ICT 4010 Data and Communication Networks

Lecture 8

Switches, Routers & VLAN

Phyela Mbewe
LIS Department
University of Zambia

September 2023

Network Interface Cards (NICs)

- **NIC:**
  - Connectivity component (common to every networking device)
  - Includes a transceiver
    - Transmits and receives data
  - Operates at the Physical and Data Link layer
    - Assemble and disassemble data frames
    - Interpret physical addressing information
    - Determines if a host can transmit data

Also known as network interface controller

NIC connection

How NICs are connected:

- Expansion card
  - could be plugged into a computer port or router

- Expansion slots on the motherboard
  - Circuit board for additional devices (such as NIC, sound card etc.)
  - NIC is inserted into expansion slot
  - *modern NICs are built into the computer motherboard*

NIC connection

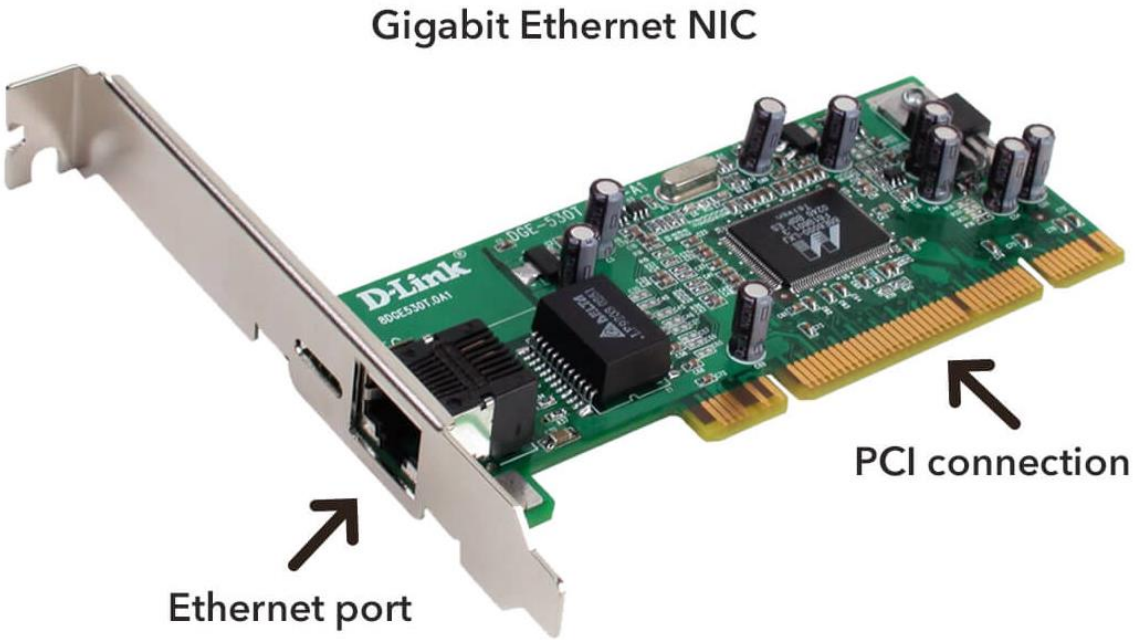
PCI Expansion slot

- The most common form of internal expansion for a PC.
- Some PCs have a mixture of PCI and PCI Express slots.
  - PCI Express is recommended

NIC connection

- Peripheral Component Interconnect Express (PCIe)
  - an interface standard for connecting **high-speed** components.
  - Every desktop PC motherboard has a number of PCIe slots
    - can be use to add GPUs, RAID cards, Wi-Fi cards, NIC, SSD add-on cards etc.

NIC connection



NIC connection

- Externally attached NICs
  - Simple installation into a variety of slots
  - Installing and configuring software may be required

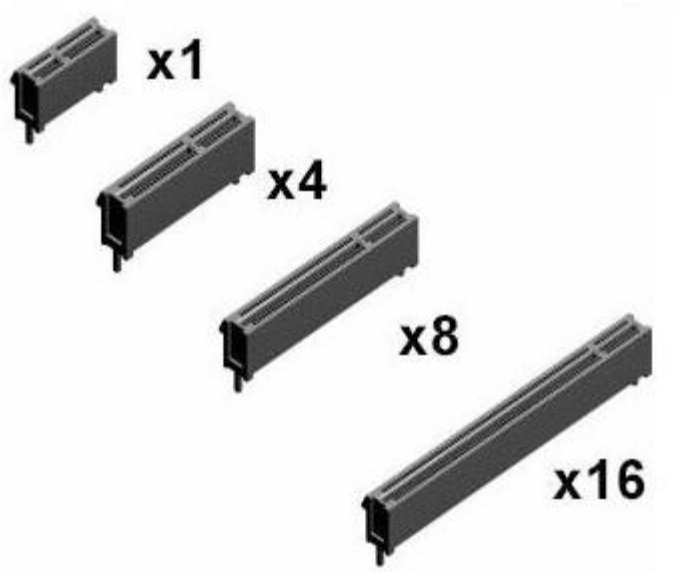
- On-Board NICs
  - Connect device directly to motherboard
  - Advantages
    - Saves space
    - Frees expansion slots

NIC connection

External NIC
also referred to as a USB NIC

NIC connection – PCIe slots

- PCIe slots, 5 physical sizes:
  - x1, x4, x8, x16, x32.
    - The number after the x indicates how many lanes (how data travels to and from the PCIe card) that PCIe slot has.
    - A PCIe x1 slot has one lane and can move data at one bit per cycle
    - A PCIe x2 slot has two lanes and can move data at two bits per cycle (speed of the cpu)



PCIe Generations

	Bandwidth
PCIe 1.0	8 GB/s
PCIe 2.0	16 GB/s
PCIe 3.0	32 GB/s
PCIe 4.0	64 GB/s
PCIe 5.0	128 GB/s
PCIe 6.0	256 GB/s

Repeaters and Hubs

- Repeaters
  - Operate in Physical OSI model layer
  - Do not interpret data
  - Just regenerates signal

- Hub
  - Repeater with more than one output port
  - Typically contains multiple data ports
    - connects printers, servers, and workstations

Bridges

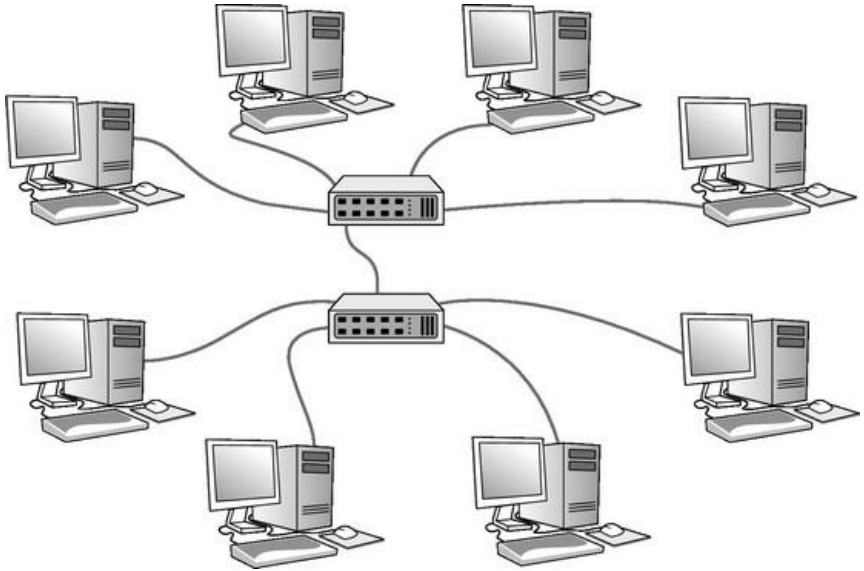
- Device that connect two network segments
- Operate at Data Link OSI layer
- Single input and single output ports
- Analyze incoming frames and makes decisions on where to direct them based on the destination MAC address
- Includes a filtering database
  - Contains known MAC addresses and network locations
- *Not common anymore*

Switches

- Connectivity devices that subdivide a network into segments
- Traditional switches
  - Operate at Data Link OSI model layer
- Modern switches
  - Can operate at Layer 3 or Layer 4 (which blurs line between switches and routers)
- Switches interpret MAC address information (just like bridge)
- A switch can handle many ports
  - Bridge has only 2 ports.

Switches

- Switching:
  - the process of channeling data received from any number of input ports to another designated port that will transmit the data to its desired destination.



Switches

- Advantages
  - Better performance and security compare to network bridges
  - intelligent device which maintains its forwarding table to forward data frames, Hubs do not maintain forwarding tables
    - *(note: bridges also maintain forwarding tables as such this is an advantage compared to hubs)*

- Disadvantages
  - Can be overwhelmed by heavy traffic
  - More expensive compare to network bridges
  - Proper design and configuration is needed in order to handle multicast packets

Switches

- Switching Modes:
  - Cut-through mode
  - Store-and-forward mode

Switching Modes

- Cut-through mode
  - Switch reads frame's header only
  - Forwarding decision is made before receiving the entire packet
    - Uses frame header: first 14 bytes which contains the destination MAC address
  - Cannot verify data integrity using frame
    - Cannot detect corrupt packets

Switching Modes

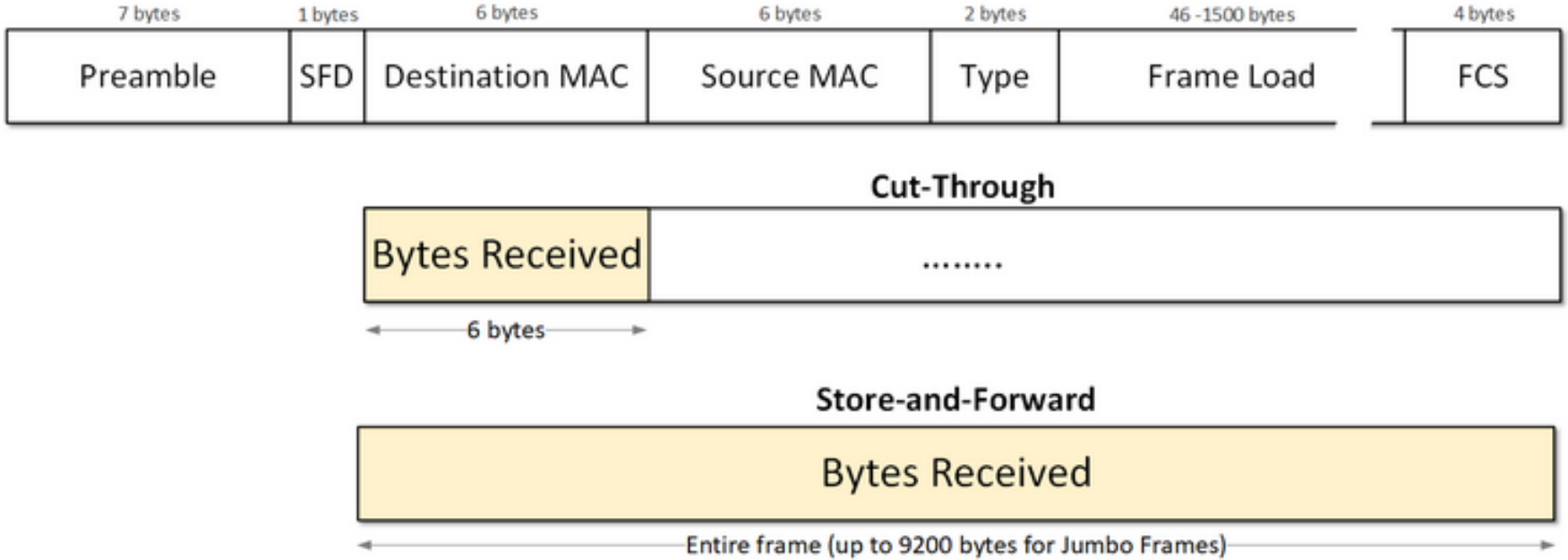
- Cut-through mode (cont'd.)
  - Advantage:
    - Speed
  - Disadvantage
    - Data buffering (switch flooded with traffic)
    - Cannot verify data integrity
  - Best use
    - Small workgroups needing speed
    - Low number of devices

Switching Modes

- Store-and-forward mode
  - Switch reads entire data frame into memory
  - Checks for accuracy before transmitting information (frame check)
  - Transmit data more accurately than cut-through mode
  - Slower than cut-through mode
  - Best uses
    - Larger LAN environments
  - Can transfer data between segments running different transmission speeds

Switching Modes

Switching modes illustration



***exercise** find out more on SFD and FCS of a frame (data unit)

Switching Modes

- Both switching modes base their forwarding decisions on the destination MAC address of the Ethernet frames.

- They also learn MAC addresses and build their MAC tables as they examine the source MAC address (SMAC) fields in the Ethernet header as frames are being forwarded.

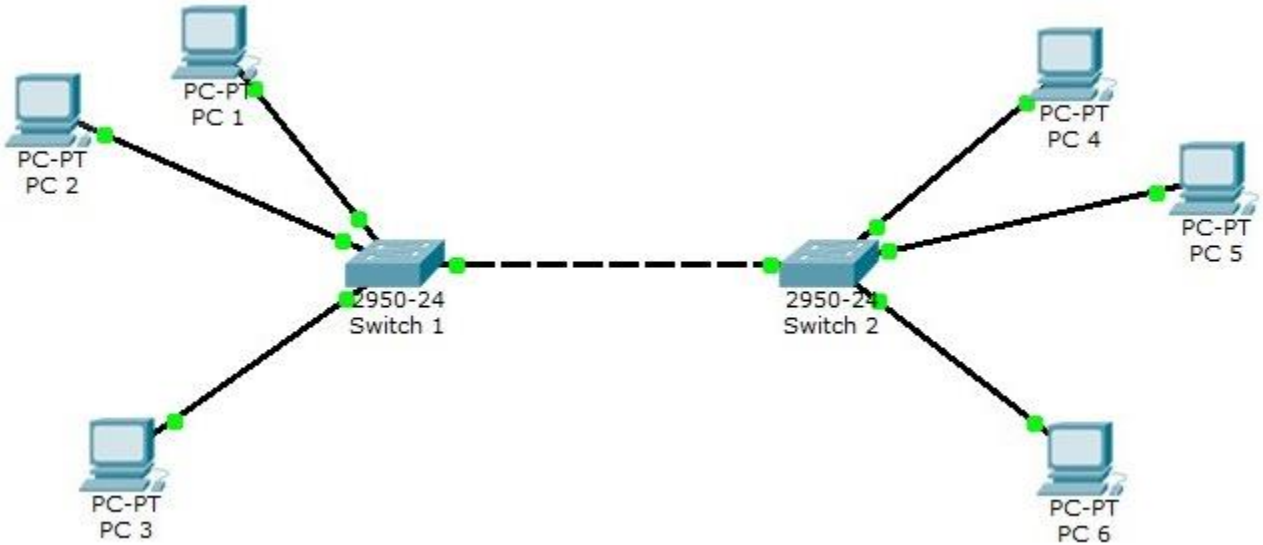
- **These switching modes differ in how much of the frame must be received and examined by the switch before the frame start being forwarded out**

VLANs

- VLANs (virtual local area networks)
  - Concept of partitioning a physical network
  - Logically separated networks, not physical
    - VLANs Group ports into separate broadcast domains
- Broadcast domain:
  - All nodes can reach each other by a broadcast message
- Collision domain
  - Data packets can collide with one another when being sent on a shared medium

VLANs

illustration of 2 VLANs via 2 Switches



VLAN 1

VLAN 2

VLANs

- VLAN Advantage
  - Flexible
    - Ports from multiple switches or segments can be grouped
      - i.e. ports (interfaces) for VLAN 1 will have their own broadcast domain and ports for VLAN 2 will have their own broadcast domain
    - Any end node type (PCs, printers) can belong to VLAN
  - Reasons for using VLANs
    - Separating user groups
    - Isolating connections
    - Identifying priority device groups
    - Grouping legacy protocol devices / older devices
    - Separating large networks into smaller divided networks

VLANs

- Switches are typically preconfigured with one VLAN:
  - **There is one default VLAN (named VLAN 1)**
  - **Cannot be deleted or renamed**

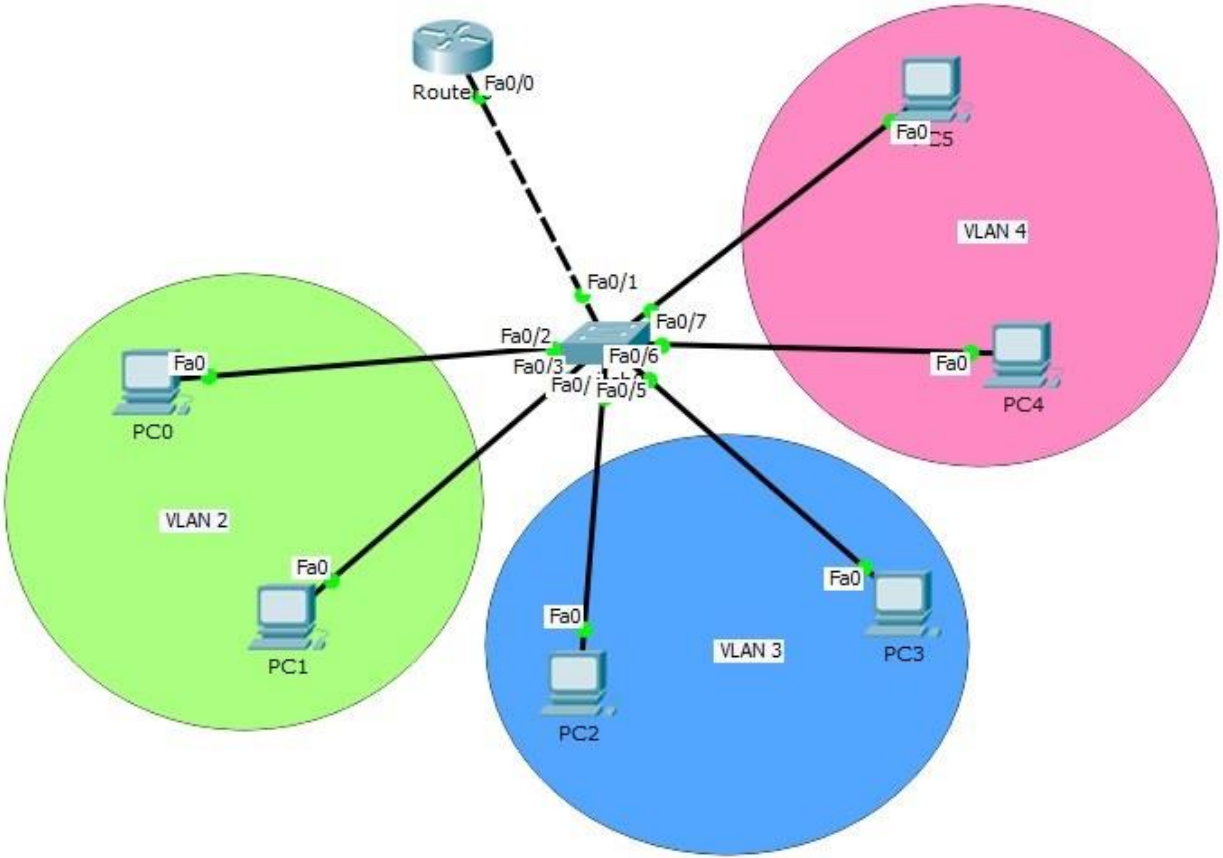
- Users *(managing the switches)* can create additional VLANs
  - Users can Indicate the VLAN each port belongs

- VLAN are maintained using switch software

- Dividing potential problems:
  - VLANs can be used to cutting off groups from rest of the network

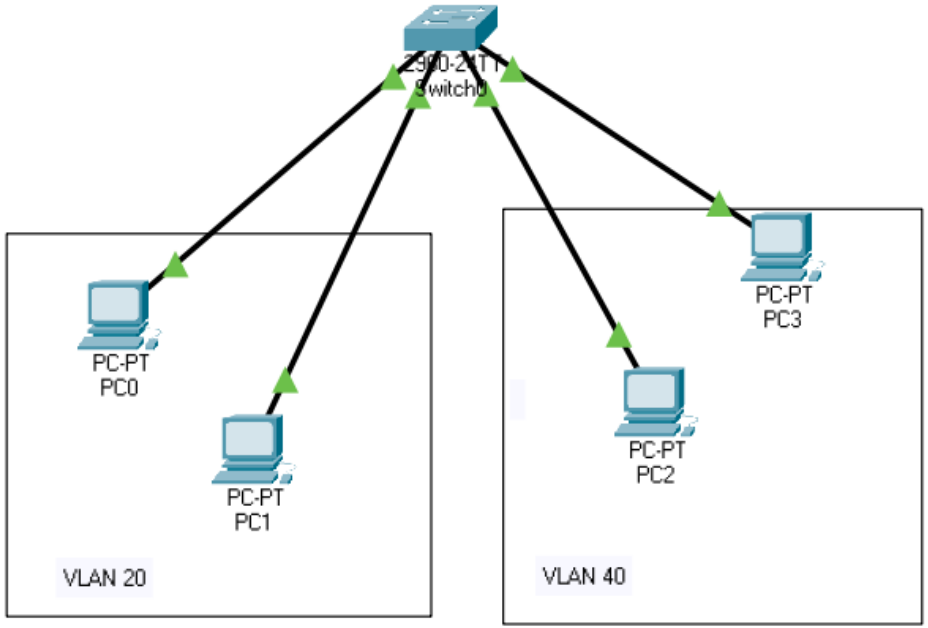
VLANs

illustration of multiple VLANs via 1 switch with grouped interfaces (ports)



Creating 2 VLANs – Basic Switch Commands

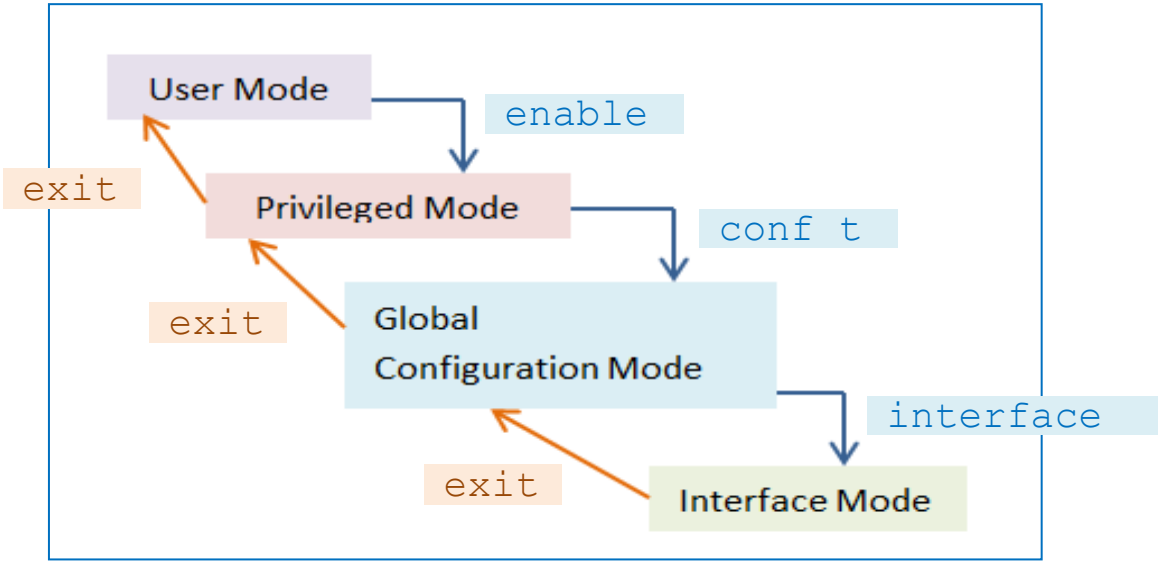
- Creating 2 VLANs through basic switch commands, objectives:
  - Setting up 2 VLANs through switch commands, *within packet tracer*
    - Grouping interfaces (ports) together to form VLANs
    - *(the same commands can be used on real switch operating systems beyond packet tracer)*



Creating 2 VLANs– exit command

- **Exit command and Switch Modes**

Note that switches (Cisco / Packet Tracer) will utilize commands similar to the routers: The `exit` command can be used to return to a previous mode within a switch



Creating 2 VLANs

- **Show vlan** command
  - shows all the ports associated with a VLAN

syntax:
`show vlan`

  - When in *Privileged Mode*
    - Type and enter `show vlan` to display available vlans

```
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa
                                                Fa0/5, Fa0/6, Fa0/7, Fa
                                                Fa0/9, Fa0/10, Fa0/11,
                                                Fa0/13, Fa0/14, Fa0/15,
                                                Fa0/17, Fa0/18, Fa0/19,
                                                Fa0/21, Fa0/22, Fa0/23,
                                                Gig0/1, Gig0/2
1002 fddi-default                     active
```

Creating 2 VLANs

- **Switchport access vlan** command
  - assigns an interface (or range of interfaces) to a VLAN
  - used when in *Interface Mode (for a specific interface)*

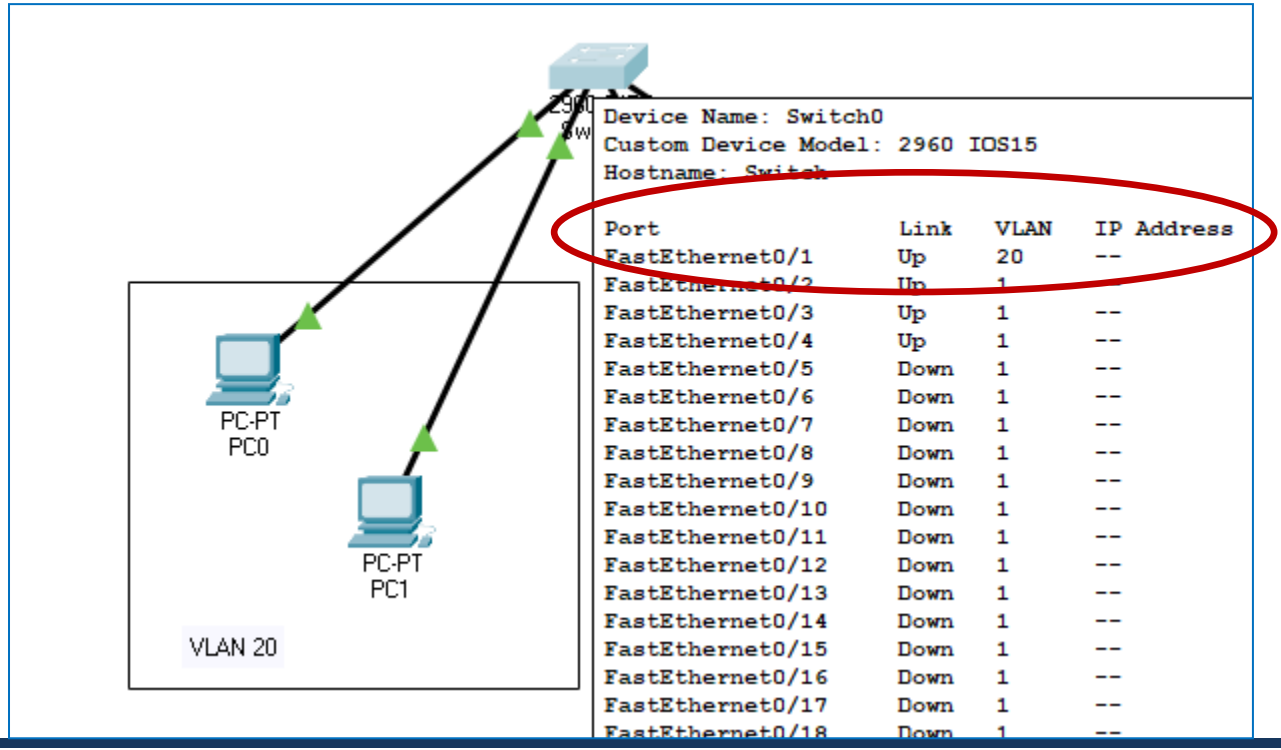
syntax:
`switchport access vlan` `vlan_id`

```
Switch>en
Switch#config t
Enter configuration commands, one per line.  End
Switch(config)#interface Fa0/1
Switch(config-if)#switchport access vlan 20
% Access VLAN does not exist. Creating vlan 20
Switch(config-if)#exit
Switch(config)#
```

Creating 2 VLANs

- **Switchport access vlan** command (cont.)

Interface Fa0/1 will now be assigned to VLAN 20



Creating 2 VLANs

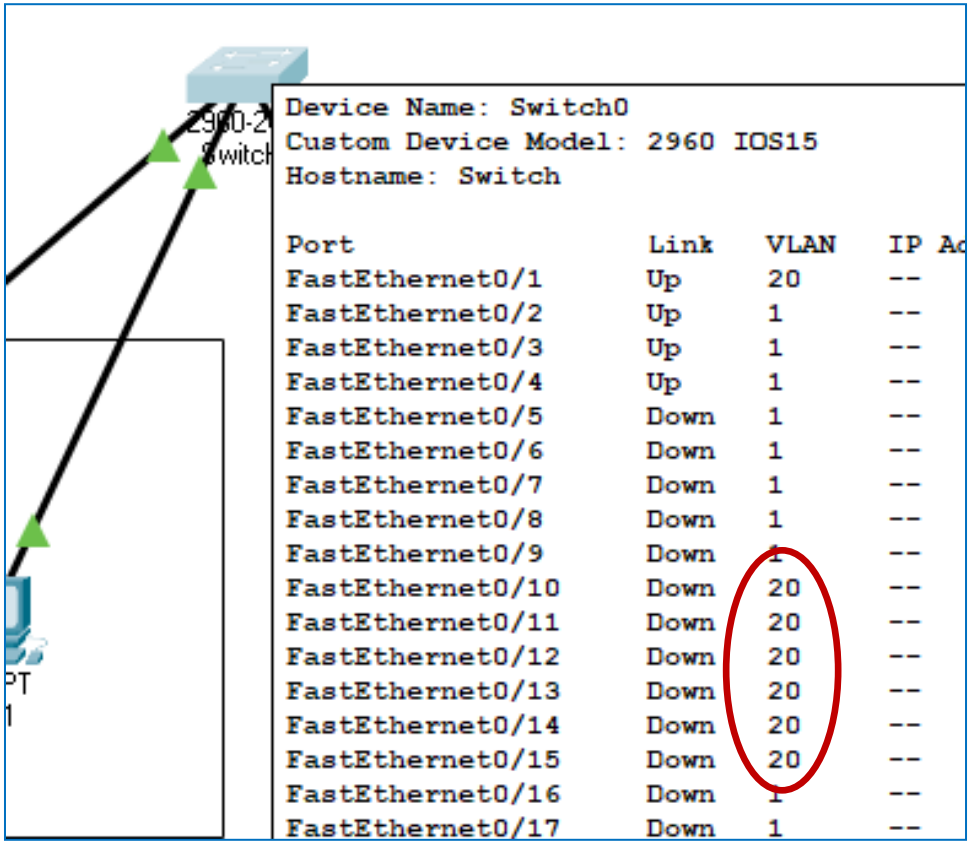
- **Switchport access vlan** command (cont.)
  - can also be used for a range of interfaces, assigning multiple interfaces to a VLAN

```
Switch(config)#
Switch(config)#interface range Fa0/10-15
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#exit
Switch(config)#
```

Creating 2 VLANs

- **Switchport access vlan** command (cont.)

Interfaces Fa0/10 up to Fa0/15 will now be assigned to VLAN 20



Creating 2 VLANs

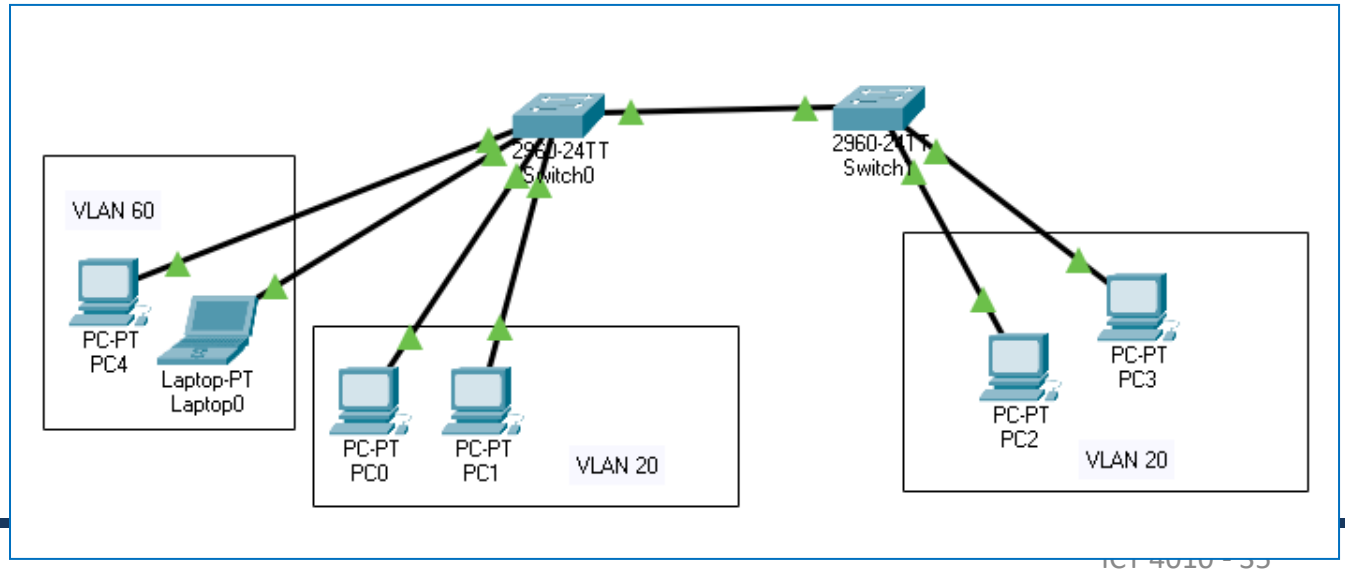
- **No switchport access vlan** command
  - assigns an interface (or range of interfaces) to the default VLAN, which is VLAN 1
  - used when in ***Interface Mode*** *(for a specific interface or range of interfaces)*

syntax:

```
no switchport access vlan
```

Creating VLANs - Trunking

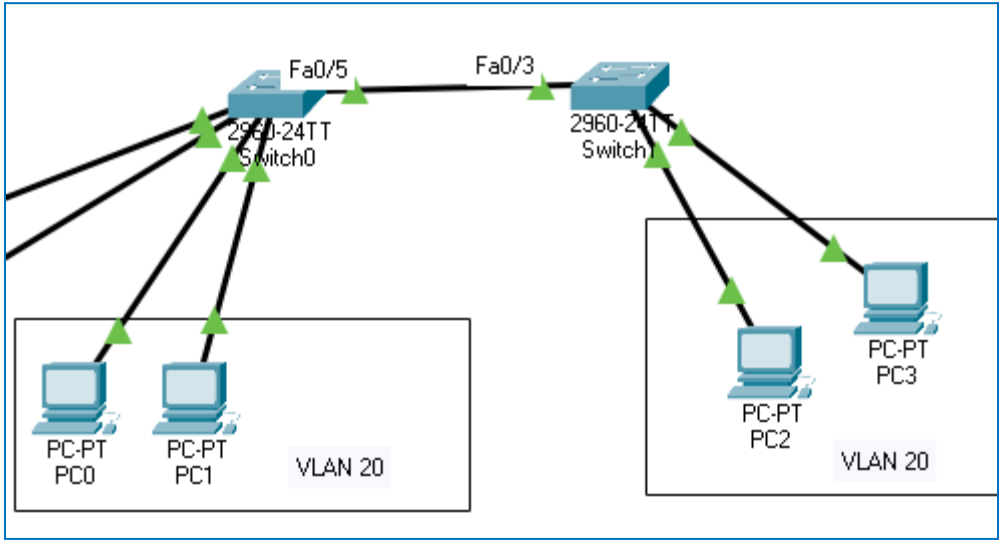
- VLANs on one switch will have no connection to VLANs on another switch **even if the VLANs have the same VLAN ID**, without a **trunk port**
  - e.g. the broadcast domain for VLAN 20 on Switch0 (below) will only include PC0 and PC1
  - However the connection(cable) between the switches can be configured as a **trunk port**, this will allow all devices in VLAN 20 to be in the same broadcast domain **across multiple switches**



Creating VLANs - Trunking

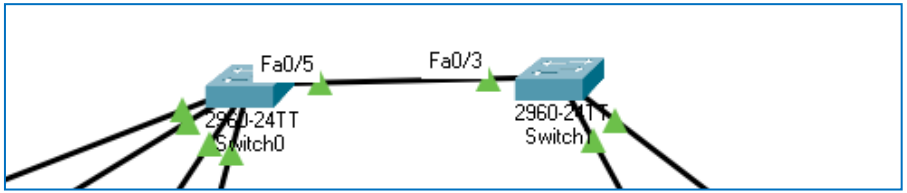
- **Trunk port:**
  - A port (interface) on a switch that allows data to flow across the network linking multiple VLANs
    - Allows for VLANs across multiple switches to be in the same broadcast domain whereby the VLANs have the same VLAN ID

***Exercise**: find out the Switch command that can be used for Switch0's Fa0/5 interface and Switch1's Fa0/3 interface which will set the interfaces as **trunk ports**



Creating VLANs - Trunking

- **Trunking and tagging:**
  - When a **frame** (data unit) is sent over a trunk port, the frame will include extra data referred to as a VLAN tag, this tag indicates the VLAN the frame is to be sent to
    - Frames sent from a switch to a switch, over a trunk port, will **include** a VLAN tag
    - Frames sent from a switch to an end device (access port) will **not include** a VLAN tag, any existing VLAN tag will be removed by the switch before the frame is forwarded
    - The switches control the addition and removal of VLAN tags from frames depending on:
      - if the frame is being sent over a *trunk port* or over an *access port*



VLAN and Subnet Differences

VLANs	Subnetting
VLAN is a logical local area network that contains broadcasts only for hosts that belong to that specific VLAN. Can create logical networks across multiple physical networks	Subnet is an IP address range that helps hosts communicate over OSI Layer 3. *Creates logical networks within the same physical network*
Hosts on a VLAN can have a greater geographical distance (than subnet devices)	Hosts are typically limited in geographical distance by the location of switches and routers connecting the subnet hosts
VLAN is an OSI Layer 2 term whereby MAC addresses (and frames) are utilized with switches	Subnet is an OSI Layer 3 term whereby packets are utilized with routers

VLAN and Subnet Differences

VLANs	Subnetting
Primary advantage of VLANs is that the can separate or control the broadcast domain	Primary advantage of Subnetting is to control network communication across hosts in the same IP subnet. When other subnets go down or have technical failures, a subnet is not affected.
VLANs are set through configuring interfaces on Switches	Subnetting is achieved based on IP addresses that are assigned to network hosts

Network managers can use a combination of both **Subnetting and VLANs** when designing and implementing networks

Routers

- Multiport connectivity device which Integrates LANs and WANs
- Operate at Network layer (Layer 3)
  - Directs data between network nodes from one segment or network to another
  - Uses logical addressing, Protocol dependent
- Slower than switches and bridges
  - Need to interpret Layers 3 information
- Traditional stand-alone LAN routers
  - Being replaced by **Layer 3 switches,** which have routing capabilities

Router Characteristics and Functions

- Intelligence
  - Determine shortest, fastest path between two nodes
  - Connects dissimilar network types
- Connecting Large LANs and WANs
- Routing capabilities
  - Interpret Layer 3 addressing
  - Determine best data path
  - Reroute traffic

Router Types

- Interior router
  - Directs data between nodes on a LAN
- Exterior router
  - Directs data between nodes external to a LAN
- Border routers
  - Connect autonomous LAN with a WAN

Routing Types

- Static routing
  - Router configured to use specific path between nodes
- Dynamic routing
  - Automatically calculates best path between nodes

Routing Tables

- Routing tables (database)
  - Maintain information of where hosts are and how to reach them

Routing Protocols

- How to decide on best path:
  - Path is decided by routing protocol

- Routing factors used to determine the best path
  - Number of hops
  - Transmission speed
  - Delay on a potential path - Current network activity
  - Maximum transmission unit (MTU)
  - Reliability of potential path
  - Cost (assigned by an administrator)

Routing Protocols

- Distance vector protocols
  - Distance vector protocols can measure the distance, called **hops**, it takes data to arrive at its destination within a system or application.
  - The number of hops:
    - refers to the specific number of routers the data may run through before reaching its ultimate destination.

- 3 Distance vector protocols:
  - RIP (Routing Information Protocol)
  - RIPv2 (Routing Information Protocol version 2)
  - BGP (Border Gateway Protocol)

Router Protocols

- Link State Protocols
  - Link state protocols find the best routing path and share information with nearby routers.
    - they calculate the speed and the cost of resources associated with each potential path.
    - they apply algorithms and alert other routers when pathways have changed.
- 2 Link State Protocols:
  - OSPF (Open Shortest Path First)
  - IS-IS (Intermediate System to Intermediate System)

Router Protocols

- Link State Protocols
  - Link state protocols can store 3 types of tables:
  - **Routing tables:**
    - stores information about the most efficient data routes
  - **Neighbor tables:**
    - stores information and details from other close routers
  - **Topology tables:**
    - stores information about the organization (structure) of entire networks
  -

Router Protocols

- BGP (Border Gateway Protocol)
  - standardized routing protocol for the Internet
    - a distance vector protocol
    - Many factors determine the best paths
    - complex algorithms
    - main protocol for Internet traffic

Router Protocols

- OSPF (Open Shortest Path First) Protocol
  - Each OSPF router maintains databases containing other routers' information
    - a link state protocol
    - Complex algorithm for determining best paths
    - Can be used with Interior routers (internal networks) or border routers (connects local/organization network to the internet)

***Exercise**: find out more about RIP, RIP 2 and IS-IS protocols compared to BGP and OSPF

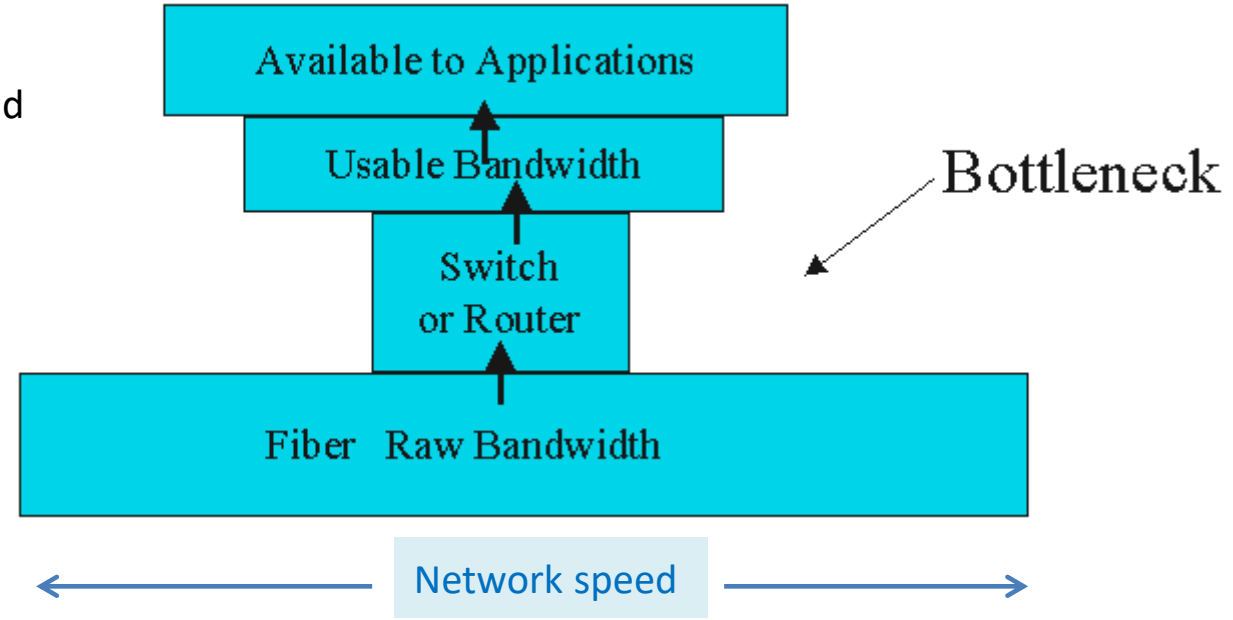
Router Protocols

- **Hybrid routing protocol:**
- **EIGRP** (Enhanced Interior Gateway Routing Protocol)
  - Uses both Link State and Distance Vector characteristics
    - Most popular of the router protocols
    - Works on Cisco network routers only
    - Supports large networks
    - Fast convergence time

- **Convergence Time:**
    - The time the router takes to recognize the best path after a network change or network outage.

Switches, Routers and Network Speed

- Note that network speeds will be restricted to the transmission rate of switches and routers
  - how much data switches and routers can forward per second



Switches, Routers and Network Speed

- **Fast Ethernet Switch:**
  - transfer rate of up to 100 Megabits per second (100 Mbps)
  - Can still be used as a desktop switch
  - works with Cat5 cables connecting to PCs, servers, routers etc.

Switches, Routers and Network Speed

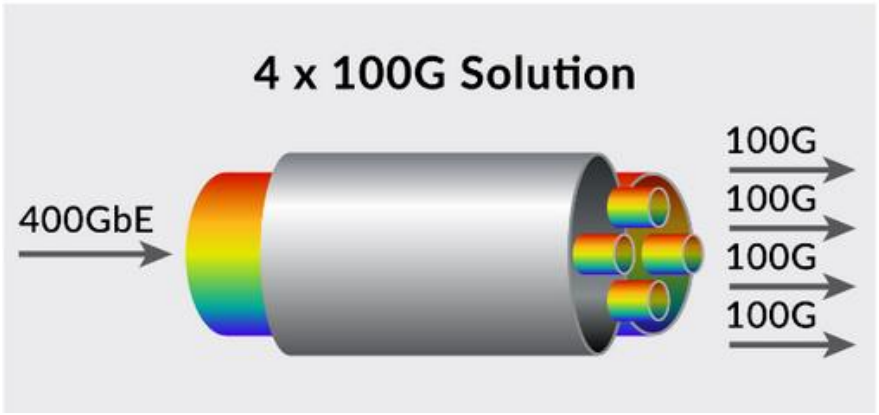
- **Gigabit Ethernet Switch:**
  - An Ethernet switch that can theoretically transfer up to 1 Gigabit per second (1 Gbps or 1000 Mbps)
  - works with cat5e and cat6 cables that follows the 1000BASE-T cabling standard

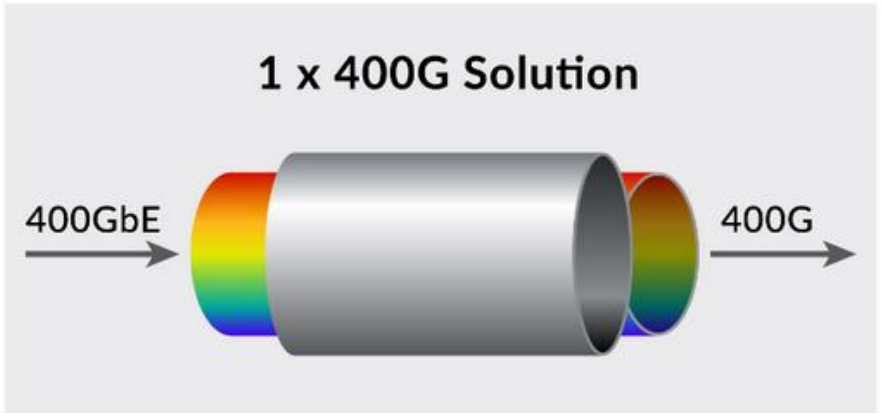
Switches, Routers and Network Speed

- **Gigabit Networks – Beyond 1 Gbps**
  - **Ethernet development** has now improved to 400G (400GBase-R networks) using fiber optical lanes / cables
    - From 1 Gbps Ethernet in 1997
    - 10 Gbps in 2004
    - 100 Gbps in 2010
    - 4-lane (4×25 Gbps) 100 Gbps in 2014
    - The IEEE officially approved its 802.3bs standard for 200G and **400G Ethernet** on December 6, 2017
  - Driven by the demands of ever-increasing Internet traffic through cloud data centers, there will always a need for more bandwidth

Switches, Routers and Network Speed

- **Gigabit Networks – Beyond 1 Gbps**
  - 4-lane (4×100 Gbps) 400 Gbps has been replaced with the IEEE **400G Ethernet** standard
  - Powerful high-end routers with a single **400G port** will support the 400G (or 400Gbps) network speeds





Switches, Routers and Network Speed

- **Gigabit Networks and Consumer restrictions**
  - Despite the faster 100 Gbps and 400 Gbps networks (as of 2021):
    - most PC motherboards come with a 2.5 Gbps port
    - high-end motherboards come with 10 Gbps ports, with a theoretical limit of 1.25 Gigabytes per second speeds, more than enough for local network environments.
    - However, there are no affordable internet connections for the average citizen to reach 10 Gbps speeds.

Switches, Routers and Network Speed

- **Gigabit Networks and Consumer restrictions**
  - Despite the faster 100 Gbps and 400 Gbps networks (as of 2021):
    - In the USA, fiber internet **service** is available to businesses almost everywhere. However, Fiber internet service for residential users is more limited, but growing.
    - The faster fiber optical networks are mostly utilized by data centers, the **Internet backbone** and specific organizations
    - Furthermore, very powerful servers will be required to manage 400 Gbps network speeds

***Exercise**: find out more about the Internet Backbone