5. Campus Topology Design

CHAPTER 5

Dr. Mahmud Mansour

Do You Have a Good Design?

- When you already know how to add a new building, floor, WAN link, remote site, e-commerce service, and so on
- When new additions cause only local change, to the directly-connected devices
- When your network can double or triple in size without major design changes
- When troubleshooting is easy because there are no complex protocol interactions to wrap your brain around

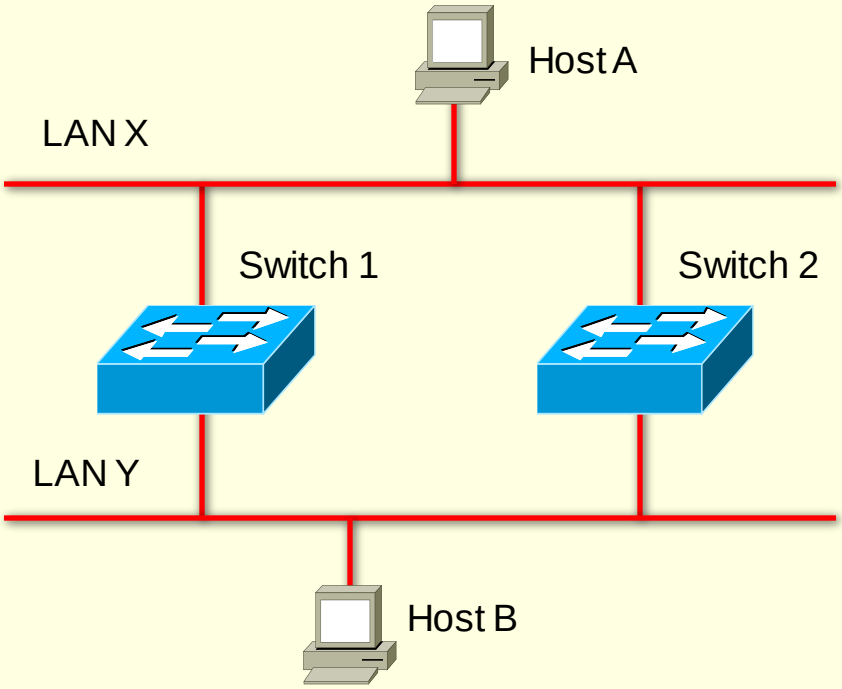
Campus Topology Design

- Use a hierarchical, modular approach
- Minimize the size of bandwidth domains
- Minimize the size of broadcast domains
- Provide redundancy
  - Mirrored servers
  - Multiple ways for workstations to reach a router for off-net communications

Campus Network Design

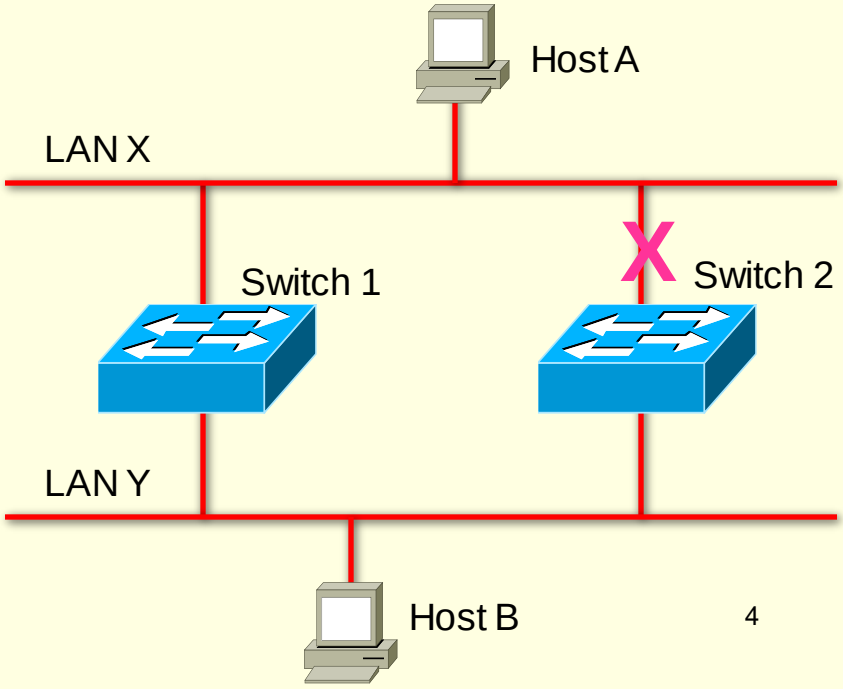
- **Campus access layer:** This module contains end-user workstations and IP phones connected to switches or wireless access points. Services offered by this module include network access, broadcast control, protocol filtering, and the marking of packets for quality of service (QoS) features.
- **Campus distribution layer**: The job of this module is to aggregate wiring closets within a building and provide connectivity to the campus core via routers (or switches with routing modules). This module provides routing, QoS, and access control methods for meeting security and performance requirements. Redundancy and load sharing are recommended for this module. For example, each building should have two equal-cost paths to the campus core.
- **Campus core layer:** The campus core interconnects the access and distribution modules with the data center, network management, and edge modules. The campus core provides redundant and fast-converging connectivity. It routes and switches traffic as quickly as possible from one module to another. This module usually uses high-speed routers (or switches with routing capability) and provides QoS and security features.

Campus Redundant Design



Redundant Bridges/switches

Use STP to Avoid Loops



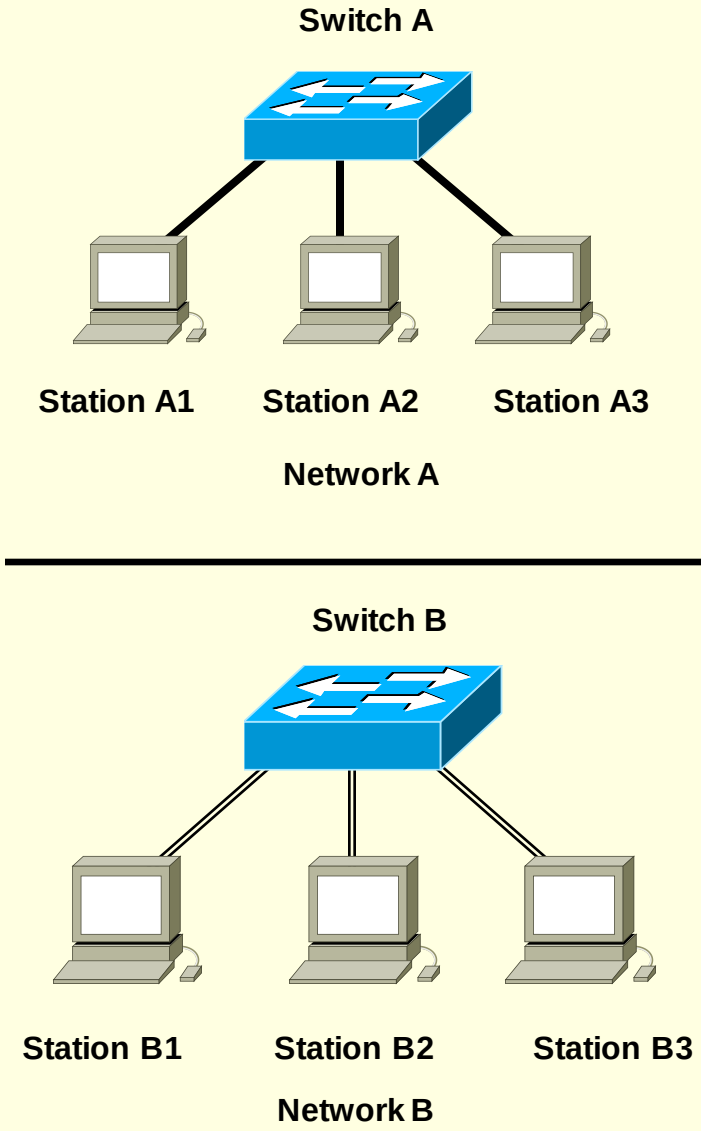
Bridges (Switches) Running STP

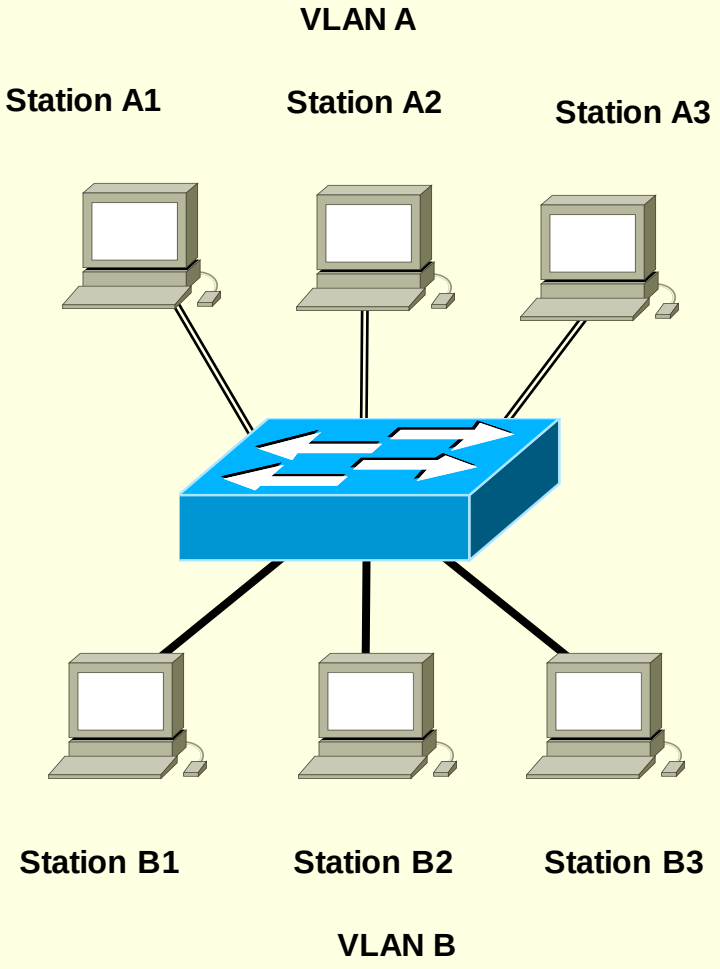
- Bridges elect a single bridge as the Root Bridge.
- Calculate the shortest path to the Root Bridge and choose a port (Root Port) that provides the shortest path to the Root Bridge.
- The Designated Port is a port on the LAN segment that is closest to the Root Bridge.
- All ports on the Root Bridge are Designated Ports.
- For each LAN segment, elect a Designated Bridge and a Designated Port on that bridge.
- The Root and Designated ports are selected in the spanning tree. These ports forward traffic. Other ports block traffic.

Virtual LANs (VLANs)

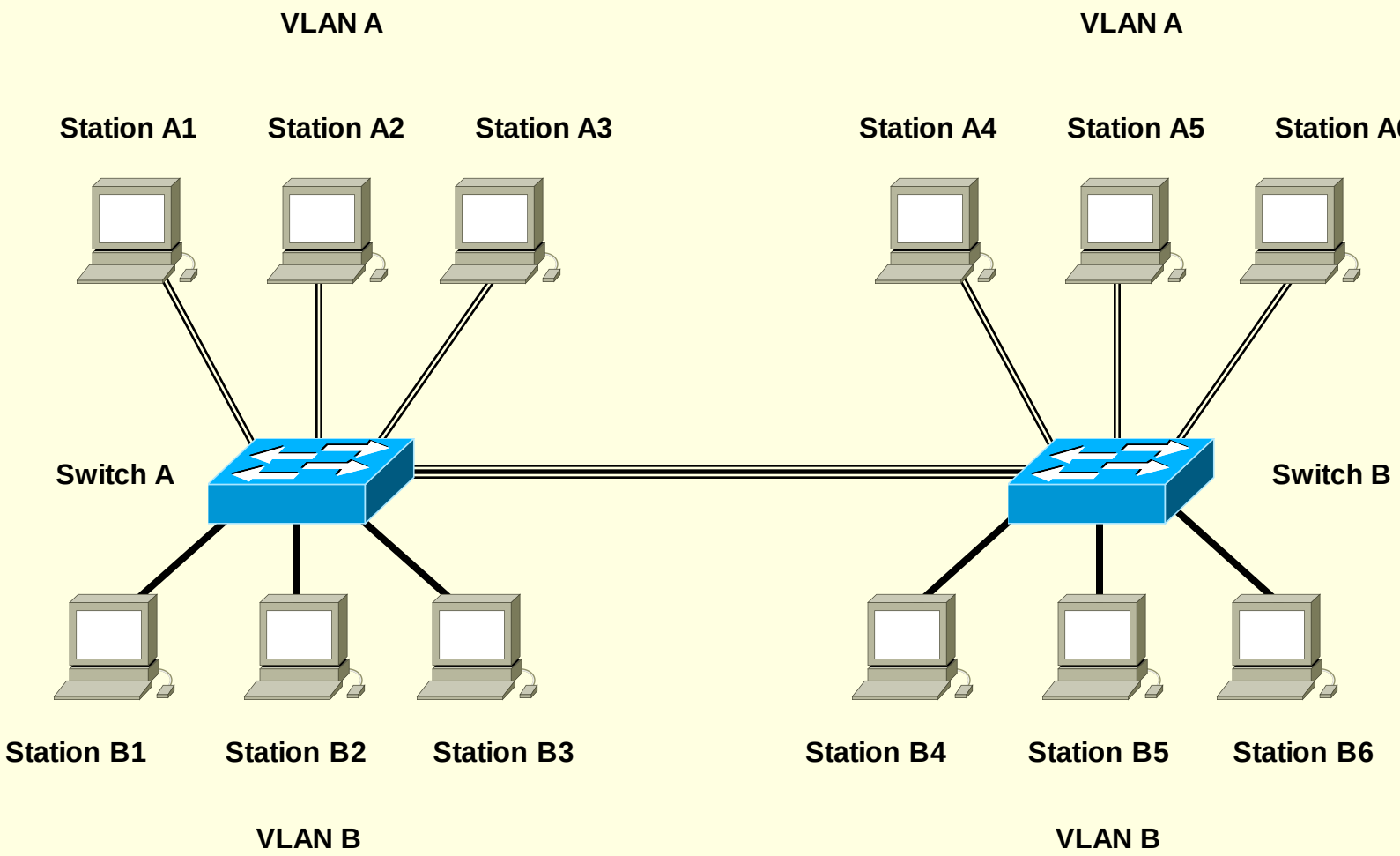
- An emulation of a standard LAN that allows data transfer to take place without the traditional physical restraints placed on a network
- A set of devices that belong to an administrative group
- Designers use VLANs to constrain broadcast traffic

Real LANs vs. VLANs





VLANs Span Switches



WLANs and VLANs

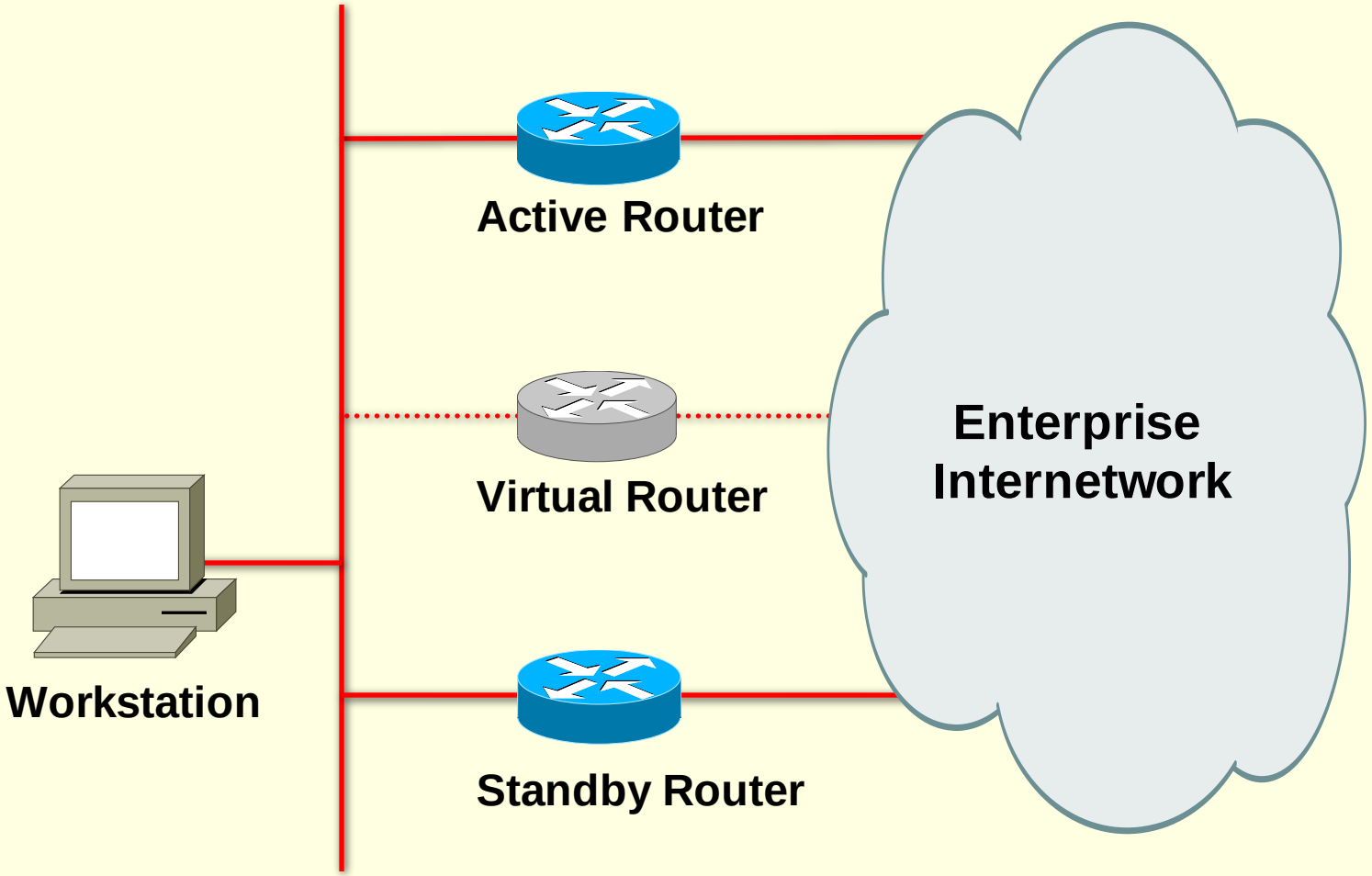
- A wireless LAN (WLAN) is often implemented as a VLAN
- Facilitates roaming
- Users remain in the same VLAN and IP subnet as they roam, so there's no need to change addressing information
- Also makes it easier to set up filters (access control lists) to protect the wired network from wireless users

Workstation-to-Router Communication

A workstation has many possible ways to discover a router on its network, depending on the protocol it is running and also the implementation of the protocol:

- Proxy ARP (not a good idea)
- Listen for route advertisements (not a great idea either)
- ICMP router solicitations (not widely used)
- Default gateway provided by DHCP (better idea but no redundancy)
  - Use Hot Standby Router Protocol (HSRP) for redundancy

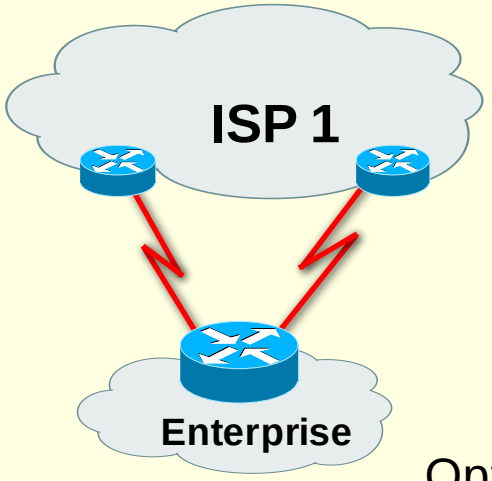
HSRP – VRRP - GLBP



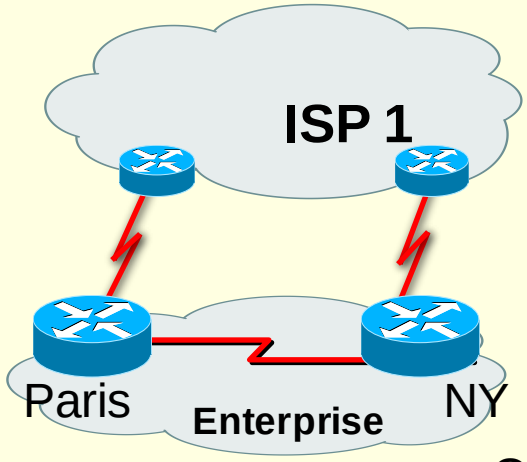
FHRP Comparison

Protocol	HSRP CISCO-PROPRIETARY	VRRP Multi-Vendor	GLBP CISCO-PROPRIETARY
Terminology	One Active Router, one Standby Router, other Routers in Standby group	One Master, one or more Backup Virtual Routers	Active Virtual Gateway (AVG), Standby Virtual GW (SVG), Active Virtual Forwarders (AVFs)
Virtual object	0000.0C07.ACXX (v1, XX is Group ID) 0000.0C9F.FXXX (v2, XXX is Group ID) 0005.73A0.0000 - 0005.73A0.0FFF (IPv6)	0000.5E00.01XX (v1,v2,v3,XX is VRID) 0000.5E00.0200 - 0000.5E00.02FF (IPv6)	0007.b400.XXYY(XX is Group ID,YY is the Gateway number)
Communication Method and Destination	IP Multicast 224.0.0.2 (v1) 224.0.0.102 (v2)	IP Multicast 224.0.0.18 (IPv4) FF02:0:0:0:0:0:0:12 (IPv6)	IP Multicast 224.0.0.102
Communication Protocol	IPv4, UDP port 1985 IPv6, UDP port 2029	IPv4 and IPv6, protocol 112 (IANA)	IPv4 and IPv6, UDP port 3222
Load Balancing	NO	NO	YES
Authentication	Default: No authentication Plain text authentication MD5 authentication (newly added)	Default: No authentication Plain text authentication MD5 authentication	Default: No authentication Plain text authentication MD5 authentication
Active Selector	Priority – One router is elected as Active, another as Standby router. The remaining routers are in a listen state. Highest value wins. Default: 100	Priority – Highest value wins. Default: 100, 254 for router with the same IP as the virtual IP	Priority - One gateway is elected as AVG; another is elected as standby virtual GW (SVG). The remaining routers are in a listen state. Highest value wins. Default: 100
Hello and Hold Time	HELLO - Interval between successive HSRP Hello messages from a given router. Default: 3 sec HOLD - Interval between the receipt of a Hello, and the presumption that the sending router failed. Default: 10 sec	Unlike HSRP and GLBP, VRRP does not learn timers from the master router. VRRP requires that the hello timer of all routers in the group match. HELLO – Default: 1 sec, HOLD - Default: 3 sec	HELLO - Interval between successive GLBP Hello messages from a given router. Default: 3 sec HOLD - Interval between the receipt of a Hello, and the presumption that the sending router failed. Default: 10 sec
Preemption	Use of preemption allows a HSRP device whose priority has become higher to take over the role as the active router in HSRP. Default: preempt off	With preemption enabled, VRRP switches to a backup if that backup comes online with a priority higher than the new master. Default: preempt on. Exception: The router that owns the IP address (es) associated with the virtual router always preempts.	AVG Preemption allows a backup virtual gateway to become AVG, if it has a higher priority than the current AVG. Default: preempt off AVF (Forwarder) Preemption is similar, except that the forwarder preemption uses weighting instead of priority, and it is enabled by default with delay of 30 seconds.

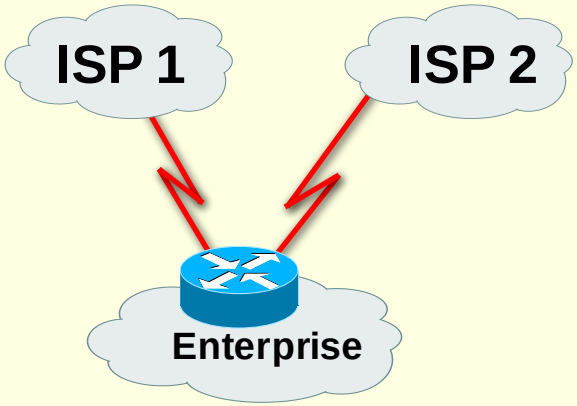
Multihoming Internet



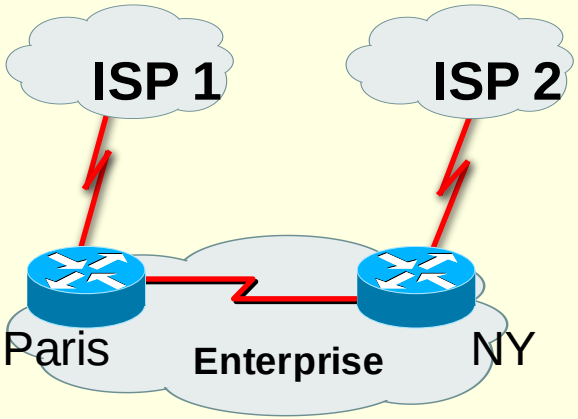
Option A



Option C



Option B



Option D

	Number of Routers at the Enterprise	Number of Connections to the Internet	Number of ISPs	Advantages	Disadvantages
Option A	1	2	1	WAN backup; low cost; working with one ISP can be easier than working with multiple ISPs.	No ISP redundancy; router is a single point of failure; this solution assumes the ISP has two access points near the enterprise.
Option B	1	2	2	WAN backup; low cost; ISP redundancy.	Router is a single point of failure; it can be difficult to deal with policies and procedures of two different ISPs.
Option C	2	2	1	WAN backup; especially good for geographically dispersed company; medium cost; working with one ISP can be easier than working with multiple ISPs.	No ISP redundancy.
Option D	2	2	2	WAN backup; especially good for geographically dispersed company; ISP redundancy.	High cost; it can be difficult to deal with policies and procedures of two different ISPs.

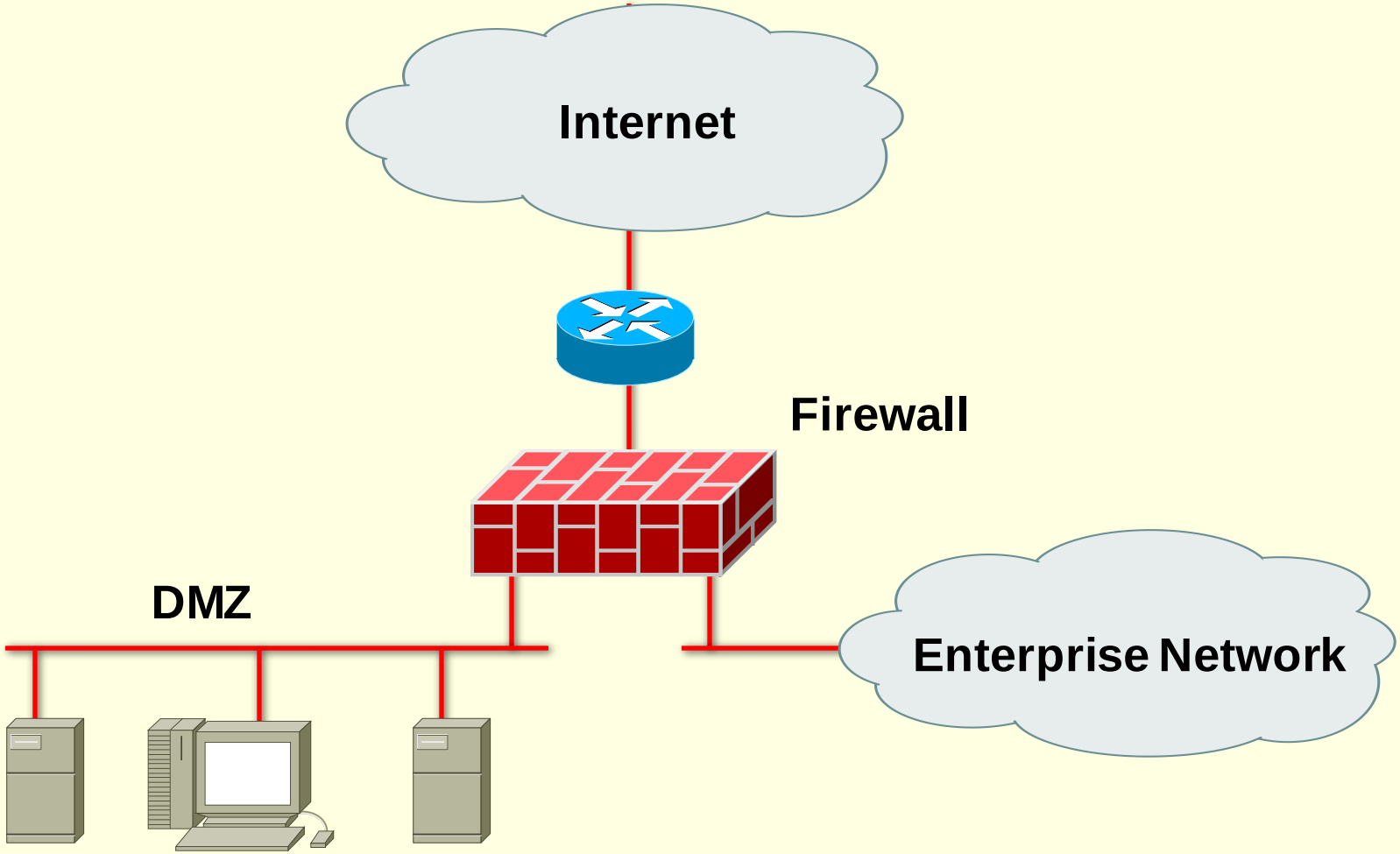
Virtual Private Network (VPN)

VPN applications for enterprise networks can be divided into two main categories:

- **Site-to-site VPNs:** Site-to-site VPNs focus on connecting geographically dispersed offices and extending the classic enterprise WAN. A site-to-site VPN can also add interconnections between multiple organizations, in which case it is sometimes called an extranet VPN.

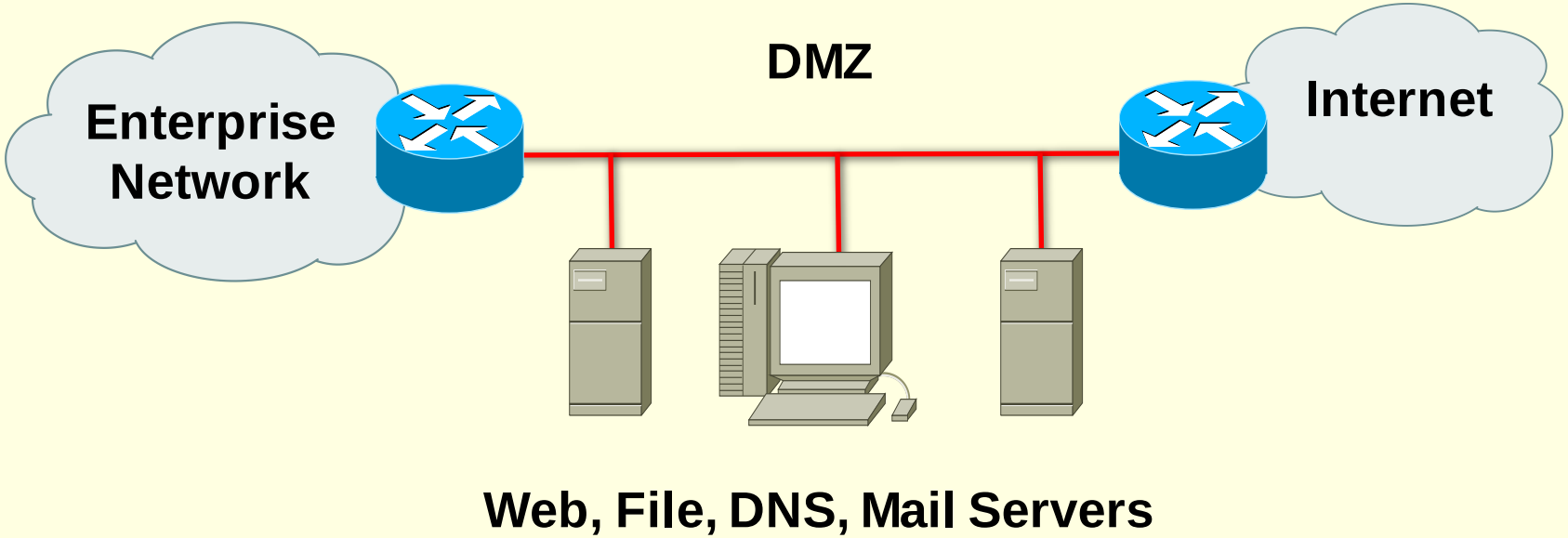
- **Remote-access VPNs:** Remote-access VPNs focus on remote users and business partners who access the network on an as-needed basis.

Security Topologies



Web, File, DNS, Mail Servers

Security Topologies



Disadvantages

- the configuration on the routers might be complex
- the traffic for the enterprise network flows through the DMZ.