VLANs

LAN: A group of devices in a single location/A single broadcast domain including all devices in that domain.
Broadcast Domain: a group of devices which will receive a broadcast frame FFFF.FFFF.FFFF sent by one of its members.
A router receives the broadcast frame but doesn't forward it to other networks, can contain a router interface.
Lots of unnecessary broadcast traffic can reduce network performance. (broadcast or unknown unicast flooding).
You can apply security policies on a router or a firewall, in a single LAN PCs can reach each other directly without traffic passing through the router, so configured security policies would have no effect.
Segmenting at layer3 (Subnetting) routers need to have n interfaces connected to the switch yet a switch will forward a broadcast frame which is the same problem.
Segmenting at layer2 VLANs: the switch considers each VLAN as a separate LAN and doesn't forward traffic between them including broadcast/ unknown unicast traffic, they are per-interface.
The switch doesn't perform inter- VLAN routing, but through the router.
Command: show vlan brief → shows vlans on a switch, by default 1 ->for all interfaces, 1002-1005 for FDDI, token ring.
Command: switchport mode access (a switch port belonging to a single VLAN usually connects to end hosts.
Trunk ports: switch ports belonging to multiple VLANs.
Command: switchport access VLAN <number> → assigns VLAN to a port.
Command: vlan <num> to create or configure a VLAN , name<name> to change VLAN name.
Ping 255.255.255.255 a broadcast to the network not routed by the router only to local subnet, while a subnet broadcast IP address can be used by other subnets to send a broadcast to a certain subnet.

Trunk ports: carry traffic from multiple VLANs on a single interface.
VLAN tagging: allows the receiving switch to know which VLAN the frame belongs to. trunk/tagged – access/untagged.
Trunking protocols: ISL → Inter Switch Link (1- 4094) that is probably not used or supported and IEEE 802.IQ dot1q.
The dot1q tag is 4 bytes inserted between Source MAC address and type/length in Ethernet header.
Dot1q consists of TPID → tag protocol identifier, TCI → tag control information.
TPID: 2 bytes always set to a value of 0x8100 indicated the frame is dot1q tagged.
TCI: 1- PCP → priority code point: 3 bits used for CoS (class of sevice) to prioritize important traffic in congested nets.
2- DEI: drop eligible indicator, a bit used to indicate frames that can be dropped if network is congested.
3- VID or VLAN ID: 12 bits to identify the VLAN the frame belongs to (0,4095) are reserved can't be used.
1-1005 → normal VLANs, 1006-4094 → extended VLANs, some older switches can't use the extended range.
Native VLAN: by default VLAN 1 on all trunk ports, however can be configured manually on all trunk ports.
The switch doesn't add dot1q tag to frames in native VLAN, when a witch receives it, it assumes it belongs to native VLAN, so it's important that it matches between switches in order not to drop the frame even if tagged with native tag.
Command: switchport mode trunk. After switchport trunk encapsulation dot1q if switch dupports dot1q and ISL.
Command: show int trunk (mode → on → manually configured).
Command: switchport trunk allowed vlan <vlans> to configure allowed vlans. (add , all by default, except, none, remove).
For security purposes make native VLAN an unused VLAN and must match on different switches.
Show vlan brief shows only access ports assigned to each vlan.

ROAS → router on a stick to divide one physical interface into a number of separate sub interfaces.
Int g0/0.vlan number → encapsulation dot1q vlan number.
The router will tag frames sent out of each sub interface with the vlan tag configured on the subinterface.
switchport trunk native vlan <vlan number> for native vlan.

Smaller frames in native VLAN lead to more frames per second.
For a native VLAN on a router use command: encapsulation dot1q <vlan-id> native or configure IP address of the native on the physical interface. (there is no need for a sub interface).
A router sub interface can't have both a vlan and a native vlan unlike a switch interface.

Multilayer switches: using a multilayer/layer 3 switch which are capable of both switching and routing (layer 3 aware). Preferred in large networks.
SVIs (Switch Virtual Interfaces) are the virtual interfaces you can assign IP addresses to in a multilayer switch by configuring end hosts to use them as their default gateway.
If a switch doesn't know the destination mac address after routing the frame it floods the frame unlike the router that sends an ARP request first.
For security purposes don't connect a multilayer switch directly to the internet, put a router in between.
Multilayer switches interfaces can work as router interfaces.
Command: default interface <interface> to reset an interface to its default settings.
Command : ip routing allows layer 3 routing on a switch.
Command: no switchport to change the interface from a layer 2 switchport to a layer 3 routed port.
Command: show interfaces status.
To create a SVI for a vlan use the command interface vlan <vlan> that is shutdown by default.
Creating an SVI to a vlan doesn't create the vlan if it doesn't exist.
For a SVI to be in up/up state:
1- the vlan must exist on the switch. 2- the vlan must not be shutdown. 3- the SVI must not be shutdown.
4- the switch must have at least one access or trunk port in the VLAN in up/up state.
Command: show interface <interface> switch port shows vlan status of an interface.