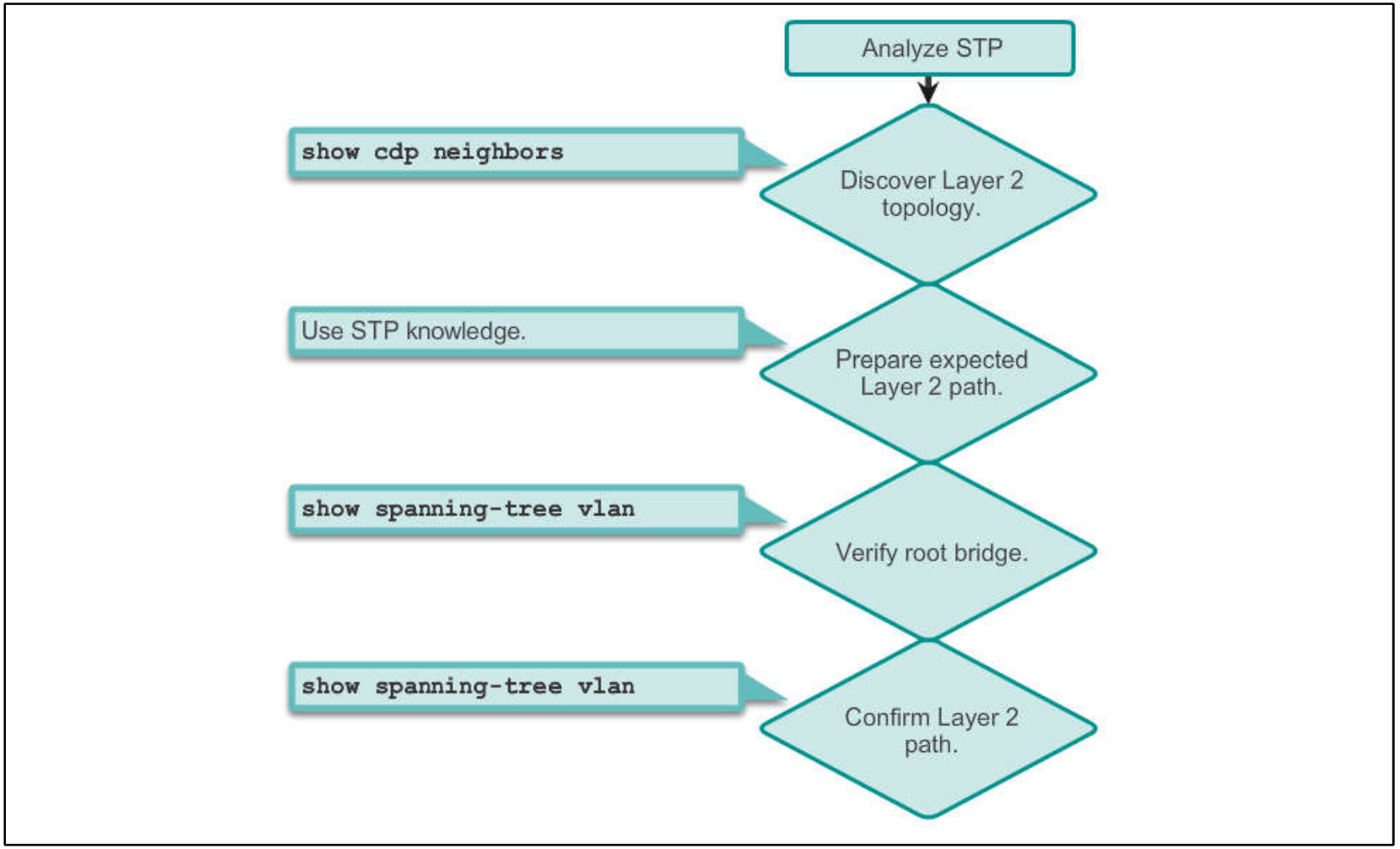
```
S1# show running-config
Building configuration...

Current configuration : 1595 bytes
!
version 12.2
 <output omitted>

!
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 1 priority 24576
spanning-tree vlan 10 priority 4096
spanning-tree vlan 20 priority 28672
!
 <output omitted>
```

Spanning Tree Mode

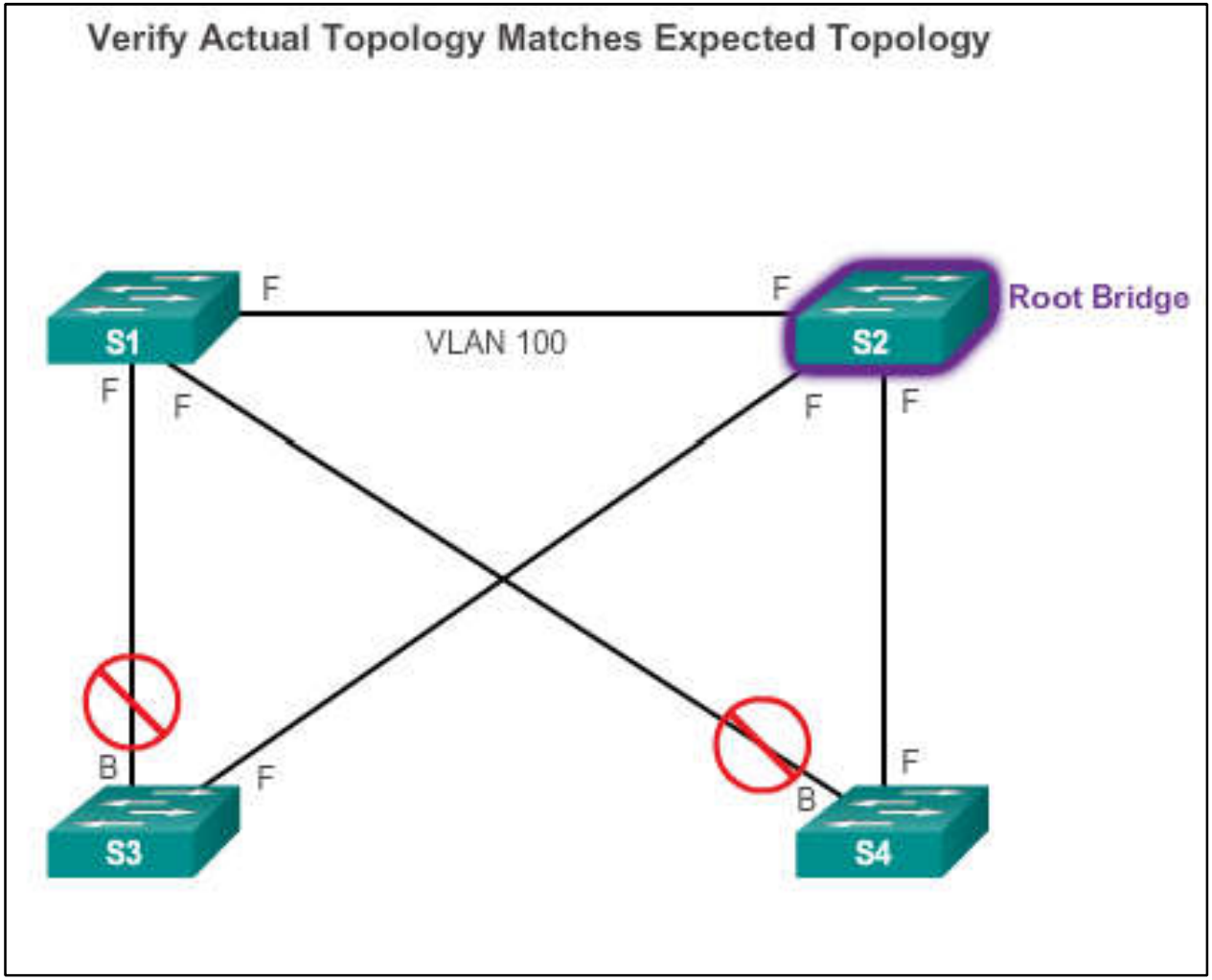
```
S1# configure terminal
S1(config)# spanning-tree mode rapid-pvst
S1(config)# interface f0/2
S1(config-if)# spanning-tree link-type point-to-point
S1(config-if)# end
S1# clear spanning-tree detected-protocols
```

Cisco IOS Command Syntax	
Enter global configuration mode.	**configure terminal**
Configure Rapid PVST+ spanning-tree mode.	**spanning-tree mode rapid-pvst**
Enter interface configuration mode and specify an interface to configure. Valid interfaces include physical ports, VLANs, and port channels.	**interface** *interface-id*
Specify that the link type for this port is point-to-point.	**spanning-tree link-type point-to-point**
Return to privileged EXEC mode.	**end**
Clear all detected STP.	**clear spanning-tree detected-protocols**

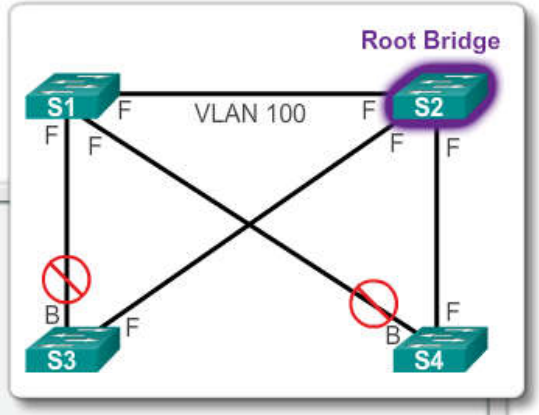
การวิเคราะห์ STP Topology



Expected Topology versus Actual Topology



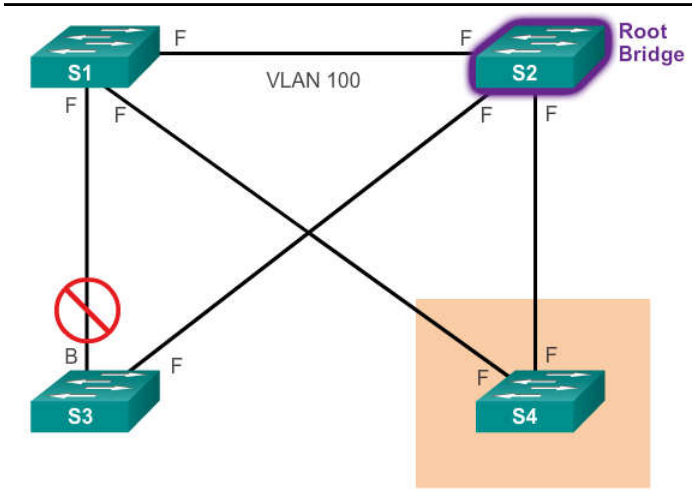
การแสดงสถานะ Spanning Tree

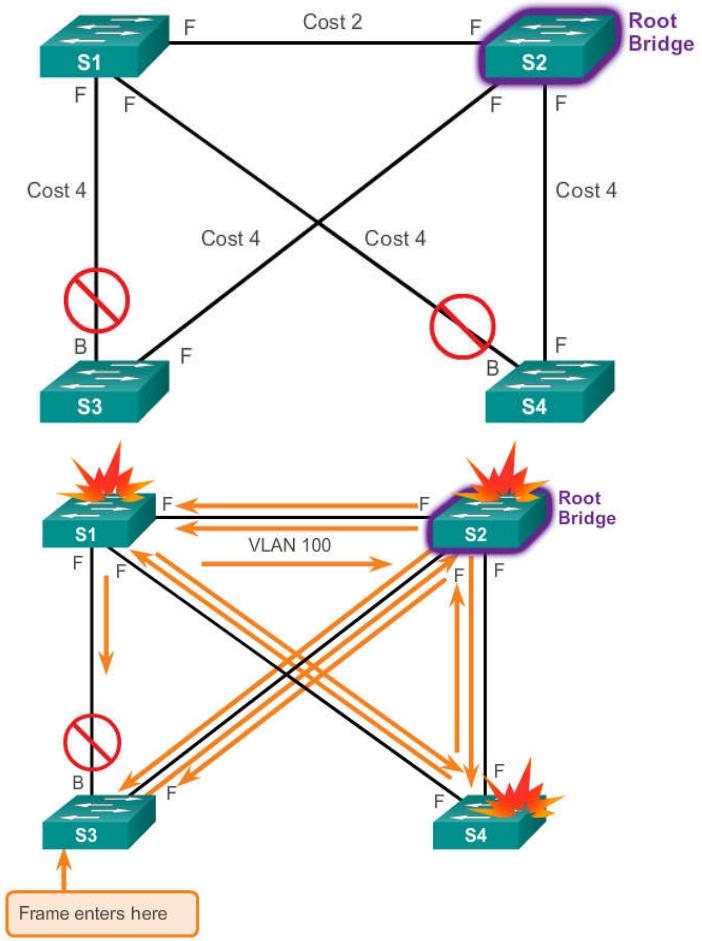



```
S1# show spanning-tree vlan 100

VLAN0100
 Spanning tree enabled protocol rstp
 Root ID     Priority    28772
             Address     0000.0c9f.3127
             Cost        2
             Port        88 (TenGigabit9/1)
             Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
 Bridge ID   Priority    28772 (priority 28672 sys-id-ext 100)
             Address     0000.0cab.3724
             Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
             Aging Time  300

Interface        Role Sts Cost      Prio.Nbr Type
---------        ---------------    --------------------------------
Gi3/1            Desg FWD 4         128.72   P2p
Gi3/2            Desg FWD 4         128.80   P2p
Te9/1            Root FWD 2         128.88   P2p
```

ผลที่ตามมาของความล้มเหลวใน Spanning-Tree

- STP จะย้ายอย่างน้อยหนึ่งหรือมากกว่าหนึ่งพอร์ตเข้าสู่สถานการณ์ส่งต่อ (forwarding state.)
- เฟรมใด ๆ ที่ถูกส่งออกไปทุกพอร์ตโดยสวิทช์เข้าสู่ลูป





การแก้ไขปัญหา Spanning Tree

- วิธีหนึ่งที่จะแก้ไขความล้มเหลวของต้นไม้ทอดข้ามคือ การลบเชื่อมโยงซ้ำซ้อนในเครือข่ายสวิทซ์ด้วยตนเอง ไม่ว่าจะทางกายภาพหรือผ่านการกำหนดค่า จนกว่าลูปทั้งหมดจะถูกตัดออกไปจากโครงสร้างเครือข่าย
- ก่อนที่จะฟื้นฟูการเชื่อมโยงซ้ำซ้อน ให้ตรวจสอบและแก้ไขสาเหตุของความล้มเหลวของต้นไม้ทอดข้าม
- ตรวจสอบเครือข่ายด้วยความระมัดระวัง เพื่อให้แน่ใจว่าได้แก้ไขปัญหาแล้ว