WAN Architectures

WAN: a network exits over a large geographical area, to connect geographically separate LANs, usually refers to enterprises private connections, over public/shared connections as internet VPNs can be used to create private WAN connections.
Hub and Spoke topology is equivalent to start topology in WANS.
Leased line: a dedicated physical link, typically connecting two sites using serial connections, leased lines have higher cost, installation lead time, slower speed than Ethernet WAN.

MPLS: Muli Protocol Label Switching, similar to the internet, service providers' MPLS networks are shared infeastructure, used by many customer enterprises to make WAN connections,The label switching in the name of MPLS allows VPNS to be created over the MPLS infrastructure through the use of labels.
CE → Customer edge router connects to PE → provider edge router→ connects to P→ Provider core router, when PE routers receive frames from CE routers they add a label to the frame between layer2,3 headers (called layer 2.5 protocol), these labels are used to make forwarding decisions within service provider network not dest IP, only P, Pe routers use MPLS not CE routers.
When using a layer 3 MPLS VPN, the CE, PE routers can peer using static or dynamic routing protocols, to share routing information.
When using a Layer 2 MPLS VPN, the CE and PE routers don't form peerings, the service provider network is transparent to CE routers as if the CE routers directly connected, their WAN interfaces will be in the same subnet as if SP is a big switch between CEs, if a routing protocol is used, the 2 CE routers will peer directly with each other.
Many different technologies can be used to connect to a service provider MPLS network for WAN service.
as CATV, Ethernet Fiber, Wireless, ...etc.

Private WAN technologies can be used to connect to a service provider 's internet infrastructure.
DSL: Digital Subscriber Line provides internet connectivity to customers over phone lines, and can share the same phone line already installed.
A DSL modem (modulator/demodulator): is required to convert data into format suitable to be sent over the phone lines, might be a separate device or incorporated into the home router.
CATV: uses lines used for TV service, a cable modem is required to convert data into a format suitable to be sent over CATV cables.
Single Homed: 1 connection to 1 ISP. Dual Homed: 2 connections to 1 ISP.
MultiHomed: 1 connection to each of 2 ISPs. Dual Multihomed: 2 connections to each of 2 ISPs.

Private WAN services provide security as leased lines use dedicated physical connections, MPLS use tags.
Site to site VPNs (Ipsec): 1- the sending device encrypts original packet with a session key, encapsulates the encrypted packet with a VPN header and a new IP header, sends it on the other side of the tunnel.
2- the receiving device decrypts the data to get the original packet and then forward it to its destination.
A tunnel is only formed between two endpoints, the site's router undergoes this process, broadcast and multicast traffic is not supported, configuring a full mesh of tunnels between many sites is an intensive task.
GRE (Generic Routing Encapsulation): creates tunnels like Ipsec but don't encrypt the original packet so not secure.
GRE over IPsec: the original packet is encapsulated by a new IP header and a GRE header, then encrypted and encapsulted within Ipsec VPN header and a new IP header.
DMVPN (Dynamic Multipoint VPN): allow routers to dynamically create a full mesh of IPsec tunnels without having to manually configure every single tunnel, by configuring tunnels between a hub and spoke, the hub router gives each router information about how to form an IPsec tunnel with the other routers.
GRE can be used to tunnel any layer 3 protocol.

Remote Access VPNs are used to allow end devices to access company's internal resources securely over the internet.
Typically use TLS (Transport Layer Security): that also provides HTTPS security.
A VPN client software is installed on end devices, that form secure tunnels to one of the company's routers/firewalls acting as a TLS server, allowing end users to securely access resources on the company's internal network without being directly connected to it.
Site to Site connect two end devices together (typically permanent) while remote access connect an end device to a site with on demand access. .

Command: interface tunnel <tunnel number>.
Command: tunnel source <interface connected to ISP>.
Command: tunnel destination <other router WAN's interface IP address>.
Command: ip address <tunnel IP address>.