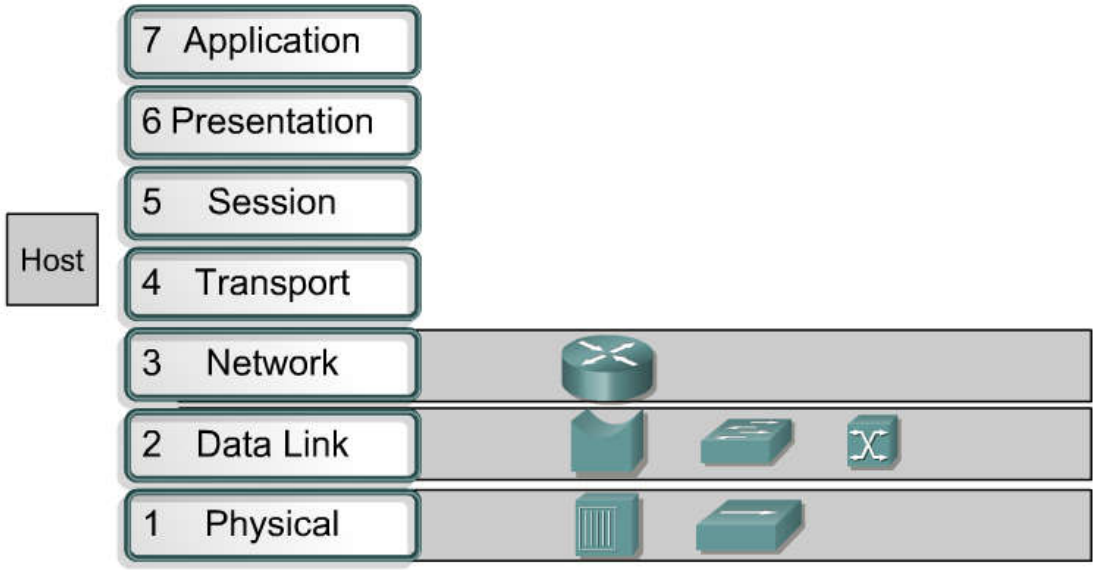
การสลับเส้นทางขั้นพื้นฐานและการทำงานของบริดจ์

Basic Switching and Bridge

วัตถุประสงค์การเรียนรู้

- เพื่อให้นักศึกษาสามารถใช้คำสั่งในการกำหนดค่าการทำงานสวิทซ์เบื้องต้นได้
- เพื่อให้นักศึกษาสามารถเข้าใจการทำงานของสวิทซ์
- เพื่อให้นักศึกษาสามารถจำแนกชนิดของสวิทซ์ได้

Overview



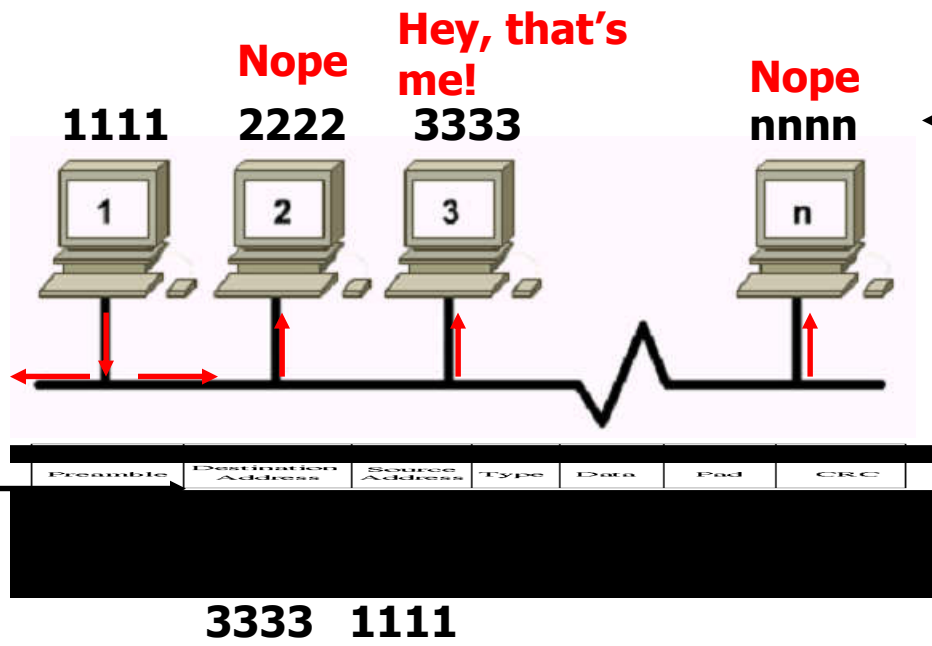
Routers

Switches, Bridges

Hub, Repeaters

- Ethernet networks used to be built using **repeaters**.
- When the performance of these networks began to suffer because too many devices shared the same segment, network engineers added bridges to create multiple collision domains.
- As networks grew in size and complexity, the **bridge evolved into the modern switch**, allowing microsegmentation of the network.
- Today's networks typically are built using **switches and routers**, often with the routing and switching function in the same device.

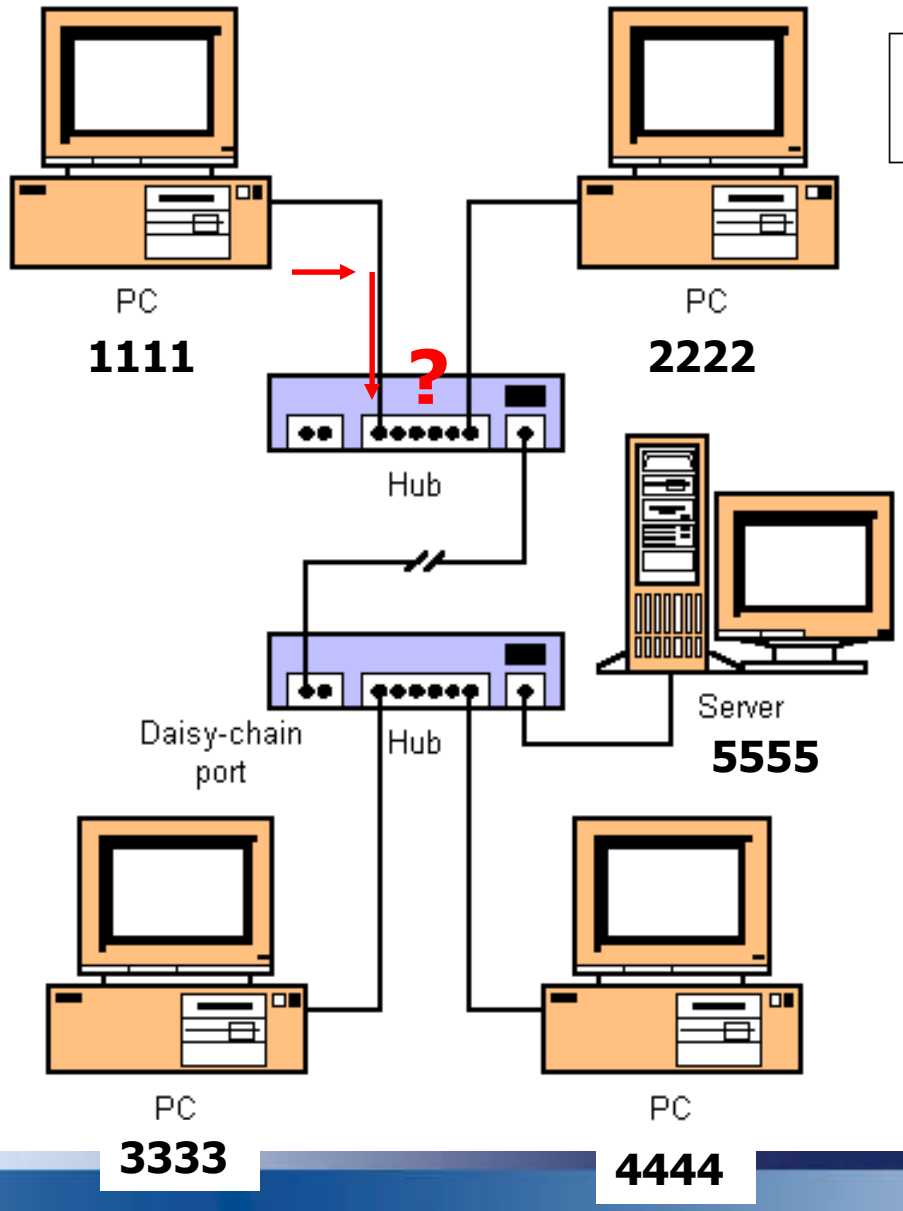
CSMA/CD and Collisions10BaseT



And as we said,

- When information (frame) is transmitted, every PC/NIC on the shared media copies part of the transmitted frame to see if the destination address matches the address of the NIC.
- If there is a match, the rest of the frame is copied
- If there is NOT a match the rest of the frame is ignored.

Sending and receiving Ethernet frames via a hub

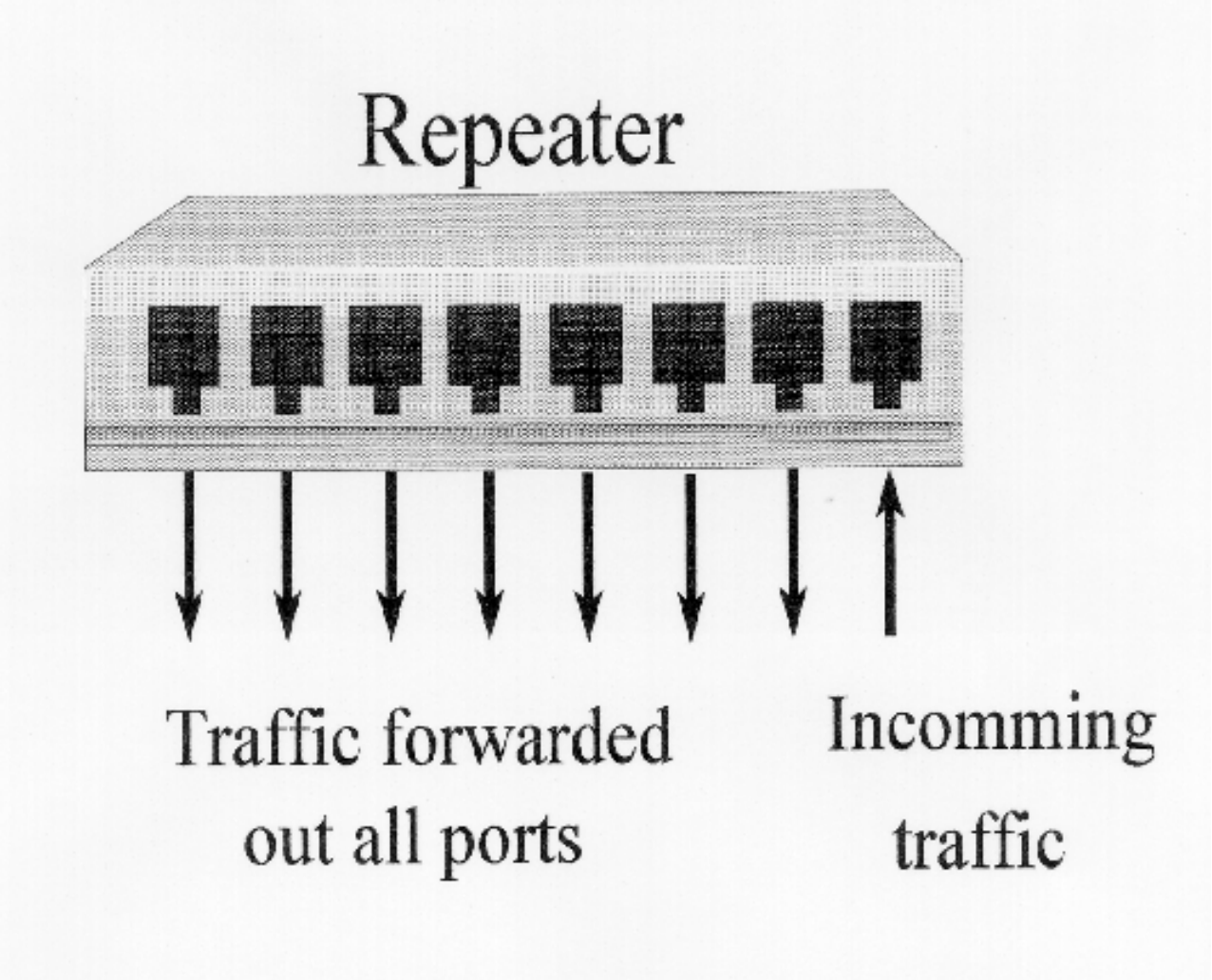


Preamble	Destination Address	Source Address	Type	Data	Pad	CRC
	3333	1111				

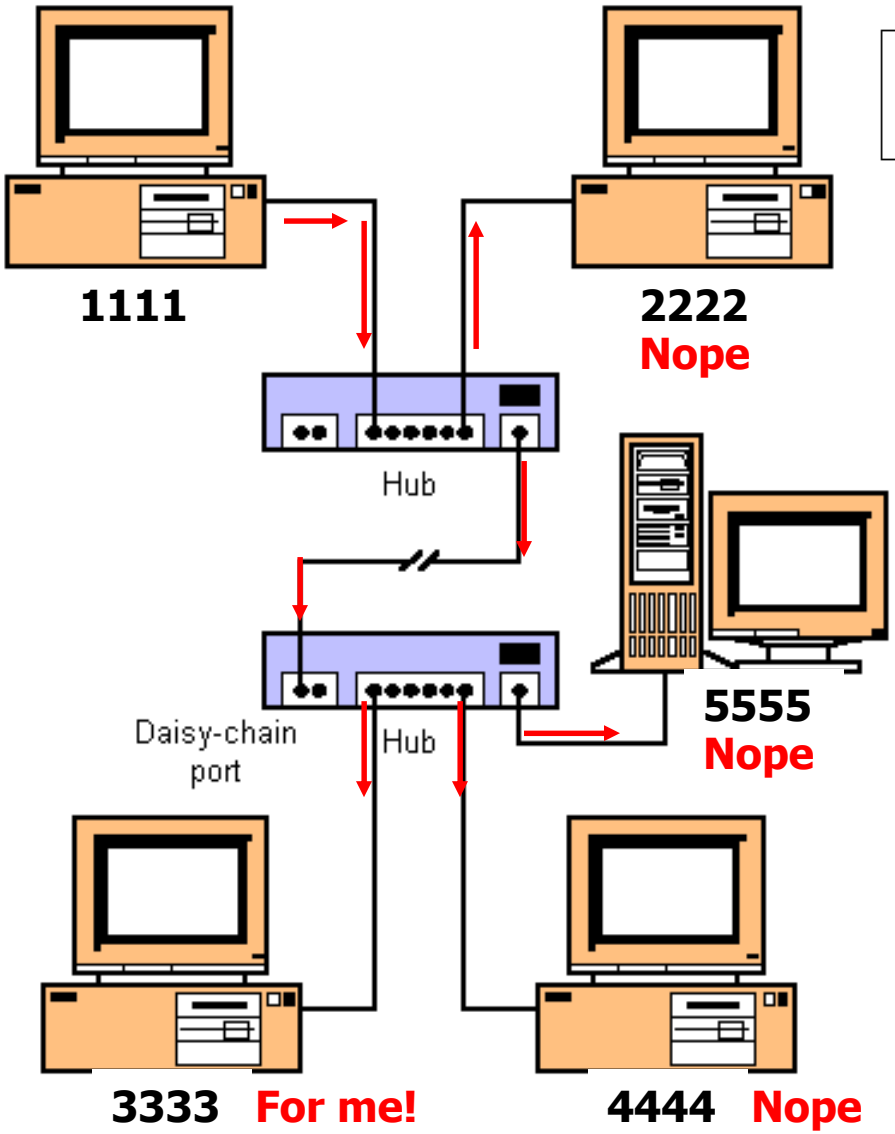
- So, what does a hub do when it receives information?
- Remember, a hub is nothing more than a multiport repeater.

Sending and receiving Ethernet frames via a hub

Hub or



Sending and receiving Ethernet frames via a hub

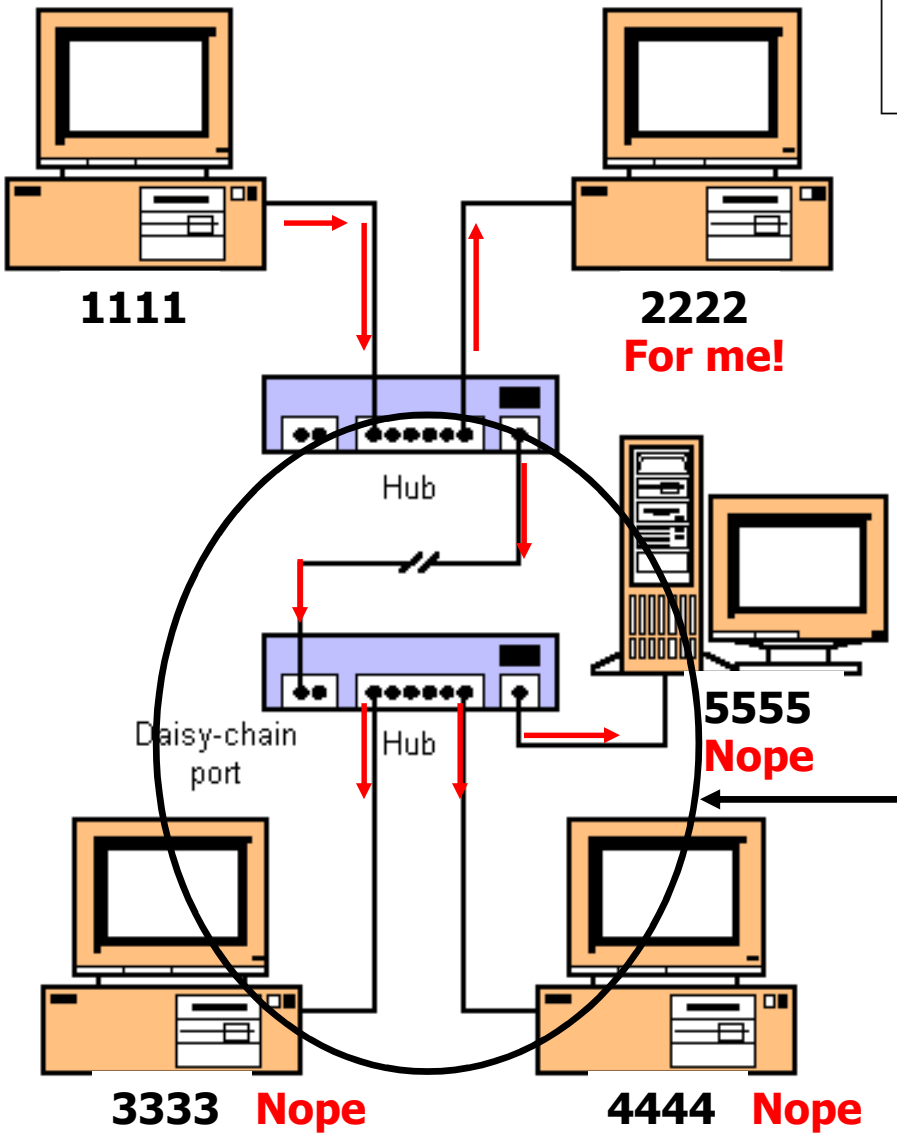


Preamble	Destination Address	Source Address	Type	Data	Pad	CRC

3333 1111

- The hub will **flood** it out all ports except for the incoming port.
- Hub is a layer 1 device.
- A hub does NOT look at layer 2 addresses, so it is fast in transmitting data.
- Disadvantage with hubs: A hub or series of hubs is a single **collision domain**.
- A collision will occur if any two or more devices transmit at the same time within the collision domain.
- More on this later.

Sending and receiving Ethernet frames via a hub

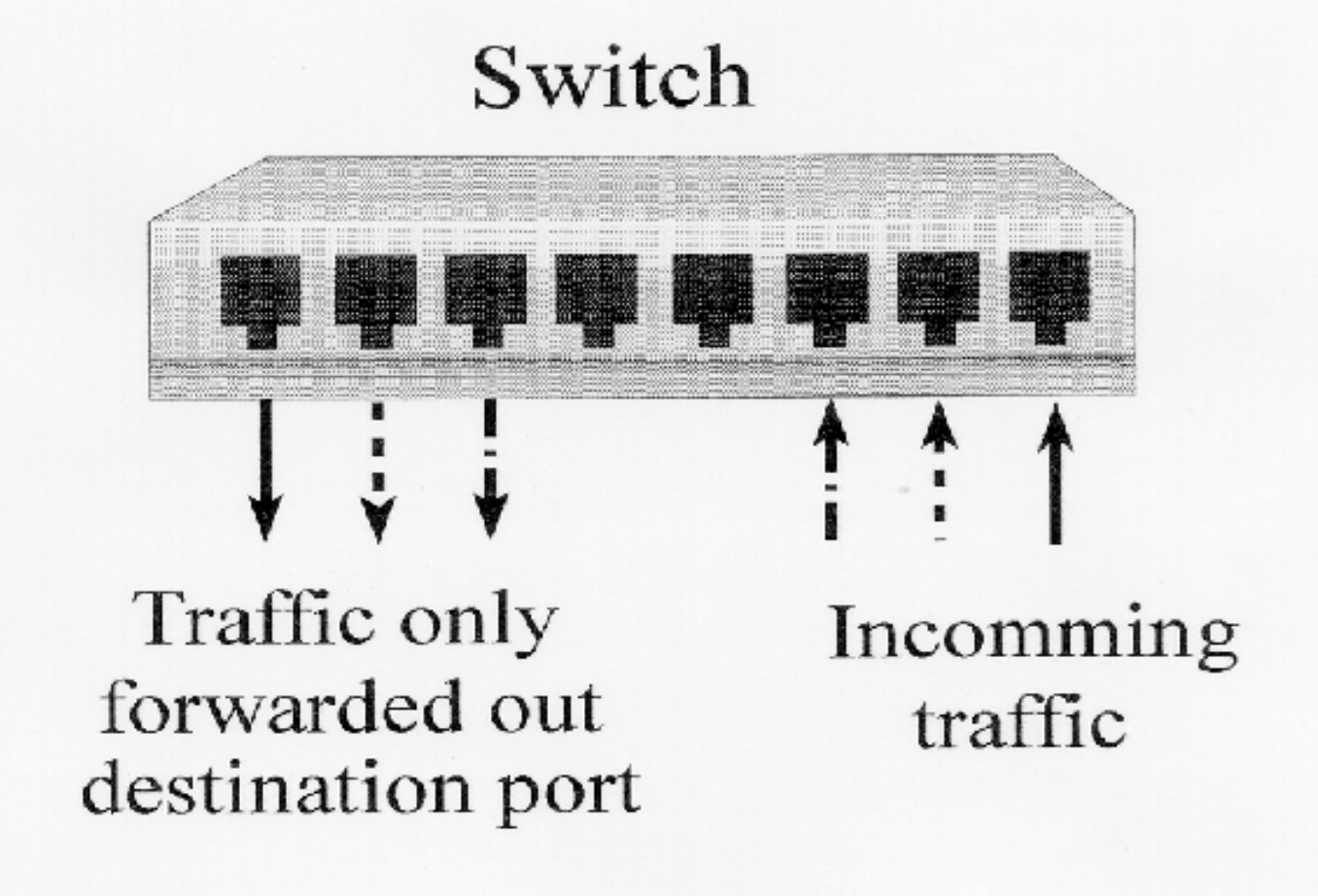


Preamble	Destination Address	Source Address	Type	Data	Pad	CRC
	2222	1111				

- Another disadvantage with hubs is that is take up unnecessary bandwidth on other links.

Wasted bandwidth

Sending and receiving Ethernet frames via a switch



บริดจ์และสวิตซ์

- ในยุคเริ่มต้นของเน็ตเวิร์กอุปกรณ์พื้นฐานที่ช่วยในการเชื่อมต่อเน็ตเวิร์กก็คือ อุปกรณ์บริดจ์(Bridge)
- ปัจจุบันอุปกรณ์บริดจ์ได้เลือนหายไปจากการใช้งานในเนตเวิร์กจริงแล้ว แต่ยังจำเป็นต้องใช้ประกอบการเรียนรู้อยู่ เช่น เรื่องของอัลกอริทึม Spanning Tree เป็นต้น
- อุปกรณ์ที่อาศัยหลักการพื้นฐานมาจากบริดจ์และให้ประสิทธิภาพที่สูงกว่าก็คือ อุปกรณ์สวิตซ์ (Switch)
- ทั้งบริดจ์และสวิตซ์นั้นทำงานอยู่ในเลเยอร์ที่ 2 ของ OSI Model เนื่องจากส่งผ่าน (forward) เฟรมโดยการพิจารณาจากหมายเลข MAC Address ปลายทางเป็นหลักเหมือนกัน

สวิตช์ (Switch)

- สวิตช์บางทีเรียก ”สวิตช์ฮับ (Switching Hub)” ทำหน้าที่ในเลเยอร์ที่ 2
- ช่วงแรกเรียกว่า“บริดจ์(Bridge)” ส่วนใหญ่บริดจ์จะมีแค่สองพอร์ต และใช้สำหรับแยกคอลลิชันโดเมน สวิตช์ จึงอาจหมายถึง บริดจ์ที่มีมากกว่าสองพอร์ต
- สวิตช์ฉลาดกว่าฮับ สามารถส่งข้อมูลที่ไดรับมาจากพอร์ตหนึ่งไปยังเฉพาะพอร์ตที่เป็นปลายทางเท่านั้น ทำให้คอมพิวเตอร์ที่เชื่อมต่อกับพอร์ตที่เหลือสามารถส่งข้อมูลถึงกันและกันได้เวลาเดียวกัน
- อัตราการรับส่งข้อมูลหรือแบนด์วิธไม่ขึ้นอยู่กับจำนวนคอมพิวเตอร์ที่เชื่อมต่อ
- คอมพิวเตอร์ทุกเครื่องจะมีแบนด์วิธเท่ากับแบนด์ของสวิตช์
- ปัจจุบันส่วนใหญ่นิยมใช้สวิตช์มากกว่าฮับ เพราะจะไม่มีปัญหาเกี่ยวกับการชนของข้อมูลในเครือข่าย

บริดจ์และสวิตช์ (ทำงานที่ Data Link Layer)

- แต่ละพอร์ตจะถือว่าเป็นคนละ “Collision Domain" กัน เครื่องคอมพิวเตอร์ที่เชื่อมต่อเข้าพอร์ตจะได้รับแบนด์วิดธ์ในการใช้งานไปเต็มๆ เช่น 10 Mbps หรือ 100 Mbps เป็นต้น (เรียกว่าได้ “dedicated bandwidth”) โดยที่ไม่ต้องไปแชร์ร่วมกับใคร
- ที่เป็นเช่นนี้ได้เพราะบริดจ์หรือสวิตช์นั้นมีความฉลาดมากขึ้นในการล่งผ่านเฟรม โดยมันจะพิจารณาจากตาราง "MAC Address Table”เพื่อตรวจเช็กดูว่าเฟรมนั้นมีหมายเลข MAC Address ปลายทางเป็นอะไรและจะล่งเฟรมนั้นออกไปเฉพาะพอร์ตที่เหมาะสมเท่านั้น
- ทำให้ ณ ขณะเวลาใดเวลาหนึ่ง การสื่อสารสามารถเกิดขึ้นได้พร้อมๆ กันหลายๆ คู่ เช่นเครื่อง A, B,C และ อ เชื่อมต่อเข้าพอร์ตสวิตช์ตัวเดียวกัน ในขณะที่เครื่อง A คุยกับเครื่อง B, เครื่องC ก็สามารถคุยกับเครื่อง D ได้พร้อมๆ กันในเวลาเดียวกัน
- ซึ่งพฤติกรรมลักษณะนี้อุปกรณ์อย่างฮับนั้นไม่สามารถกระทำได้

ความแตกต่างของบริดจ์(Bridge) กับสวิตช์(Switch)

- ความเร็วในการทำงาน สวิตช์งานได้เร็วกว่าบริดจ์ เพราะ
  - สวิตช์มีการใช้งานชิป (chip) ที่เรียกว่า Application Specific Integrated Circuit (ASIC) ซึ่งเป็นฮาร์ดแวร์พิเศษที่ได้รับการสร้างขึ้นมาด้วยจุดประสงค์เฉพาะทาง คือ การส่งผ่าน (forward) เฟรมที่รับเข้ามาจากพอร์ตต้นทางให้ออกไปยังพอร์ตปลายทางขั้นตอนในการส่งผ่านเฟรมจะกระทำอย่างเบ็ดเสร็จภายใต้ฮาร์ดแวร์ ASIC พิเศษนี้
  - บริดจ์ทำงานด้วยกระบวนการทางซอฟต์แวร์ปกติ คือโหลดเฟรมเข้าสู่หน่วยความจำและใช้ซีพียูแยกต่างหากในการวิเคราะห์เฟรม แล้วค่อยส่งผ่านออกไปที่พอร์ตปลายทาง พฤติกรรมการทำงานด้วยซอฟต์แวร์แบบเก่านี้จะช้ากว่าการทำงานด้วยฮาร์ดแวร์พิเศษ ASIC ที่ใช้ในสวิตช์ค่อนข้างมาก

ความแตกต่างของบริดจ์(Bridge) กับสวิตช์(Switch)

- จำนวนพอร์ต โดยทั่วไป บริดจ์นั้นมีจำนวนพอร์ตไม่มากนัก เช่น 4 พอร์ต ในขณะที่สวิตช์นั้นมีจำนวนพอร์ตอย่างน้อยๆ ก็เริ่มต้นที่ 12 พอร์ต หรือ 24 พอร์ตเป็นหลัก ทำให้สามารถรองรับการเชื่อมต่อจากเครื่องคอมพิวเตอร์ของผู้ใช้ได้ในจำนวนที่มากกว่า
- ต้นทุนต่อพอร์ตของสวิตช์จะต่ำกว่าบริดจ์
- สวิตช์มีความยืดหยุ่นในการเซตคอนฟิกูเรชันต่างๆ มากกว่าบริดจ์
- สวิตช์สามารถแบ่งออกเป็น LAN เสมือนย่อยๆ ที่เรียก'ว่า VLAN ได้ ในขณะที่บริดจ์ทำไม่ได้
- ในปัจจุบันไม่พบผู้ค้ารายไหนทำการจำหน่ายบริดจ์แล้ว มีแต่จำหน่ายสวิตช์

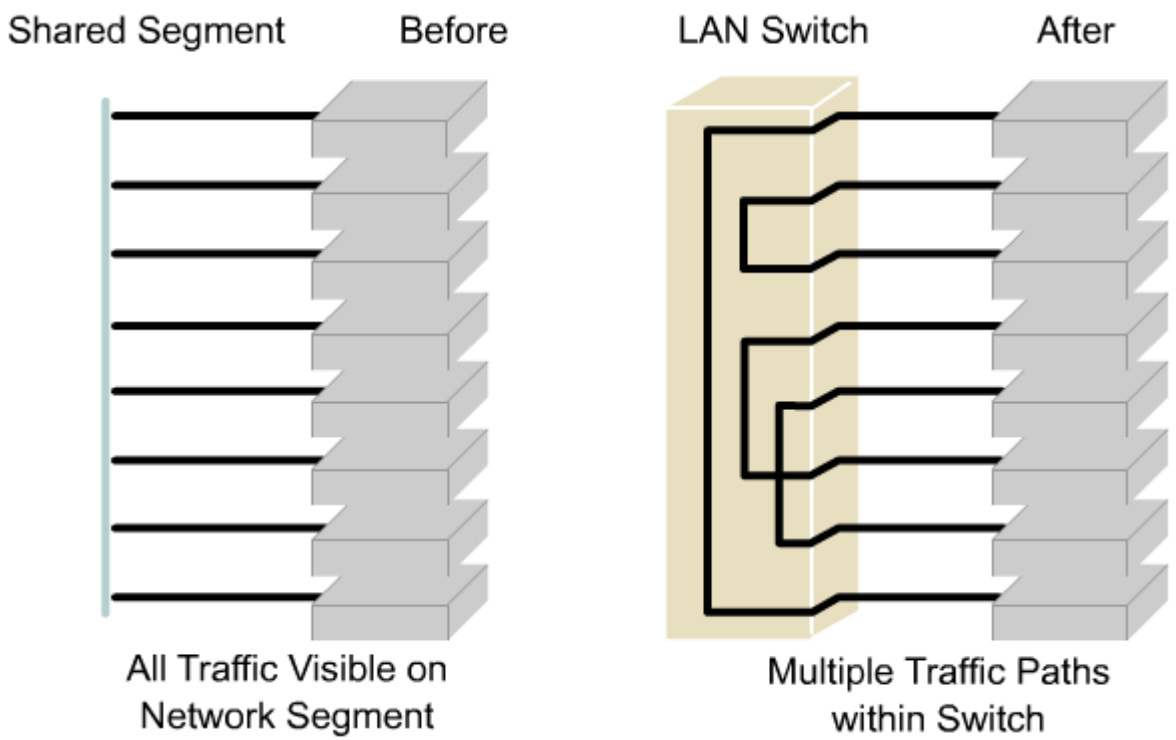
หน้าที่ของบริดจ์กับสวิตซ์

- การเรียนรู้MAC Address เพื่อสร้างตาราง MAC Address Table กระบวนการนี้เรียกว่า "Address Learning”
- การตัดสินใจส่งผ่านเฟรม โดยส่งผ่านเฟรมออกไปเฉพาะพอร์ตที่เหมาะสมเท่านั้น และไม่ส่งออกไปรบกวนแบนด์วิดธ์ของพอร์ตอื่นๆ กระบวนการนี้เรียกว่า “Forwarding/Filtering”
- การป้องกันการเกิดลูป ซึ่งจำเป็นต้องทำเมื่อบริดจ์/ สวิตซ์มีเส้นทางสำรองอื่นๆ มากกว่า 1 เส้นทางในการส่งเฟรมไปยังเครื่องปลายทาง กระบวนการนี้เรียกว่า “Loop Avoidance”

Switching as a General Concept

- พื้นฐานการส่งข้อมูลของสวิทช์ จะตัดสินใจจากพอร์ตขาเข้าและพอร์ตปลายทาง
- LAN สวิทช์ ใช้ตารางที่อยู่ในการกำหนดวิธีการส่งต่อผ่านสวิทช์
- LAN สวิตช์อีเธอร์เน็ตส่งต่อเฟรมโดยใช้ที่อยู่ MAC ปลายทางของเฟรม

Switched Fabric



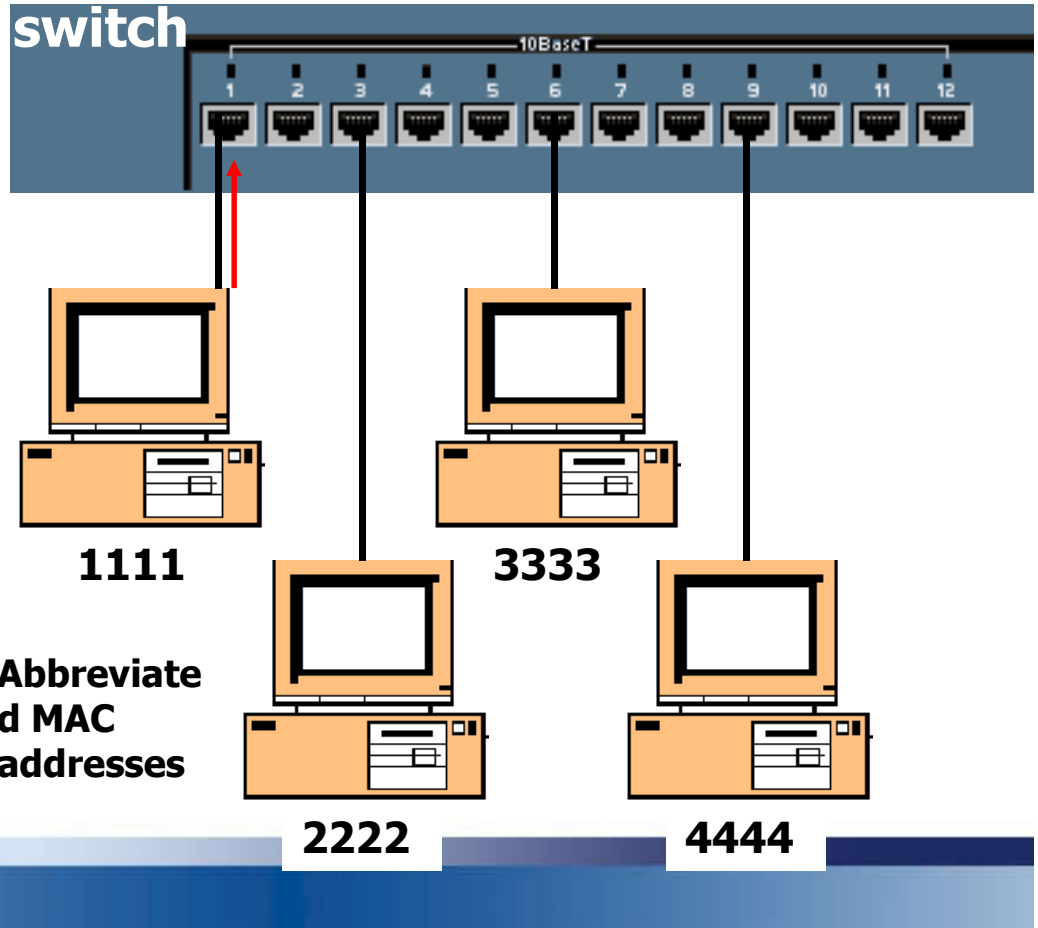
Sending and receiving Ethernet frames via a switch

Source Address Table

Port	Source MAC Add.	Port	Source MAC Add.

Preamble	Destination Address	Source Address	Type	Data	Pad	CRC

3333 1111



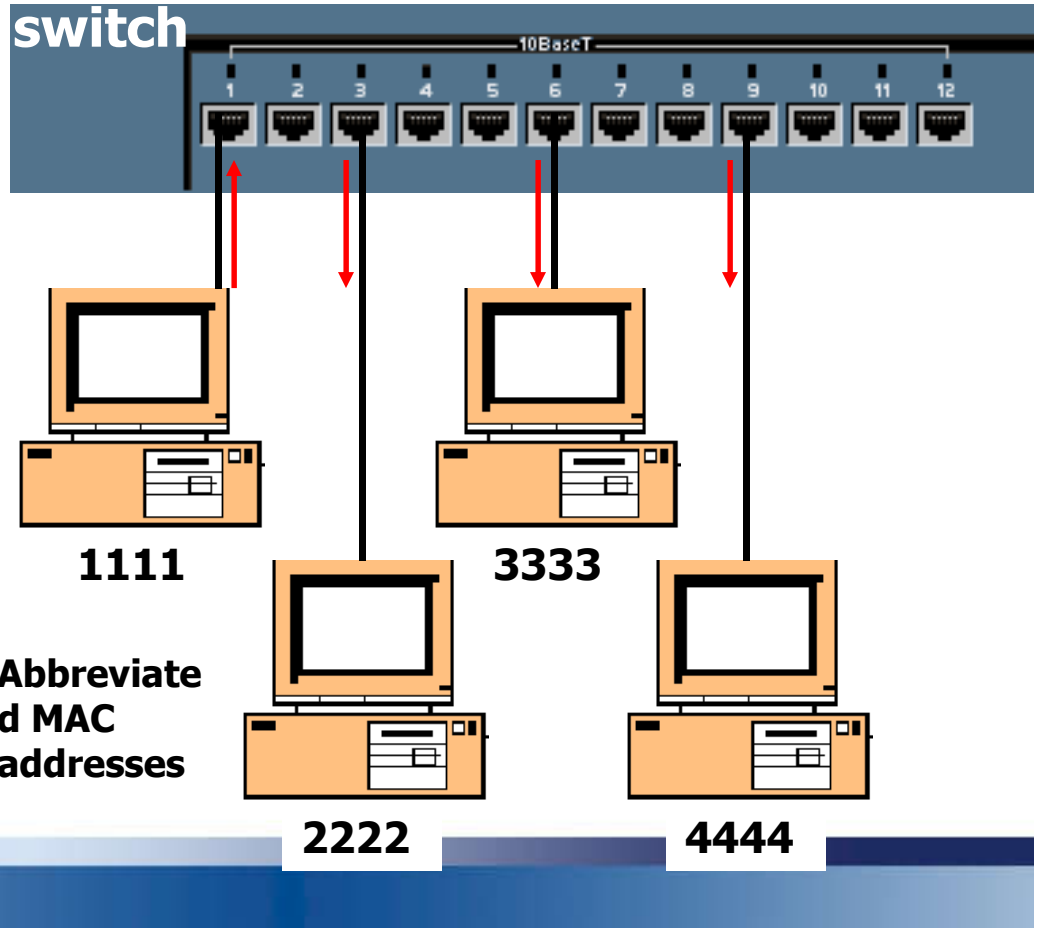
- Switches are also known as **learning bridges** or **learning switches**.
- A switch has a source address table in cache (RAM) where it stores source MAC address after it learns about them.
- A switch receives an Ethernet frame it searches the source address table for the Destination MAC address.
- If it finds a match, it **filters** the frame by only sending it out that port.
- If there is not a match if **floods** it out all ports.

No Destination Address in table, Flood

Source Address Table

Port	Source MAC Add.	Port	Source MAC Add.
1	1111		

Preamble	Destination Address	Source Address	Type	Data	Pad	CRC
	3333	1111				

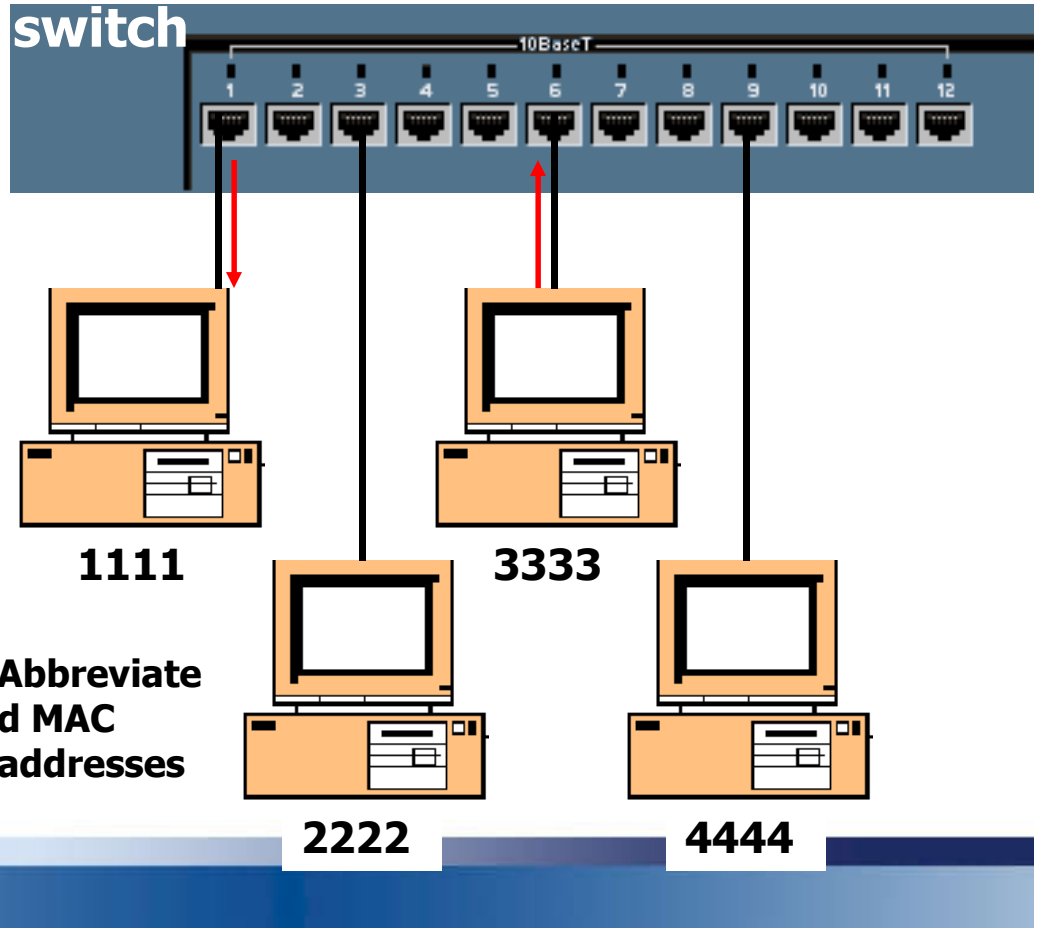


- How does it learn source MAC addresses?
- First, the switch will see if the SA (1111) is in it's table.
- If it is, it resets the timer (more in a moment).
- If it is NOT in the table it adds it, with the port number.
- Next, in our scenario, the switch will **flood** the frame out all other ports, because the DA is not in the source address table.

Destination Address in table, Filter

Source Address Table

Port	Source MAC Add.	Port	Source MAC Add.
1	1111	6	3333



Preamble	Destination Address	Source Address	Type	Data	Pad	CRC

1111 3333

- Most communications involve some sort of client-server relationship or exchange of information. (You will understand this more as you learn about TCP/IP.)
- Now 3333 sends data back to 1111.
- The switch sees if it has the SA stored.
- It does NOT so it adds it. (This will help next time 1111 sends to 3333.)
- Next, it checks the DA and in our case it can **filter** the frame, by sending it only out port 1.

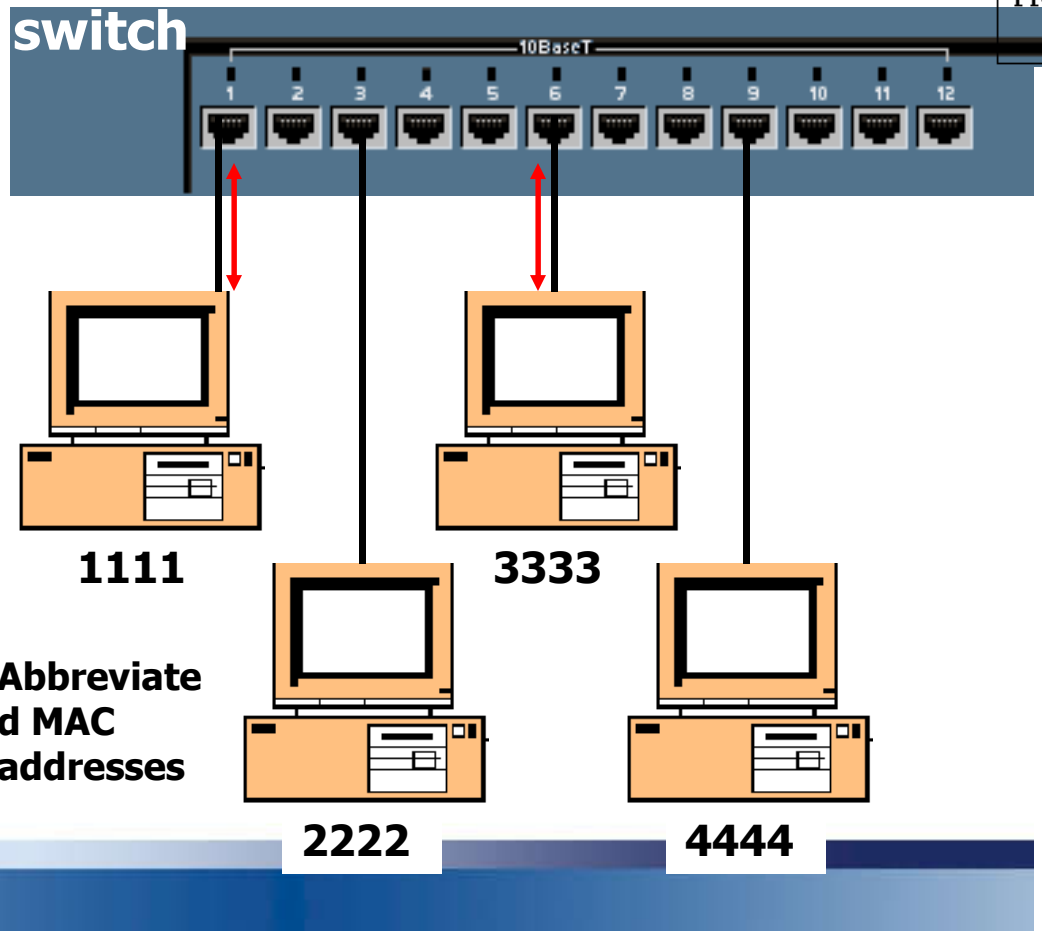
Destination Address in table, Filter

Source Address Table

Port	Source MAC Add.	Port	Source MAC Add.
1	1111	6	3333

Preamble	Destination Address	Source Address	Type	Data	Pad	CRC
	3333	**1111**				

Preamble	Destination Address	Source Address	Type	Data	Pad	CRC
	1111	**3333**				



- Now, because both MAC addresses are in the switch's table, any information exchanged between 1111 and 3333 can be sent (filtered) out the appropriate port.
- **What happens when two devices send to same destination?**
- **What if this was a hub?**
- **Where is (are) the collision domain(s) in this example?**

No Collisions in Switch, Buffering

Source Address Table

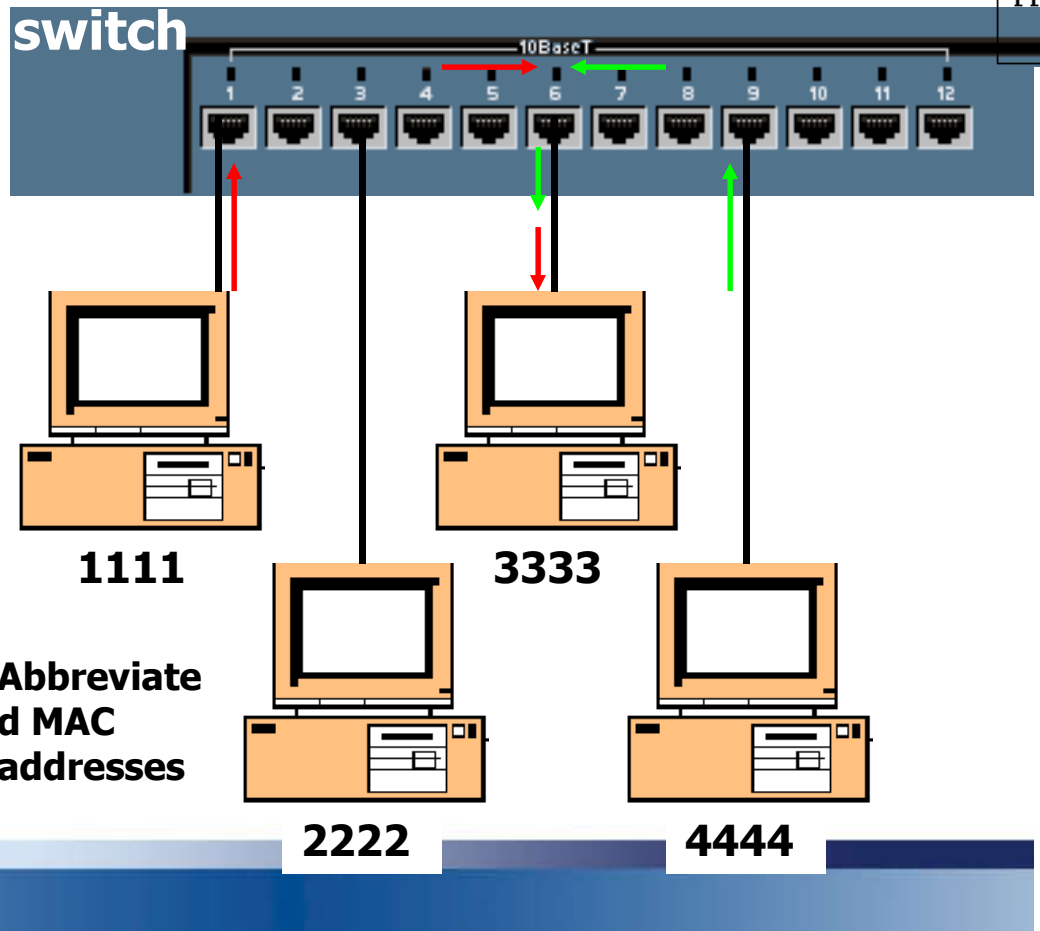
Port	Source MAC Add.	Port	Source MAC Add.
1	1111	6	3333
9	4444		

Preamble	Destination Address	Source Address	Type	Data	Pad	CRC

3333 **1111**

Preamble	Destination Address	Source Address	Type	Data	Pad	CRC

3333 **4444**



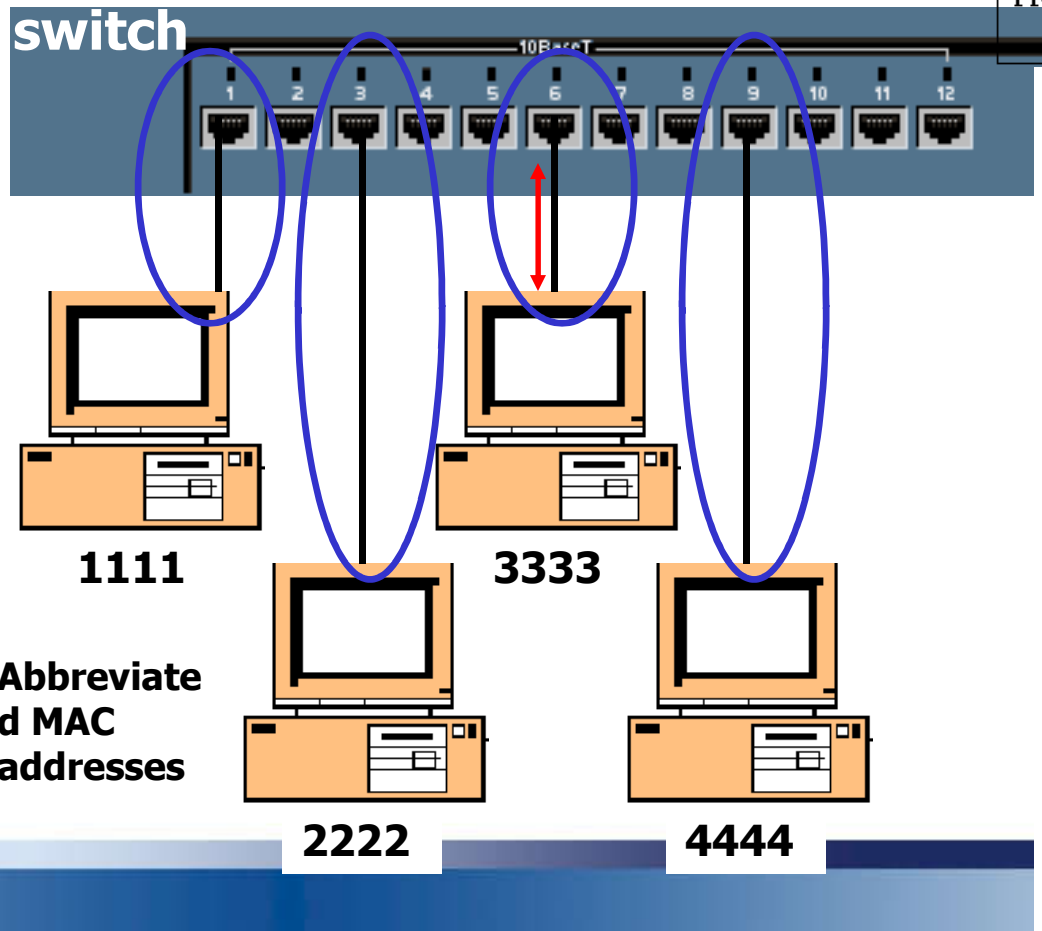
- Unlike a hub, a collision does NOT occur, which would cause the two PCs to have to retransmit the frames.
- Instead the switch buffers the frames and sends them out port #6 one at a time.
- The sending PCs have no idea that their was another PC wanting to send to the same destination.

Collision Domains: Half Duplex VS full Duplex

Source Address Table

Port	Source MAC Add.	Port	Source MAC Add.
1	1111	6	3333
9	4444		

Collision Domains



Preamble	Destination Address	Source Address	Type	Data	Pad	CRC

3333 **1111**

Preamble	Destination Address	Source Address	Type	Data	Pad	CRC

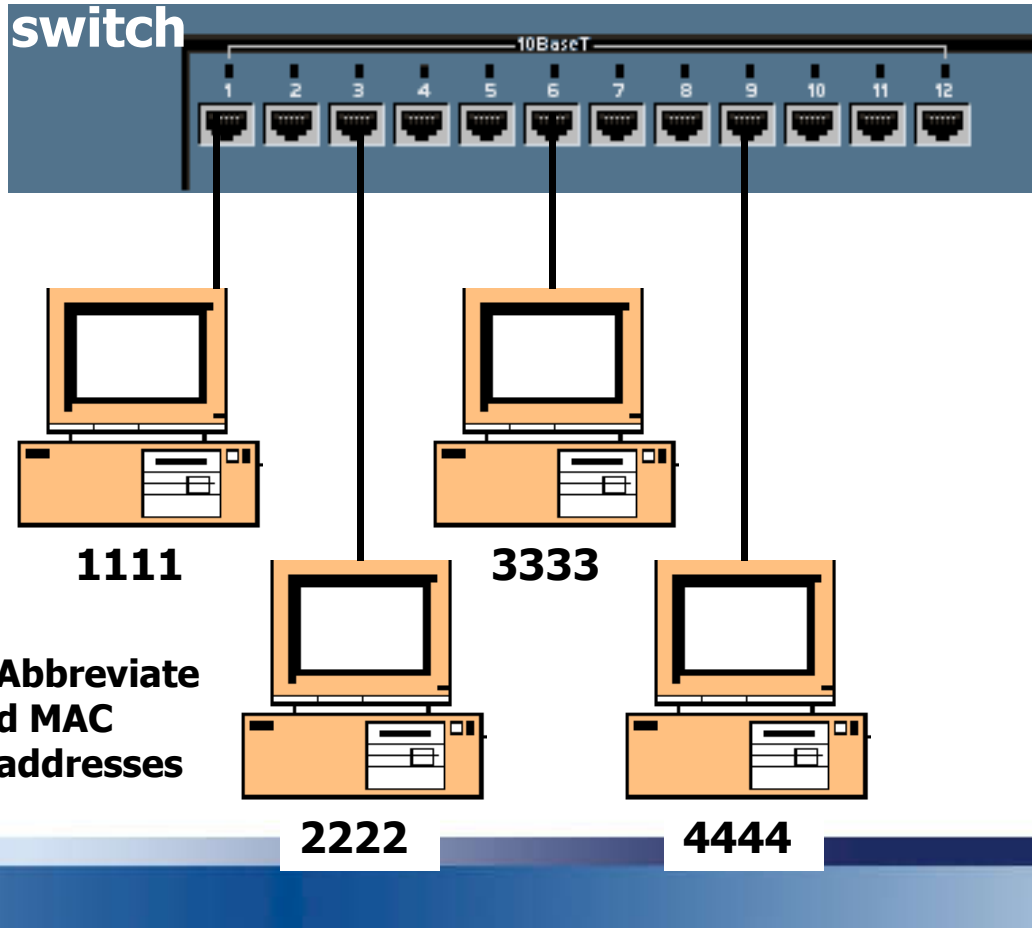
3333 **4444**

- In half duplex mode and when there is only one device on a switch port, the collision domain is only between the PC and the switch.
- With a **full-duplex** PC and switch port, there will be no collision, since the devices and the medium can send and receive at the same time.

Other Information

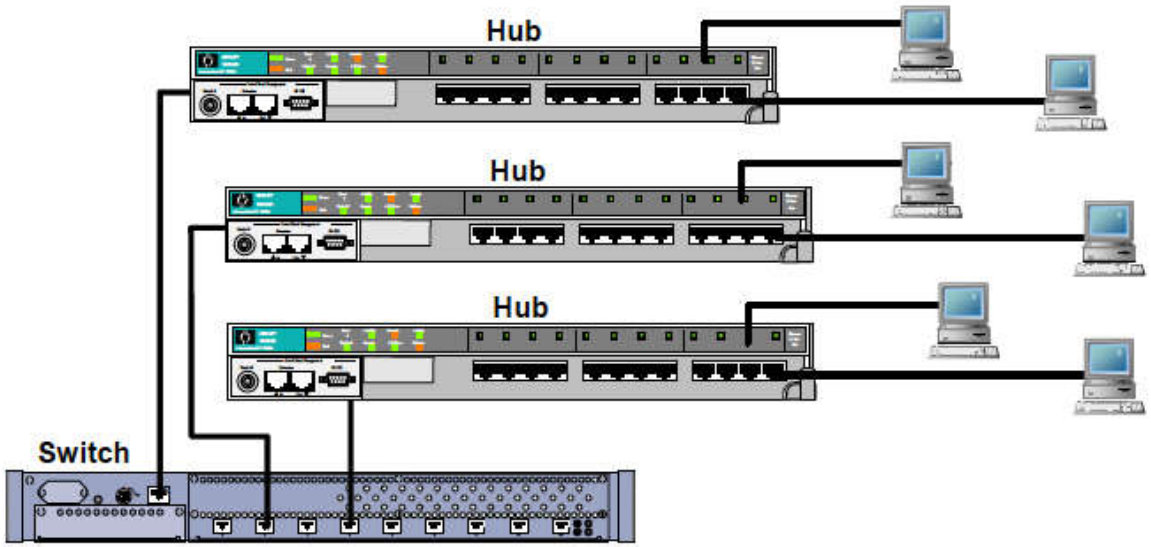
Source Address Table

Port	Source MAC Add.	Port	Source MAC Add.
1	1111	6	3333
9	4444		



Preamble	Destination Address	Source Address	Type	Data	Pad	CRC

- How long are addresses kept in the Source Address Table?
  - 5 minutes is common on most vendor switches.
- How do computers know the Destination MAC address?
  - ARP Caches and ARP Requests
- How many addresses can be kept in the table?
  - Depends on the size of the cache, but 1,024 addresses is common.
- What about Layer 2 broadcasts?
  - Layer 2 broadcasts (DA = all 1's) is flooded out all ports.



- มีโอกาสเป็นไปได้เหมือนกันที่ภายในตาราง MAC Address Table จะมีการแมปหมายเลข MAC Address มากกว่า 1 แอดเดรสเข้ากับหมายเลขพอร์ตของสวิตช์เพียงพอร์ตเดียว อย่างในกรณีของการนำเอาฮับมาต่อกับพอร์ตของสวิตช์ก่อน แล้วจากนั้นพอร์ตของอับจึงค่อยลากสายไปยังเครื่องคอมพิวเตอร์ของผู้ใช้

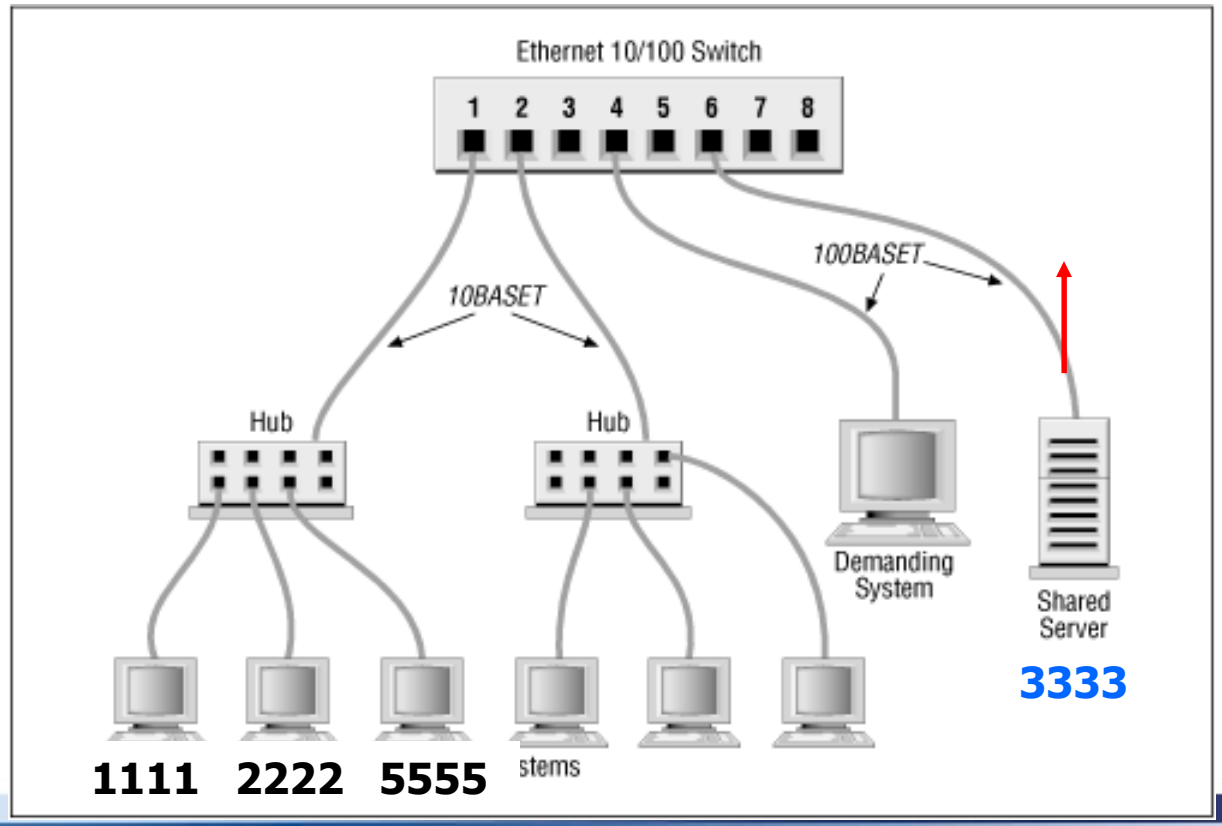
What happens here?

Source Address Table

Port	Source MAC Add.	Port	Source MAC Add.
1	1111	6	3333
1	2222	1	5555

Preamble	Destination Address	Source Address	Type	Data	Pad	CRC

1111 **3333**



- Notice the Source Address Table has multiple entries for port #1.

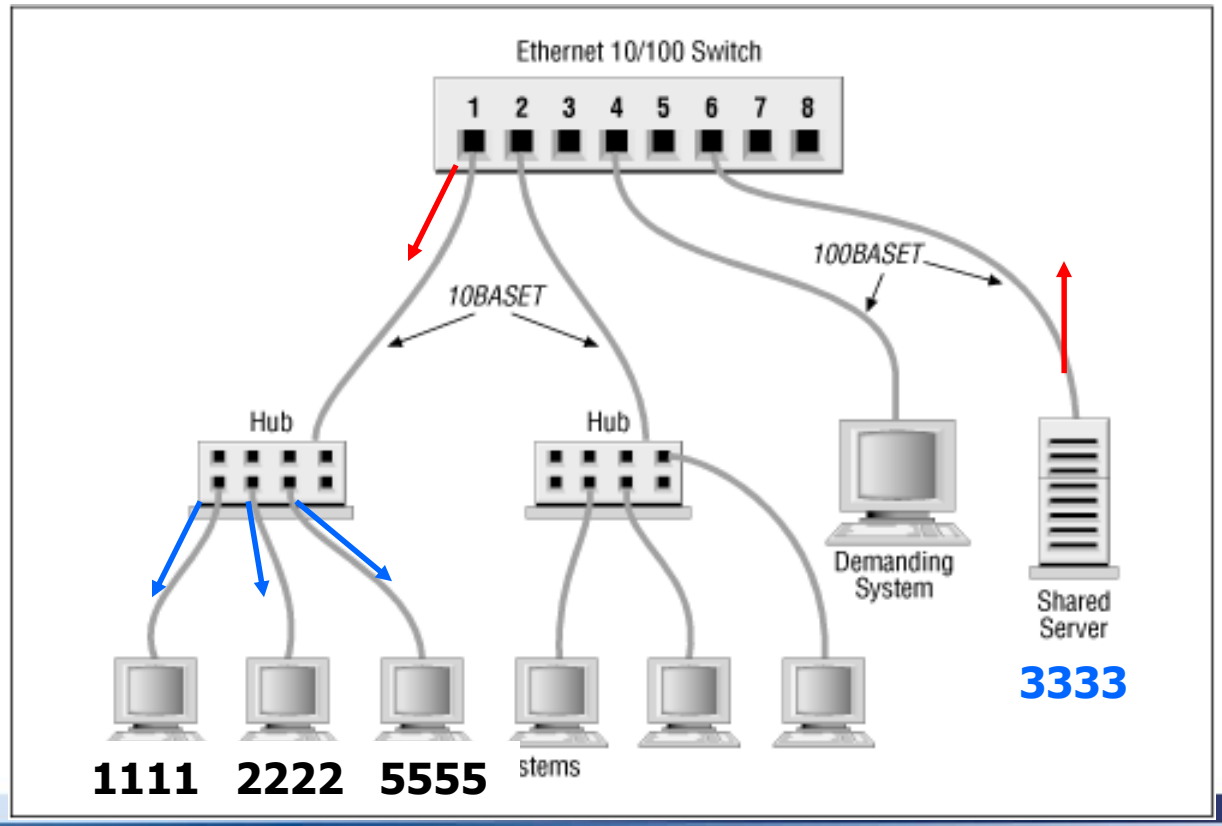
What happens here?

Source Address Table

Port	Source MAC Add.	Port	Source MAC Add.
1	1111	6	3333
1	2222	1	5555

Preamble	Destination Address	Source Address	Type	Data	Pad	CRC

1111 **3333**



- The switch filters the frame out port #1.
- But the hub is only a layer 1 device, so it floods it out all ports.
- Where is the collision domain?

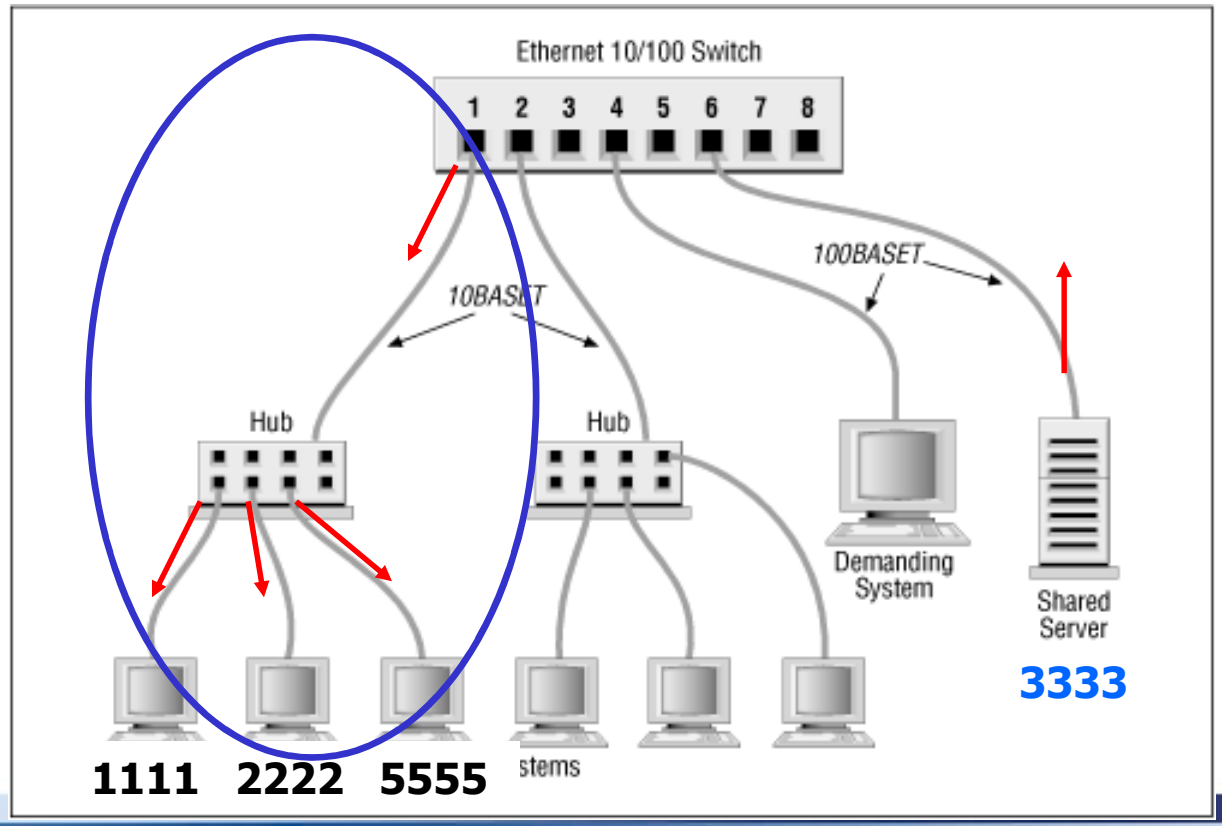
What happens here?

Source Address Table

Port	Source MAC Add.	Port	Source MAC Add.
1	1111	6	3333
1	2222	1	5555

Preamble	Destination Address	Source Address	Type	Data	Pad	CRC

1111 **3333**

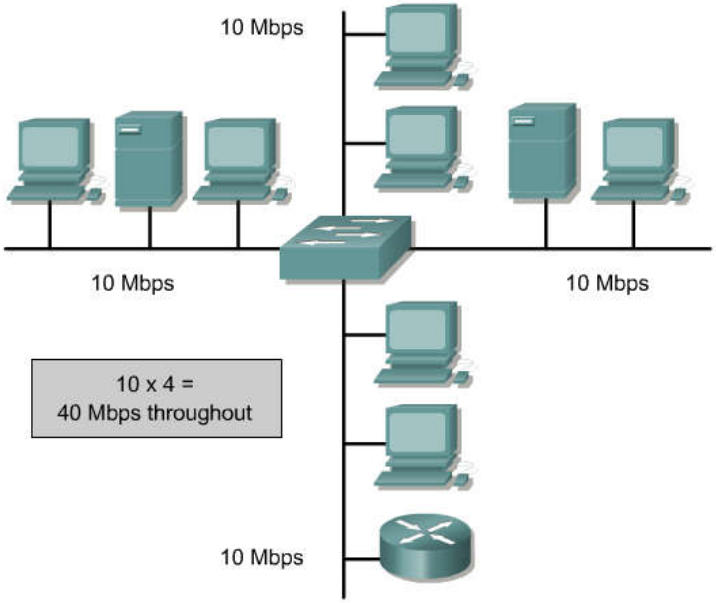


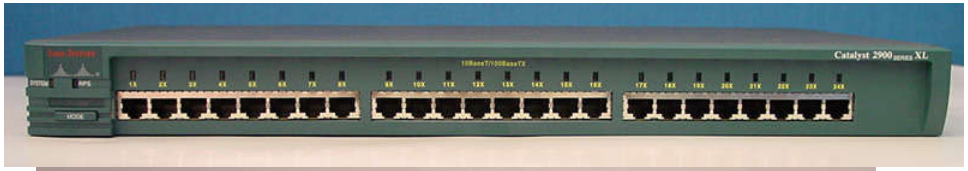
Collision Domain

- ในทำนองกลับกัน ก็เป็นไปได้เหมือนกันที่จะทำให้ทราฟฟิกที่ถูกส่งไปยัง MAC Address ปลายทาง 1 MAC Address วิ่งออกไปทางพอร์ตมากกว่า 1 พอร์ต เช่น กรณีการทำการกระจายโหลด (Load Balance) ไฟร์วอลล์ทั้ง 2 ตัวจะมี MAC Address เสมือน (Virtual MAC) เหมือนกัน จำเป็นต้องเซตคอนฟิกให้ทราฟฟิกที่ส่งไปยัง MAC Address เสมือนดังกล่าววิ่งออกไปทางพอร์ต 2 พอร์ตที่ต่อเข้าหาไฟร์วอลล์ทั้ง 2 ตัว

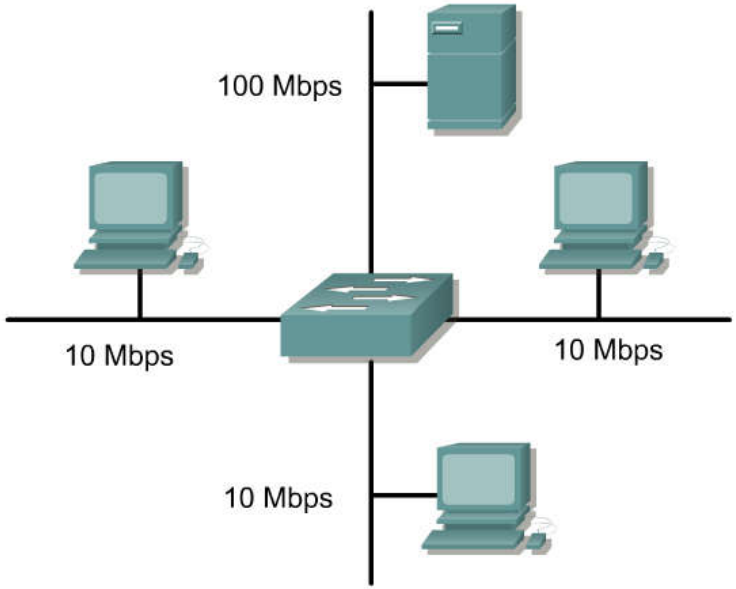
Symmetric and asymmetric switching

Symmetric Switching



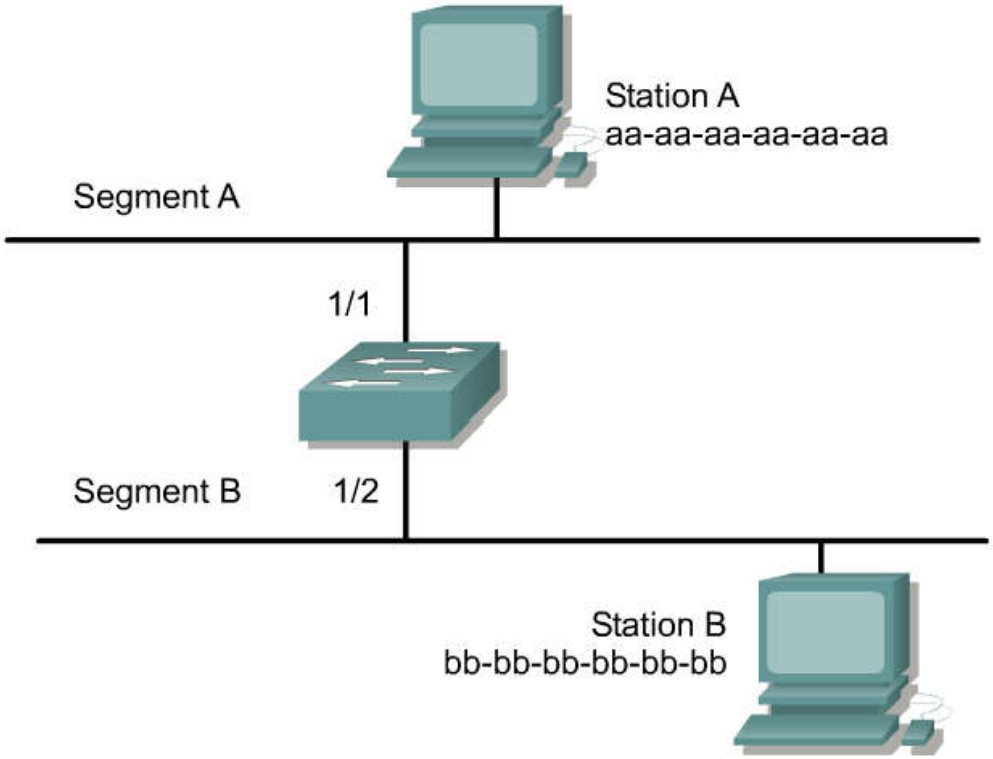


Asymmetric Switching



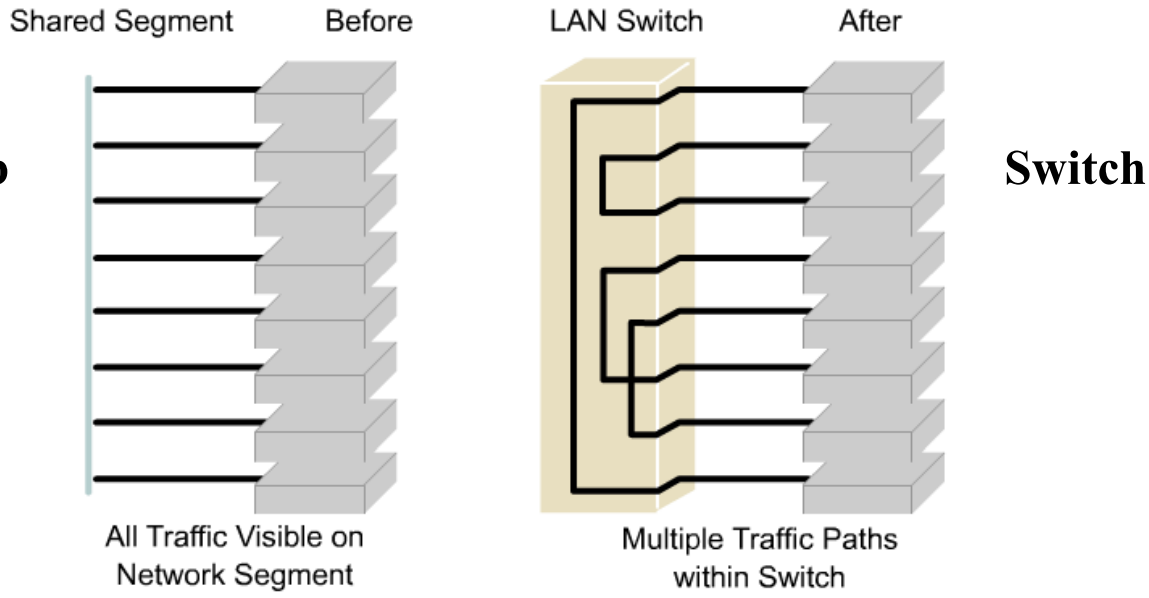
Note: Most switches are now 10/100, which allow you to use them symmetrically or asymmetrically.

Functions of a switch



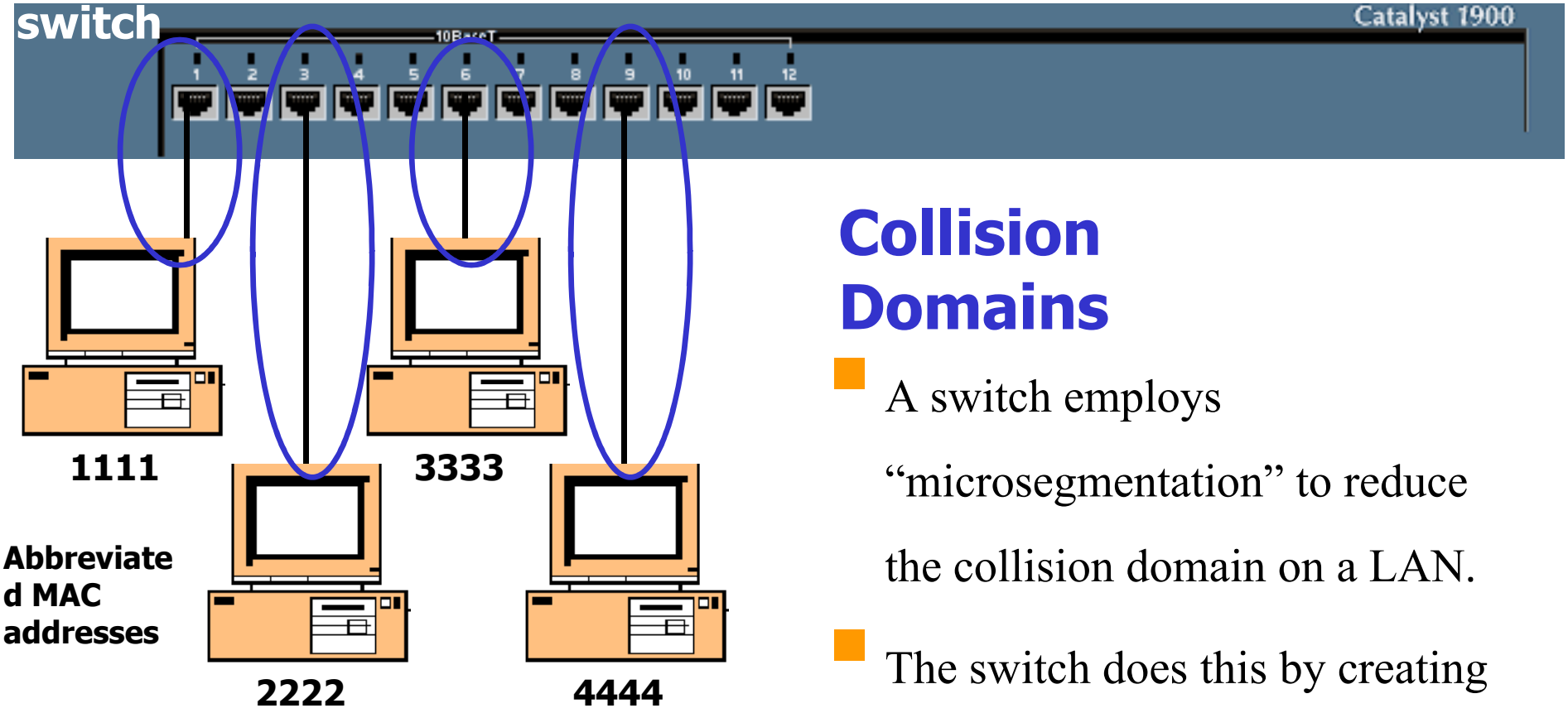
- The main features of Ethernet switches are:
  - Isolate traffic among segments
  - Achieve greater amount of bandwidth per user by creating smaller collision domains

Why segment LANs? (Layer 2 segments)



- First is to isolate traffic between segments.
- The second reason is to achieve more bandwidth per user by creating smaller collision domains.

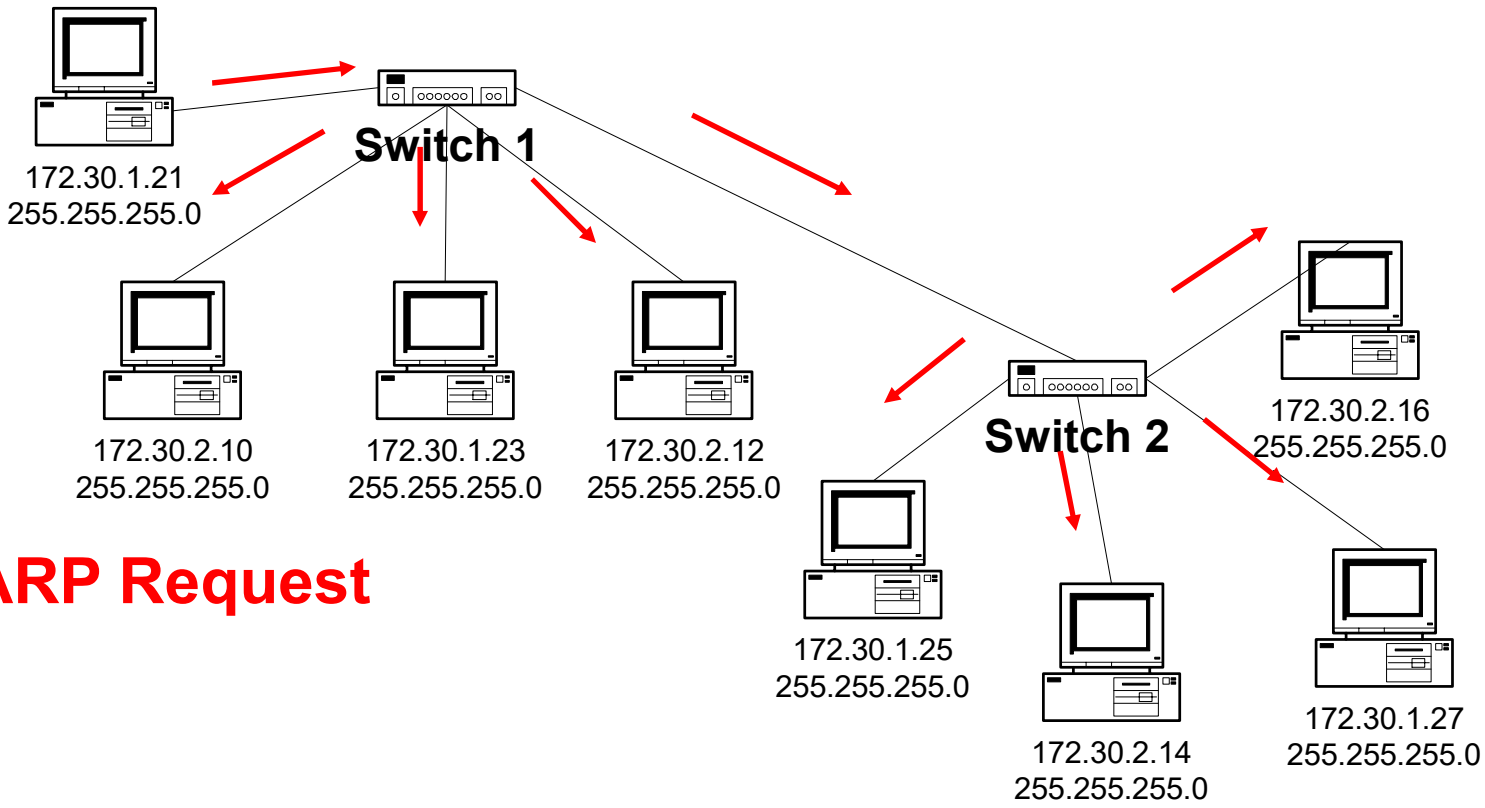
Why segment LANs? (Layer 2 segments)



Collision Domains

- A switch employs "microsegmentation" to reduce the collision domain on a LAN.
- The switch does this by creating dedicated network segments, or point-to-point connections.

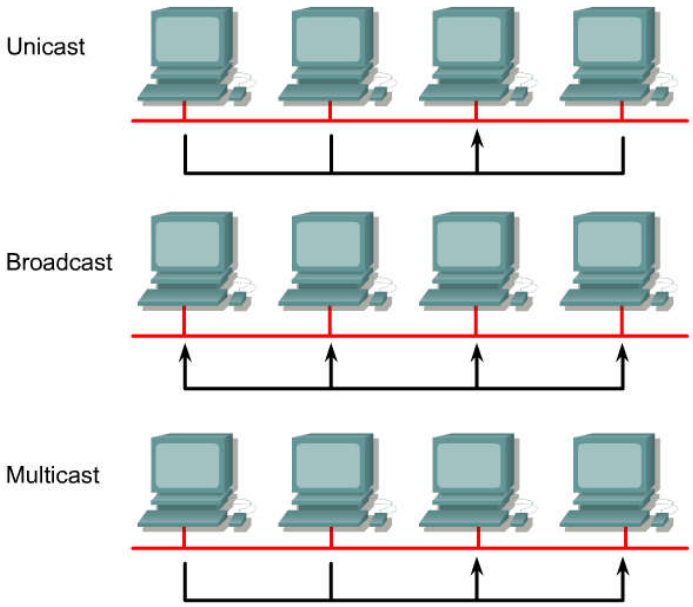
Broadcast domains



- **ARP Request**

- Even though the LAN switch reduces the size of collision domains, all hosts connected to the switch are still in the same broadcast domain.
- Therefore, a broadcast from one node will still be seen by all the other nodes connected through the LAN switch.

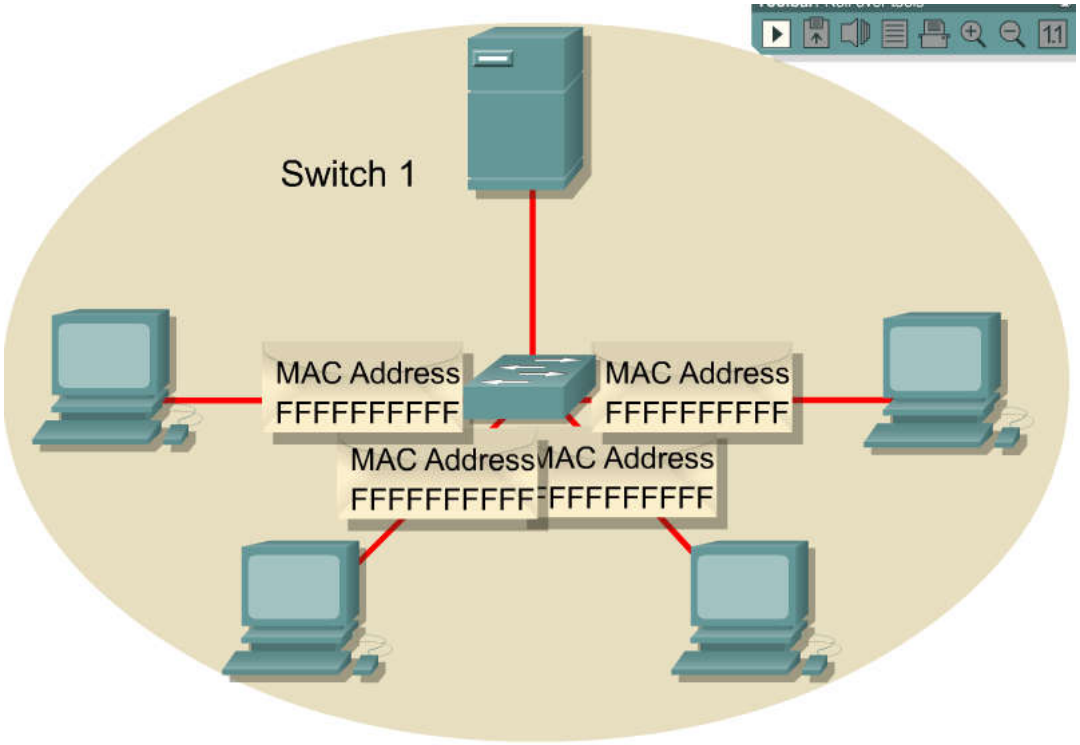
Switches and broadcast domains



These are logical not physical representations of what happens to these frames.

- Switches flood frames that are:
  - Unknown unicasts
  - Layer 2 broadcasts
  - Multicasts (unless running multicast snooping or IGMP)
    - Multicast are special layer 2 and layer 3 addresses that are sent to devices that belong to that “group”.

Switches and broadcast domains



- When a device wants to send out a Layer 2 broadcast, the destination MAC address in the frame is set to all ones.
- A MAC address of all ones is FF:FF:FF:FF:FF:FF in hexadecimal.
- By setting the destination to this value, all the devices will accept and process the broadcasted frame.

บรอดคาสต์โดเมน (Broadcast Domain)

- มัลติคาสต์โดเมน (Multicast Domain) หมายถึง กลุ่มของหมายเลข MAC ซึ่งแต่ละโหนดสามารถโปรแกรมให้อยู่ในกลุ่มนี้ได้
- บรอดคาสต์โดเมน (Broadcast Domain) เป็นกรณีพิเศษของมัลติคาสต์โดเมน หมายถึง ทุกโหนดที่อยู่ในวง LAN เดียวกัน ดังนั้นเฟรมข้อมูลที่ส่งไปยังบรอดคาสต์โดเมน ทุกๆ โหนดที่เชื่อมต่อเข้ากับเครือข่ายจะได้รับเฟรมนั้น
- สวิตช์ถูกออกแบบมาสำหรับเชื่อมต่อหลายๆ คอลลิชันโดเมนเป็นวง LAN เดียวกัน
- สวิตช์จะทำการ ฟลัด (Flood) หรือส่งเฟรมข้อมูลรอดคาสต์ไปยังทุกๆ พอร์ตสวิตช์ ยกเว้นพอร์ตที่รับเฟรมข้อมูลนั้นมา
- ด้วยวิธีนี้เฟรมแบบบรอดคาสต์สามารถส่งไปยังทุกๆ โหนดในเครือข่าย ดังนั้นบางที่สวิตช์ก็ทำหน้าที่เป็นรีพีทเตอร์เหมือนกัน

บรอดคาสต์โดเมน (Broadcast Domain)

- การส่งเฟรมข้อมูลแบบมัลติคาสต์หรือบรอดคาสต์นั้นมีข้อดีอยู่หลายประการ
- บางโปรโตคอลในเลเยอร์เหนือกว่าใช้การส่งข้อมูลแบบบรอดคาสต์เพื่อสำหรับการค้นหาที่อยู่ในเลเยอร์นั้น
- โปรโตคอล DHCP (Dynamic Host Configuration Protocol) จะใช้การส่งข้อมูลแบบบรอดคาสต์เมื่อคอมพิวเตอร์ถูกเปิดเพื่อใช้งานครั้งแรกเพื่อค้นหาเซิร์ฟเวอร์ที่แจกจ่ายหมายเลขไอพีและค่าคอนฟิกอื่นๆ
- ส่วนมัลติคาสต์นี้อาจถูกใช้โดยบางโปรแกรมมัลติมีเดียเพื่อส่งวีดีโอและเสียงไปยังกลุ่มของโหนดที่รอรับเฟรมนี้อยู่ หรือเกมที่เล่นผ่านเครือข่ายก็ใช้การสื่อสารระหว่างผู้เล่นโดยการส่งเฟรมแบบมัลติคาสต์ทุกๆ เครือข่ายก็จะมีการส่งข้อมูลแบบบรอดคาสต์

บรอดคาสต์โดเมน (Broadcast Domain)

- โดยทั่วไปแล้วสวิตช์ส่งต่อเฟรมแบบบรอดคาสต์ไปยังทุกๆ โหนดในเครือข่าย ดังนั้นจึงมีความจำเป็นที่ต้องจำกัดจำนวนสวิตช์ที่ใช้เครือข่าย เพราะถ้ามีการบรอดคาสต์ข้อมูลมากเกินไป อาจทำให้เครือข่ายช้าเกินไป
- เลเยอร์ 3 สวิตช์ หรือเราท์เตอร์นั้นจะช่วยลดอาการบรอดคาสต์ในเครือข่ายได้ เนื่องจากเราท์เตอร์นั้นจะไม่ส่งต่อเฟรมข้อมูลแบบบรอดคาสต์

Using Hubs

- Layer 1 devices
- Inexpensive
- In one port, out the others
- One collision domain
- One broadcast domain

Using Switches

- Layer 2 devices
- Layer 2 filtering based on Destination MAC addresses and Source Address Table
- One collision domain per port
- One broadcast domain across all switches

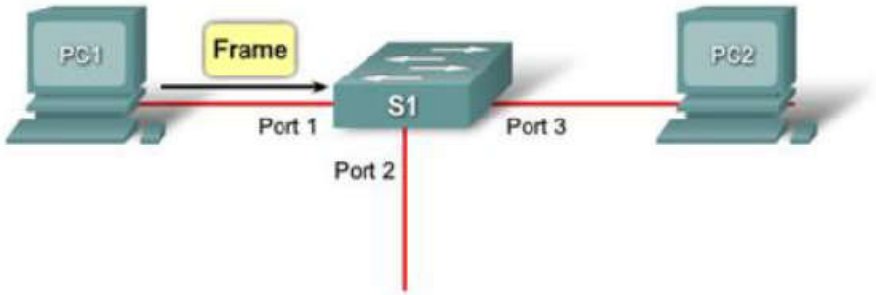
สรุป Switch MAC Address Table

1. สวิทช์ได้รับ broadcast frame จาก PC 1 พอร์ต 1

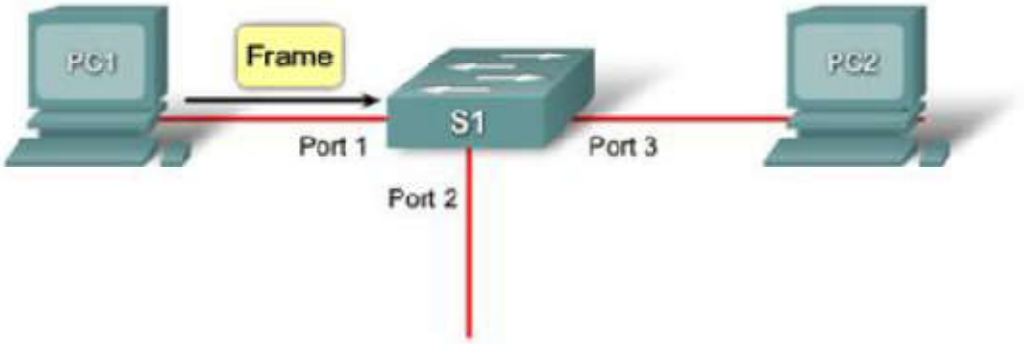
2. สวิทช์นำที่อยู่ MAC ต้นทาง และหมายเลขพอร์ตสวิทช์ที่ได้รับเฟรมลงในตารางที่อยู่

3. เพราะที่อยู่ปลายทางคือ broadcast สวิทช์ส่งจึงเฟรมไปยังทุกพอร์ต(floods) ยกเว้นพอร์ตที่ได้รับเฟรม

4. อุปกรณ์ปลายทางตอบกลับการ broadcast ด้วยที่อยู่ unicast เฟรมไปยัง PC1



Switch MAC Address Table



5. สวิทช์นำ MAC Address ต้นทาง ของ PC2 และหมายเลขพอร์ตของสวิตช์ที่ได้รับเฟรม ลงในตารางที่อยู่ ซึ่งที่อยู่ปลายทางของเฟรมและพอร์ตที่เกี่ยวข้อง จะปรากฏในตาราง MAC Address

6. สวิทช์สามารถส่งต่อเฟรม ระหว่างอุปกรณ์ต้นทางและอุปกรณ์ปลายทางโดยไม่ต้อง flood เพราะมีรายการในตารางที่อยู่ที่พร้อมพอร์ตที่เกี่ยวข้อง

ประเภทของการประมวลผลเฟรมภายในของสวิตช์

- Store and Forward
- Cut Through (Fast Forward)
- Fragment Free (Modified Cut Through)

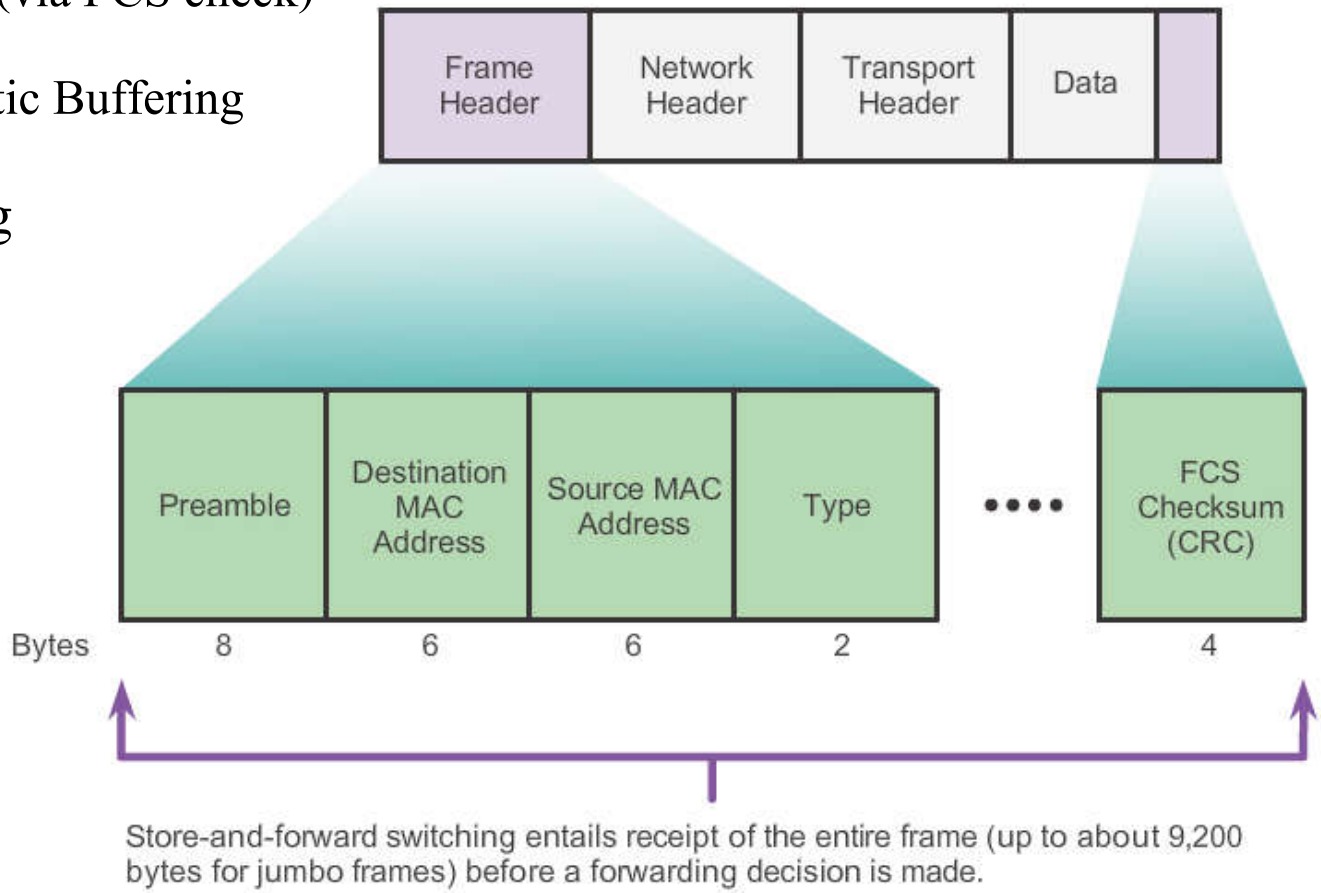
Store and Forward

A store-and-forward switch receives the entire frame, and computes the CRC. If the CRC is valid, the switch looks up the destination address, which determines the outgoing interface. The frame is then forwarded out the correct port.

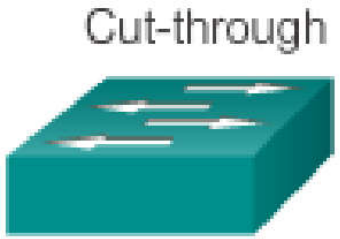
- สวิตช์จะรอจนกระทั่งได้รับเฟรมทั้งเฟรมเข้ามาก่อนจึงค่อยตัดสินใจว่าจะส่งผ่านเฟรมออกไปทางพอร์ตไหน
- เพื่อให้สวิตช์ได้มีโอกาสได้ตรวจเช็คความสมมูรณ์ของบิตข้อมูลจากฟิลด์ FCS(Fcheck Sequence) ก่อนที่จะพิจารณาส่งต่อไปยังปลายทาง
- วิธีนี้เป็นวิธีที่ดีที่สุด แต่ช้าที่สุด เนื่องจากมันจะต้องเสียเวลาในการรับเฟรมเข้ามาทั้งเฟรมเสียก่อน

Store-and-Forward Switching

- Store-and-Forwarding allows the switch to:
  - Check for errors (via FCS check)
  - Perform Automatic Buffering
- Slower forwarding



Cut-through Switching



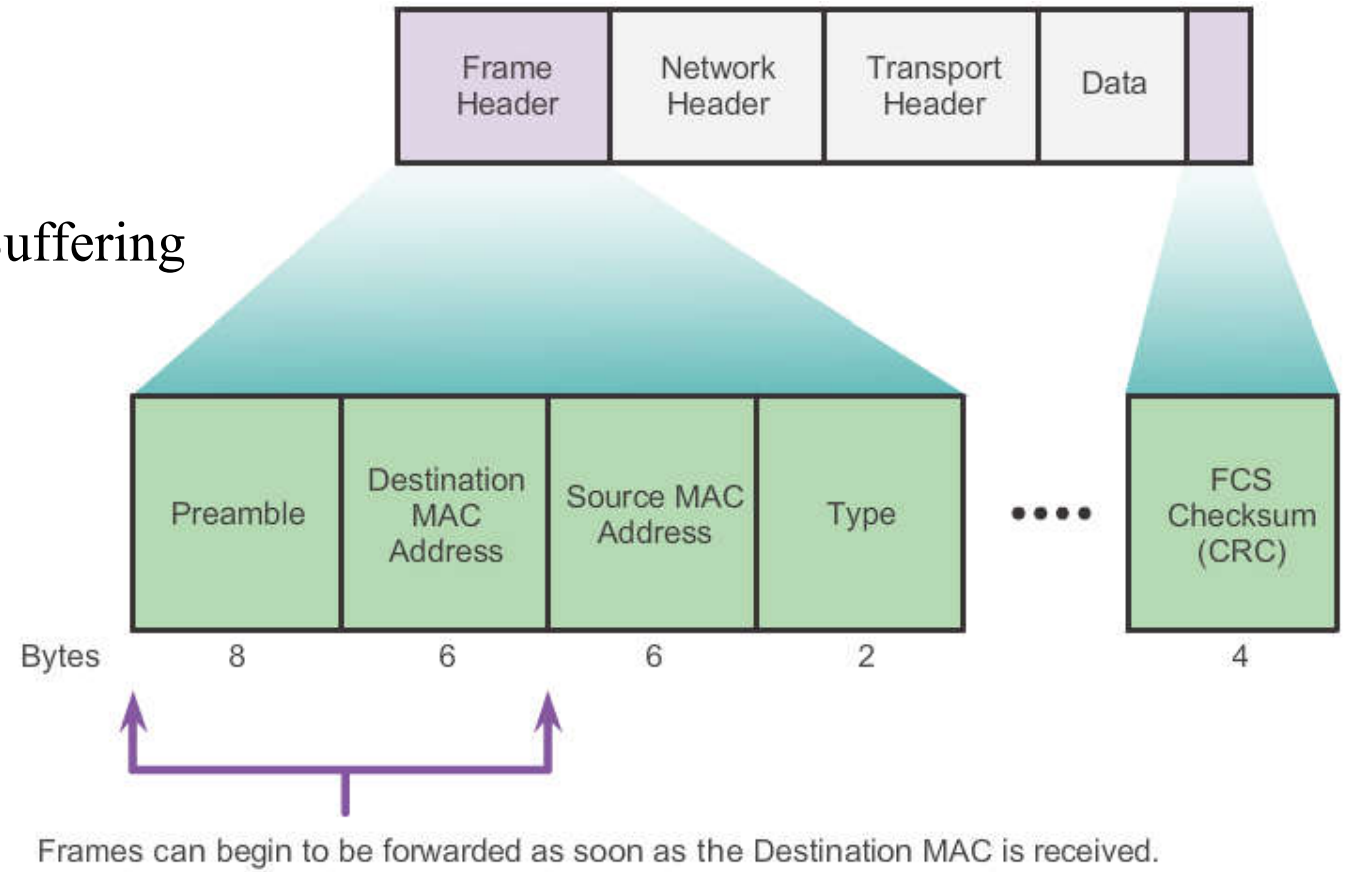
A cut-through switch forwards the frame before it is entirely received. At a minimum, the destination address of the frame must be read before the frame can be forwarded.

- เมื่อสวิตช์ได้รับเฟรมเข้ามาเพียงแค่ส่วนเฮดเดอร์(header) ก็จะรีบอ่านดูว่าหมายเลข MAC Address ปลายทาง เบอร์อะไรและตัดสินใจว่าจะส่งผ่านเฟรมออกไปทางพอร์ตไหน
- เมื่อตัดสินได้ก็จะส่งเฟรมออกไปในทันทีโดยไม่รอให้ได้รับเนื้อหาของเฟรมที่ครบถ้วนทั้งเฟรมเข้ามาก่อน

- ข้อดี ให้ความเร็วเพิ่มขึ้นอีกเล็กน้อยในการส่งผ่านเฟรม
- ข้อเสีย สวิตช์อาจปล่อยผ่านเฟรมที่ไม่สมบูรณ์ออกไปได้ เพราะฟิลด์ส่วนที่ทำการตรวจเช็คความสมบูรณ์ของบิตข้อมูล ที่เรียกว่า Frame Check Sequence (FCS) ถูกเก็บอยู่ที่ส่วนท้าย (trailer) ของเฟรม

Cut-Through Switching

- Cut-Through allows the switch to start forwarding in about 10 microseconds
- No FCS check
- No Automatic Buffering



Fragment Free (Modified Cut Through)

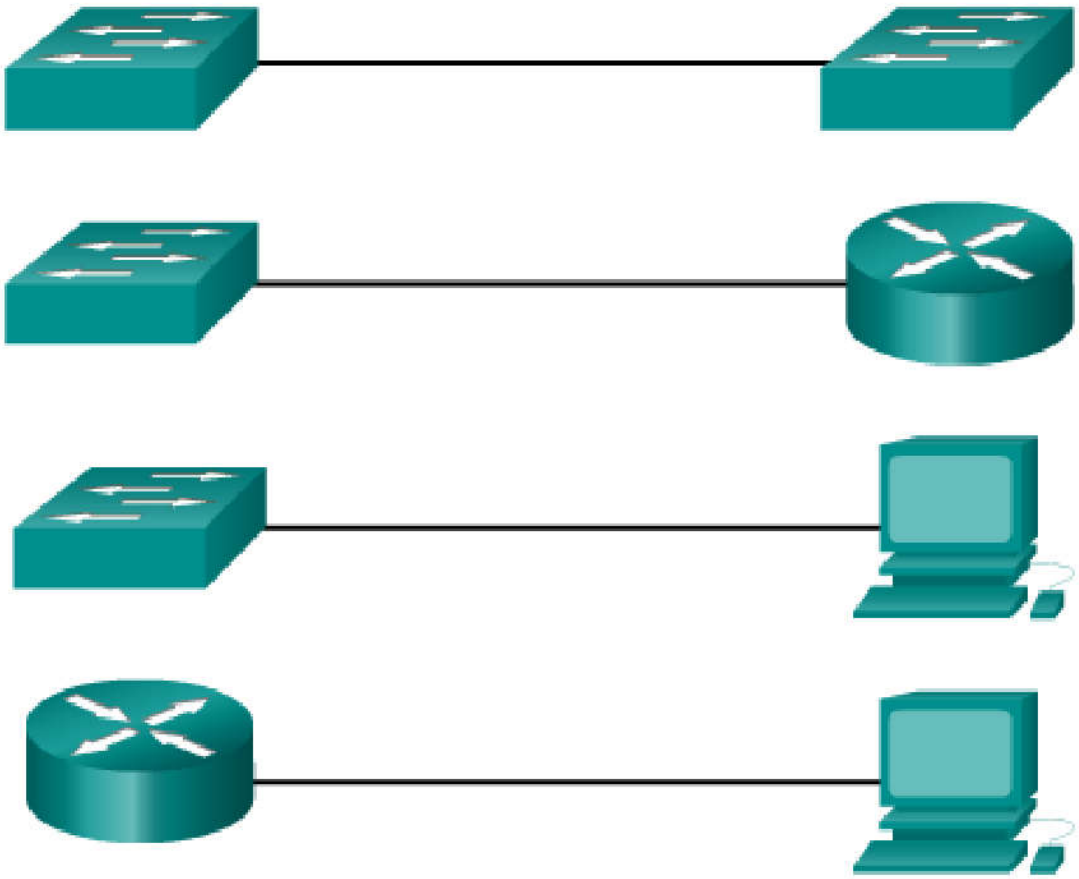
- จะคล้ายๆกับแบบ Cut-through คือมีการส่งผ่านเฟรมโดยที่ไม่จำเป็นต้องรอให้ได้รับเนื้อหาของเฟรมครบถ้วนก่อน
- แต่พยายามลดข้อผิดพลาดในการส่งเฟรมที่ไม่สมบูรณ์ออกไปโดยอาศัย หลักความจริงที่ว่าอัลกอริทึมของ CSMA/CD จะสามารถตรวจจับได้ว่ามีการชน (collision) เกิดขึ้นภายในช่วง 64 ไบต์แรกของเฟรมข้อมูล
- การประมวลผลแบบ Fragment-free จึงรอให้ได้รับเฟรมเข้ามาอย่างน้อย 64ไบต์แรกก่อนแล้วจึงค่อยตัดสินใจว่าจะส่งเฟรมออกไปทางไหน
- เมื่อตัดสินใจได้แล้วก็จะส่งเฟรมออกไปทางพอร์ตที่เหมาะสมทันที
- การประมวลผลแบบนี้ถึงแม้จะช้ากว่าแบบCut-throughแต่มันก็จะให้ความเร็วที่ดีกว่าแบบ Store-and-Forward

Frame Forwarding Methods on Switches

- ด้วยประสิทธิภาพในการประมวลผลที่สูงมากของ ASIC และสวิตช์รุ่นใหม่ ประกอบกับความเร็วของเน็ตเวิร์กที่เพิ่มขึ้นอย่างมากจาก 10 ไปอยู่ที่ 100 และไปถึงระดับกิกะบิต (1000Mbps) หรือสูงกว่า
- จึงทำให้สวิตช์ไม่จำเป็นต้องย่นระยะเวลาการประมวลผลและส่งผ่านเฟรมด้วยวิธีการแบบ Cut-through และ Fragment-free อีกต่อไป
- สวิตช์ส่วนใหญ่ในปัจจุบันจึงมักประมวลผลด้วยวิธีการแบบ Store-and-Forward ตามปกติ
- แต่อย่างไรก็ดีคงต้องศึกษาจากคู่มือเฉพาะของแต่ละรุ่นอีกครั้งว่ามันประมวลผลในลักษณะใด

Auto-MDIX

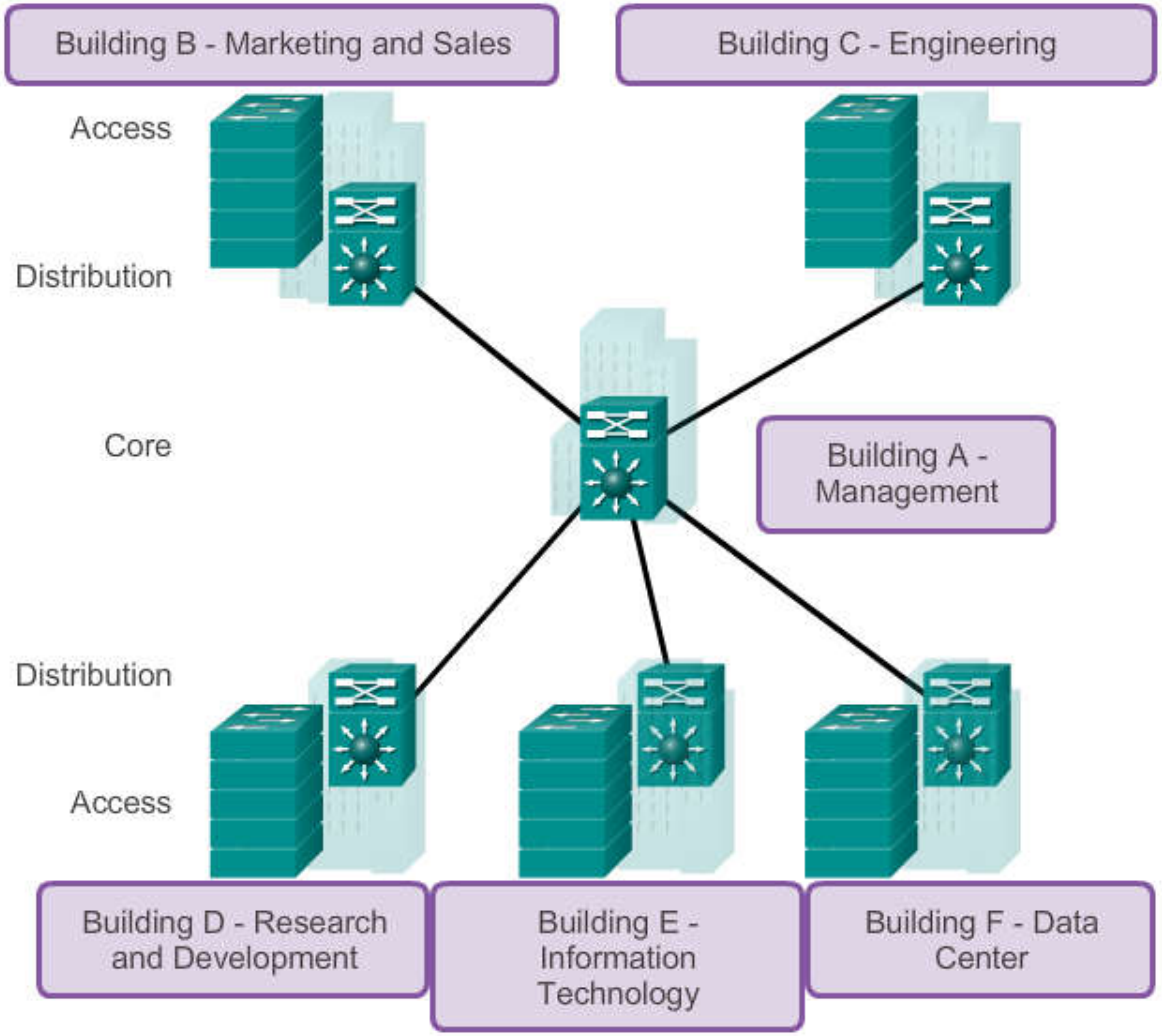
MDIX auto detects the type of connection required and configures the interface accordingly



Memory Buffering on Switches

Port-based memory	In port-based memory buffering, frames are stored in queues that are linked to specific incoming and outgoing ports.
Shared memory	Shared memory buffering deposits all frames into a common memory buffer, which all the ports on the switch share.

Core, Distribution, Access



หน้าที่ของ Switched Networks

- บทบาทของเครือข่ายสวิทซ์มีการพัฒนาอย่างต่อเนื่อง
- LAN สวิทช์ ช่วยให้การจัดการจราจรในเครือข่ายได้ง่ายและ มีความยืดหยุ่นมากขึ้น
- นอกจากนี้ยังรองรับคุณสมบัติต่างๆ เช่น คุณภาพของการให้บริการ (quality of service) การรักษาความปลอดภัยเพิ่มที่มากขึ้น การสนับสนุนเครือข่ายไร้สาย สนับสนุนโทรศัพท์แบบ IP และบริการที่แบบเคลื่อนที่

Form Factor

- Fixed

Features and options are limited to those that originally come with the switch.

Form Factor

- Modular

The chassis accepts line cards that contain th
ports.

Form Factor

- Stackable

Stackable switches, connected by a special cable, effectively operate as one large switch.

Fixed verses Modular Configuration

Switch Form Factors

Fixed Configuration Switches

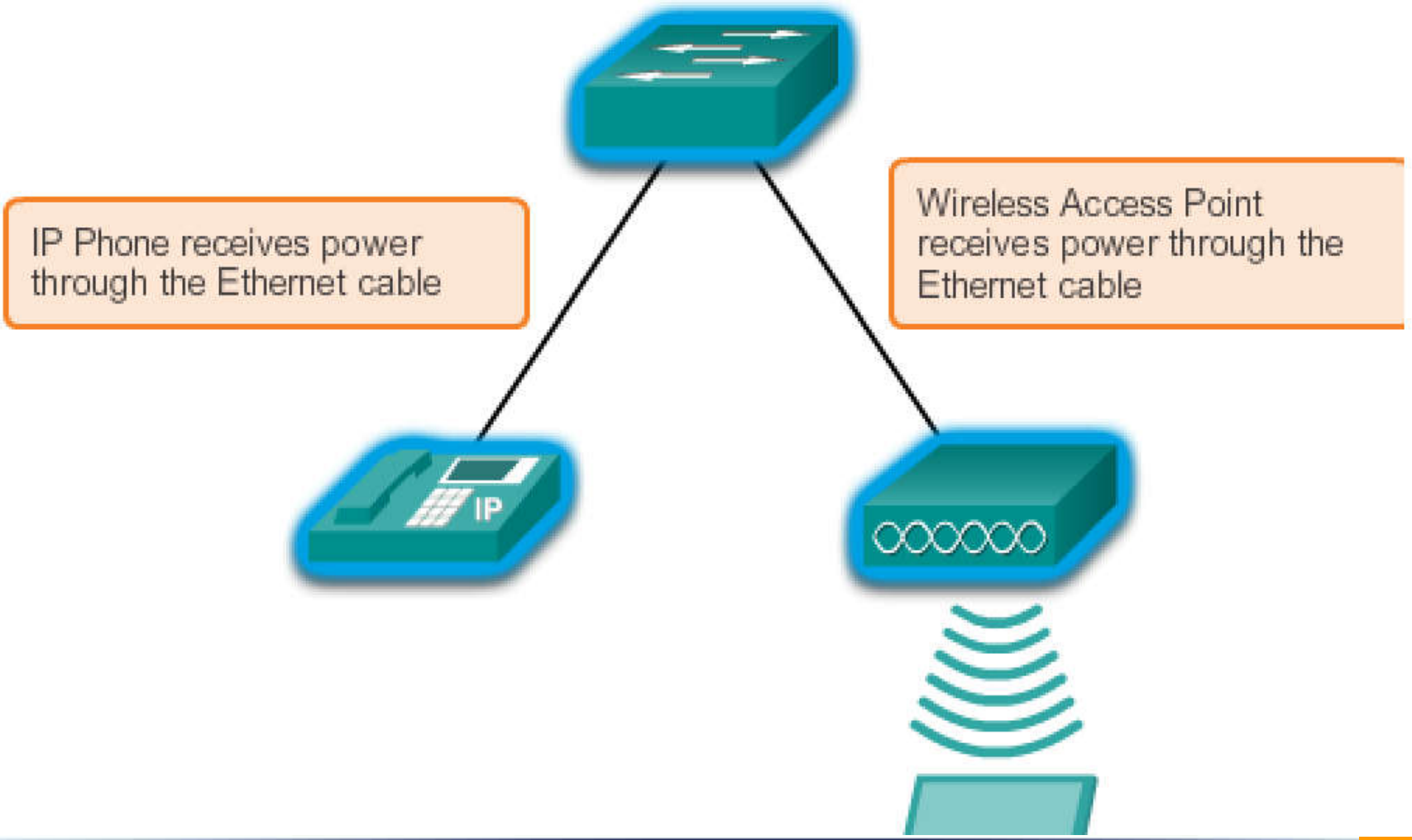
Features and options are limited to those that originally come with the switch.

Modular Configuration Switches

The chassis accepts line cards that contain the ports.

Stackable Configuration Switches

POE (Power Over Ethernet)



Module Options for Cisco Switch Slots

Cisco optical Gigabit Ethernet SFP

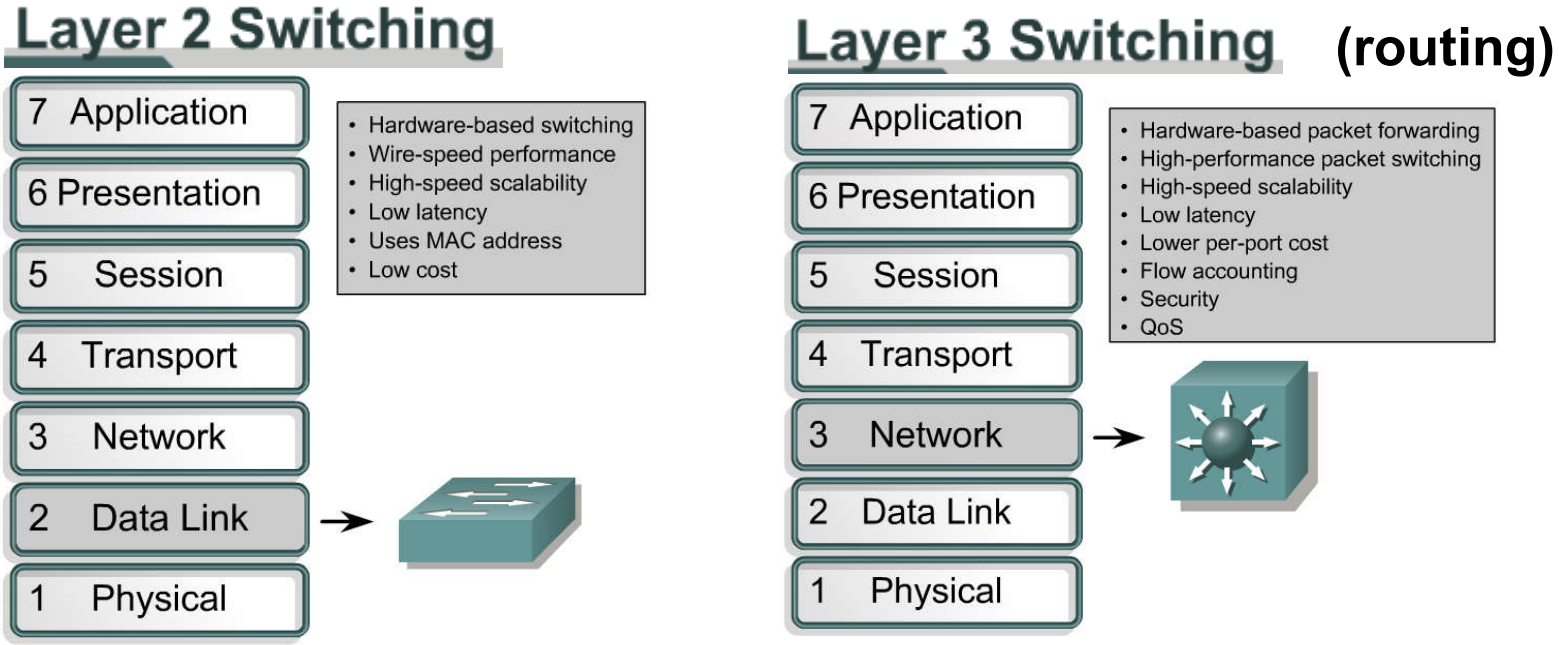
Cisco 1000BASE-T Copper SFP

Cisco 2-channel 1000BASE-BX optical SFP

เลเยอร์ 3 สวิตช์ (Layer 3 Switch)

- สวิตช์บางประเภทสามารถรองรับการทำงานที่เลเยอร์ที่ 3 ได้ ซึ่งอุปกรณ์เครือข่ายที่ทำงานในเลเยอร์นี้จะรู้จักในชื่อ “เราท์เตอร์ (Router)”
- แต่เลเยอร์ 3 สวิตช์หมายถึงอุปกรณ์เครือข่ายที่ทำหน้าที่ทั้งในเลเยอร์ที่ 2 และเลเยอร์ที่ 3
- ข้อแตกต่างระหว่างเลเยอร์ 3 สวิตช์และเราท์เตอร์อย่างคือ สวิตช์ใช้เทคโนโลยีที่เรียกว่า “ASIC (Application Specific Integrated Circuit)” หรือเป็นวงจรควบคุมที่สร้างสำหรับทำสวิตช์โดยเฉพาะ การหาเส้นทางการทำงานของสวิตช์ก็จะเร็วกว่าเราท์เตอร์มาก

Layer 2 and layer 3 switching



- A layer 3 switch is typically a layer 2 switch that includes a routing process, I.e. does routing. (Oh yea, also known as routing. Got to love those people in Marketing.)
- Layer 3 switching has many meanings and in many cases is just a marketing term.
- Layer 3 switching is a function of the network layer.
- The Layer 3 header information is examined and the packet is forwarded based on the IP address.

- สวิตช์เลเยอร์ 3 สามารถวิเคราะห์ข้อมูลเพื่อประกอบการตัดสินใจในการส่งผ่านแพ็กเกตสูงถึงเลเยอร์ที่ 3 เช่น เลเยอร์ของ IP
- ด้วยการค้นหาและเปรียบเทียบซับเน็ตแอดเดรสปลายทางจากตารางหาเส้นทาง (routing table) เพื่อเลือกหาเส้นทางที่ดีที่สุดในการส่งแพ็กเก็ตออกไปยังปลายทาง
- นอกจากนั้นยังสามารถรันเร้าติ้งโปรโตคอลต่างๆ เช่น RIP, EIGRP เหมือนกับเร้าเตอรทั่วๆ ไปได้
- สวิตช์เลเยอร์ 3 สามารถในการทำงานได้ทั้งเลเยอร์ 2 และเลเยอร์ 3 ด้วยพร้อมๆ กัน ขึ้นอยู่กับผู้ติดตั้งว่าจะอีนาเบิลฟีเจอร์ในเลเยอร์ 3 ขึ้นมาทำงานหรือไม่ (แต่ส่วนใหญ่แล้วมักจะอีนาเบิลขึ้นมา) ส่วนสวิตซ์เลเยอร์2 นั้นก็ทำงานได้เฉพาะแค่เลเยอร์ 2 เท่านั้น

เทคนิคที่ทำให้สวิตช์มีความสามารถถึงระดับเลเยอร์ 3

- ขึ้นอยู่กับผู้ผลิตอุปกรณ์สวิตช์ว่าจะเลือกใช้แนวทางใด สำหรับของชิสโก้ก็ขึ้นอยู่กับรุ่นและโมเดลของสวิตช์ด้วย ตัวอย่างเช่น
- สำหรับชิสโก้สวิตช์รุ่นใหญ่ที่เป็นลักษณะแบบ Chassis Based ที่มีสลอตโมดูล (slot module) ไว้ สำหรับเสียบไลน์การ์ด (Line Card) เทคนิคในการทำให้ทำงานที่เลเยอร์ 3 อาจได้แก่ การเพิ่มการ์ดพิเศษซึ่งอาจเป็นการ์ดลูก (daughter card) เข้าไปบนการ์ดประมวลผลหลัก การ์ดลูกดังกล่าวนี้มีความสามารถในการวิเคราะห์แพ็กเก็ตที่เลเยอร์ 3 และทำงานได้คล้ายๆ กับเป็น “เร้าเตอร์” ตัวเล็กๆทำงานอยู่ภายในสวิตช์อย่างเช่น การ์ด Multilayer Switch Feature Card (MSFC) บนชิสโก้สวิตช์ในตระกูล 6500

- สำหรับชิสโก้สวิตช์รุ่นปานกลางที่ไม่ใช่แบบ Chassis Based คือเป็นแบบกล่องฮาร์ดแวร์กล่องหนึ่งที่มีพอร์ต UTP อยู่ด้านหน้าและหน่วยประมวลผลต่างๆ อยู่ภายในตัวเลย โดยไม่ต้องใส่ Line Card แยกต่างหาก เทคนิคในการทำให้ทำงานที่เลเยอร์ที่ 3 ได้ ได้แก่ การปรับปรุงซอฟต์แวร์ระบบปฏิบัติการภายในที่ทำงานอยู่ภายในสวิตช์ให้เป็นแบบ “Enhanced Image”คือมีความสามารถขั้นสูงในการทำงานที่เลเยอร์ 3 ได้โดยตรงนอกเหนือจากเลเยอร์ 2 ปกติ ตัวอย่างของสวิตชรุ่นปานกลางที่ไม่ใช่ Chassis Based ที่สามารถทำงานที่เลเยอร์ 3 ได้แก่ ซิสโก้สวิตช์รุ่น 3750, 3550 เป็นต้น

Router กับ สวิตช์เลเยอร์3

- เร้าเตอร์(router) ยังคงเป็นอุปกรณ์หลักในการเชื่อมต่อเน็ตเวิร์กระหว่างมากกว่าหนึ่งสาขาผ่าน WAN อยู่
- เร้าเตอร์มีอินเตอร์เฟซต่างๆ ที่เหมาะสมและจำเป็นสำหรับการเชื่อมต่อเข้าหาเครือข่าย WAN มากกว่าสวิตช์เลเยอร์3 (แม้ว่าในปัจจุบันจะมี Line Card พิเศษบนสวิตช์เลเยอร์3 ที่สามารถทำให้มันเชื่อมต่อ WAN โดยตรงก็ตาม)
- อีกหน้าหนึ่งที่สำคัญของเร้าเตอร์ก็คือ การเชื่อมต่อและเร้าต์ (route) แพ็กเก็ตออกไปยังอินเทอร์เน็ต

Router กับ สวิตช์เลเยอร์3

- สวิตช์เลเยอร์ 3 เป็นอุปกรณ์ที่เหมาะสมและให้ความยืดหยุ่นที่ดีกว่า สำหรับการทำหน้าที่เป็นเสมือน "Core Router” ไปพร้อมๆ กับการทำหน้าที่เป็น “Core Switch” (สวิตช์ที่เป็นหัวใจหลักศูนย์กลางของเน็ตเวิร์ก LAN)
- ในการแบ่งเป็น VLAN ย่อยๆ จำเป็นต้องมีอุปกรณ์ในเลเยอร์ 3 สำหรับทำหน้าที่เร้าต์แพ็กเก็ตระหว่างเครื่องคอมพิวเตอร์ที่อยู่ต่าง VLAN กัน ซึ่งมี 2 ทางเลือกได้แก่
  - ใช้เร้าเตอร์ภายนอก หรือ
  - ใช้งานสวิตช์เลเยอร์3 (layer 3 switch)
  - ซึ่งให้ผลเหมือนกัน แต่ส่วนใหญ่สวิตช์เลเยอร์3 นั้นมักถูกเลือกมาทำหน้าที่นี้ เพราะสวิตช์รุ่นใหญ่ๆ ที่มีฟีเจอร์ของเลเยอร์ 3 ปกติจะทำหน้าที่เป็น “CORE SWITCH” ของเน็ตเวิร์ก LAN อยู่แล้ว เพิ่มความสามารถในการเร้าต์ระหว่าง VLANได้ทันทีโดยไม่ต้องเปลืองงบประมาณในการจัดหาเร้าเตอร์ตัว ใหม่

Router กับ สวิตช์เลเยอร์3

- สวิตช์เลเยอร์ 3 มีข้อดีด้านการรองรับการเชื่อมต่อบน LAN เพราะเลือกประเภทของพอร์ตได้ เช่น เลือกได้ว่าเป็นพอร์ต UTP แบบ 10 / 100 / 1000 หรือเป็น Gigabit Ethernet ที่วิ่งบนสาย UTP หรือเป็น Gigabit แบบไฟเบอร์ออปติก
- ที่สำคัญก็คือ จำนวนพอร์ตมีปริมาณมาก เริ่มต้นที่ 12 พอร์ต หรือ 24 พอร์ต สำหรับรุ่นใหญ่นั้นสามารถใส่ Line Card เพื่อเพิ่มจำนวนพอร์ตที่ต่อ LAN ได้มากขึ้นไปอีกเช่น 48 พอร์ต ในกรณีของพอร์ตต่อ LAN นี้ สวิตซ์เลเยอร์ 3 มีความได้เปรียบเหนือกว่าเร้าเตอร์เพราะเร้าเตอร์ส่วนใหญ่จะมีพอร์ตเชื่อมต่อ LAN ไม่มากนัก เช่น ซิสโก้เร้าเตอร์ในตระกูล 2600 ก็จะมีพอร์ต LAN (fast ethernet) อยู่ในหลักหน่วยเช่น 2 พอร์ต

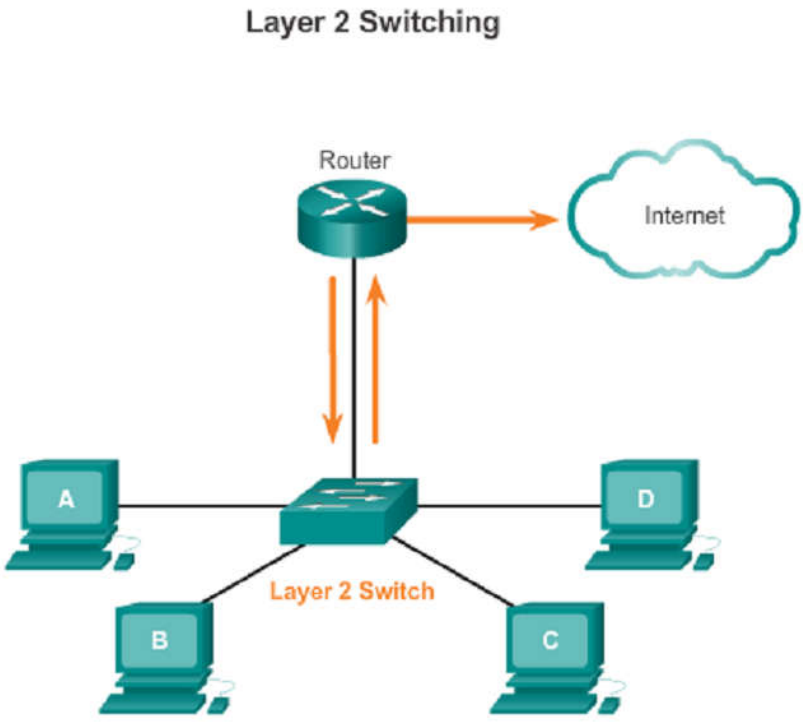
Router กับ สวิตช์เลเยอร์3

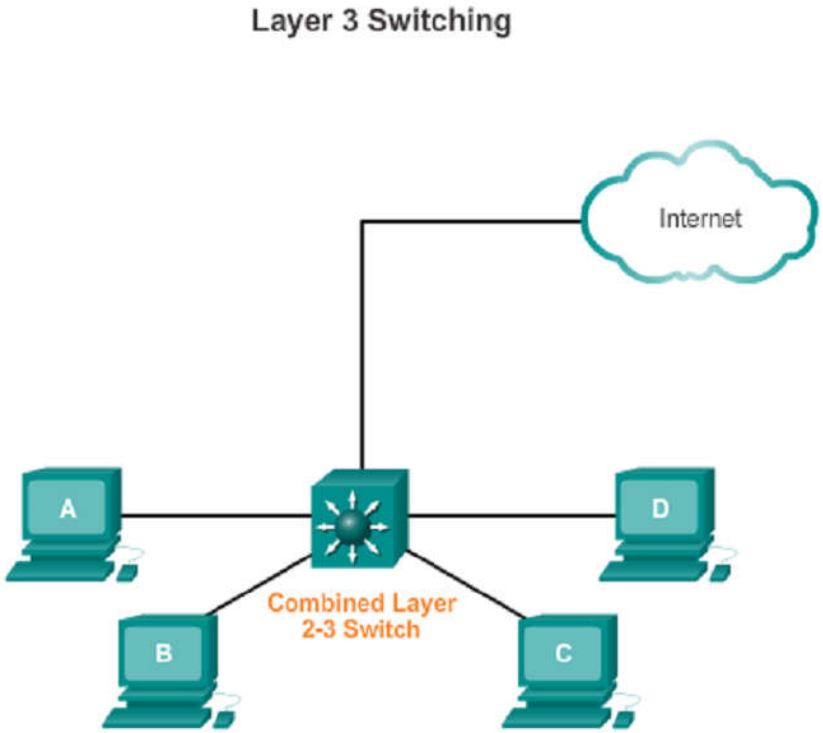
- ความเร็วในการส่งผ่านเฟรม โดยทั่วไปสวิตซ์เลเยอร์ 3 จะใช้ฮาร์ดแวร์พิเศษ ASIC เพื่อส่งผ่านเฟรม ให้อัตราความเร็วและปริมาณแพกเก็ตต่อหนึ่งวินาทีที่สูงกว่าเร้าเตอร์ เร้าเตอร์(โดยทั่วไป) จะส่งผ่านแพ็กเก็ตโดยใช้การประมวลผลด้วยซอฟต์แวรปกติ (อย่าง'ไรก็ดี เร้าเตอร์รุ่นสูง (High End Router) และเร้าเตอร์รุ่นใหม่ๆ หลายรุ่นได้รับการออกแบบให้ใช้เวลาในการประมวลผลแพ็กเก็ตที่น้อยมากๆ และส่งผ่านแพ็กเก็ตได้อย่างรวดเร็วโดยอาศัยเทคนิคใหม่ๆ หลายอย่าง

Layer 3 switching vs Router

Feature	Layer 3 Switch	Router
Layer 3 Routing	Supported	Supported
Traffic Management	Supported	Supported
WIC Support		Supported
Advanced Routing Protocols		Supported
Wirespeed routing	Supported	

Layer 2 verses Layer 3 Switching





Types of Layer 3 Interfaces

Layer 3 interfaces มี 3 ชนิดหลักๆ คือ:

- **Switch Virtual Interface (SVI)** – เป็นพอร์ตเสมือนบนสวิทต์ ซึ่งจะเกี่ยวของกับ virtual local area network (VLAN).
- **Routed Port** – เป็นพอร์ตจริงๆ ทางกายภาพบน Layer 3 switch กำหนดให้มีหน้าที่เป็นเราเตอร์พอร์ต โดยวางอินเตอร์เฟสให้เป็น Layer 3 mode ด้วยคำสั่ง **no switchport**
- **Layer 3 EtherChannel** – เป็นอินเตอร์เฟสทางตรรกะบนอุปกรณ์ Cisco เป็นการรวม Physical