ICT40120

CERTIFICATE IV IN INFORMATION TECHNOLOGY

VLANs

Your skills. Your future.

RTO 60142 | CRICOS 03041M

TasTAFE

Switches

Switches can be divided into two generalized groups: **Layer 2** (workgroup or access) and **Layer 3** (distribution and core).

A Layer 2 switch is used to connect devices locally and generally within the same subnet; they are fast but as they only deal with MAC address frames – fundamentally, not too smart.

Layer 3 switches can perform the same tasks as a Layer 2 switch but have the additional capability to act as a router.

This means they can deal with IP addresses and route traffic; with their increased functionality they often replace routers (in some situations).

Routers

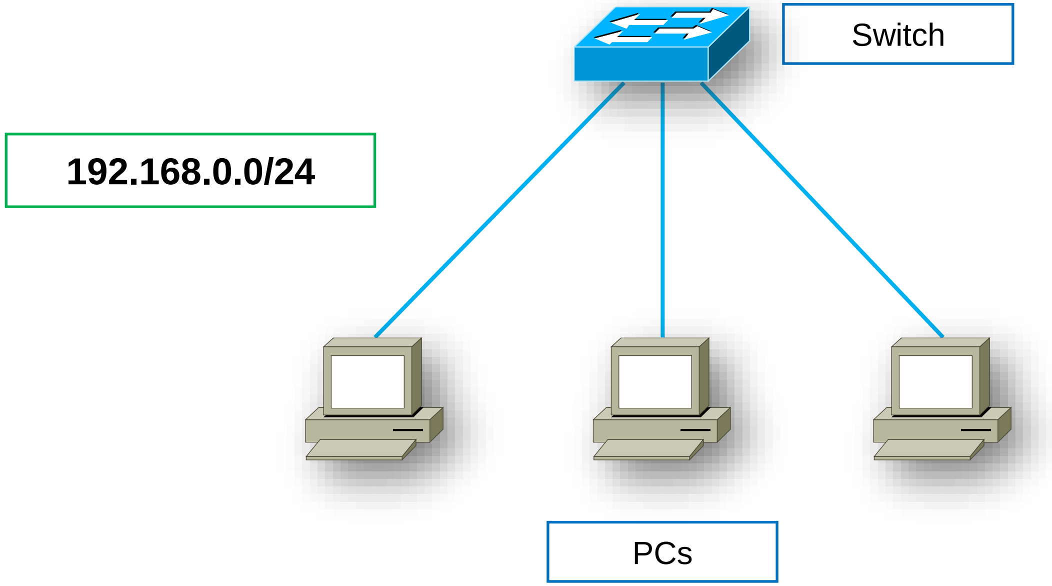
Where Layer 2 switches connect devices locally, or in a relatively small geographic area; a router can connect local networks to other networks.

Effectively routers (and Layer 3 switches) connect subnets; they are the dividing point between different networks.

Routers are slower than a switch - but smarter, they tend to have a lot more decisions to make and modern routers can perform many tasks usually associated with Layer 7 devices.

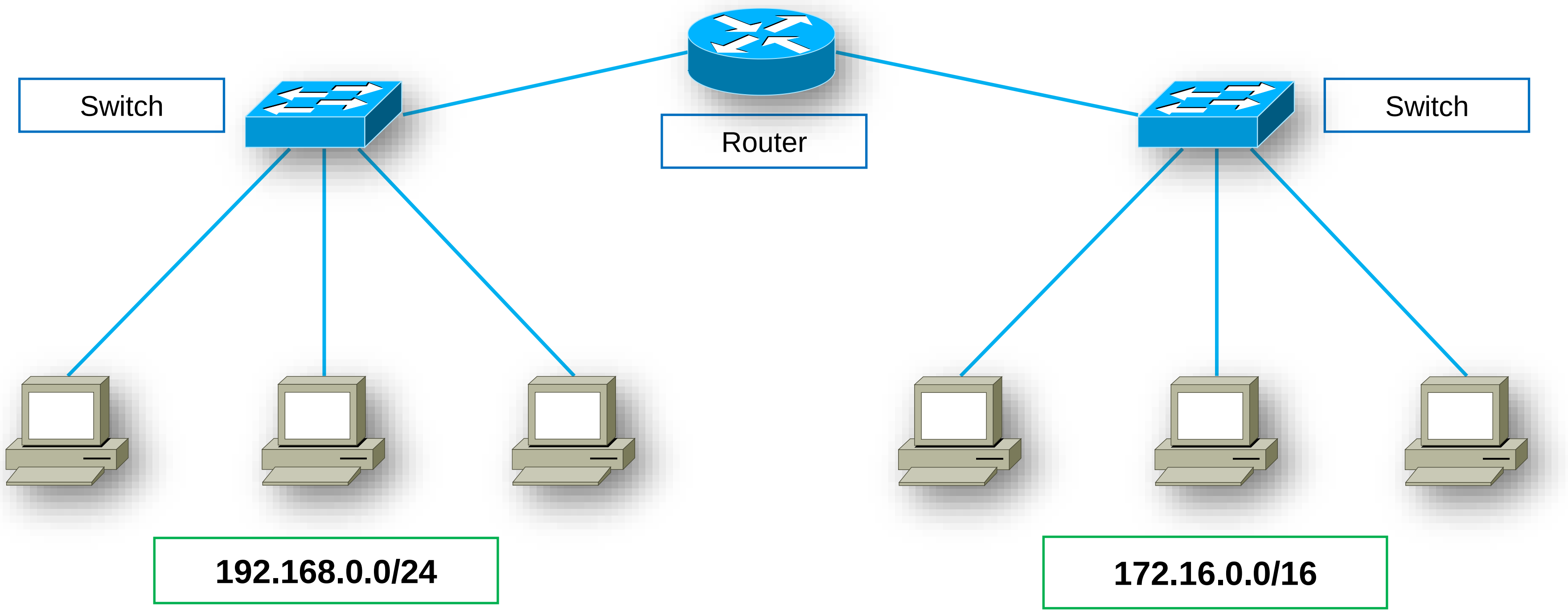
Local LAN

Networked devices - typically PCs, printers, etc connect to a switch; in a large installation usually via a patch panel and in smaller organisations directly to the switch.



Connected LANs

Wherever there is a requirement to connect different networks (subnets) you must use a router or Layer 3 switch – they understand IP addresses.



Managed

Switches can be broadly categorised as ‘managed’ or ‘unmanaged’.

Unmanaged – Also described as dumb switches (dumber than normal). You can’t log into them; they are used straight out of the box ‘as is’.

Managed – These can be logged into and configured. They are more expensive but allow much greater control.

CISCO

JUNIPER NETWORKS

hp

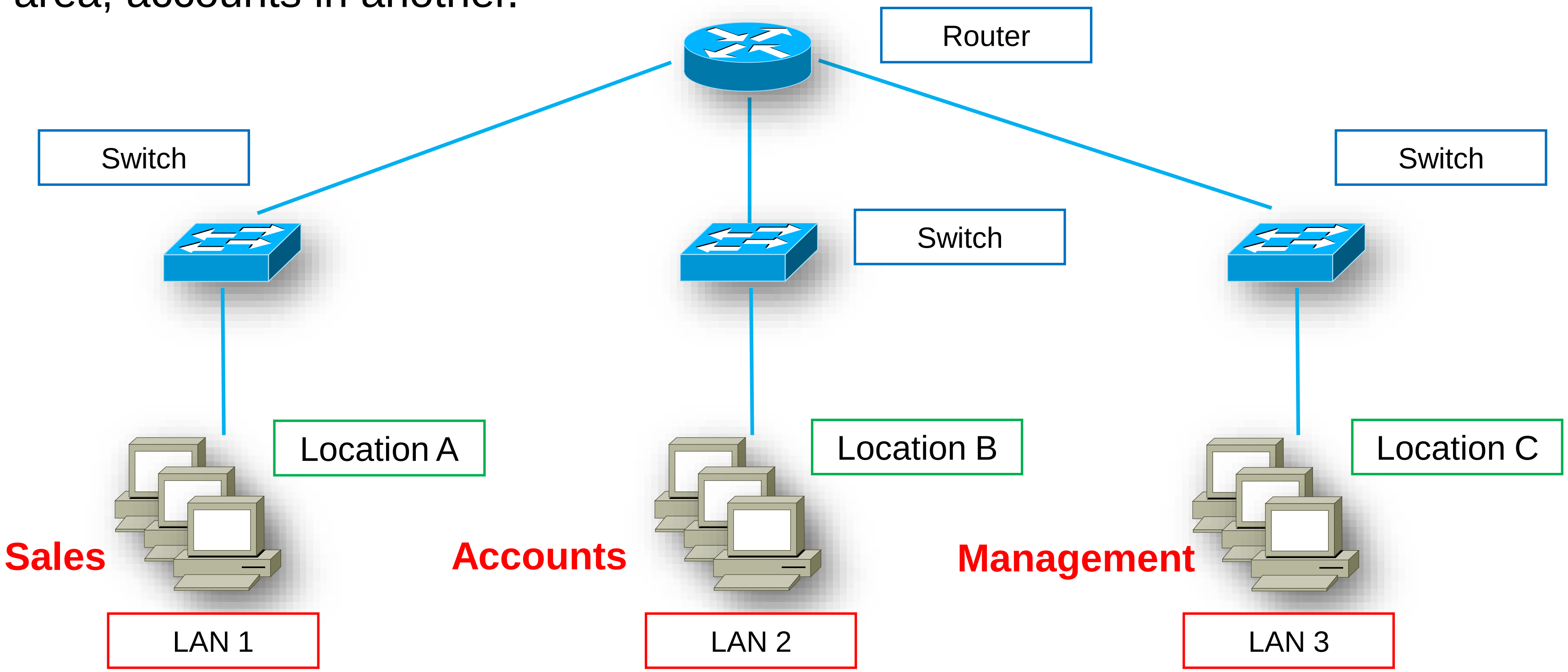
Extreme networks

Allied Telesis

Traditional LAN

A typical or traditional LAN is configured according to the physical infrastructure it is connecting.

Users are grouped based on their location in relation to the switch and cabling; for example, sales staff in one area, accounts in another.



Limitations

The traditional LAN configuration has a few drawbacks:

Security – Two groups of users in one physical location will share the same LAN.

If one group transmits sensitive data, the other may be able to intercept it.

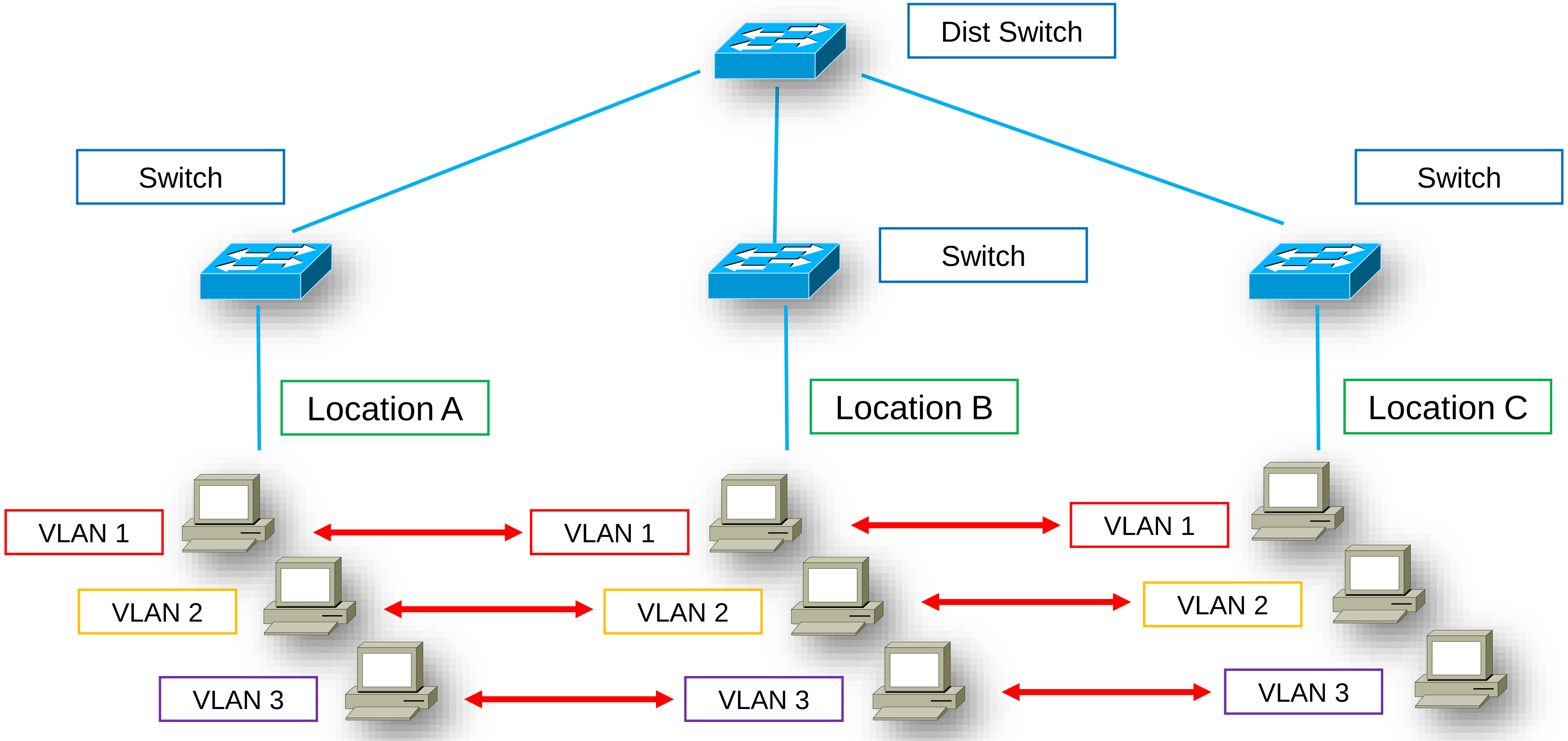
Performance – If there are a high number of users in one physical area, there could be a large amount of traffic on a LAN segment, this in turn may affect performance.

This is where Virtual LANs (VLANs) come in very handy; they break up the traditional LAN so:

- People working in a team or workgroup aren't required to work near each other to be on the same LAN.
- A person in one team can transmit sensitive information to others in their team without someone close by being able to intercept that data.
- It allows for greater flexibility when physically re-locating staff.

VLANs

Now users can be physically anywhere but connected to the one VLAN.

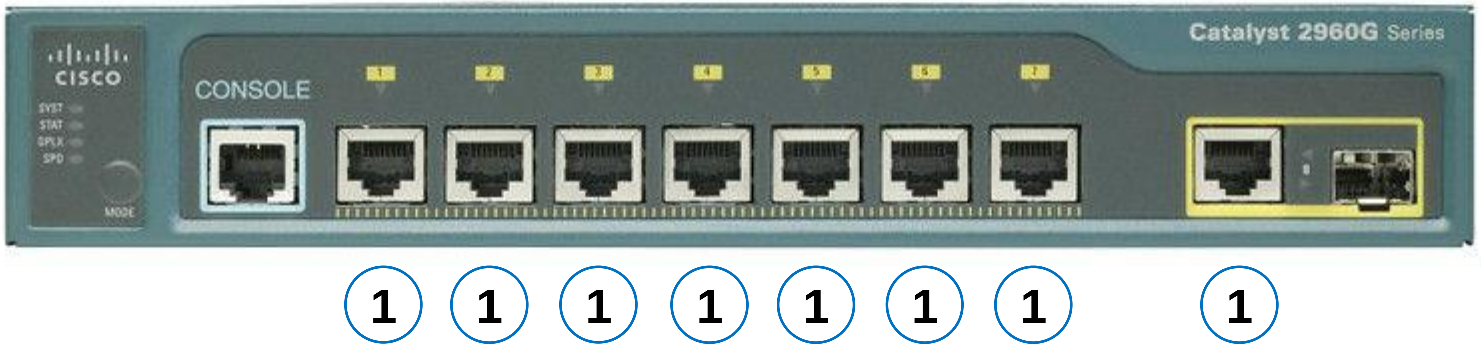


Default

When you use an ‘out of the box’ Cisco switch; it acts like any other ‘dumb’ switch.

Each port can communicate with any other port.

This is because they are on the same VLAN (`VLAN 1`).

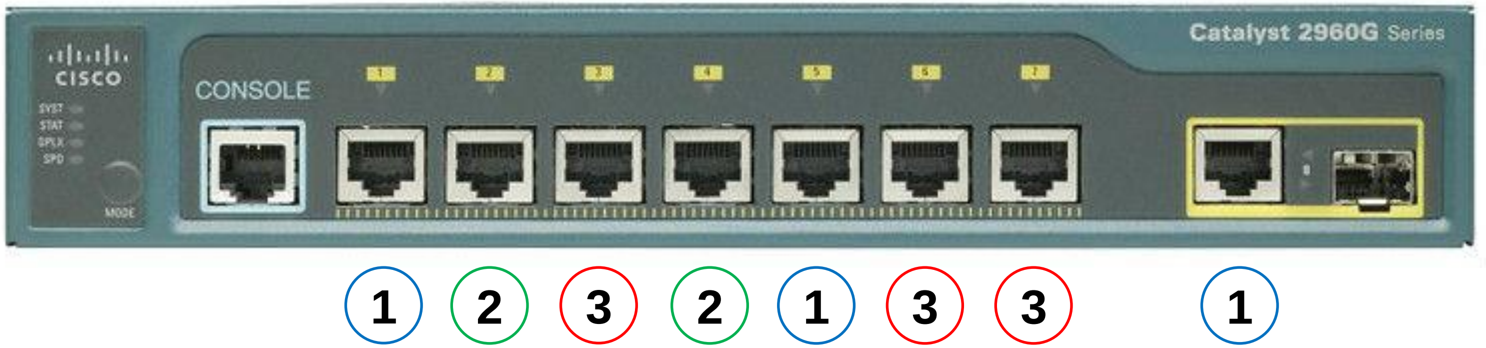


Configured

First you create the VLANs and give them a sensible name.

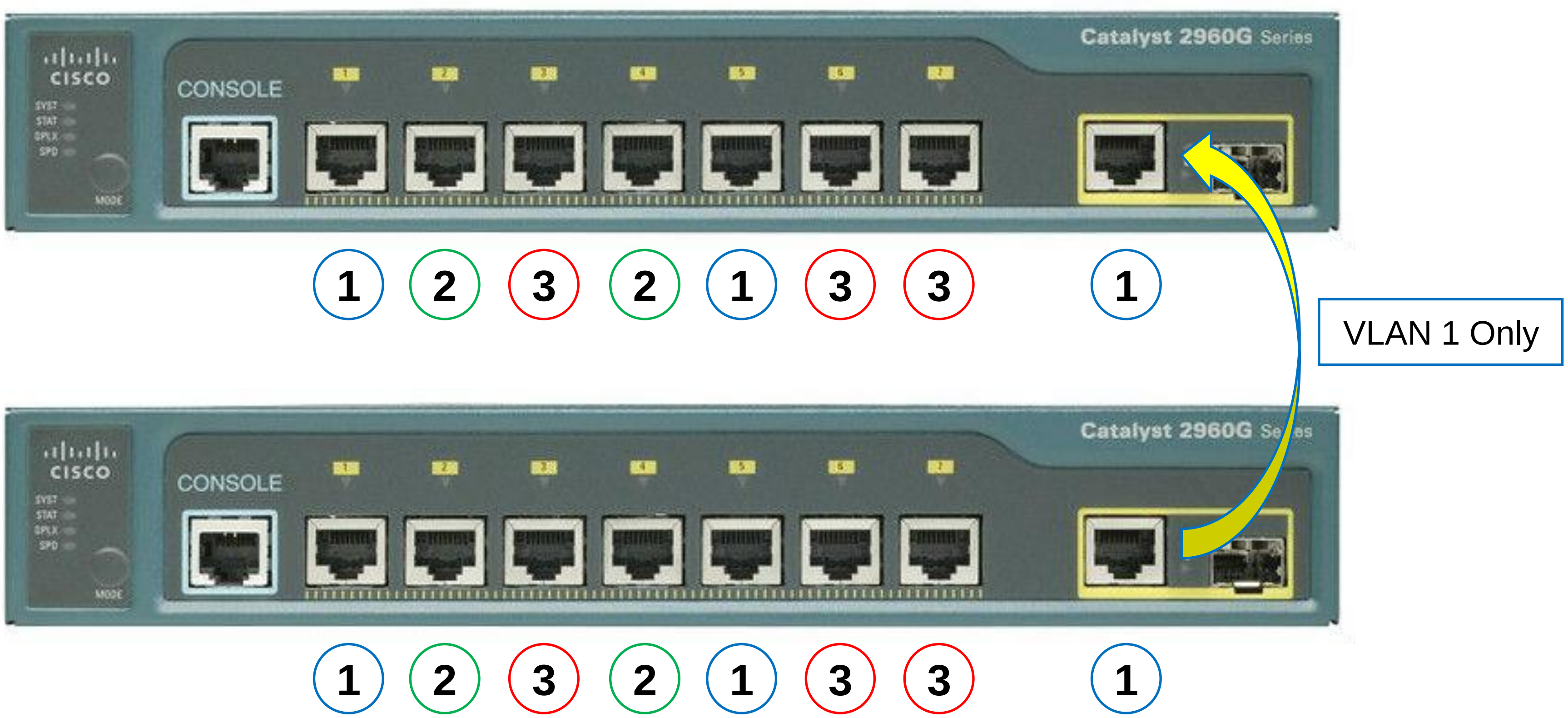
Switch ports can then be assigned to a VLAN.

Each port can then only communicate with ports on the same VLAN.



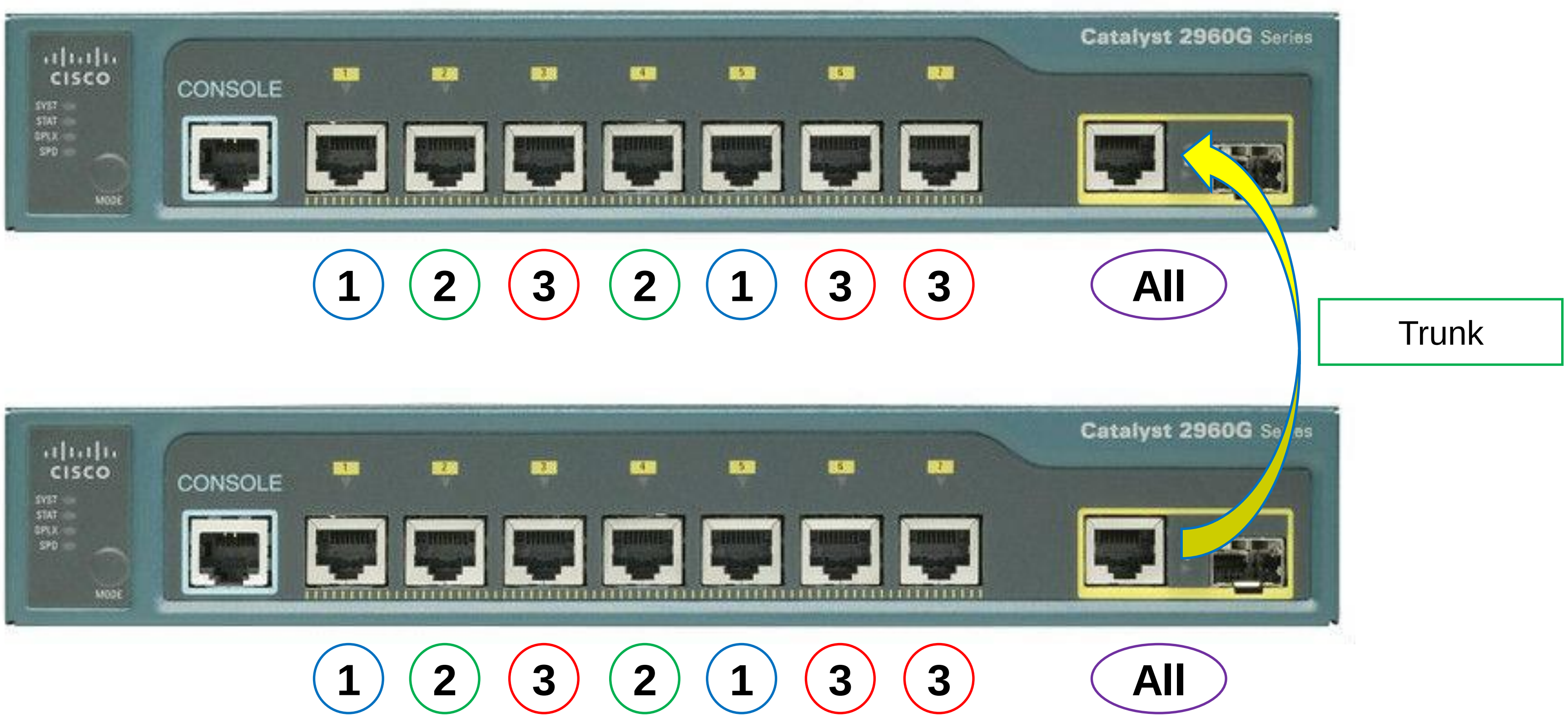
Problem

How do you get VLANs on one switch to communicate with the VLANs on another switch?



Solution

Connect the switches using a **trunk** link:



Access or Trunk

Each port on a switch can be either:

Access – Can belong to only a single VLAN at any one time.

Trunk – Can be assigned to a single VLAN, many VLANs or even all VLANs.

This makes trunk ports ideal for connecting switches; whereas access ports are ideal for connecting hosts to switches.

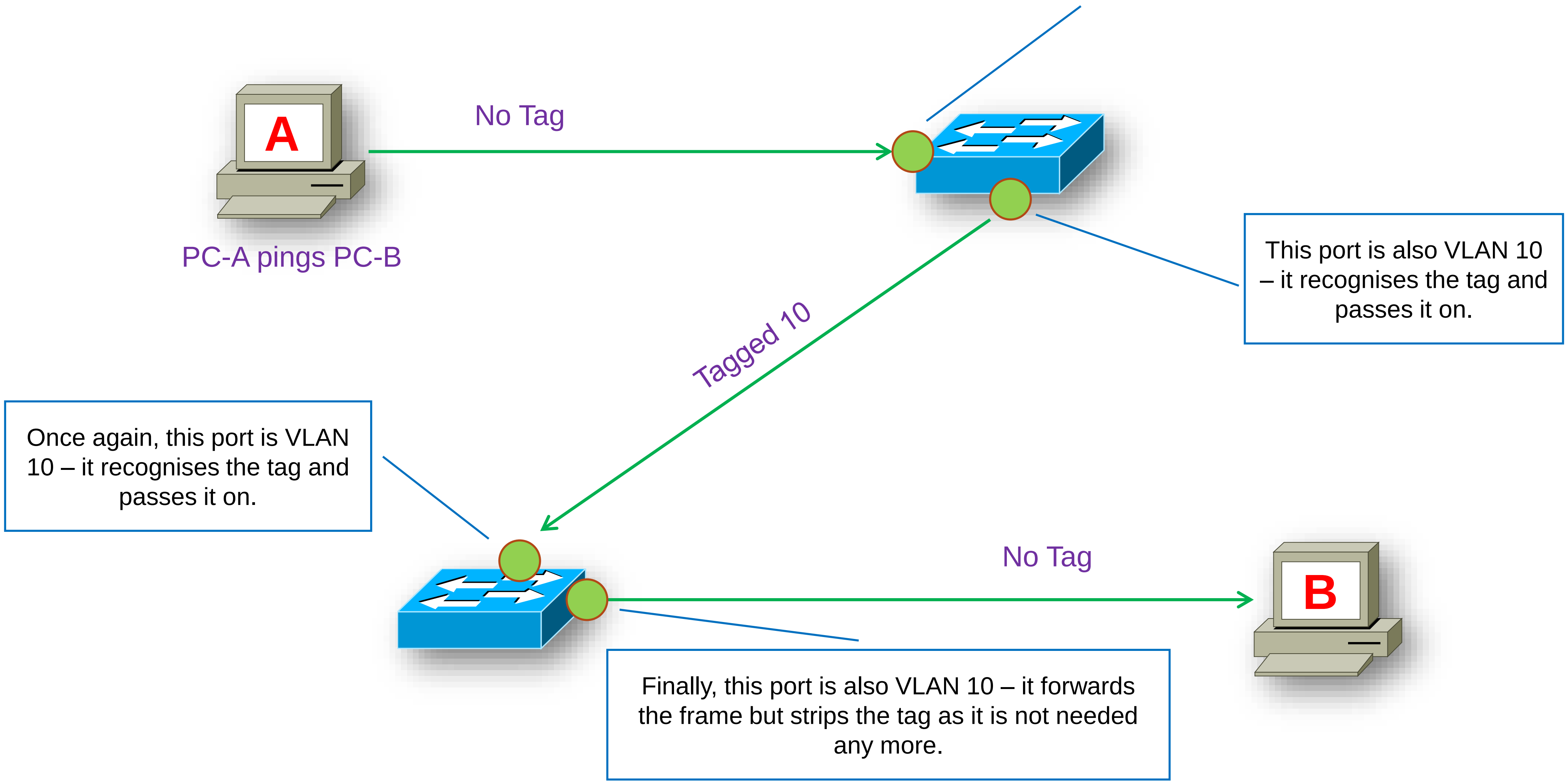
VLANs can work due to the concept of frame tagging.

Basically a “tag” – a small piece of additional code - gets added to a frame as it passes from a host through the switch port.

From there the tag will dictate what the switch or switches do with it.

Once the frame reaches its exit port the tag gets dropped.

All Access Ports



PC-A pings PC-B

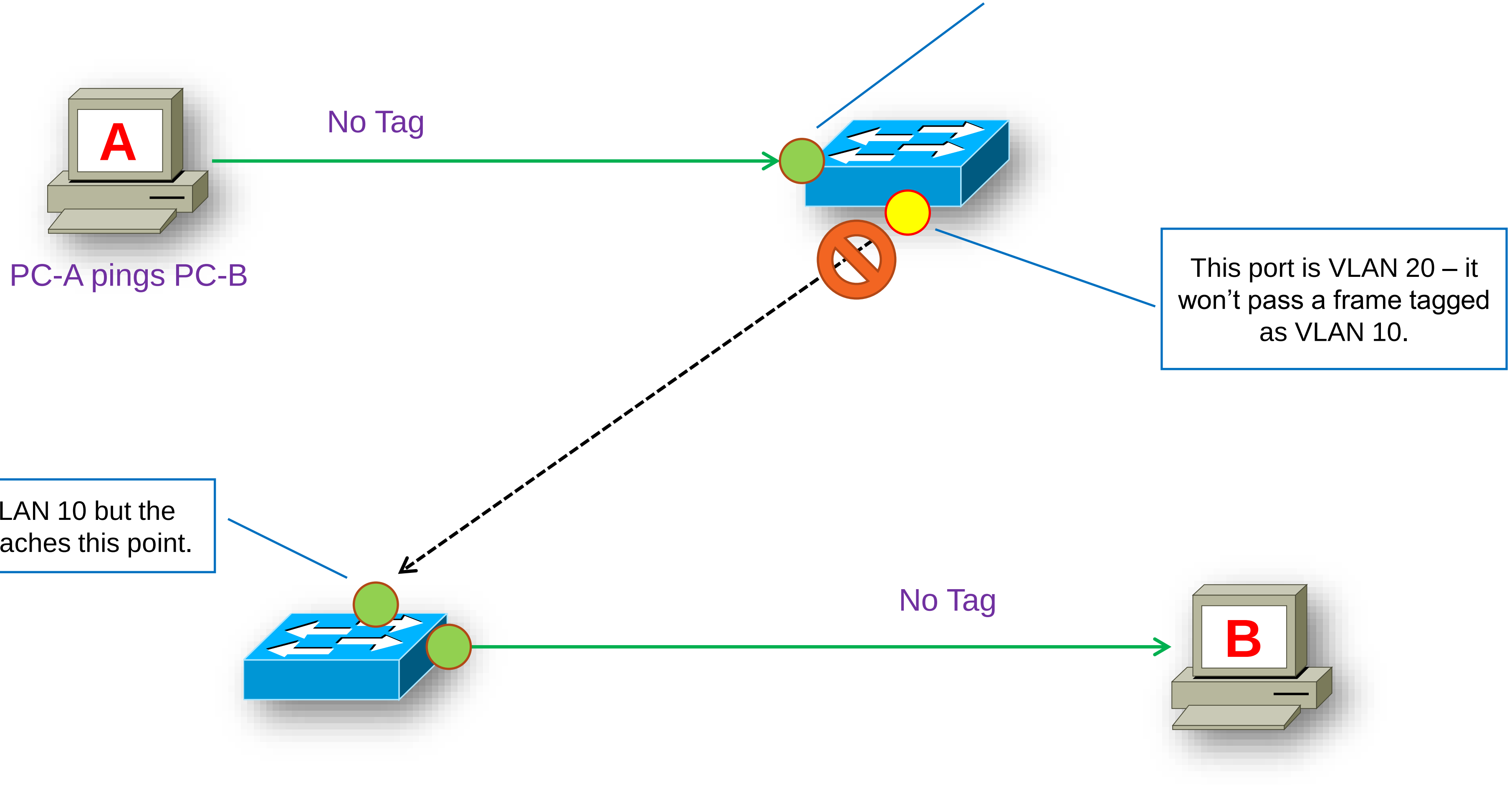
Port belongs to VLAN 10 – so frame gets tagged with a 10.

This port is also VLAN 10 – it recognises the tag and passes it on.

Once again, this port is VLAN 10 – it recognises the tag and passes it on.

Finally, this port is also VLAN 10 – it forwards the frame but strips the tag as it is not needed any more.

All Access Ports

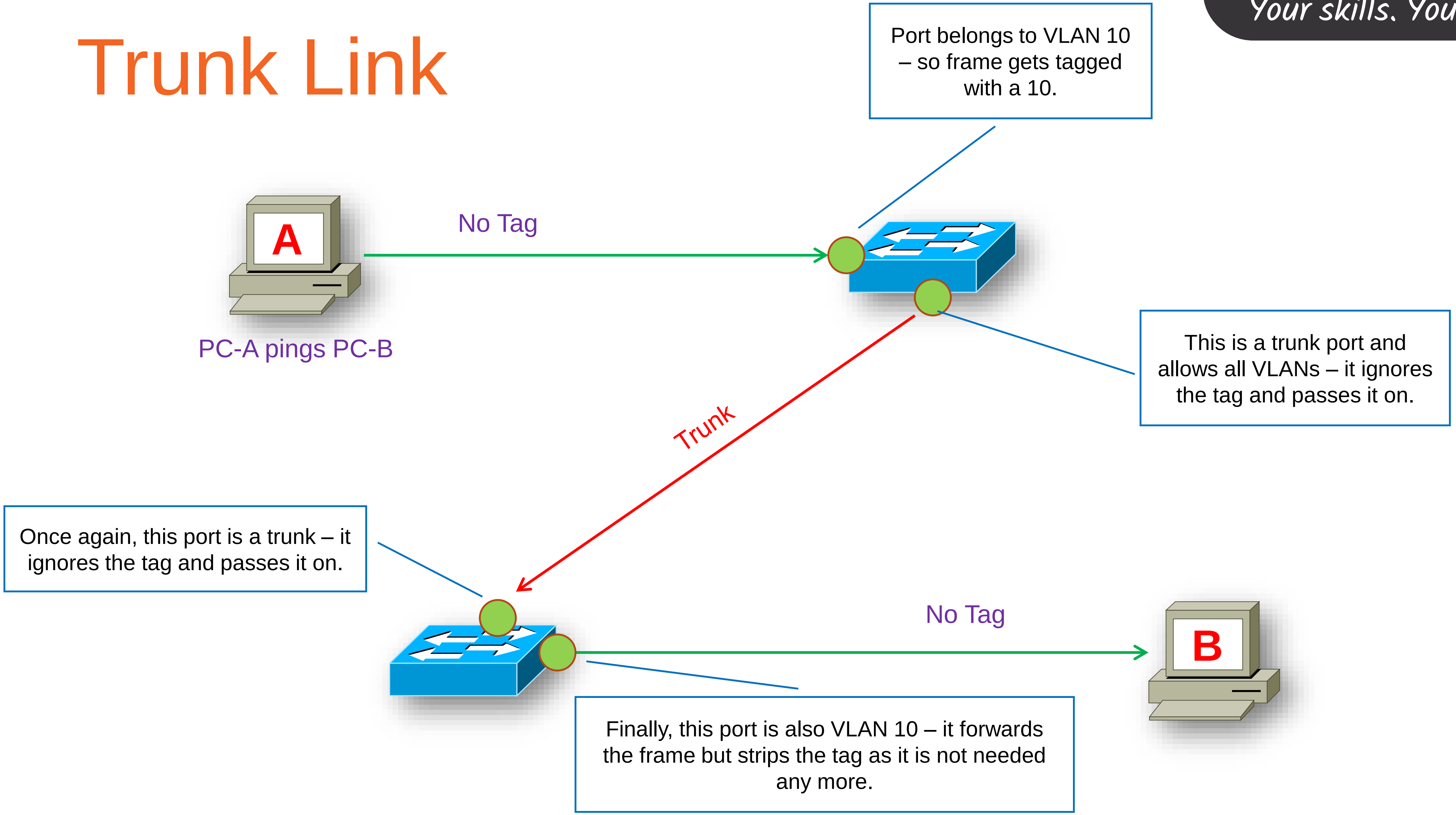


Port belongs to VLAN 10 – so frame gets tagged with a 10.

This port is VLAN 20 – it won’t pass a frame tagged as VLAN 10.

This port is VLAN 10 but the frame never reaches this point.

Trunk Link



Port belongs to VLAN 10 – so frame gets tagged with a 10.

This is a trunk port and allows all VLANs – it ignores the tag and passes it on.

Once again, this port is a trunk – it ignores the tag and passes it on.

Finally, this port is also VLAN 10 – it forwards the frame but strips the tag as it is not needed any more.

Routing VLANs

The only way to get one VLAN to talk to another VLAN is by using a router (or a Layer 3 switch) as VLANs are just like normal LAN networks in that they will have their own IP address range (subnet).

You can then introduce Access Control Lists, or ACLs, to control which VLANs can see what; one VLAN may have access to the resources of another – but the reverse may not be true.

For example: **`Management`** may see **`Sales`**, but **`Sales`** can't see **`Management`**.

TasTAFE

Your skills. Your future.

1300 655 307 | www.tastafe.tas.edu.au

RTO 60142 | CRICOS 03041M