

Top-Down Network Design

Chapter Five

Designing a Network Topology

Copyright 2010 Cisco Press & Priscilla Oppenheimer

Topology

- A branch of mathematics concerned with those properties of geometric configurations that are unaltered by elastic deformations such as stretching or twisting
- A term used in the computer networking field to describe the structure of a network



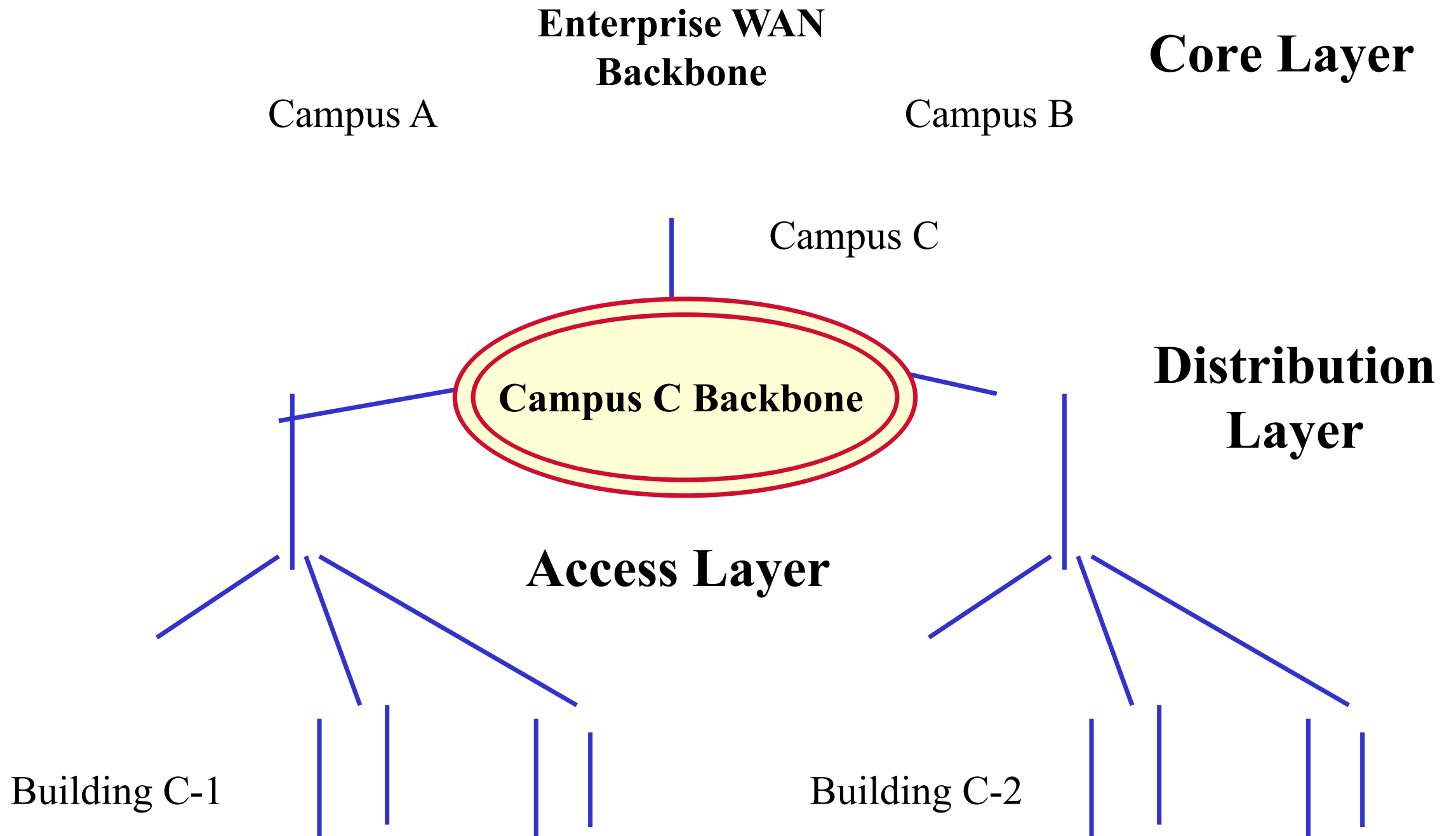
Network Topology Design Themes

- Hierarchy
- Redundancy
- Modularity
- Well-defined entries and exits
- Protected perimeters

Why Use a Hierarchical Model?

- Reduces workload on network devices
 - Avoids devices having to communicate with too many other devices (reduces “CPU adjacencies”)
- Constrains broadcast domains
- Enhances simplicity and understanding
- Facilitates changes
- Facilitates scaling to a larger size

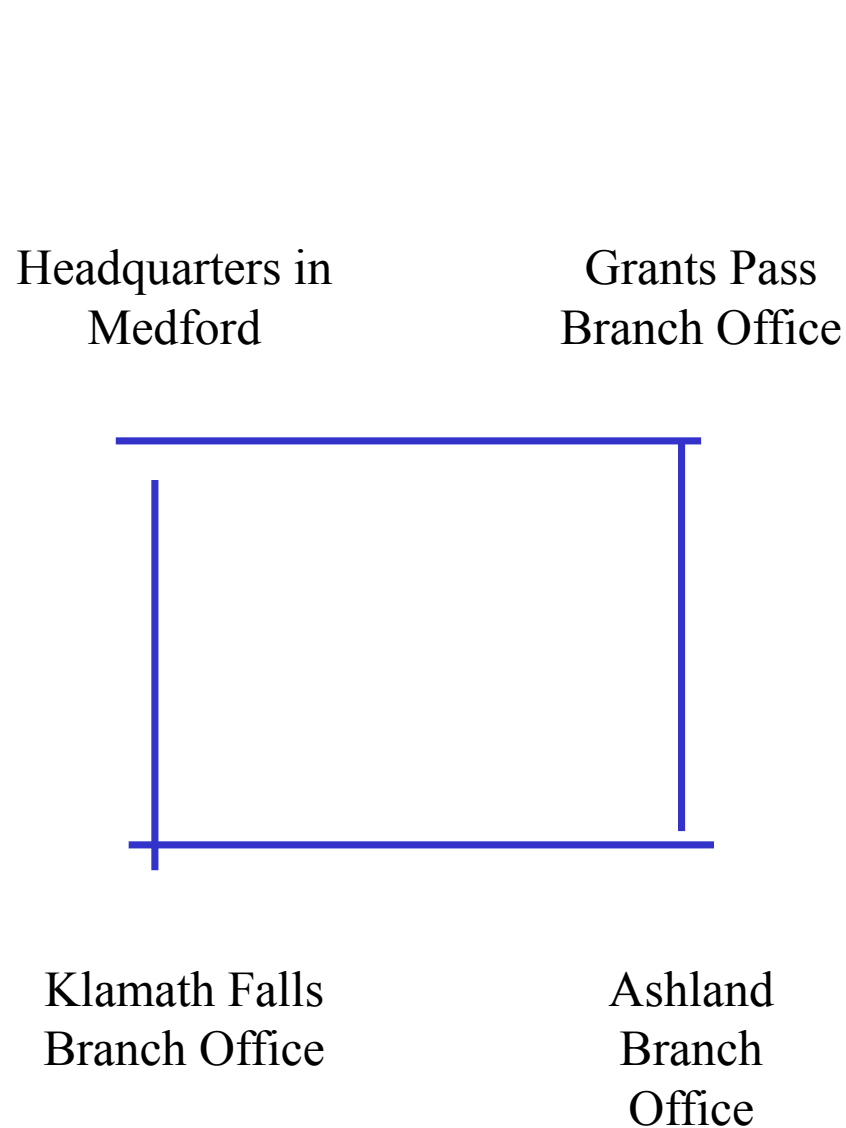
Hierarchical Network Design



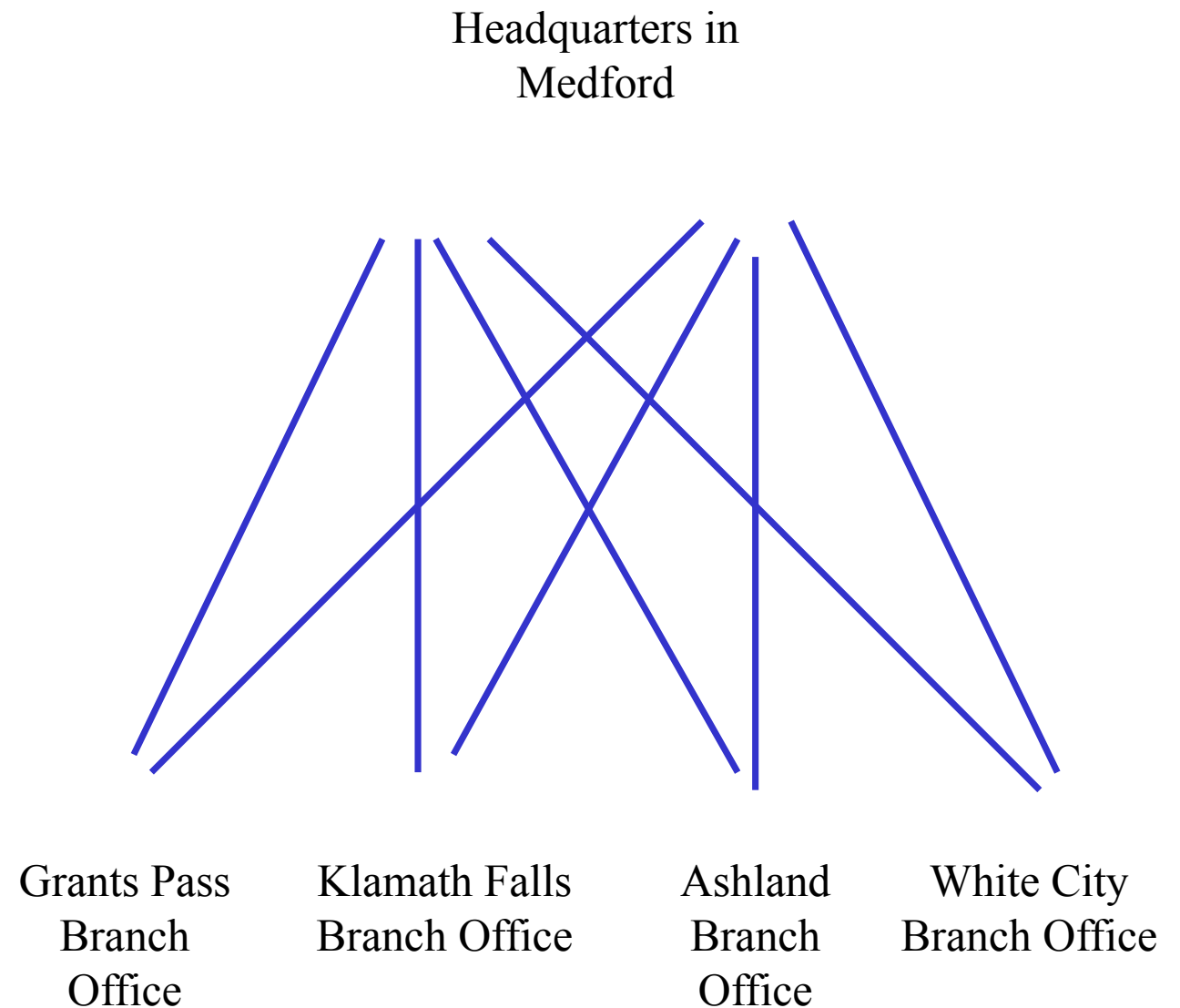
Cisco's Hierarchical Design Model

- A core layer of high-end routers and switches that are optimized for availability and speed
- A distribution layer of routers and switches that implement policies and segment traffic
- An access layer that connects users via hubs, switches, and other devices

Flat Versus Hierarchy

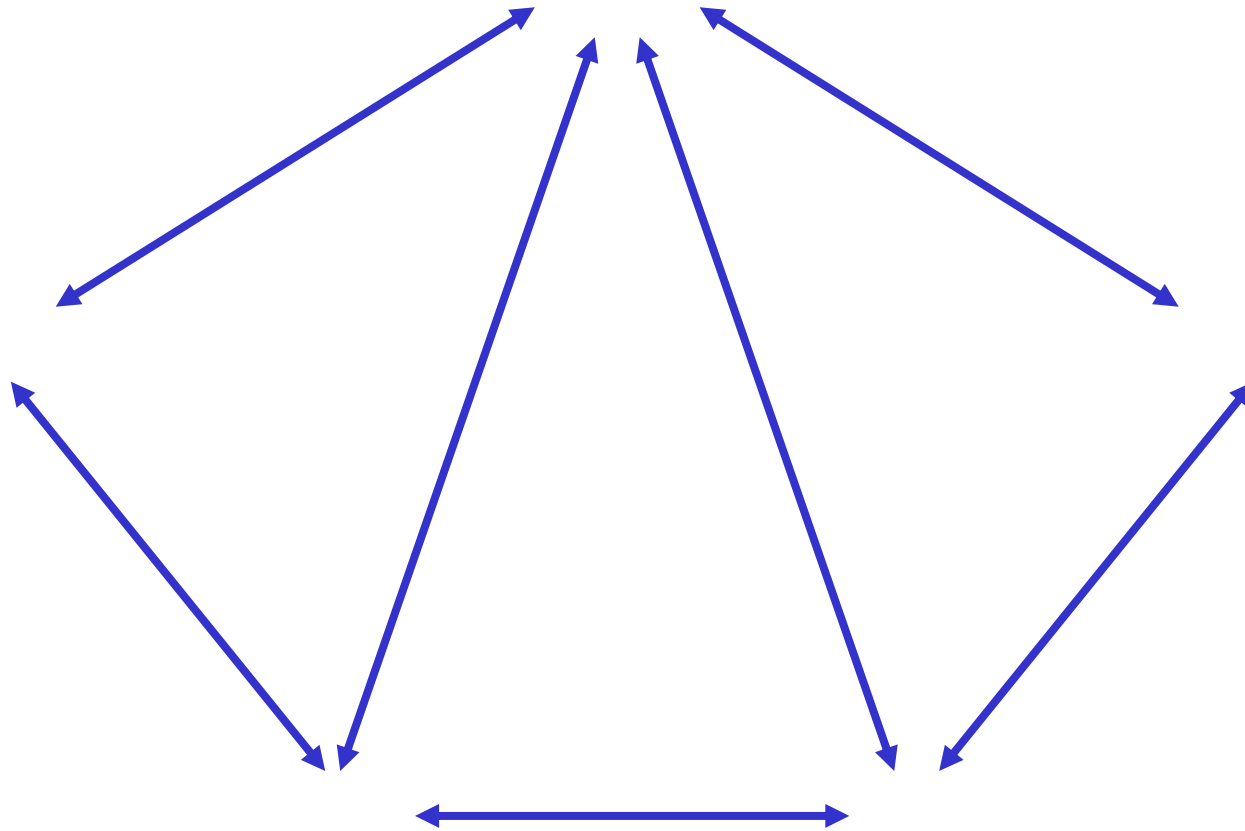


Flat Loop Topology

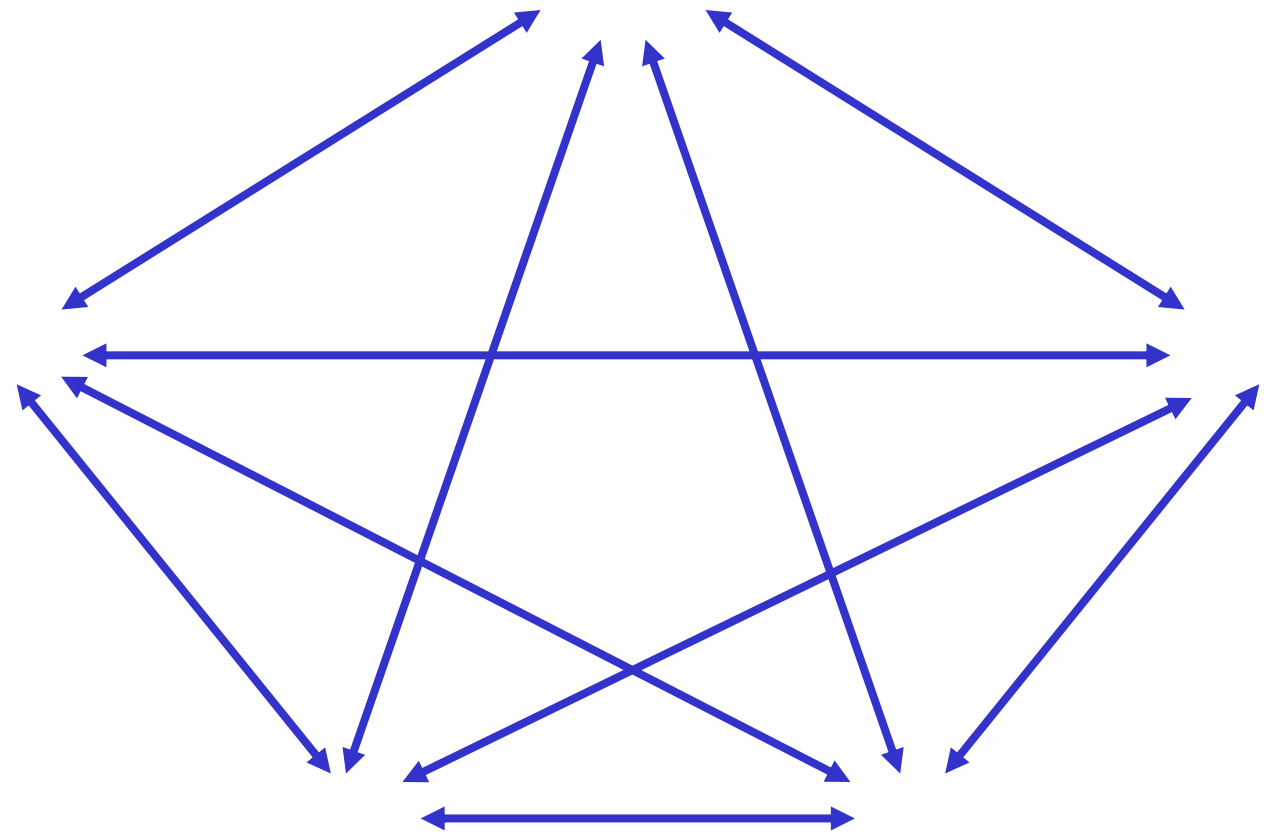


Hierarchical Redundant Topology

Mesh Designs

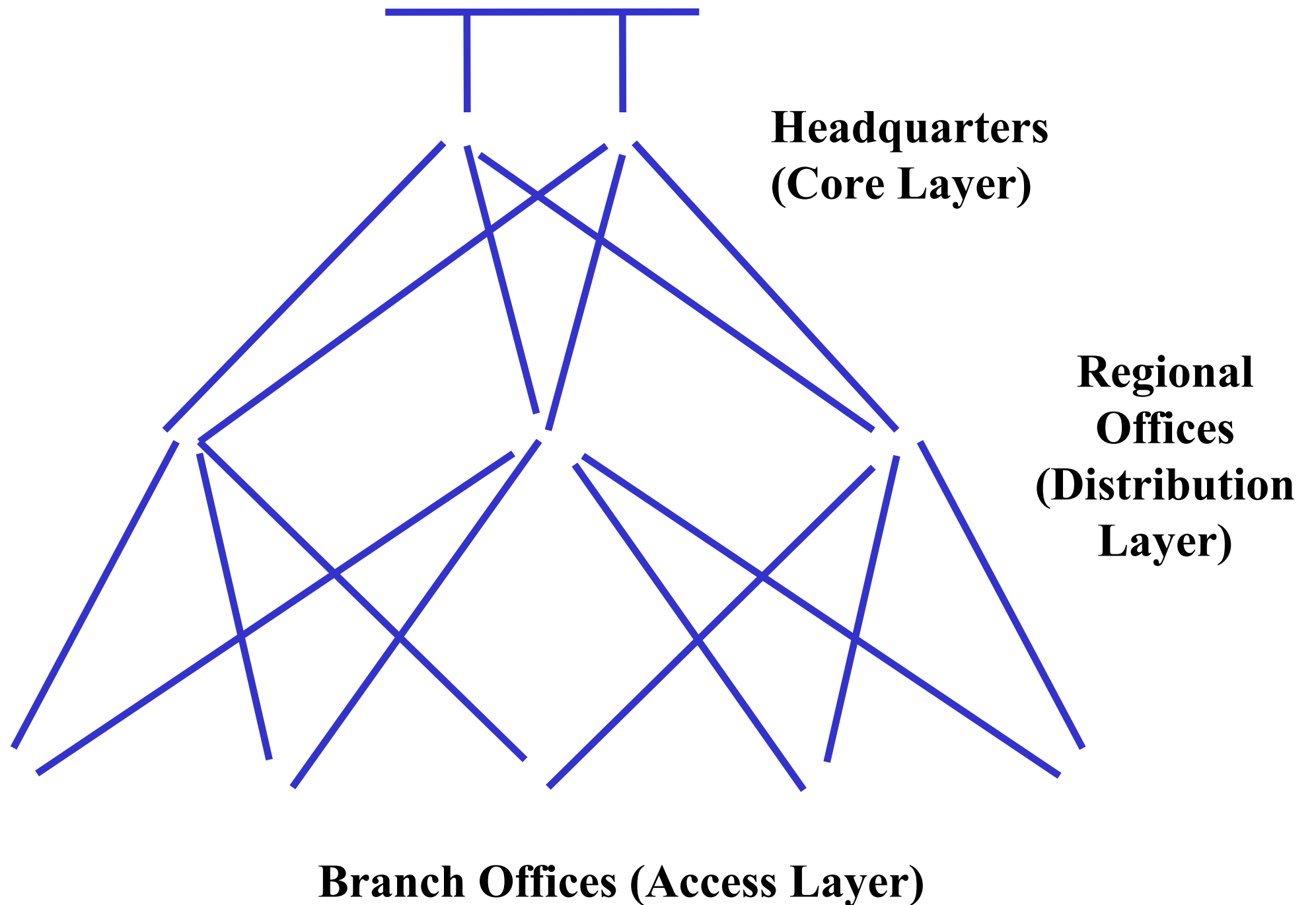


Partial-Mesh Topology

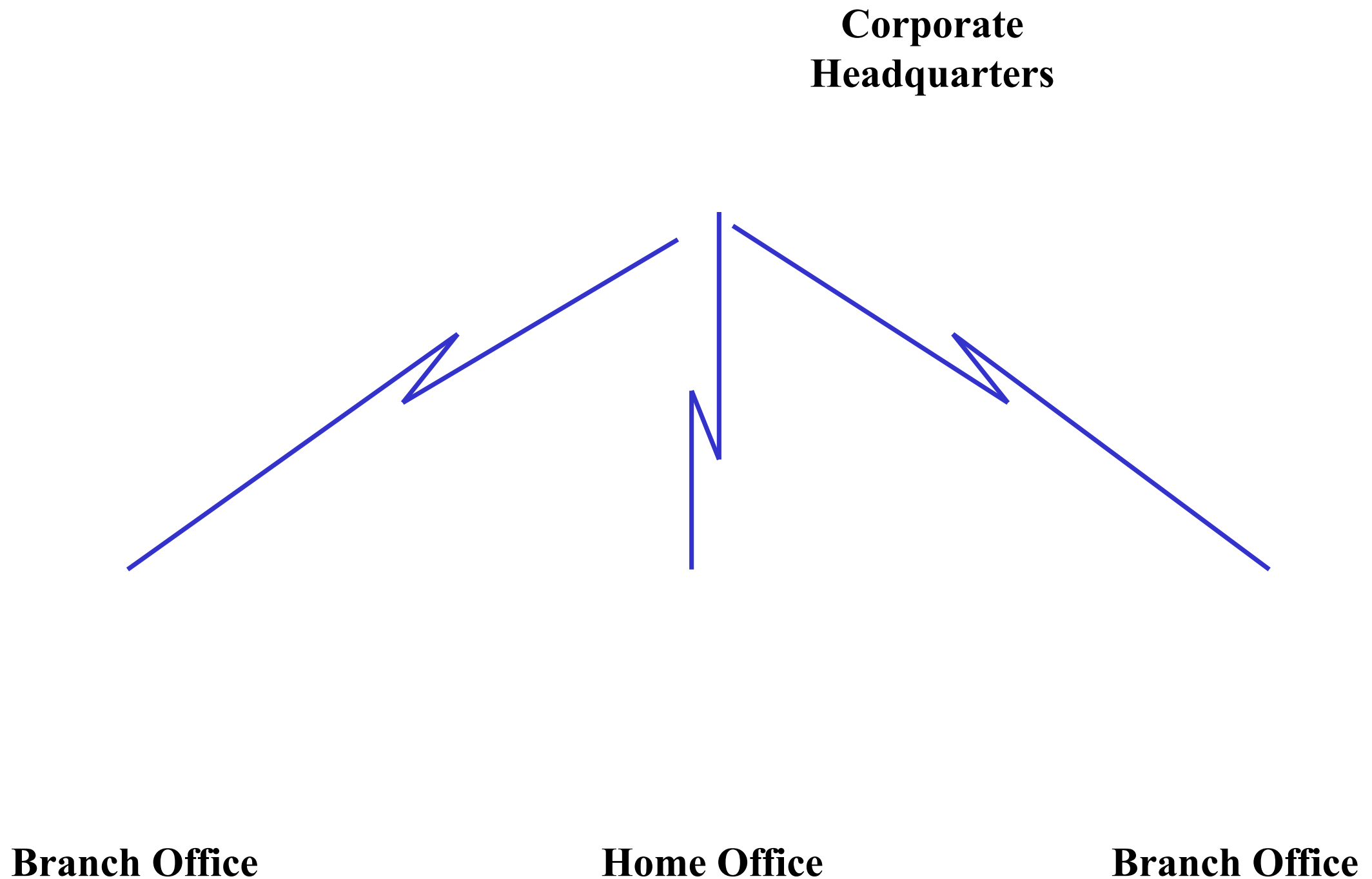


Full-Mesh Topology

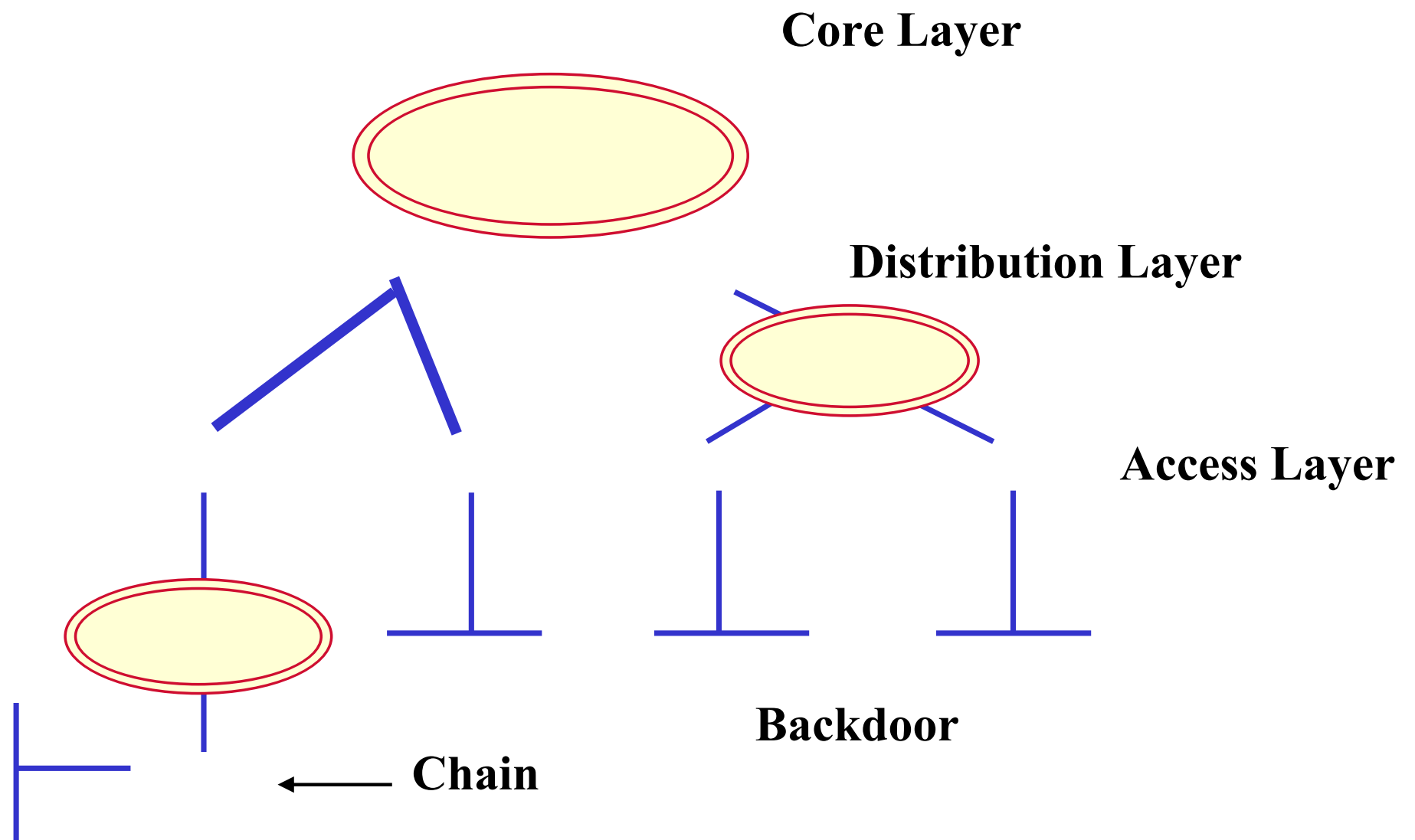
A Partial-Mesh Hierarchical Design



A Hub-and-Spoke Hierarchical Topology



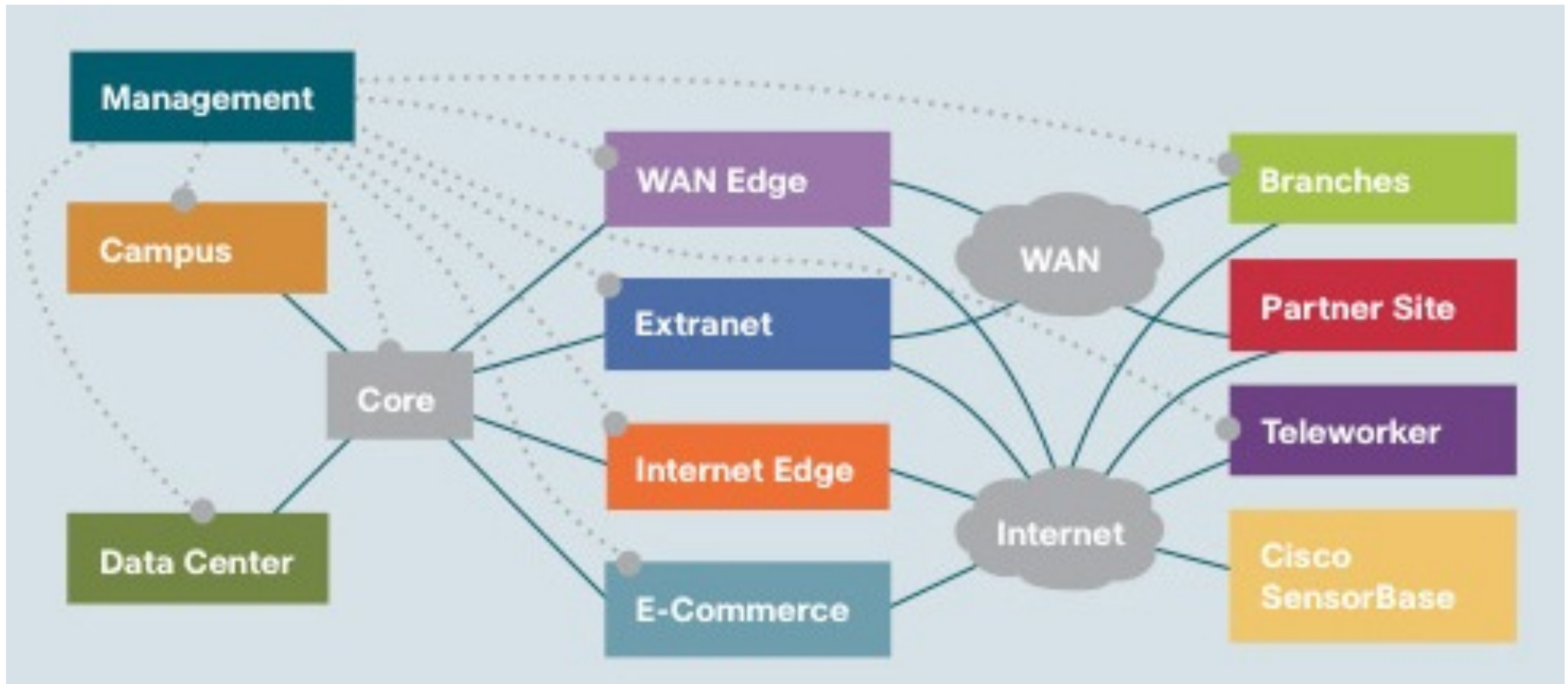
Avoid Chains and Backdoors



How Do You Know When 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

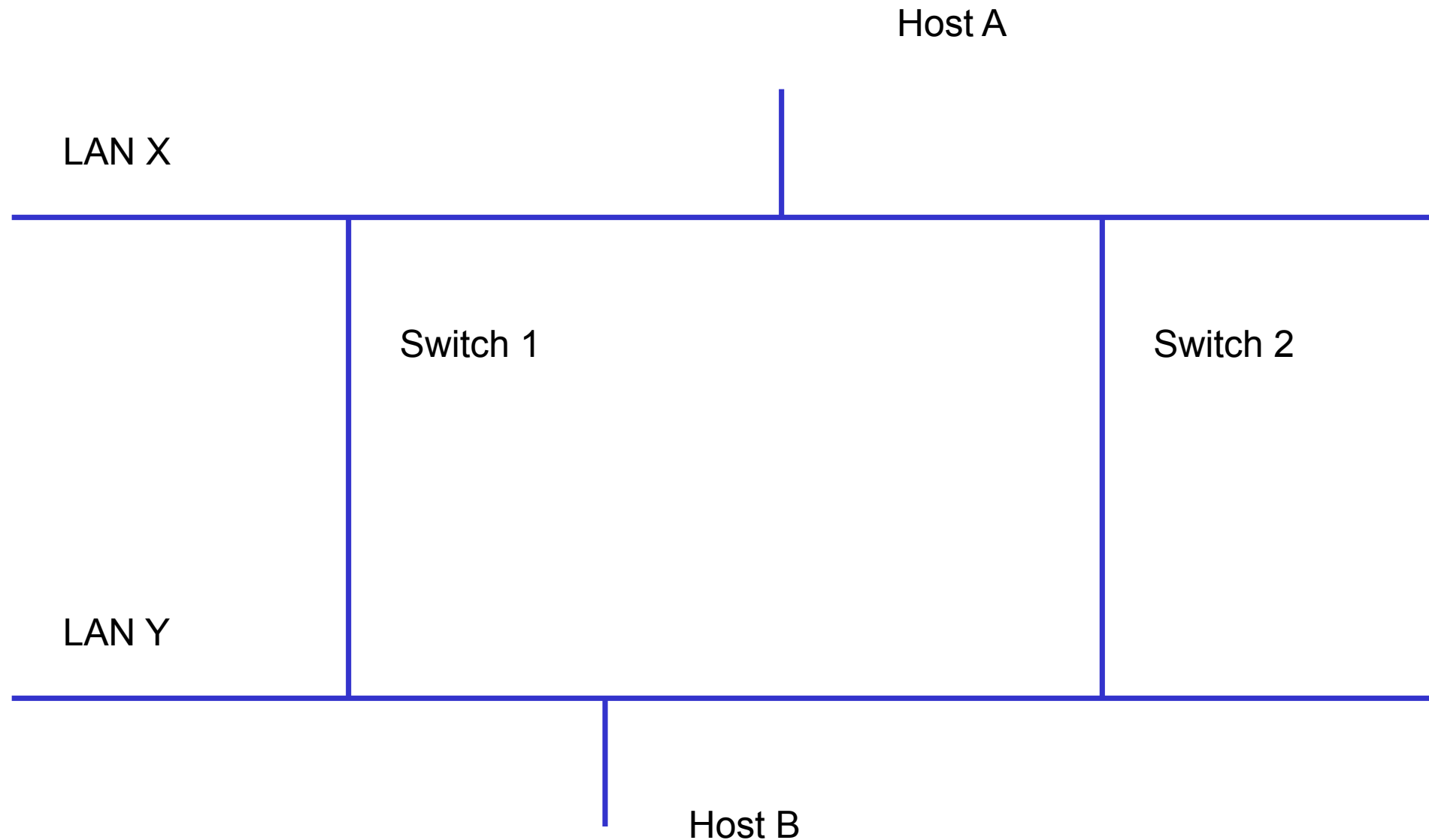
Cisco's SAFE Security Reference Architecture



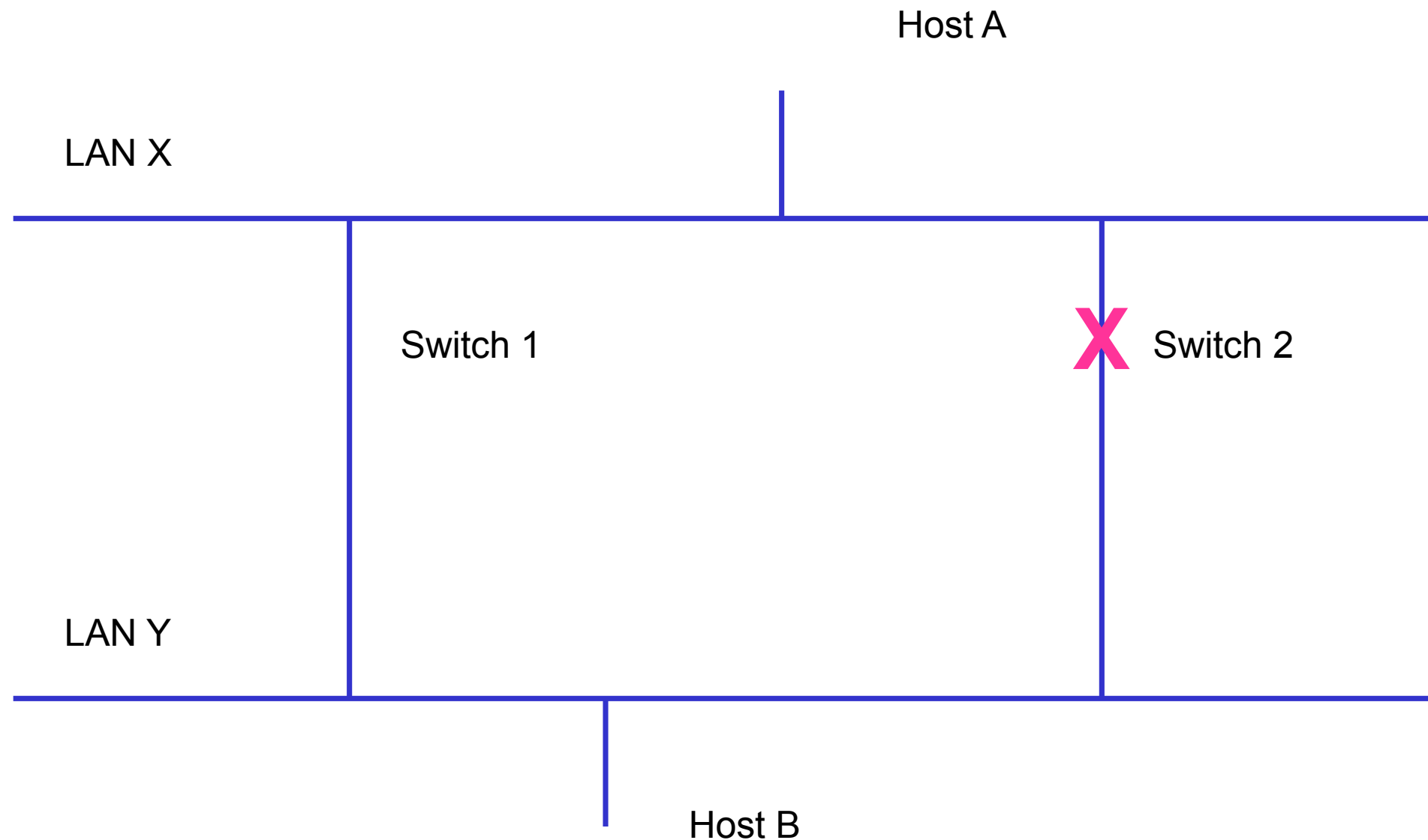
Campus Topology Design

- 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

A Simple Campus Redundant Design



Bridges and Switches use Spanning-Tree Protocol (STP) to Avoid Loops



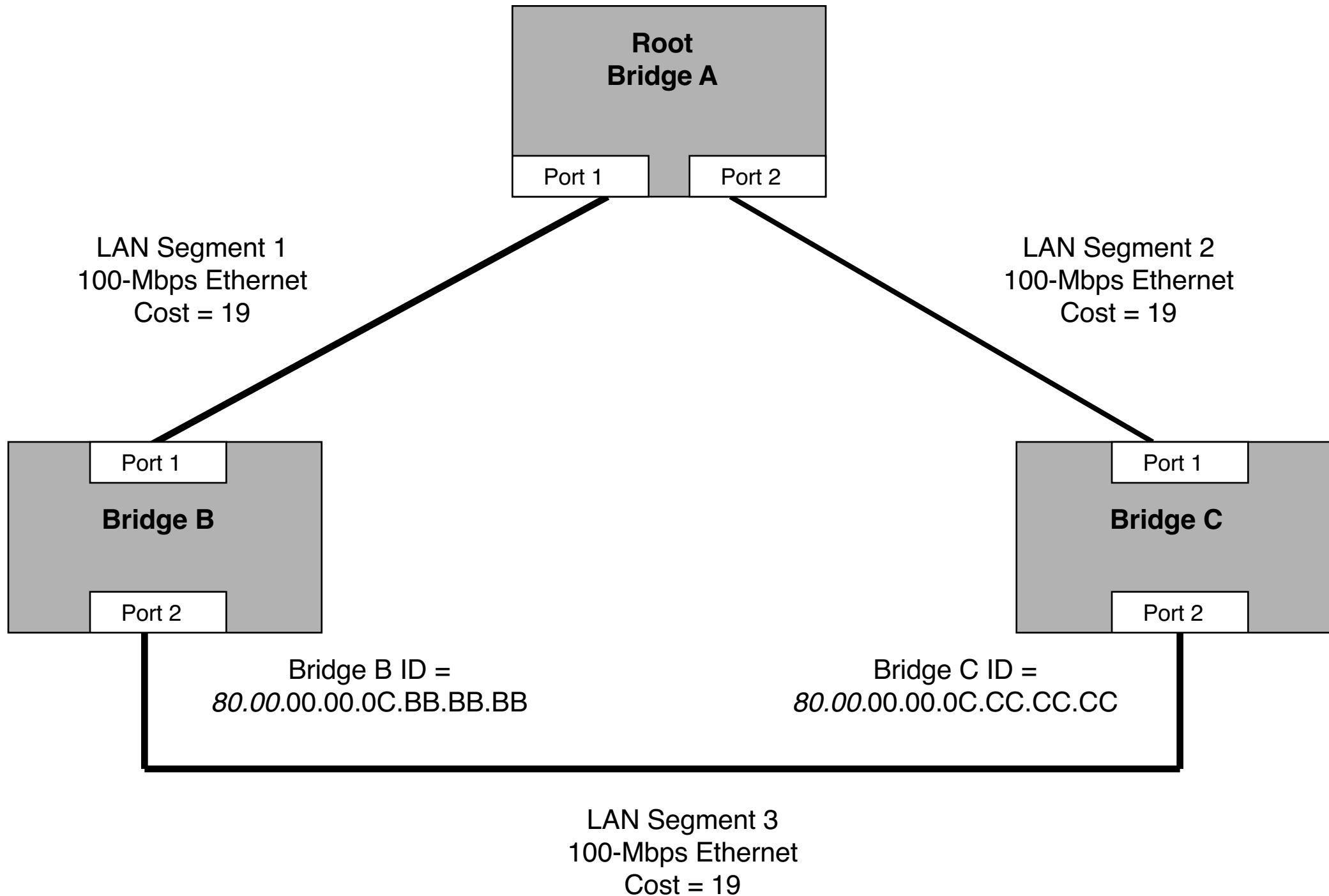
Bridges (Switches) Running STP

- Participate with other bridges in the election of a single bridge as the Root Bridge.
- Calculate the distance of the shortest path to the Root Bridge and choose a port (known as the Root Port) that provides the shortest path to the Root Bridge.
- For each LAN segment, elect a Designated Bridge and a Designated Port on that 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.)
- Select bridge ports to be included in the spanning tree. The ports selected are the Root Ports and Designated Ports. These ports forward traffic. Other ports block traffic.

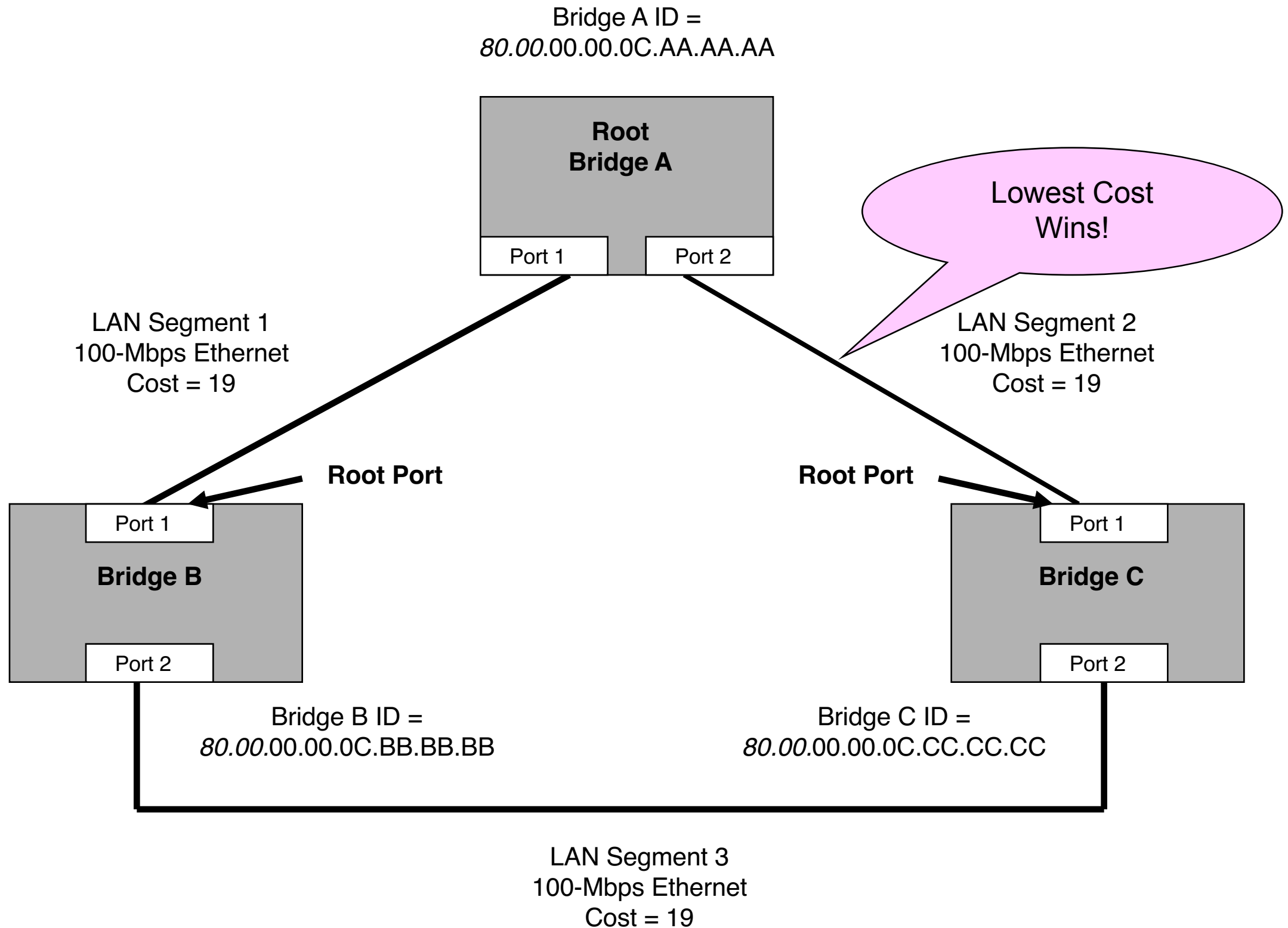
Elect a Root

Lowest Bridge ID Wins!

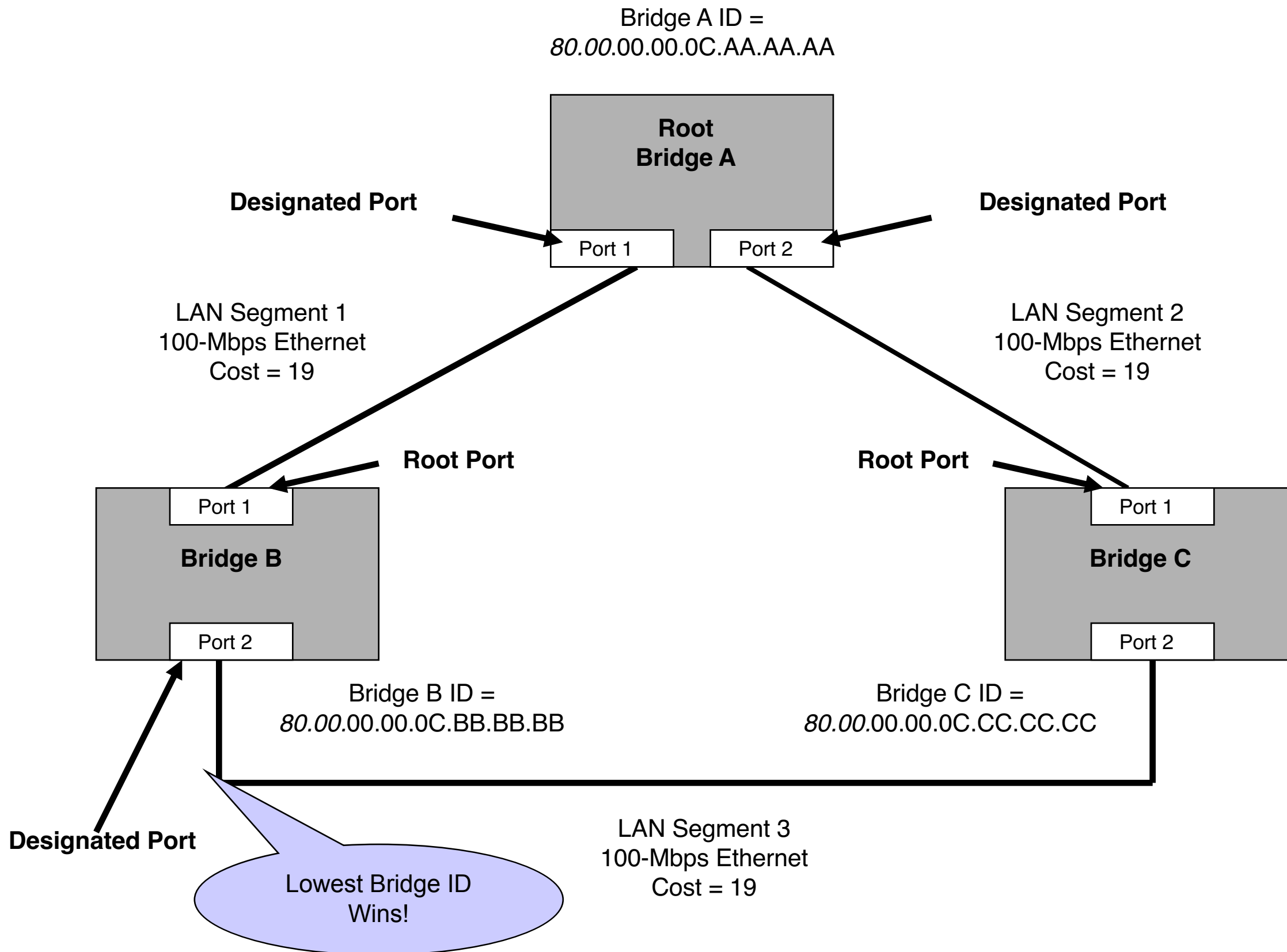
Bridge A ID =
80.00.00.00.0C.AA.AA.AA



Determine Root Ports

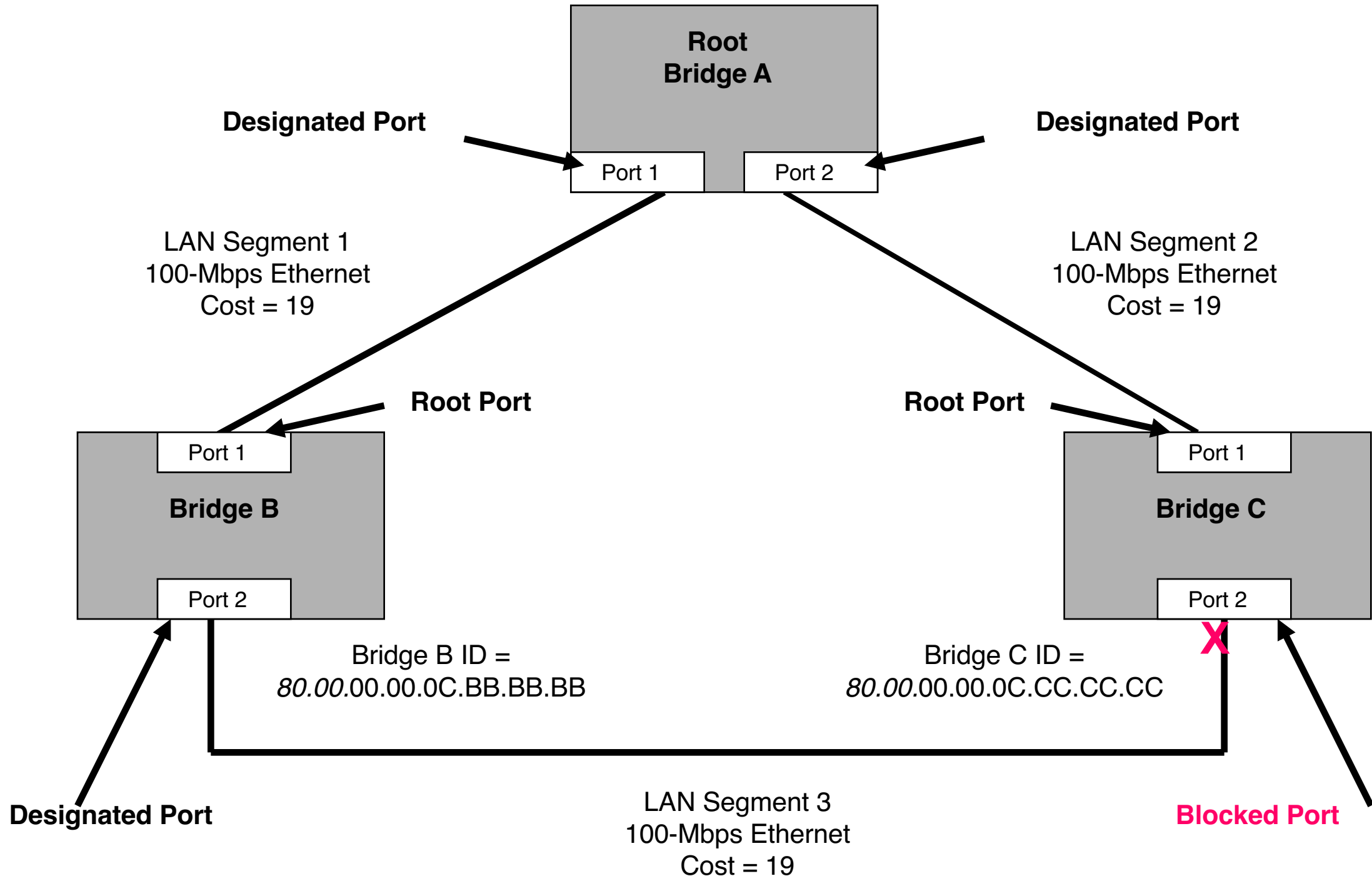


Determine Designated Ports

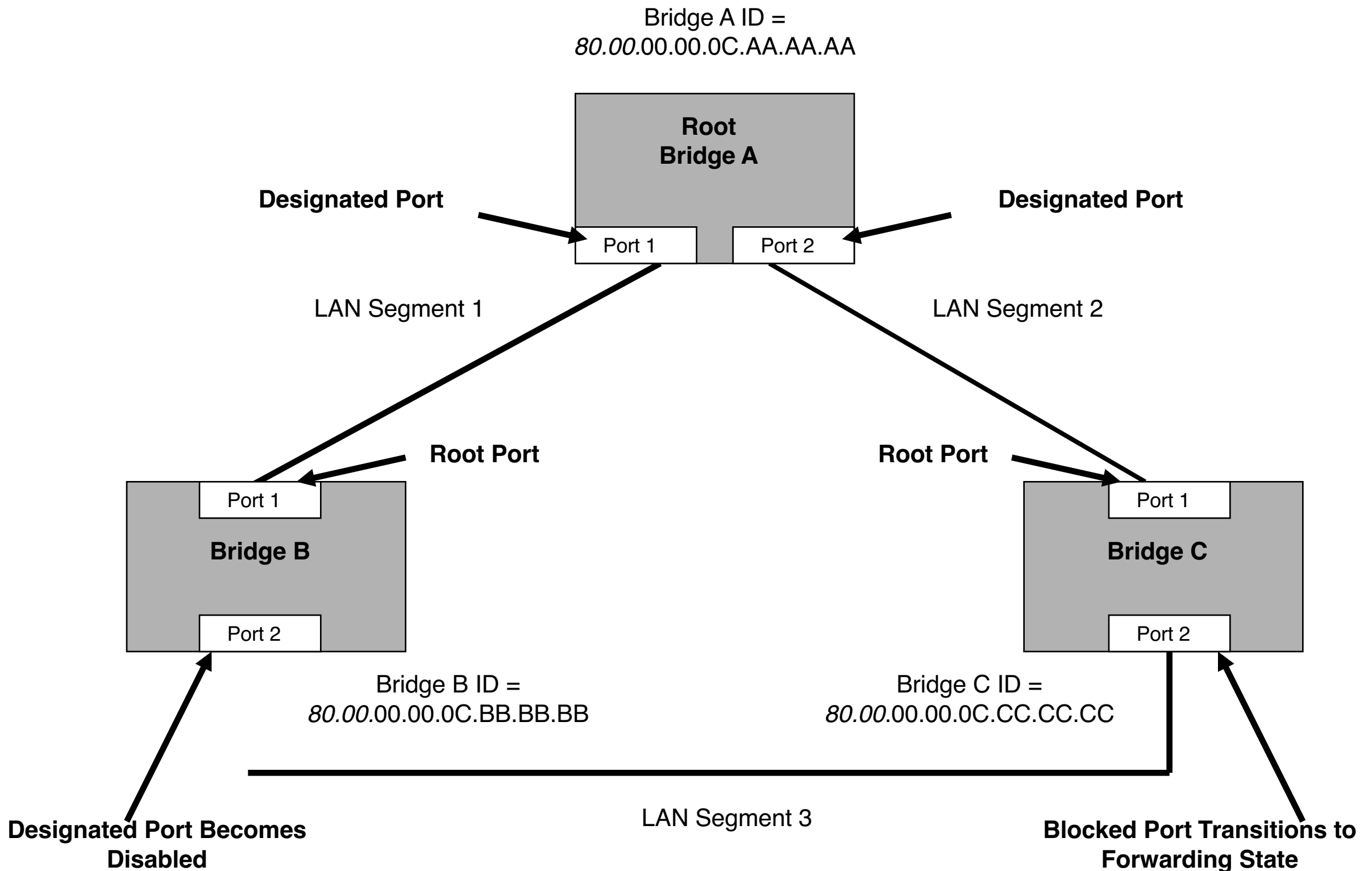


Prune Topology into a Tree!

Bridge A ID =
80.00.00.00.0C.AA.AA.AA



React to Changes



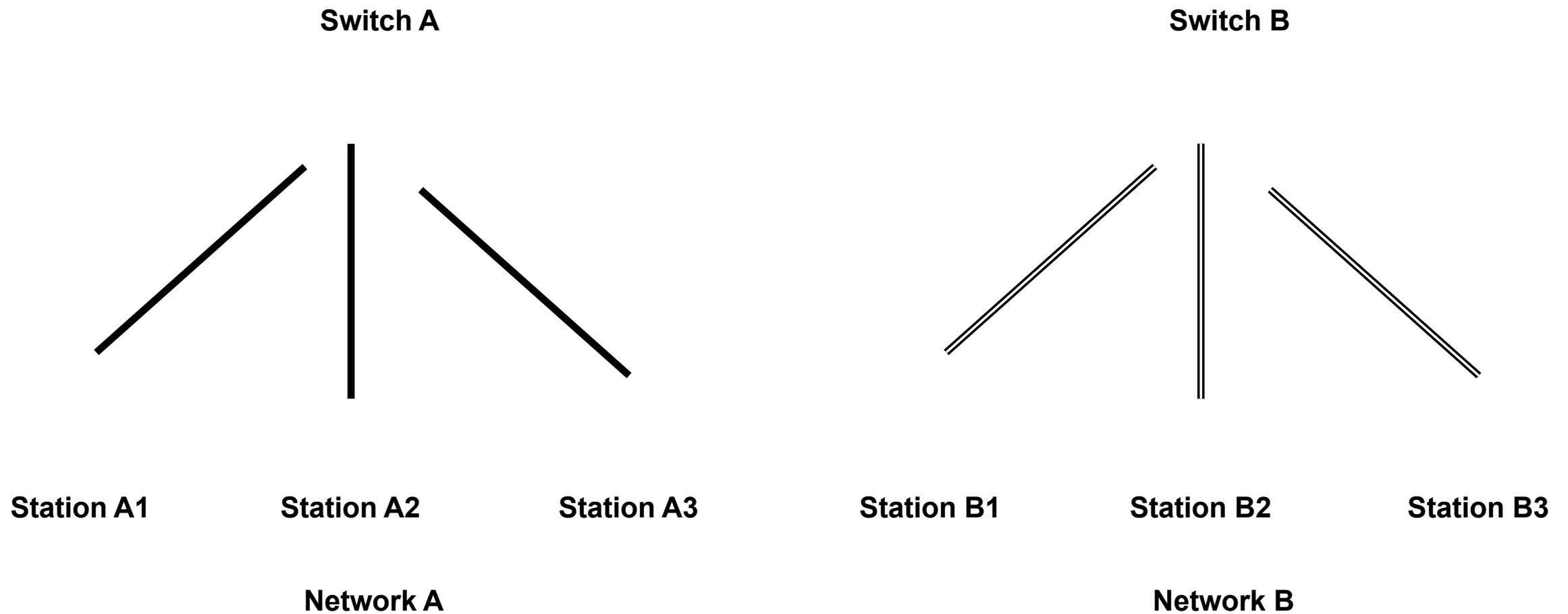
Scaling the Spanning Tree Protocol

- Keep the switched network small
 - It shouldn't span more than seven switches
- Use BPDU skew detection on Cisco switches
- Use IEEE 802.1w
 - Provides rapid reconfiguration of the spanning tree
 - Also known as RSTP

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

VLANs versus Real LANs



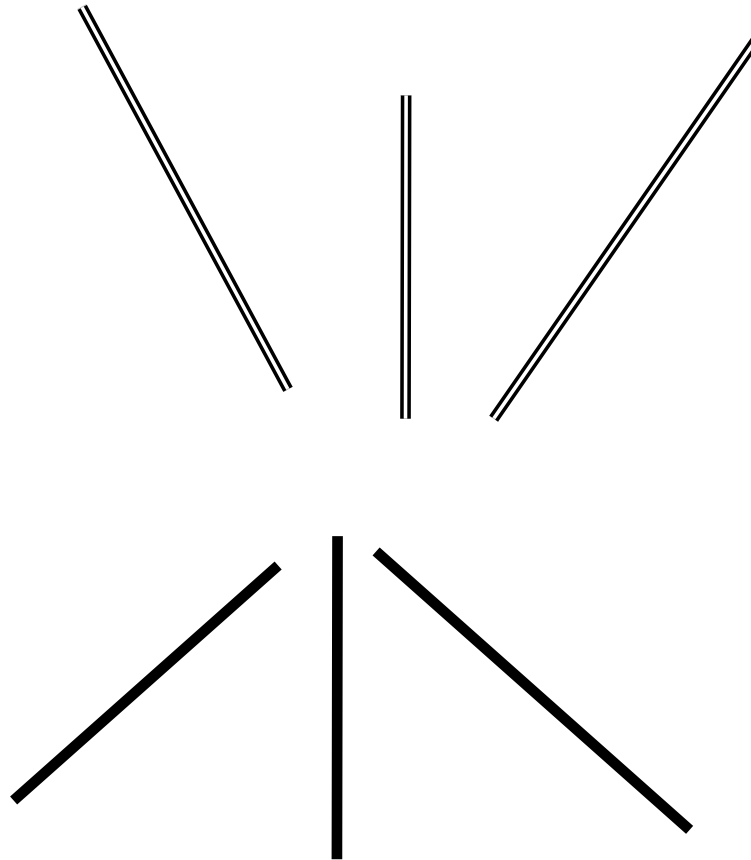
A Switch with VLANs

VLAN 1

Station A1

Station A2

Station A3

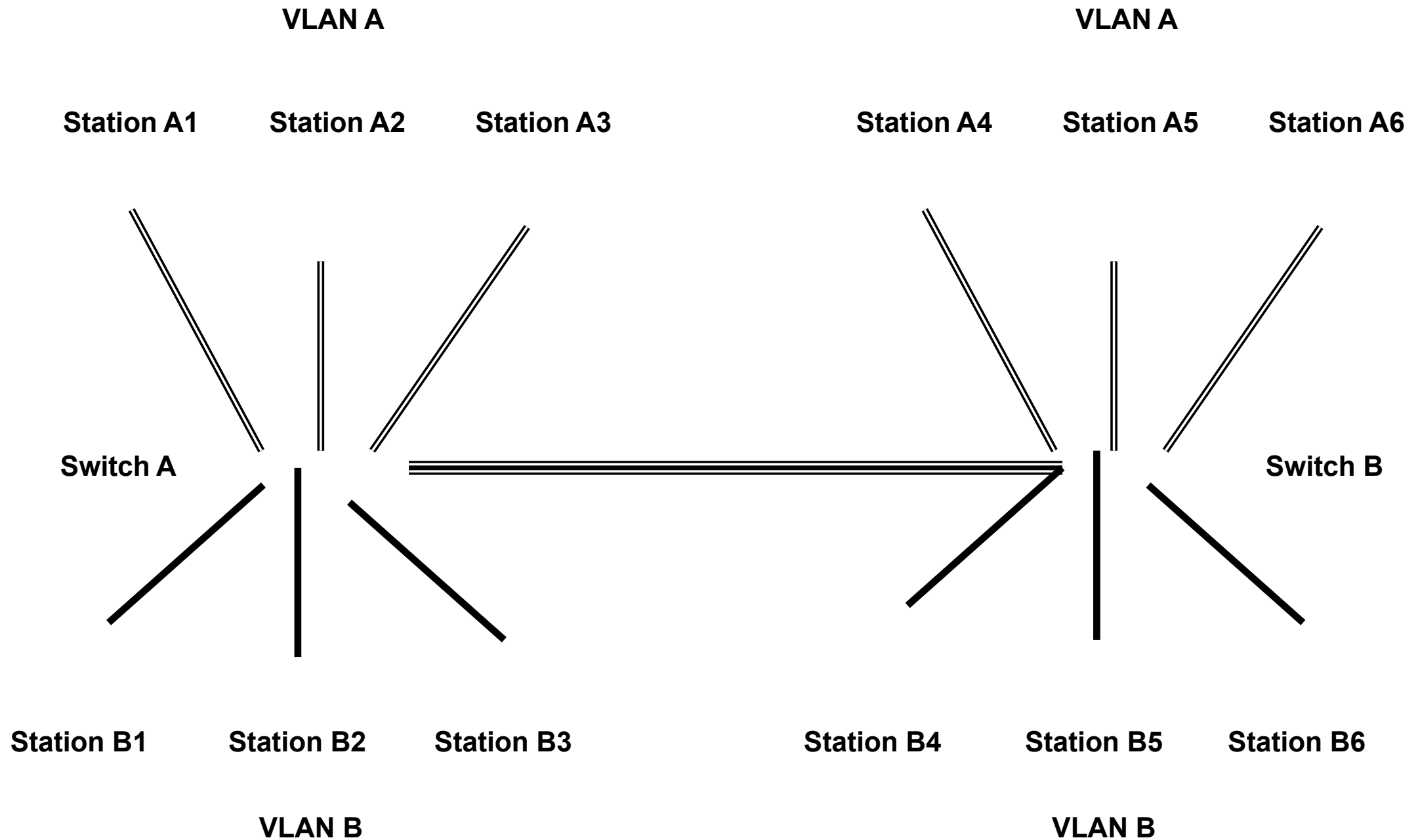


Station B1

Station B2

Station B3

VLANs Span Switches



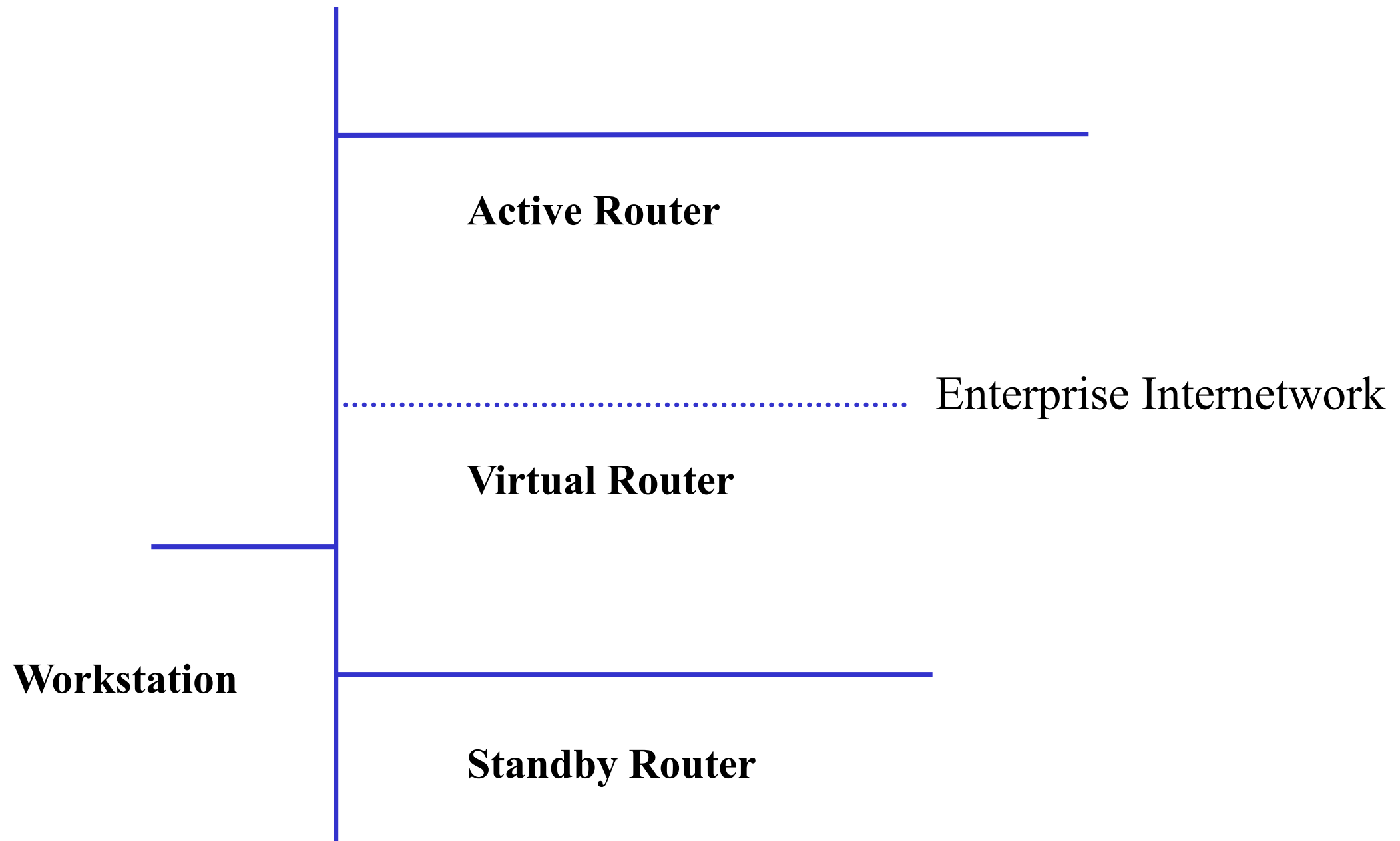
WLANs and VLANs

- 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

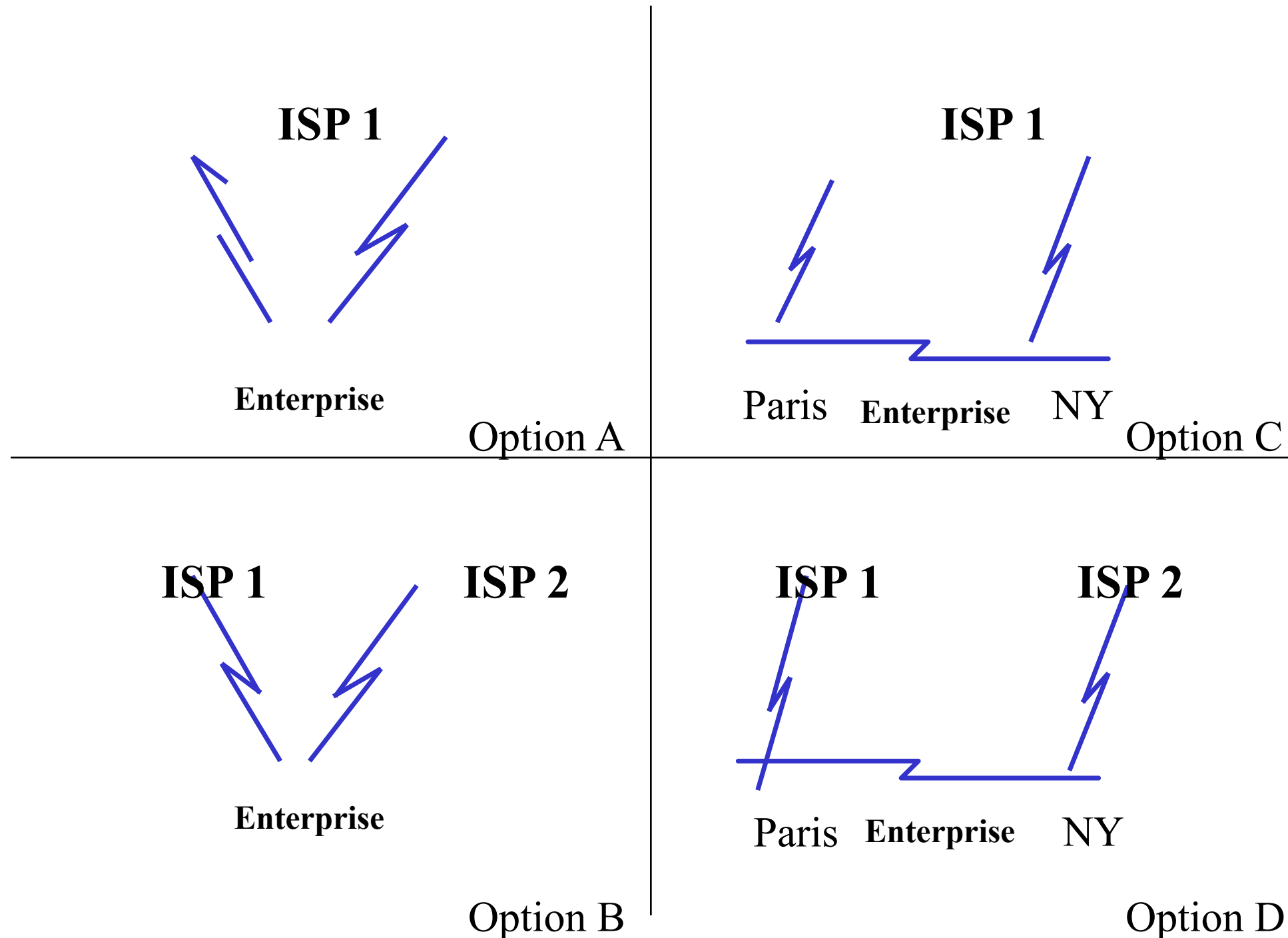
Workstation-to-Router Communication

- 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

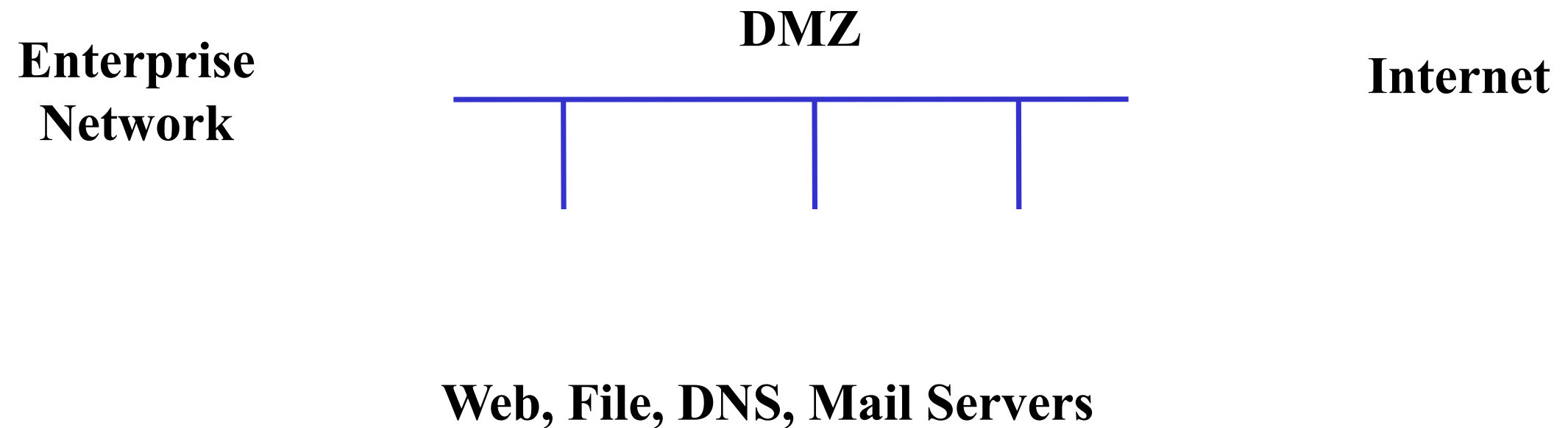
HSRP



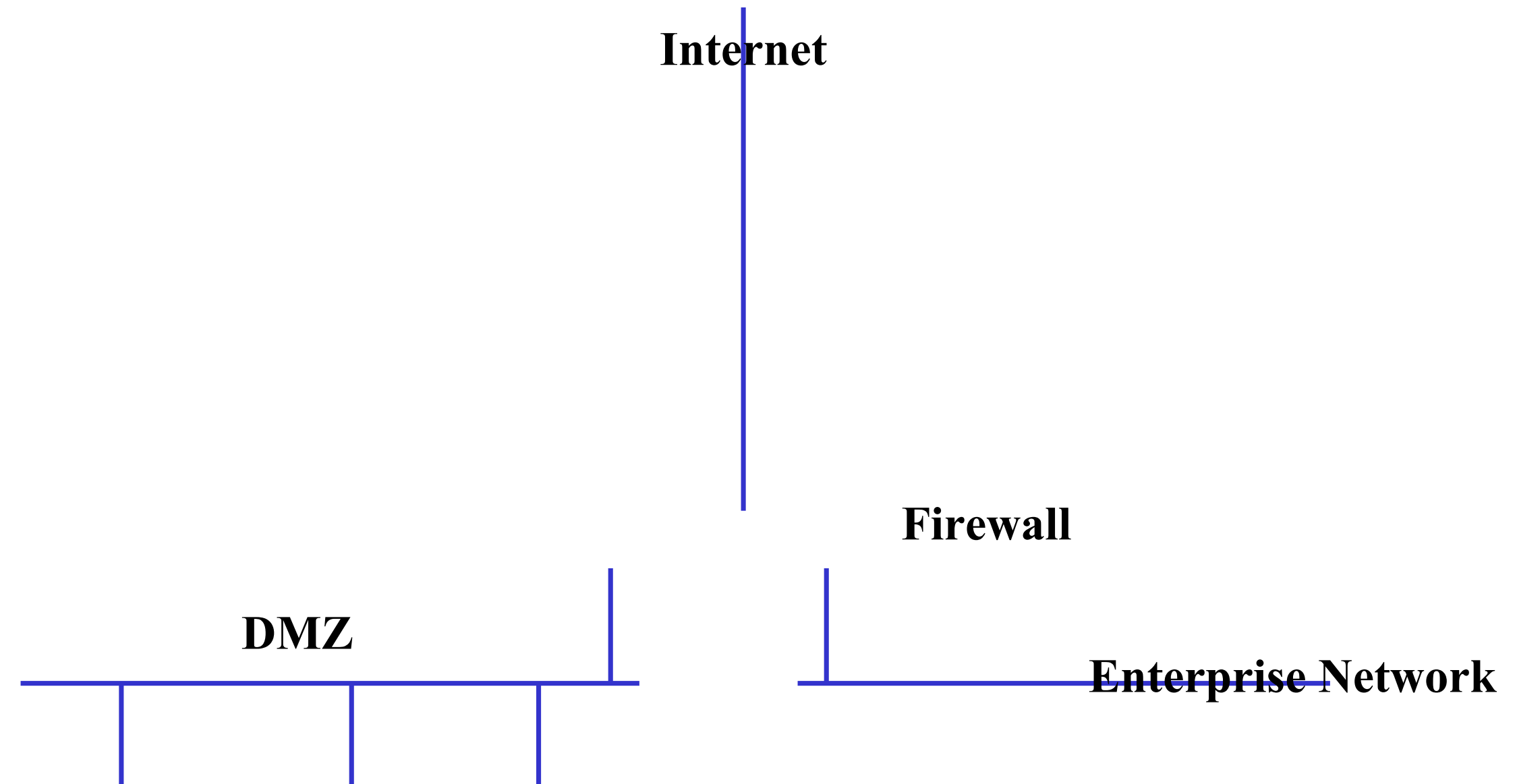
Multihoming the Internet Connection



Security Topologies



Security Topologies



Web, File, DNS, Mail Servers

Summary

- Use a systematic, top-down approach
- Plan the logical design before the physical design
- Topology design should feature hierarchy, redundancy, modularity, and security

Review Questions

- Why are hierarchy and modularity important for network designs?
- What are the three layers of Cisco's hierarchical network design?
- What are the major components of Cisco's enterprise composite network model?
- What are the advantages and disadvantages of the various options for multihoming an Internet connection?