LAN, WAN and MAN Definitions

- A Local Area Network (LAN) is a network that connects computers and other devices in a relatively small area, typically a single building or a group of buildings.
- A Wide Area Network (WAN) is a geographically distributed network that connects multiple Local Area Networks together.
- A Metropolitan Area Network (MAN) is a network that connects computers and other devices in a geographic area larger than a LAN but smaller than a WAN.

Private vs VPN Connections – Private Networks

- A private network uses links which are dedicated for an individual organisation.
- Local Area Networks are private networks.
- Wide Area Networks can also use physical links which are dedicated for an individual organisation.

- A **Virtual Private Network (VPN)** provides a virtual tunnel between private networks across a shared public network such as the Internet.
- Traffic travelling over the tunnel is encrypted and only readable by the authorised users on both sides.
- Users can share data over the tunnel as if they were connected with a dedicated private link.
- VPNs allow an organisation to use the same physical links for connectivity to the Internet and between offices.
- Because they use shared infrastructure, VPN connections are typically less expensive than dedicated physical links.

Site-to-Site VPN

- Site to Site VPN connections are terminated on a router or firewall in each office.
- Software does not need to be installed on user desktops.

- IPsec is typically used for encryption.

Remote Access VPN

- Remote Access VPN connections are between a router or firewall in the office and VPN software installed on an individual user's device.
- The user can access the VPN from anywhere with Internet connectivity.
- They usually use SSL (sometimes IPsec) for encryption.

Site-to-Site IPsec VPN Configuration Options

- **IPsec Tunnel:** open standard IPsec tunnel, does not support multicast
- **GRE (Generic Routing Encapsulation) over IPsec tunnel**: adds support for multicast
- **IPsec VTI (Virtual Tunnel Interface):** Cisco proprietary simplified configuration, supports multicast

Site-to-Site IPsec VPN Configuration Options

- **DMVPN (Dynamic Multipoint VPN):** Cisco proprietary. Scalable simple hub and spoke style configuration enables direct full mesh connectivity between all offices
- **FlexVPN:** Cisco proprietary. Very similar to DMVPN, newer technology
- **GETVPN (Group Encrypted Transport VPN):** Cisco proprietary. Scalable centralised policy for VPN over non-public infrastructure eg MPLS.

WAN Connection Options

- Multiple options are available for connecting geographically dispersed offices together.
- Not all options are available in all locations.
- What is commonly used in one region may be considered legacy in another.
- Different providers may use different terminology. I'll use the terminology used by Cisco for the CCNA exam

Primary WAN Connectivity Options

- Leased Line
- MPLS Multi Protocol Label Switching
- Satellite
- The service provider will typically provide an SLA (Service Level Agreement) with guarantees for uptime and traffic delay and loss on the link.

- Leased lines and Satellite can be used for connectivity to the Internet, for direct connectivity between offices, and/or connectivity between offices over VPN.
- MPLS uses a shared core infrastructure at the service provider. It can be used for connectivity to the Internet and/or connectivity between offices over VPN.

Optical Fiber

- Optical fiber is more suitable for long distances than copper wire
- It is commonly used for service provider backhaul connections, but can also be offered to their customers
- FTTx services:
    - Fiber to the Home
    - Fiber to the Premises
    - Fiber to the Building
    - Fiber to the Neighborhood

SONET and SDH

- SONET (in North America) and SDH (rest of the world) are the standards used in service provider optical fiber networks

SONET STS	SONET OC	SDH STM	Bit Rate Mbps
STS-1	OC-1		51.84
STS-3	OC-3	STM-1	155.52
STS-12	OC-12	STM-4	622.08
STS-48	OC-48	STM-16	2488.32
STS-192	OC-192	STM-64	9953.28

DWDM Dense Wavelength Division Multiplexing

- DWDM combines ('multiplexes') multiple optical signals into one optical signal transmitted over a single fiber strand
- Each signal is assigned a different wavelength
- DWDM allows more capacity to be added to existing infrastructure without expensive upgrades
- DWDM is used in all modern long haul optical connections

Dark Fiber

- Many service providers laid optical fiber cabling in the past and then found they didn't require it
- DWDM was a major reason for this
- The unused cabling can be offered to customers as 'Dark fiber'

WAN Backup and Small Office Solutions

- Less expensive options often aimed at home user Internet access can be used as Internet VPN WAN backup options in corporate environments
- There will typically be no corporate level SLA with these services
- These can be used as the primary WAN connection method to the corporate network from smaller offices and for home users
    - DSL Digital Subscriber Line
    - Cable
    - Wireless eg 4G

Legacy WAN Connectivity Options

- PSTN Public Switched Telephone Network
- ISDN Integrated Services Digital Network
- Frame Relay
- ATM Asynchronous Transfer Mode
- X.25

Interface Cards

- Routers will typically come with on-board Ethernet ports. Additional Ethernet interface cards can be added
- Ethernet is often used for WAN connections today
- Other WAN interfaces are modular and fit into a spare slot on the router
- There are many different types of WAN interface card
- Part numbers for different cards can be very similar
- Different cards are compatible with different router platforms
- Be careful when selecting your card!

Leased Lines

- A leased line is a dedicated physical connection between two locations.
- It has fixed, reserved bandwidth which is not shared with anyone else.
- The same bandwidth is available in both directions.
- The company may own the cable infrastructure but more commonly it is leased from a service provider for a monthly fee, hence the name ‘leased-line’.
- The first location is typically a corporate office.
- The second location is typically:
    - Another corporate office, providing point to point connectivity between the two offices
    - A data centre that’s connected to the company’s existing Wide Area Network, providing multipoint connectivity between offices
    - A data centre that’s connected to the Internet, providing Internet connectivity, and optionally corporate office connectivity over Internet VPN

Leased Lines

- Leased lines use a serial connection requiring the correct physical interface card in the router (they do not use an Ethernet port)
- Common bandwidth options:

North America	
T1	1.544 Mbps
T2	6 Mbps
T3	45 Mbps
T4	275 Mbps

Europe	
E1	2 Mbps
E2	8 Mbps
E3	34 Mbps
E4	140 Mbps

Leased Line Benefits and Drawbacks

- Leased lines have fixed, reserved bandwidth which is not shared with anyone else.
- The service provider will typically provide an SLA (Service Level Agreement) with guarantees for uptime and traffic delay and loss on the link.
- Leased lines are typically more expensive than the other options.
- There is usually a longer lead time for installation.
- Copper or fiber Ethernet connectivity options to the CPE (Customer Premises Equipment) are becoming more common than serial leased lines

Satellite

- Satellite connections share the same characteristics as cabled leased lines
- They are typically expensive and low bandwidth
- They may be the only option in hard to reach areas

Phone Lines

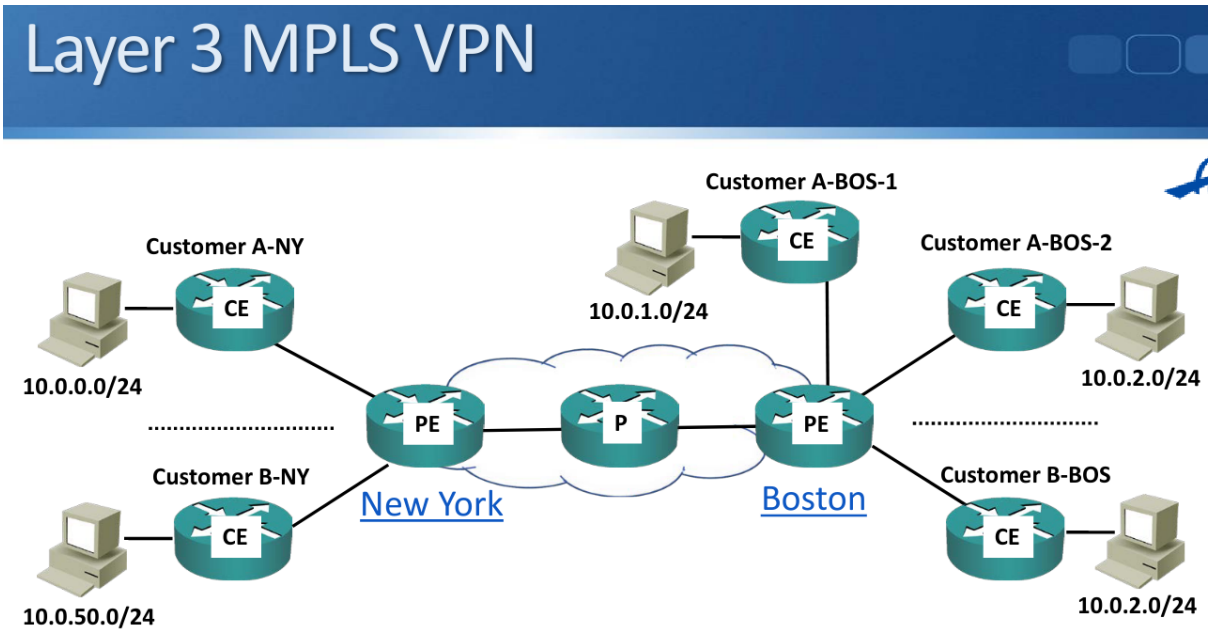
(Not asked in CCNA)

- T1 and E1 links were also commonly used for connections to the PSTN (Public Switched Telephone Network)
- The analog phone cable to your house is capable of carrying one call
- A T1 digital line is capable of carrying 24 concurrent TDM calls, an E1 can carry 30 calls

- VoIP (Voice over IP) using SIP (Session Initiation Protocol) signalling over Ethernet WAN connections to the Telco are popular today

MPLS (Multi Protocol Label Switching) VPN

- WAN connectivity can be provided over an MPLS infrastructure, usually operated by a service provider
- Traffic from multiple customers can travel over the provider's shared MPLS network, so this is a VPN service
- Different levels of SLA for uptime and traffic delay and loss are often available at different price points
- Ethernet connections are typically used to the customer router
- MPLS VPNs provide a full mesh topology by default



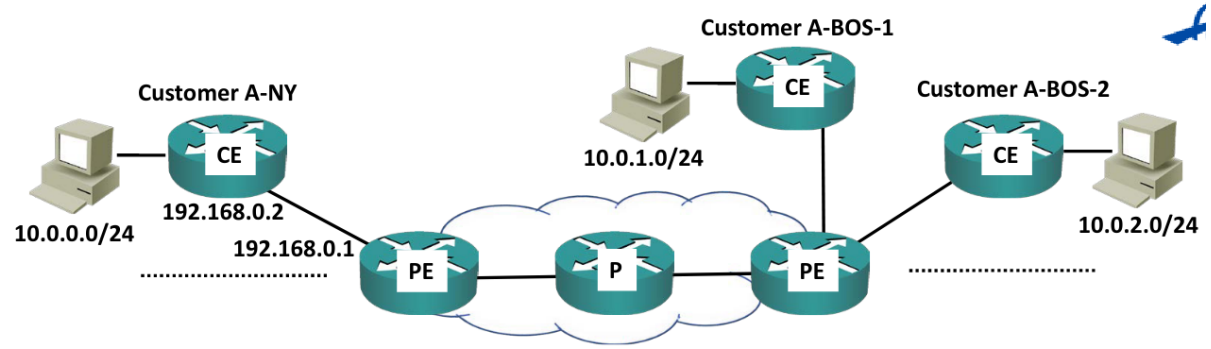
CE: Customer Edge device
PE: Provider Edge device
P: Provider core device

Layer 3 MPLS VPN

- MPLS runs across the providers core on the PE and P routers
- The customer CE routers do not run MPLS
- The customer CE routers peer at Layer 3 with the provider PE routers
- Static routes or a routing protocol runs between the CE and PE
- The PE router looks like another customer router to the customer

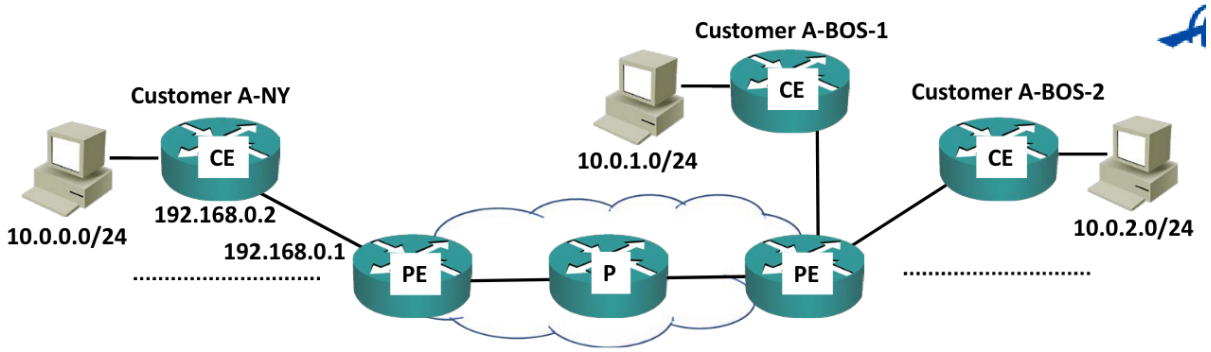
- The provider's core routers are transparent to the customer
- The customer sites are in different IP subnets

CE Router Configuration – Static Routes




```
CE1(config)#int g0/0
CE1(config-if)#ip address 192.168.0.2 255.255.255.252
CE1(config)#ip route 10.0.0.0 255.255.0.0 192.168.0.1
```

CE Router Configuration - RIP

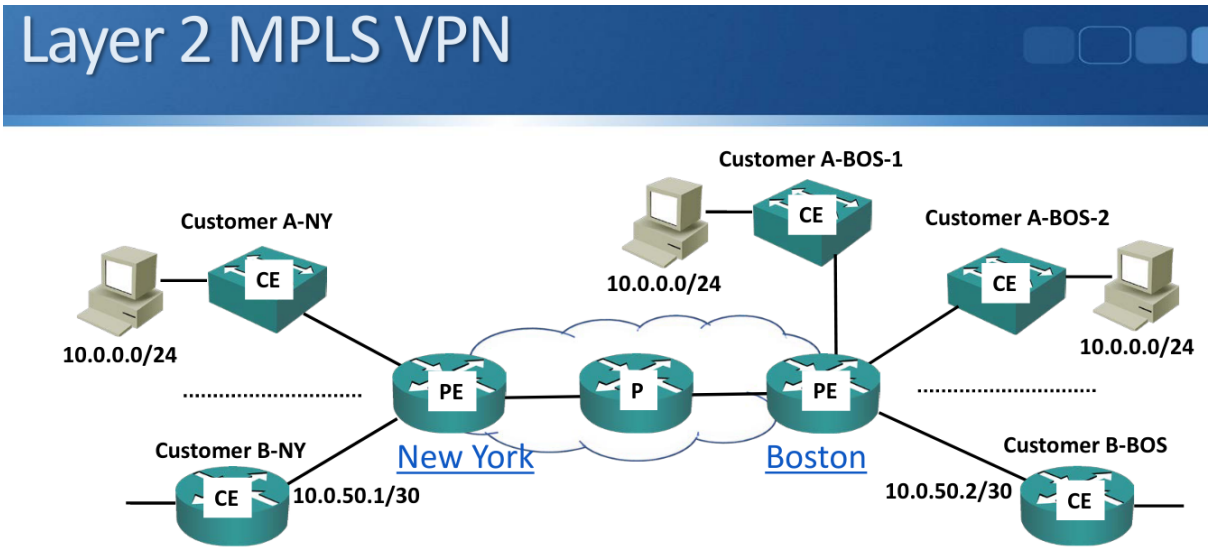



```
CE1(config)#int g0/0
CE1(config-router)#ip address 192.168.0.2 255.255.255.0
CE1(config)#router rip
CE1(config-router)#version 2
CE1 (config-router)#network 10.0.0.0
CE1 (config-router)#network 192.168.0.0
```

Layer 2 MPLS VPN

- The CE devices do not peer with the PE devices. The entire provider network is transparent to the customer
- The provider network acts like a giant switch

- The customer sites are in the same IP subnet(s)



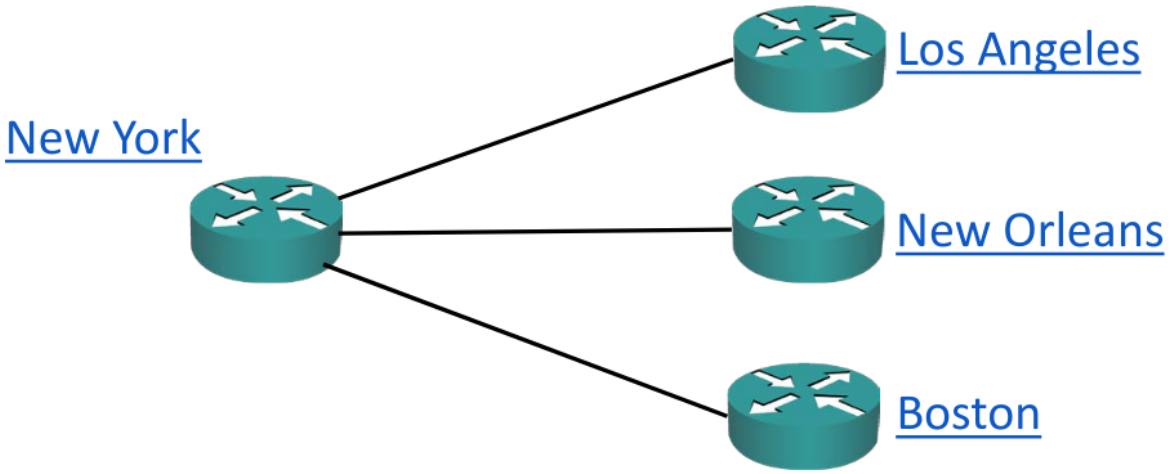
- This may be required for clustering an application over the WAN
- It can also be useful for migrating hosts during Disaster Recovery

Layer 2 MPLS VPN Terminology

- VPLS (Virtual Private LAN Service): Multipoint Layer 2 VPN
- VPWS (Virtual PseudoWire Service): Point to point Layer 2 VPN

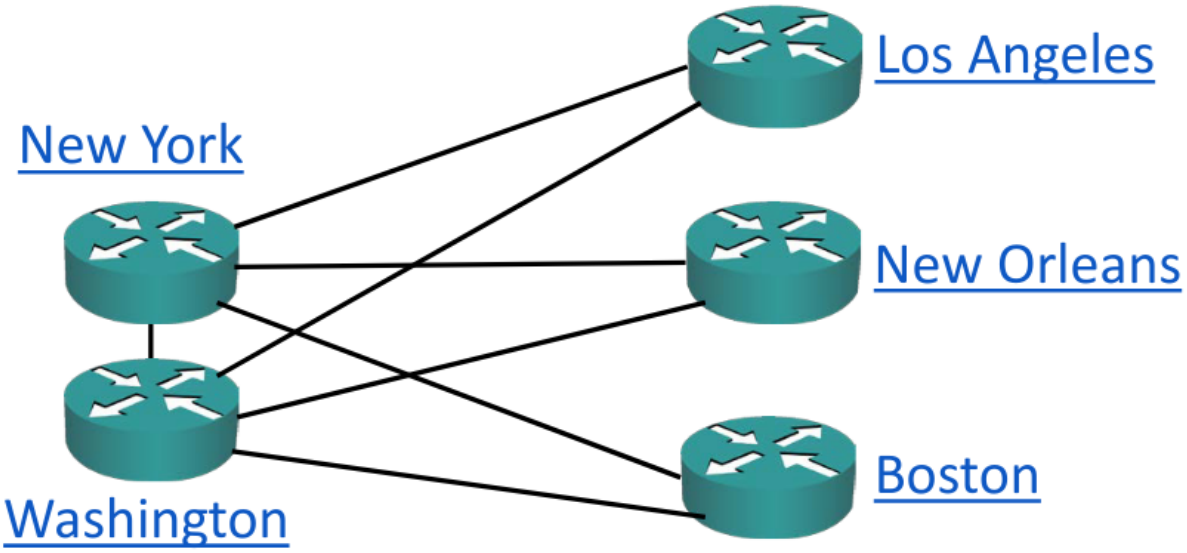
Topology Options

Hub and Spoke (Star)



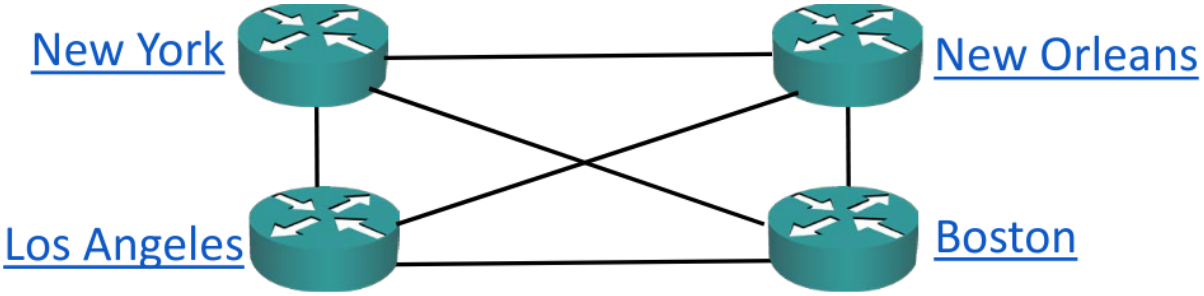
- Advantages: Simplicity, centralised security policy
- Disadvantages: Single point of failure, suboptimal traffic flow

Redundant Hub and Spoke



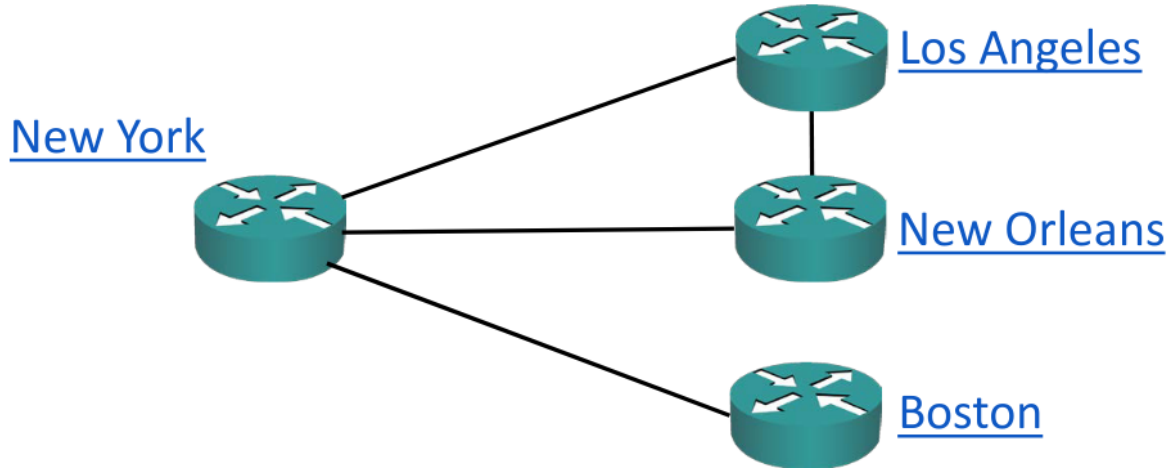
- Advantages: Removes single point of failure, centralised security policy
- Disadvantages: Higher cost, suboptimal traffic flow

Full Mesh

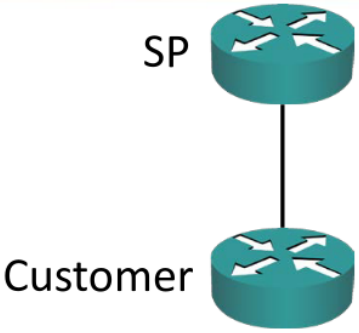


- Advantages: Optimal traffic flow
- Disadvantages: Higher complexity and cost

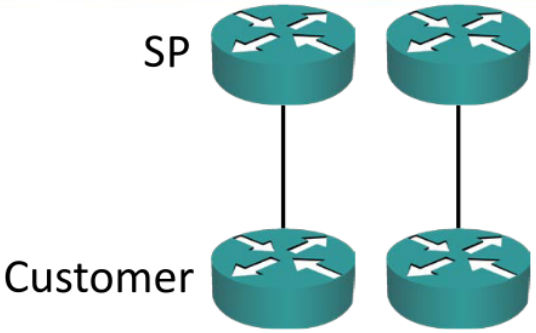
Partial Mesh



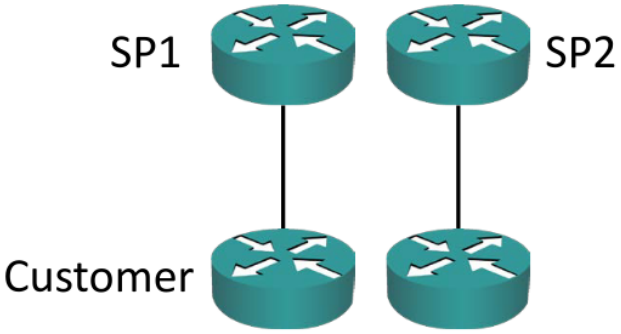
Internet Redundancy Options



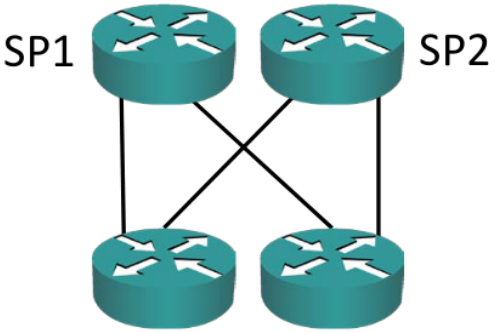
Single Homed



Dual Homed



Multihomed



Dual Multihomed