Chapter 5.2:
Network Design

NGUYỄN CAO ĐẠT
E-mail:dat@hcmut.edu.vn

Outline

- Logical Network Design
  - Design a network topology
  - Design models for addressing and naming
  - Select switching and routing protocols
  - Develop network security strategies
  - Develop network management strategies

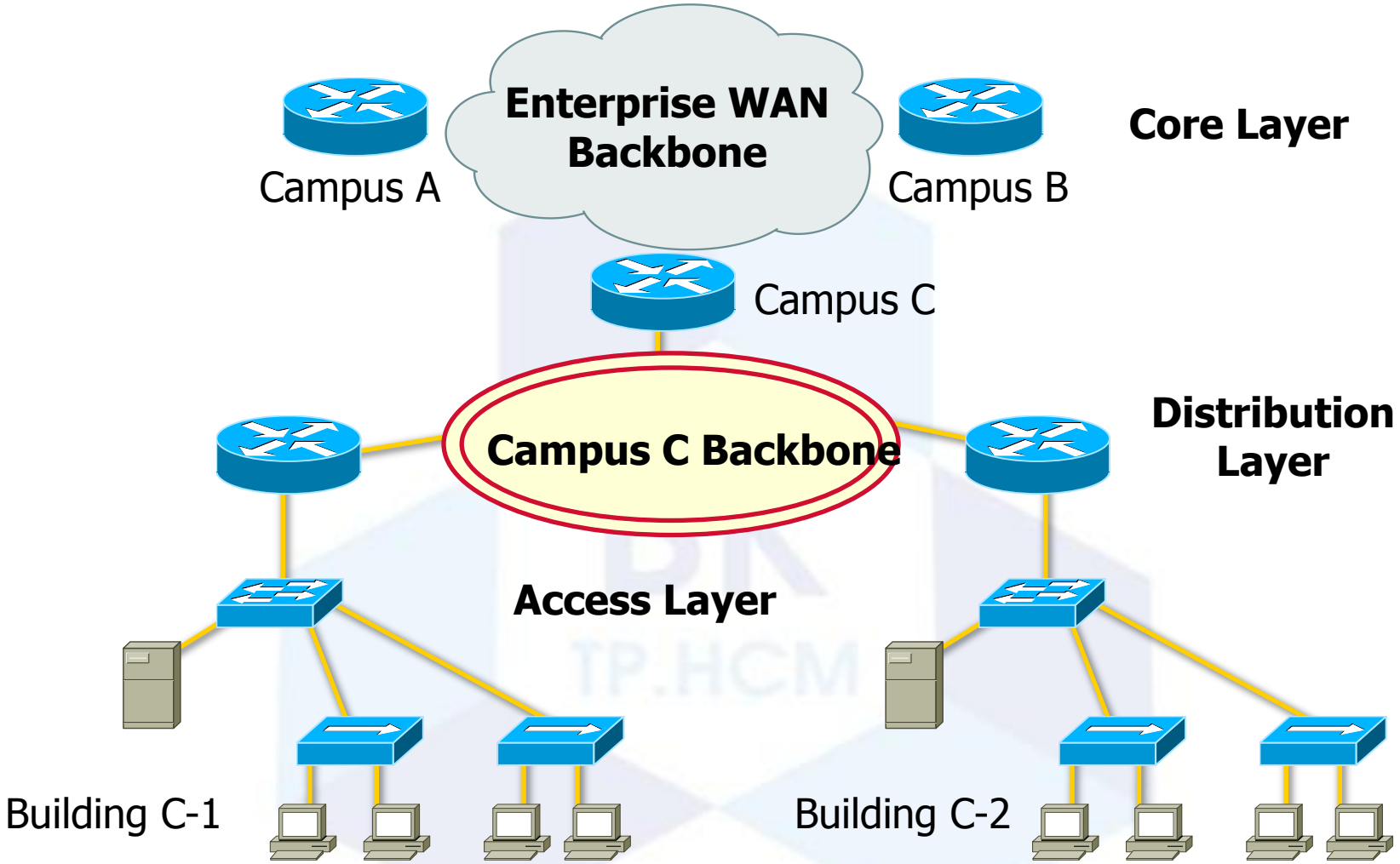
Network Topology Design Themes

- 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

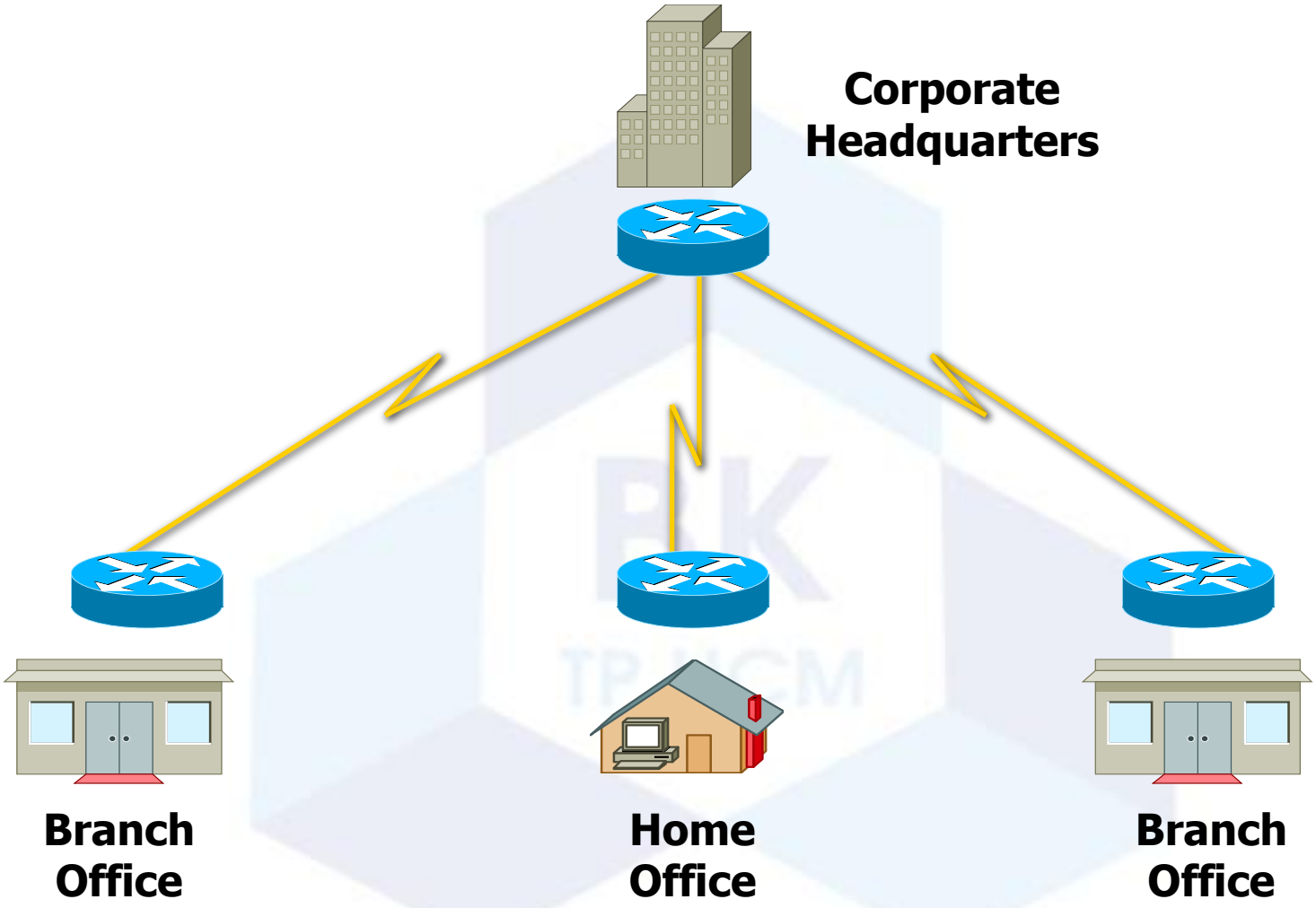
Hierarchical Network Design



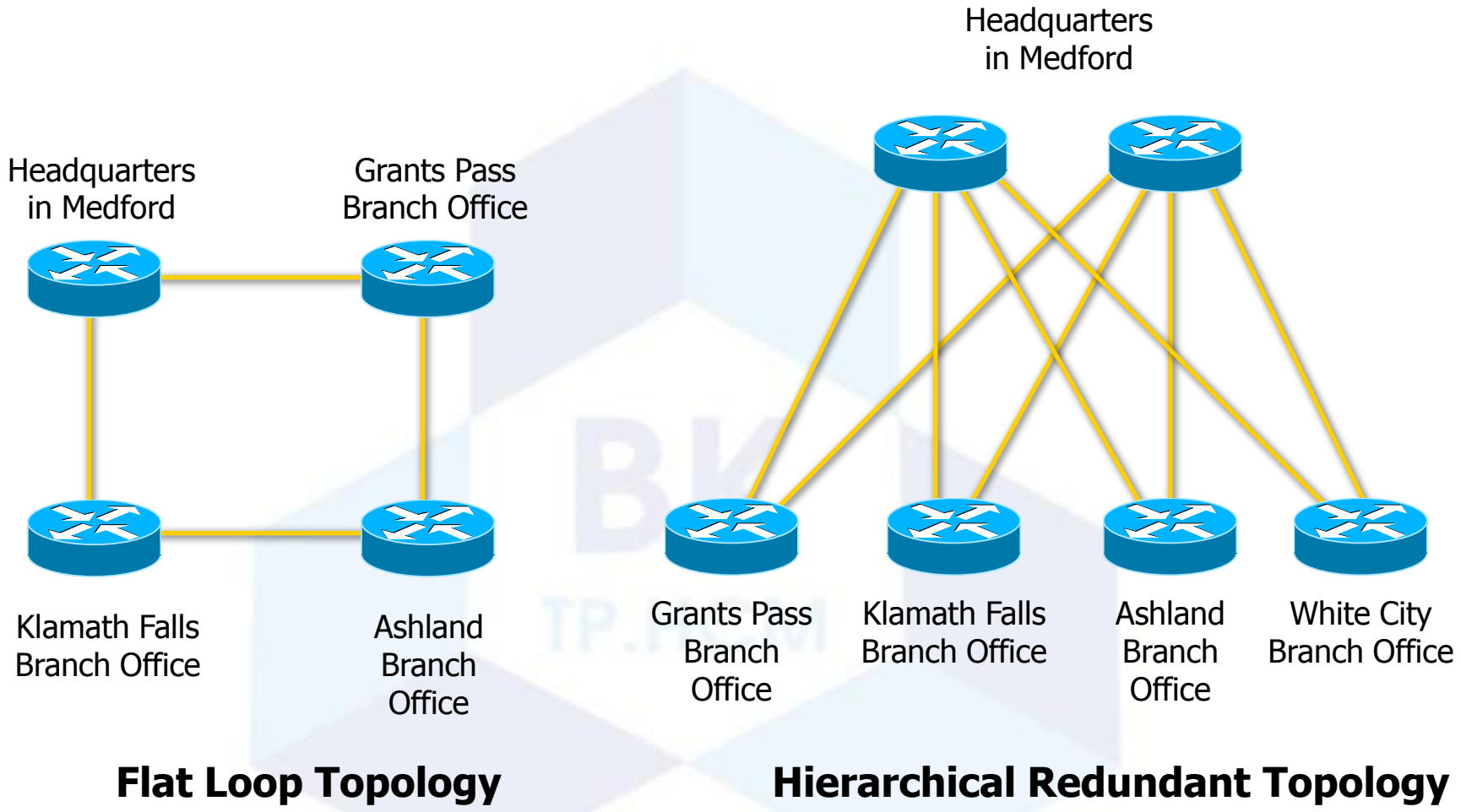
Cisco's Hierarchical Design Model

- 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

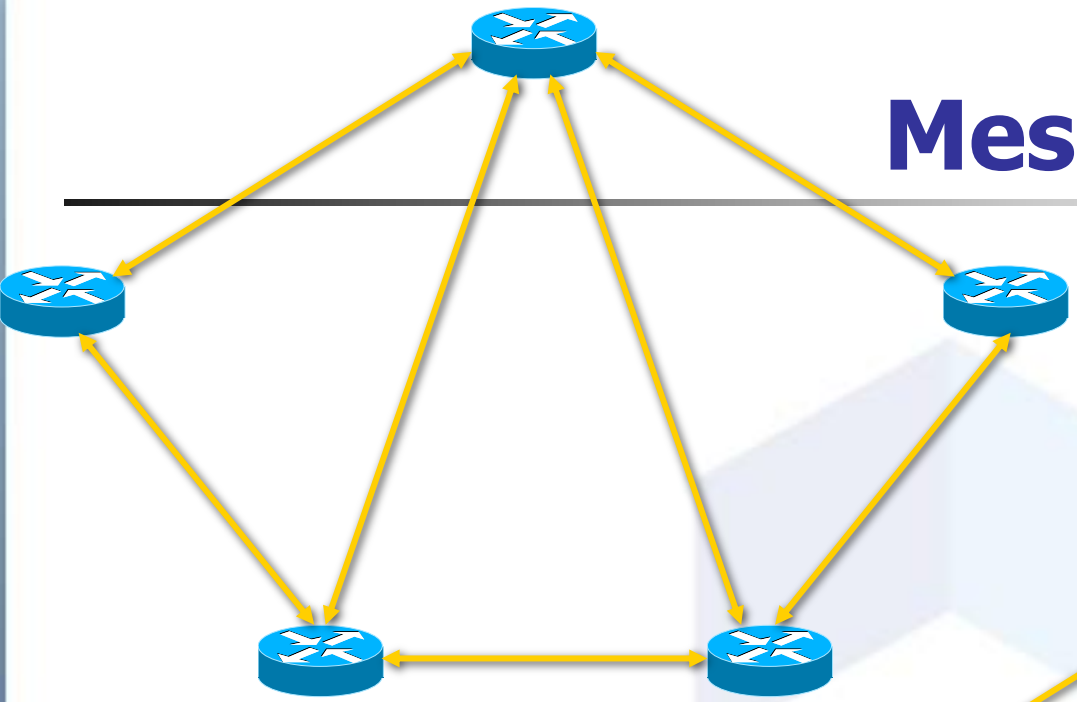
Star Hierarchical Topology



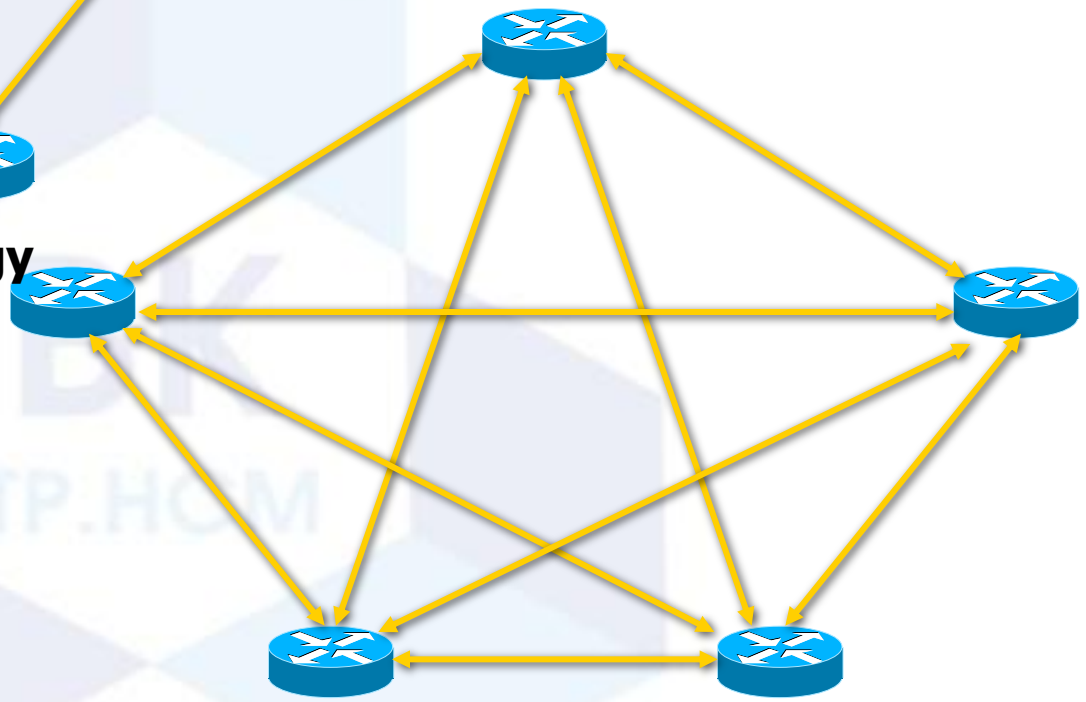
Flat Versus Hierarchy



Mesh Designs

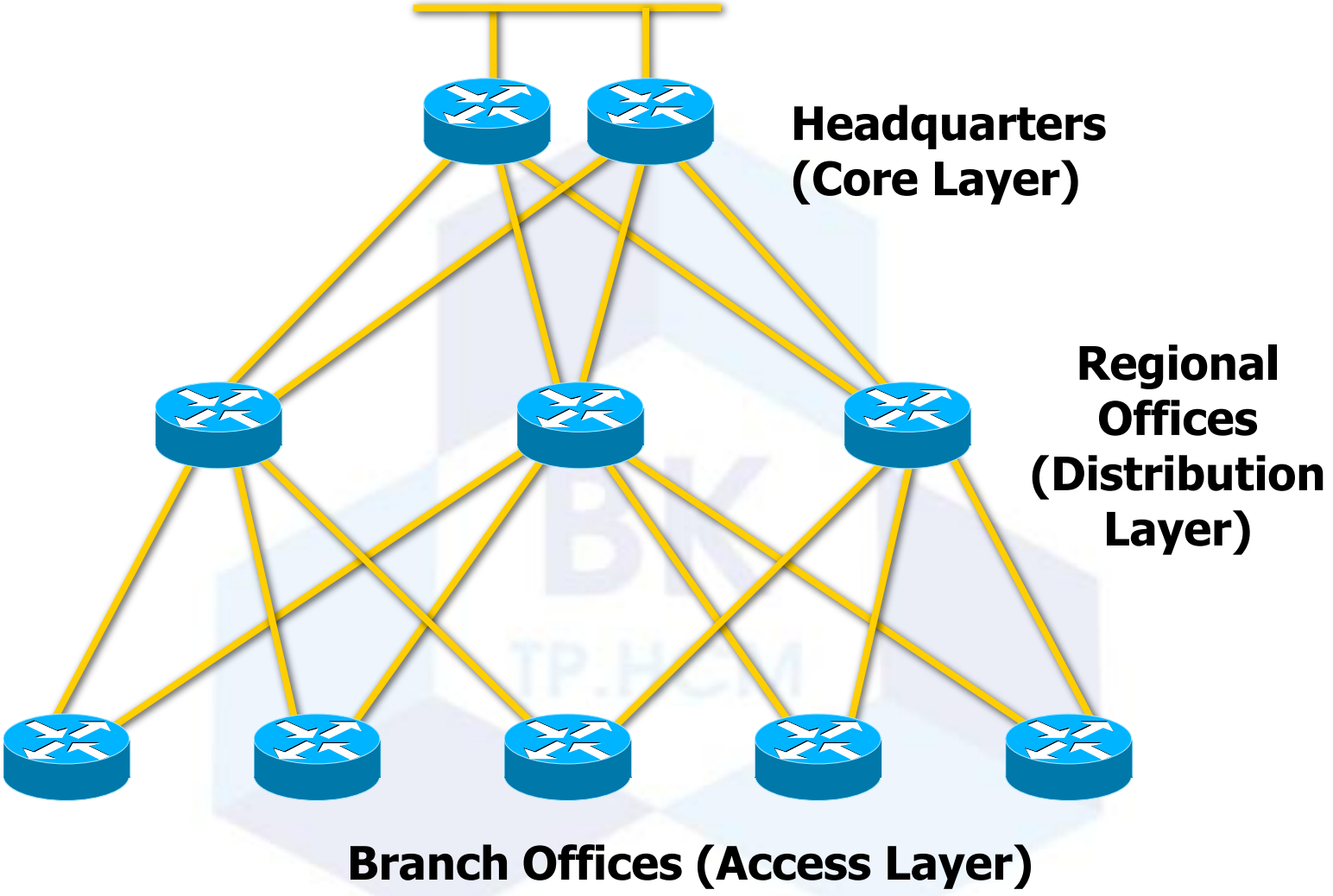


Partial-Mesh Topology

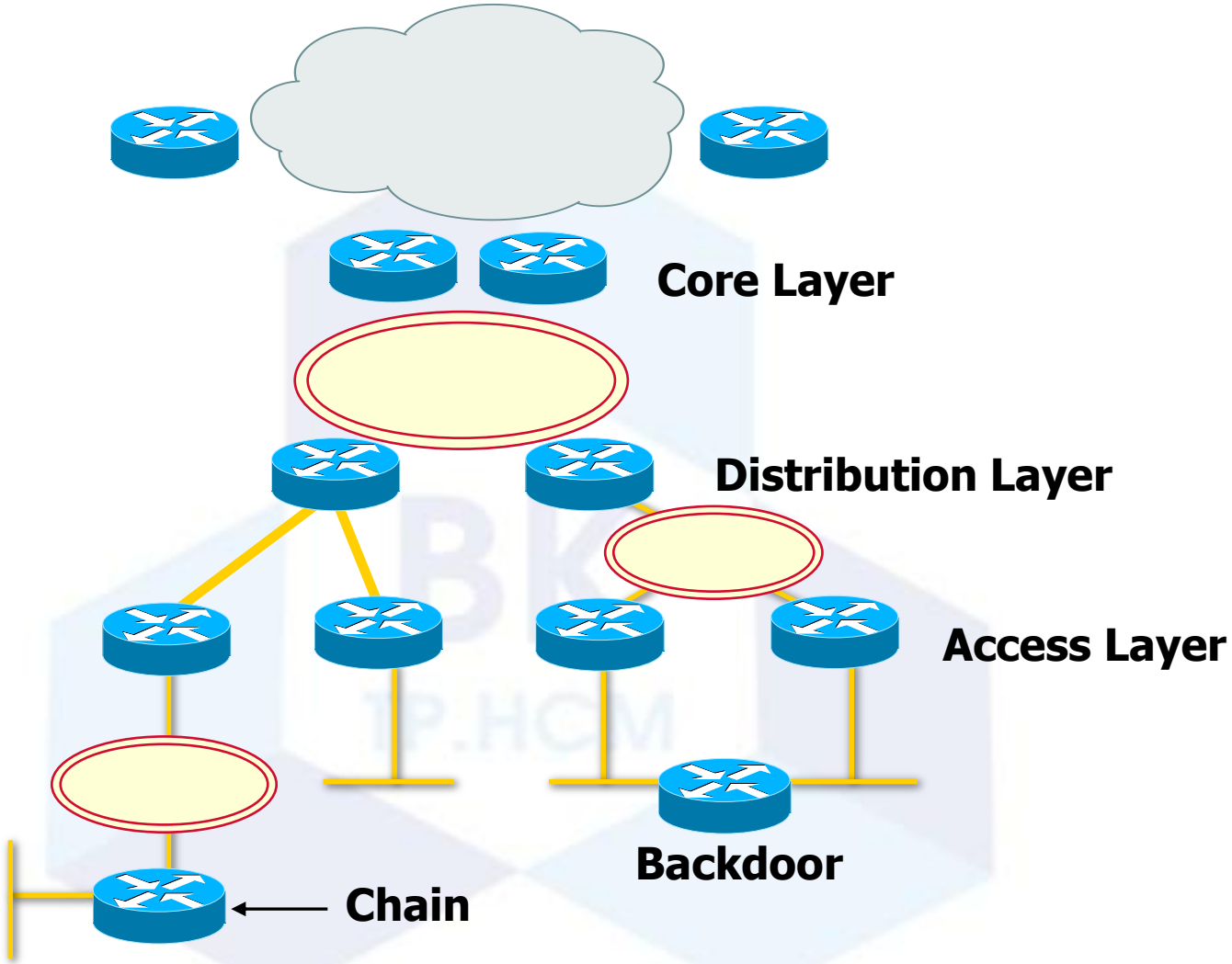


Full-Mesh Topology

A Partial-Mesh Hierarchical Design



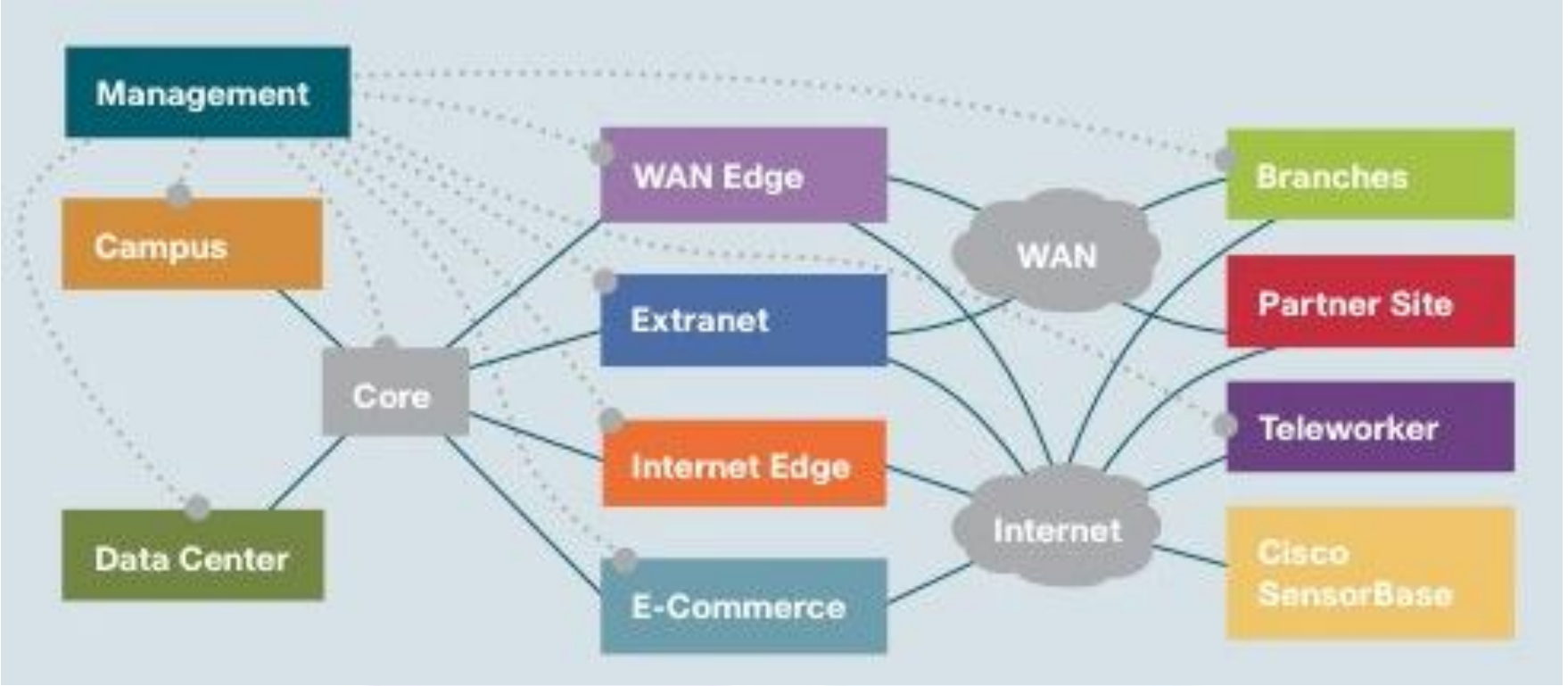
Avoid Chains and Backdoors



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



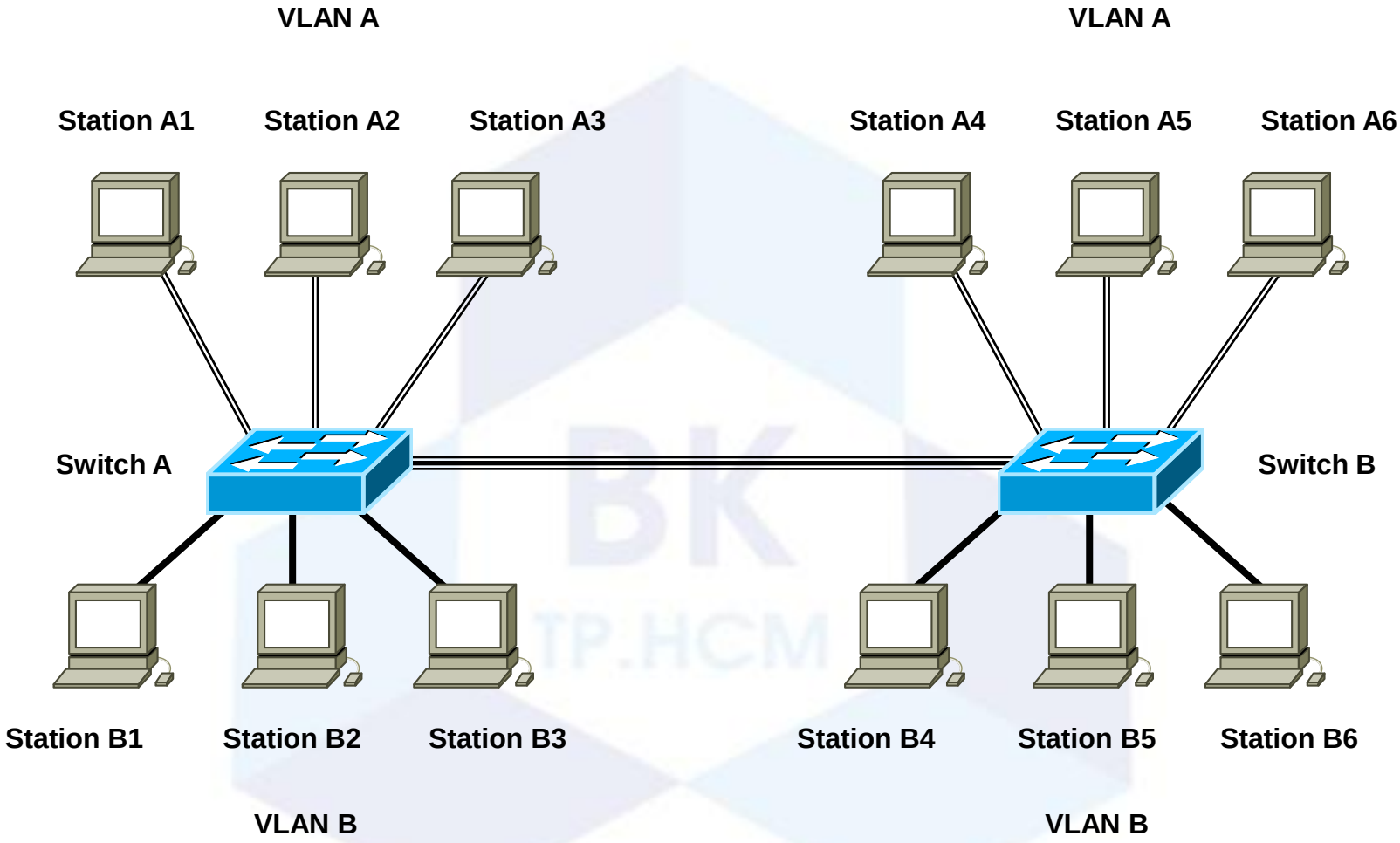
Campus Topology Design

- 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

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 Span Switches



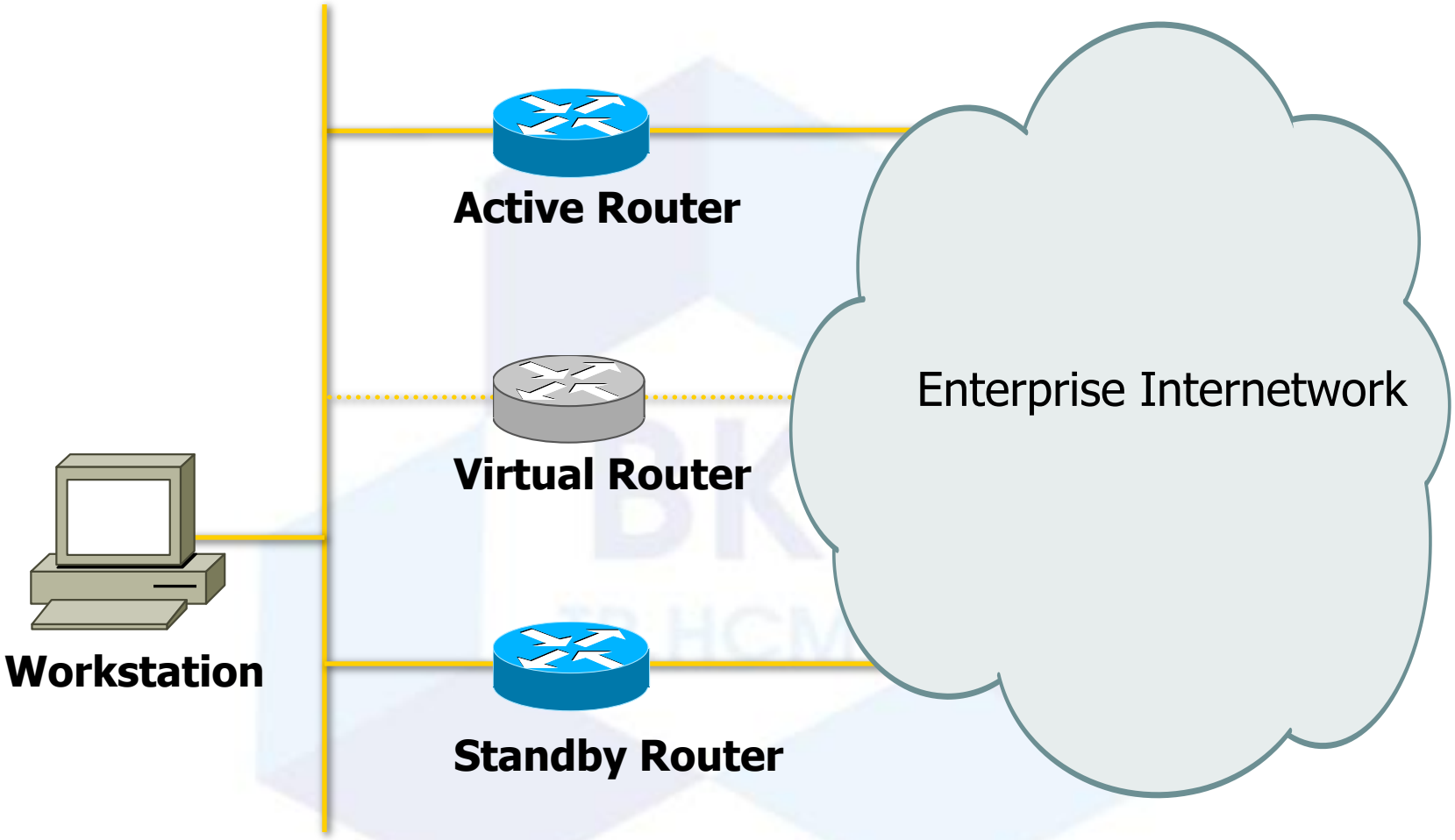
WLANs and VLANs

- 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

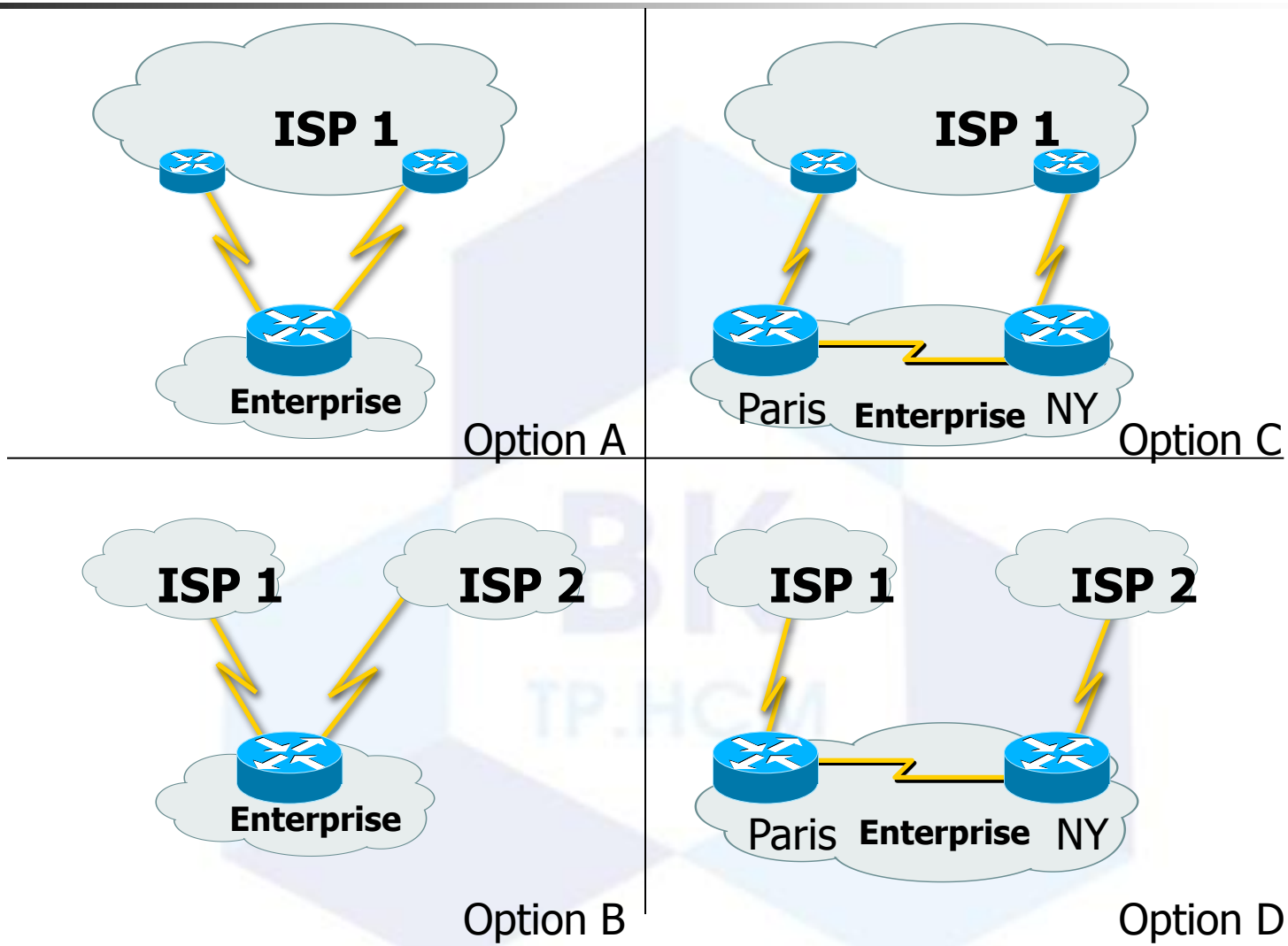
Workstation-to-Router Communication

- 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

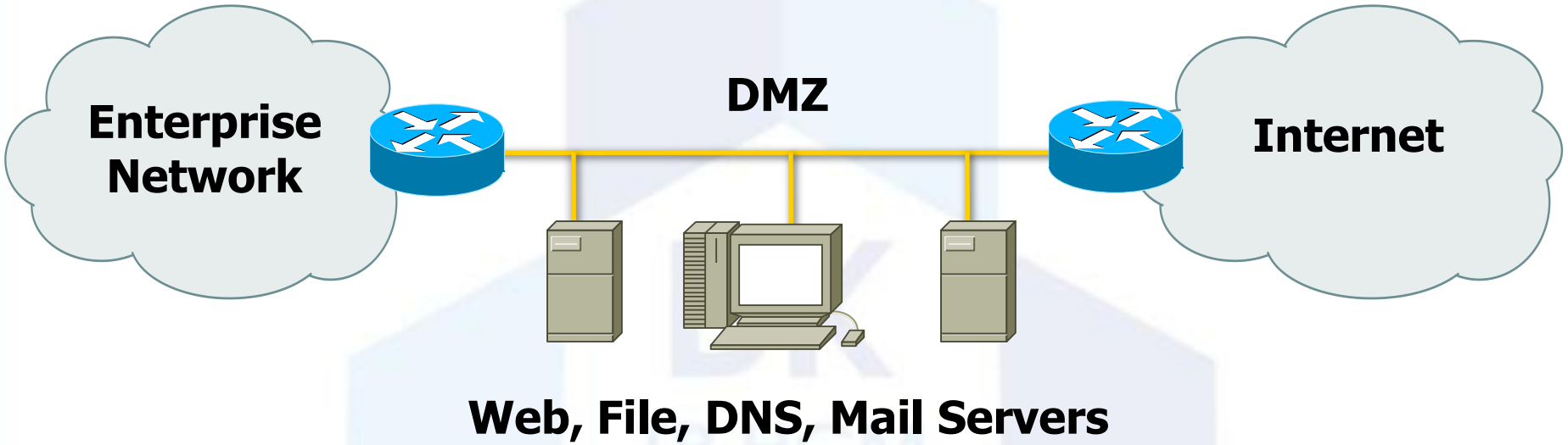
HSRP


Active Router
Virtual Router
Standby Router
Workstation
Enterprise Internetwork

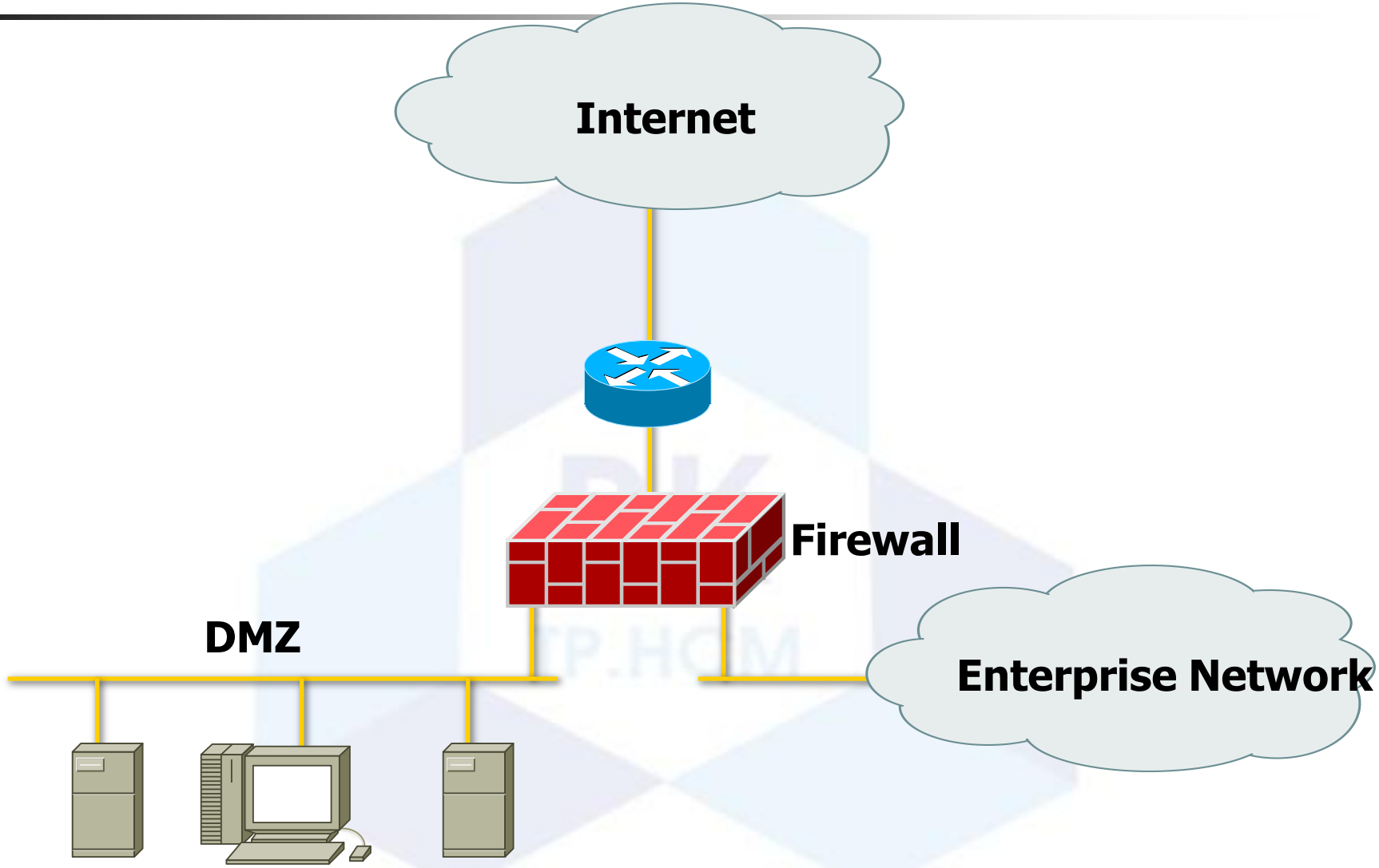
Multihoming the Internet Connection



Security Topologies



Security Topologies



Outline

- Logical Network Design
  - Design a network topology
  - Design models for addressing and naming
  - Select switching and routing protocols
  - Develop network security strategies
  - Develop network management strategies

Guidelines for Addressing and Naming

- Use a structured model for addressing and naming
- Assign addresses and names hierarchically
- Decide in advance if you will use
  - Central or distributed authority for addressing and naming
  - Public or private addressing
  - Static or dynamic addressing and naming

Advantages of Structured Models for Addressing & Naming

- It makes it easier to
  - Read network maps
  - Operate network management software
  - Recognize devices in protocol analyzer traces
  - Meet goals for usability
  - Design filters on firewalls and routers
  - Implement route summarization

Public IP Addresses

- Managed by the Internet Assigned Numbers Authority (IANA)
- Users are assigned IP addresses by Internet service providers (ISPs).
- ISPs obtain allocations of IP addresses from their appropriate Regional Internet Registry (RIR)

Private Addressing

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

Criteria for Using Static Vs. Dynamic Addressing

- The number of end systems
- The likelihood of needing to renumber
- The need for high availability
- Security requirements
- The importance of tracking addresses
- Whether end systems need additional information
  - (DHCP can provide more than just an address)

Designing Networks with Subnets

- Determining subnet size
- Computing subnet mask
- Computing IP addresses

More Practice

- Network is 172.16.0.0
- You have eight LANs, each of which will be its own subnet.
- What subnet mask should you use?
- What is the address of the first node on the first subnet?
- What address would this node use to send to all devices on its subnet?

One More

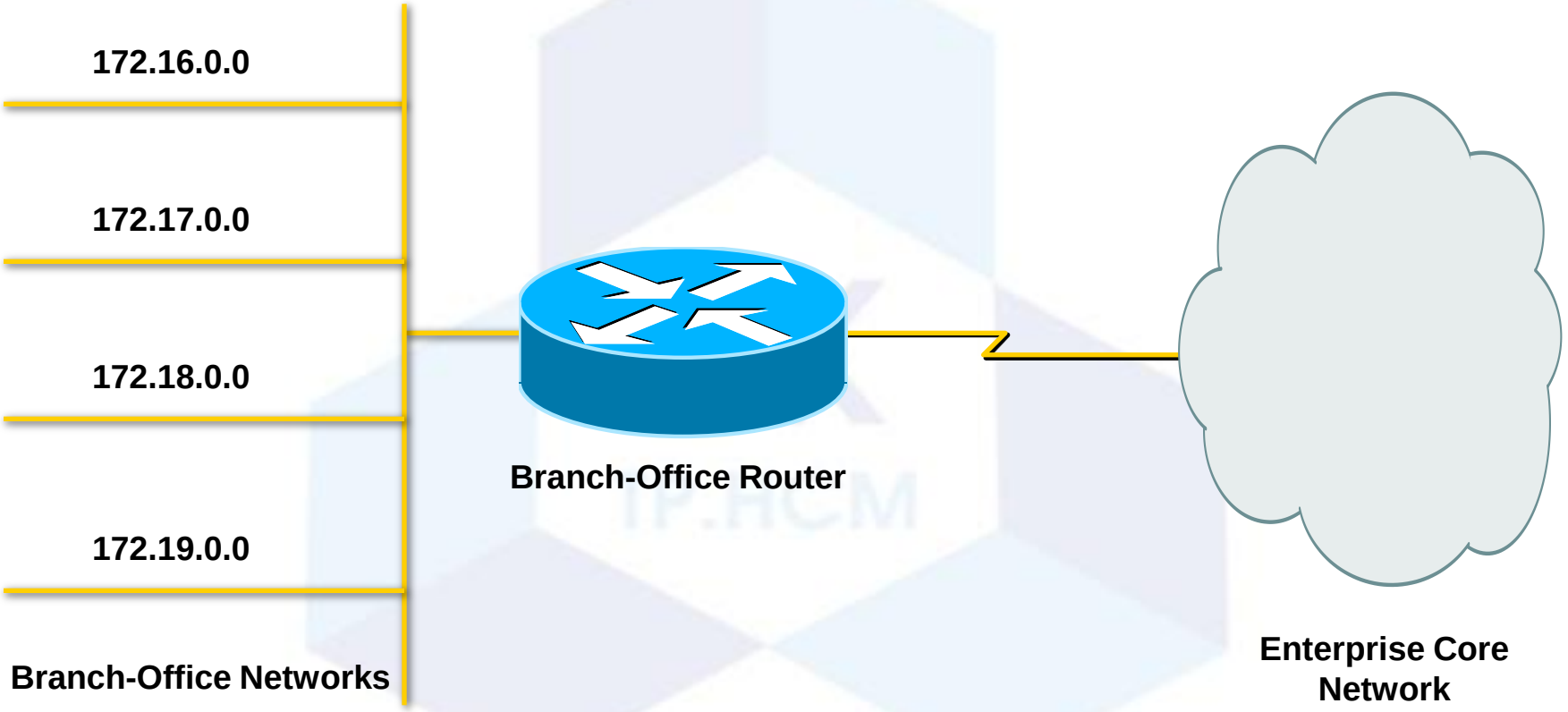
- Network is 192.168.55.0
- You want to divide the network into subnets.
- You will have approximately 25 nodes per subnet.
- What subnet mask should you use?
- What is the address of the last node on the last subnet?
- What address would this node use to send to all devices on its subnet?

Classless Addressing

- Prefix/host boundary can be anywhere
- Less wasteful
- Supports route summarization
  - Also known as
    - Aggregation
    - Supernetting
    - Classless routing
    - Classless inter-domain routing (CIDR)
    - Prefix routing

Supernetting

- Move prefix boundary to the left
- Branch office advertises 172.16.0.0/14



172.16.0.0/14 Summarization

Second Octet in Decimal	Second Octet in Binary
16	**00010**00
17	**00010**01
18	**00010**10
19	**00010**11

Upgrading to IPv6

- Dual stack
- Tunneling
- Translation

Guidelines for Assigning Names

- Names should be
  - Short
  - Meaningful
  - Unambiguous
  - Distinct
  - Case insensitive
- Avoid names with unusual characters
  - Hyphens, underscores, asterisks, and so on

Domain Name System (DNS)

- Maps names to IP addresses
- Supports hierarchical naming
  - example: frodo.rivendell.middle-earth.com
- A DNS server has a database of resource records (RRs) that maps names to addresses in the server's "zone of authority"
- Client queries server
  - Uses UDP port 53 for name queries and replies
  - Uses TCP port 53 for zone transfers

Outline

- Logical Network Design
  - Design a network topology
  - Design models for addressing and naming
  - Select switching and routing protocols
  - Develop network security strategies
  - Develop network management strategies

Switching and Routing Choices

- Switching
  - Layer 2 transparent bridging (switching)
  - Multilayer switching
  - Spanning Tree Protocol enhancements
  - VLAN technologies
- Routing
  - Static or dynamic
  - Distance-vector and link-state protocols
  - Interior and exterior
  - Etc.

Selection Criteria for Switching and Routing Protocols

- Network traffic characteristics
- Bandwidth, memory, and CPU usage
- The number of peers supported
- The capability to adapt to changes quickly
- Support for authentication

Making Decisions

- Goals must be established
- Many options should be explored
- The consequences of the decision should be investigated
- Contingency plans should be made
- A decision table can be used

Example Decision Table

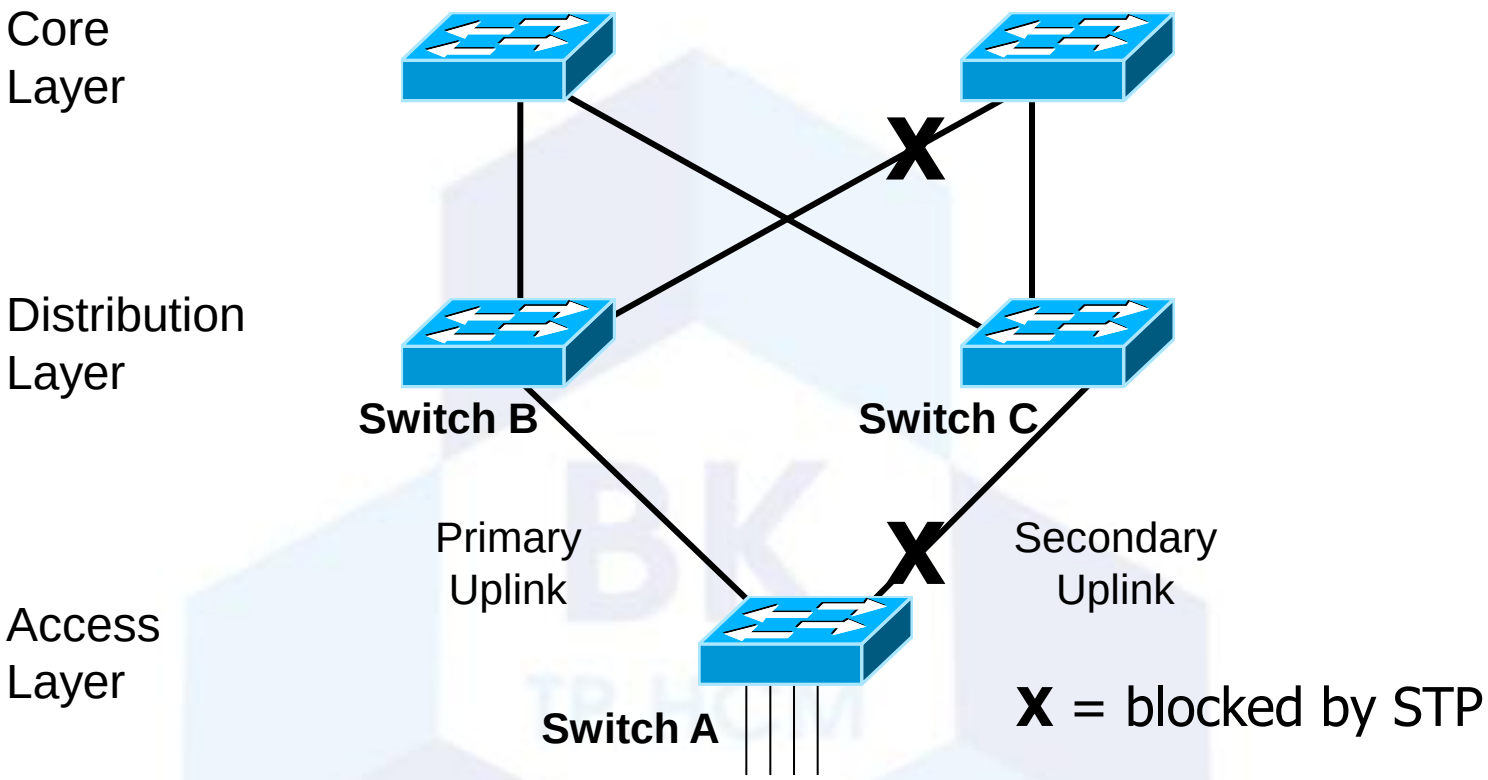
	Critical Goals			Other Goals		
	Adaptability—must adapt to changes in a large internetwork within seconds	Must scale to a large size (hundreds of routers)	Must be an industry standard and compatible with existing equipment	Should not create a lot of traffic	Should run on inexpensive routers	Should be easy to configure and manage
BGP	X*	X	X	8	7	7
OSPF	X	X	X	8	8	8
IS-IS	X	X	X	8	6	6
IGRP	X	X				
EIGRP	X	X				
RIP			X			

* X= Meets critical criteria. 1 = Lowest. 10 = Highest.

Transparent Bridging (Switching) Tasks

- Forward frames transparently
- Learn which port to use for each MAC address
- Flood frames when the destination unicast address hasn't been learned yet
- Filter frames from going out ports that don't include the destination address
- Flood broadcasts and multicasts

Redundant Uplinks



- If a link fails, how long will STP take to recover?
- Use UplinkFast to speed convergence

Protocols for Transporting VLAN Information

- Inter-Switch Link (ISL)
  - Tagging protocol
  - Cisco proprietary
- IEEE 802.1Q
  - Tagging protocol
  - IEEE standard
- VLAN Trunk Protocol (VTP)
  - VLAN management protocol

Selecting Routing Protocols

- They all have the same general goal:
  - To share network reachability information among routers
- They differ in many ways:
  - Interior versus exterior
  - Metrics supported
  - Dynamic versus static and default
  - Distance-vector versus link-sate
  - Classful versus classless
  - Scalability

Interior Versus Exterior Routing Protocols

- Interior routing protocols are used within an autonomous system
- Exterior routing protocols are used between autonomous systems

Autonomous system (two definitions that are often used):

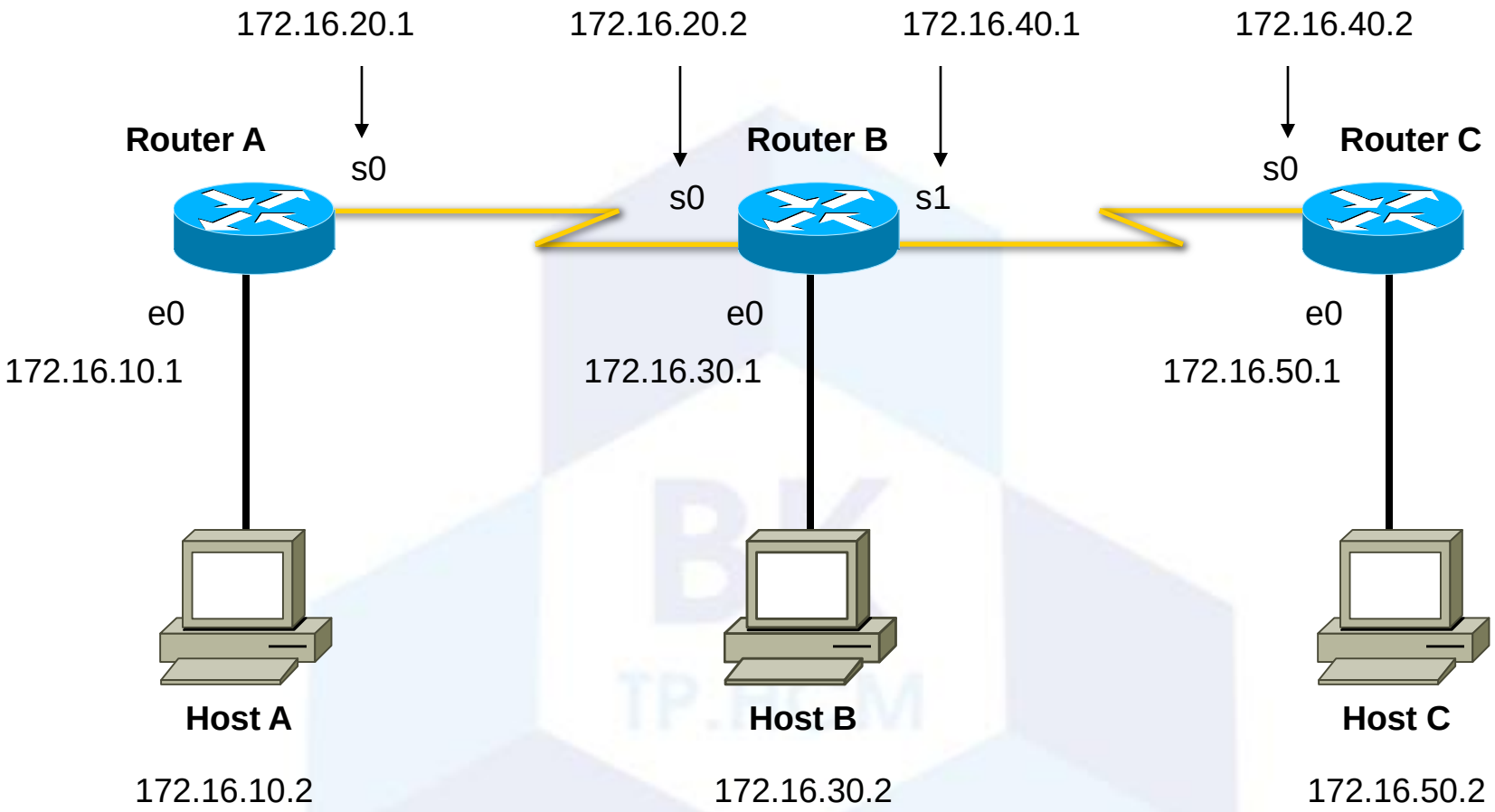
"A set of routers that presents a common routing policy to the internetwork"

"A network or set of networks that are under the administrative control of a single entity"

Routing Protocol Metrics

- Metric: the determining factor used by a routing algorithm to decide which route to a network is better than another
- Examples of metrics:
  - Bandwidth - capacity
  - Delay - time
  - Load - amount of network traffic
  - Reliability - error rate
  - Hop count - number of routers that a packet must travel through before reaching the destination network
  - Cost - arbitrary value defined by the protocol or administrator

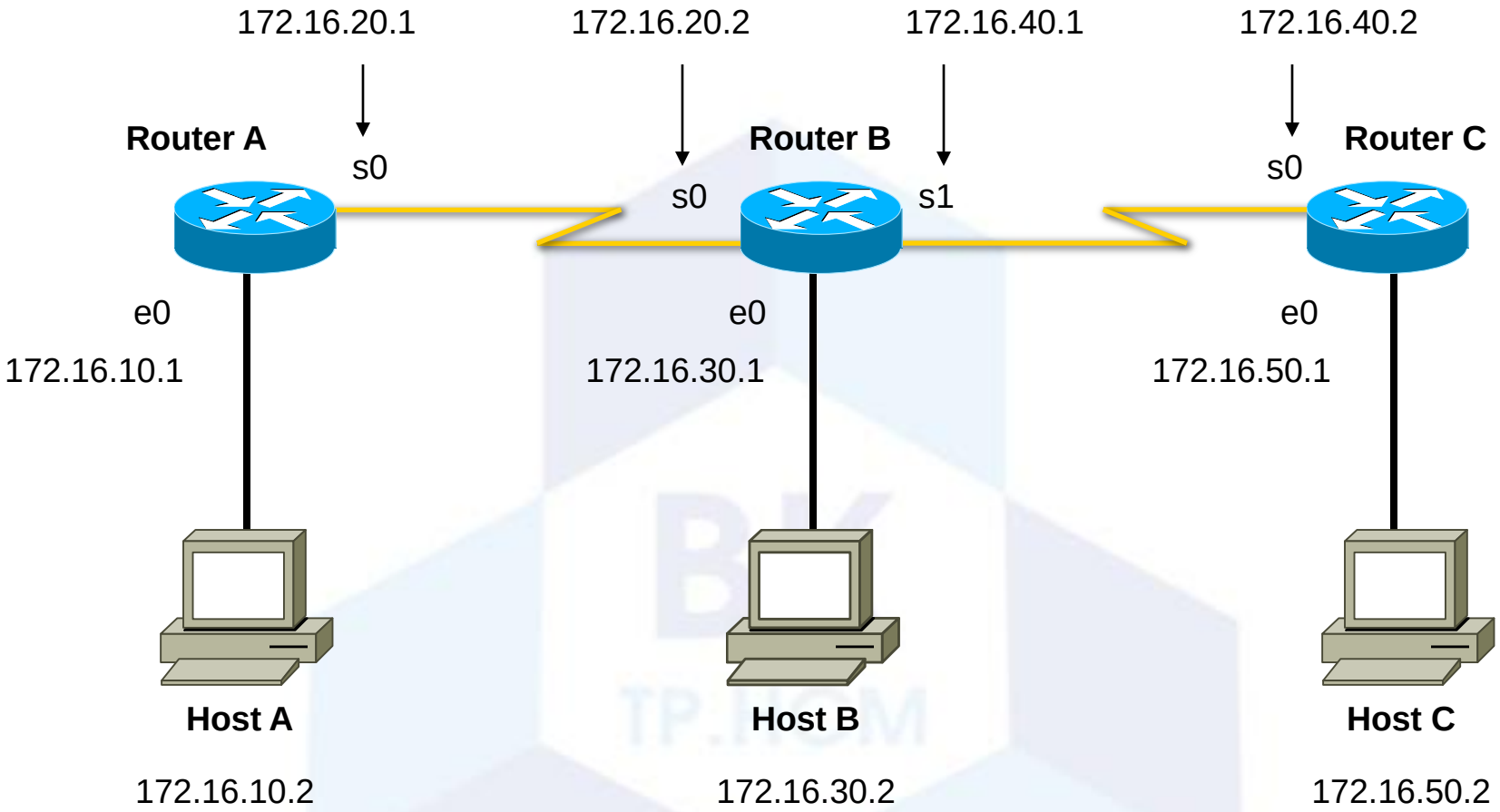
Static Routing Example



RouterA(config)#**ip route 172.16.50.0 255.255.255.0 172.16.20.2**

Send packets for subnet 50 to 172.16.20.2 (Router B)

Default Routing Example



RouterA(config)#**ip route 0.0.0.0 0.0.0.0 172.16.20.2**

If it's not local, send it to 172.16.20.2 (Router B)

Distance-Vector Routing

- Router maintains a routing table that lists known networks, direction (vector) to each network, and the distance to each network
- Router periodically (every 30 seconds, for example) transmits the routing table via a broadcast packet that reaches all other routers on the local segments
- Router updates the routing table, if necessary, based on received broadcasts

Distance-Vector Routing Tables

Router A's Routing Table

Network	Distance	Send To
172.16.0.0	0	Port 1
192.168.2.0	1	Router B

Router B's Routing Table

Network	Distance	Send To
192.168.2.0	0	Port 1
172.16.0.0	1	Router A

Link-State Routing

- Routers send updates only when there's a change
- Router that detects change creates a link-state advertisement (LSA) and sends it to neighbors
- Neighbors propagate the change to their neighbors
- Routers update their topological database if necessary

Distance-Vector Vs. Link-State

- Distance-vector algorithms keep a list of networks, with next hop and distance (metric) information
- Link-state algorithms keep a database of routers and links between them
  - Link-state algorithms think of the internetwork as a graph instead of a list
  - When changes occur, link-state algorithms apply Dijkstra's shortest-path algorithm to find the shortest path between any two nodes

Dynamic IP Routing Protocols

Distance-Vector	Link-State
▪ Routing Information Protocol (RIP) Version 1 and 2 ▪ Interior Gateway Routing Protocol (IGRP) ▪ Enhanced IGRP ▪ Border Gateway Protocol (BGP)	• Open Shortest Path First (OSPF) • Intermediate System-to-Intermediate System (IS-IS)

Outline

- Logical Network Design
  - Design a network topology
  - Design models for addressing and naming
  - Select switching and routing protocols
  - Develop network security strategies
  - Develop network management strategies

Network Security Design
The 12 Step Program

1. Identify network assets
2. Analyze security risks
3. Analyze security requirements and tradeoffs
4. Develop a security plan
5. Define a security policy
6. Develop procedures for applying security policies

The 12 Step Program (continued)

7. Develop a technical implementation strategy
8. Achieve buy-in from users, managers, and technical staff
9. Train users, managers, and technical staff
10. Implement the technical strategy and security procedures
11. Test the security and update it if any problems are found
12. Maintain security

Network Assets

- Hardware
- Software
- Applications
- Data
- Intellectual property
- Trade secrets
- Company's reputation

Security Risks

- Hacked network devices
  - Data can be intercepted, analyzed, altered, or deleted
  - User passwords can be compromised
  - Device configurations can be changed
- Reconnaissance attacks
- Denial-of-service attacks

Security Tradeoffs

- Tradeoffs must be made between security goals and other goals:
  - Affordability
  - Usability
  - Performance
  - Availability
  - Manageability

A Security Plan

- High-level document that proposes what an organization is going to do to meet security requirements
- Specifies time, people, and other resources that will be required to develop a security policy and achieve implementation of the policy

A Security Policy

- Per RFC 2196, "The Site Security Handbook," a security policy is a
  - "Formal statement of the rules by which people who are given access to an organization's technology and information assets must abide."
- The policy should address
  - Access, accountability, authentication, privacy, and computer technology purchasing guidelines

Security Mechanisms

- Physical security
- Authentication
- Authorization
- Accounting (Auditing)
- Data encryption
- Packet filters
- Firewalls
- Intrusion Detection Systems (IDS)
- Intrusion Prevention Systems (IPS)

Modularizing Security Design

- Security defense in depth
  - Network security should be multilayered with many different techniques used to protect the network
- Secure all components of a modular design:
  - Internet connections
  - Public servers and e-commerce servers
  - Remote access networks and VPNs
  - Network services and network management
  - Server farms
  - User services
  - Wireless networks

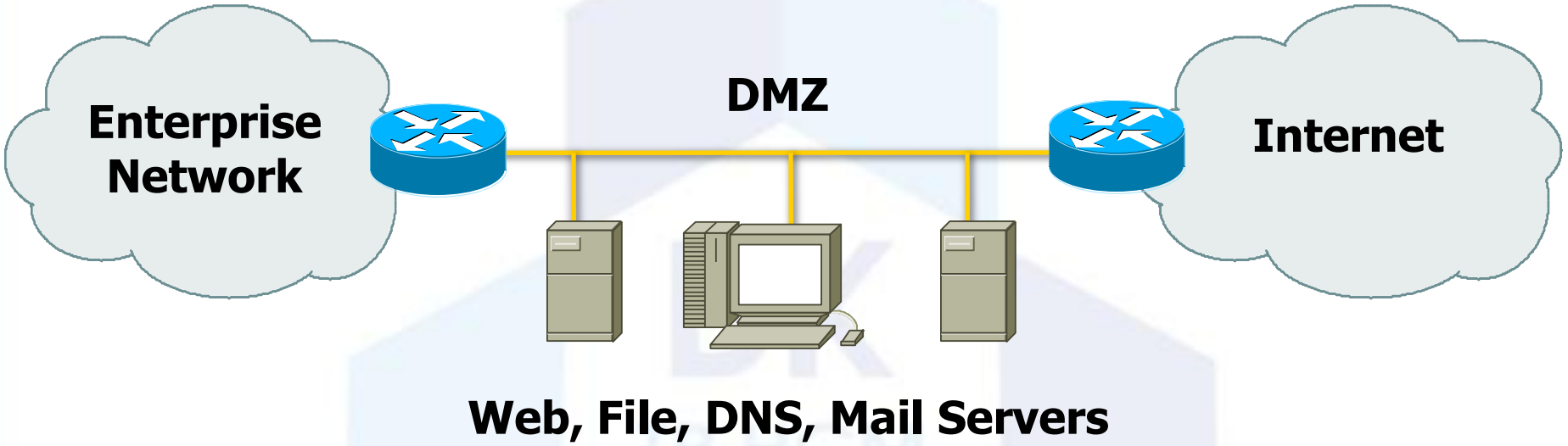
Securing Internet Connections

- Physical security
- Firewalls and packet filters
- Audit logs, authentication, authorization
- Well-defined exit and entry points
- Routing protocols that support authentication

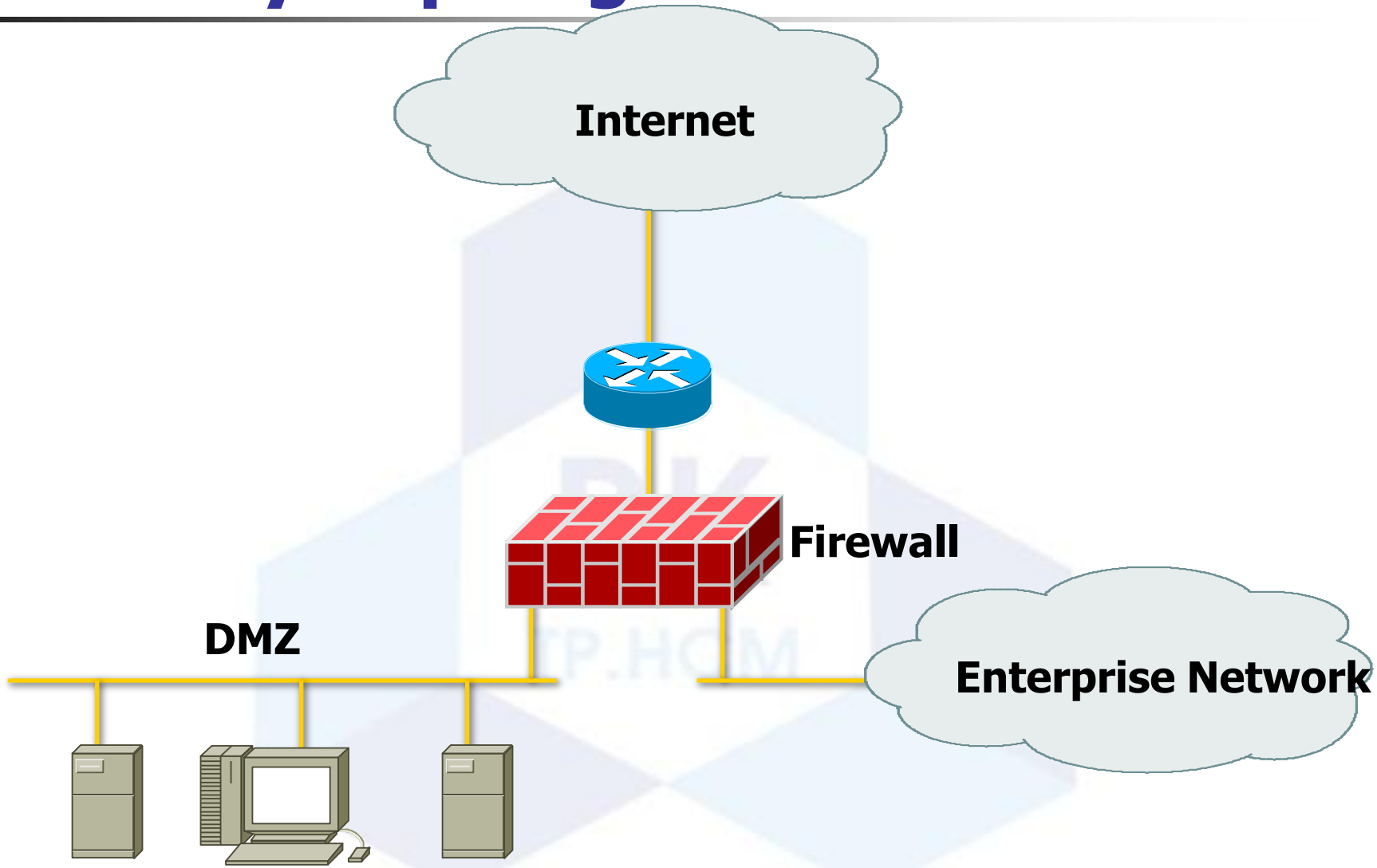
Securing Public Servers

- Place servers in a DMZ that is protected via firewalls
- Run a firewall on the server itself
- Enable DoS protection
  - Limit the number of connections per timeframe
- Use reliable operating systems with the latest security patches
- Maintain modularity
  - Front-end Web server doesn't also run other services

Security Topologies



Security Topologies



Securing Remote-Access and Virtual Private Networks

- Physical security
- Firewalls
- Authentication, authorization, and auditing
- Encryption
- One-time passwords
- Security protocols
  - CHAP
  - RADIUS
  - IPSec

Securing Network Services

- Treat each network device (routers, switches, and so on) as a high-value host and harden it against possible intrusions
- Require login IDs and passwords for accessing devices
  - Require extra authorization for risky configuration commands
- Use SSH rather than Telnet
- Change the welcome banner to be less welcoming

Securing Server Farms

- Deploy network and host IDSs to monitor server subnets and individual servers
- Configure filters that limit connectivity from the server in case the server is compromised
- Fix known security bugs in server operating systems
- Require authentication and authorization for server access and management
- Limit root password to a few people
- Avoid guest accounts

Securing User Services

- Specify which applications are allowed to run on networked PCs in the security policy
- Require personal firewalls and antivirus software on networked PCs
  - Implement written procedures that specify how the software is installed and kept current
- Encourage users to log out when leaving their desks
- Consider using 802.1X port-based security on switches

Securing Wireless Networks

- Place wireless LANs (WLANs) in their own subnet or VLAN
  - Simplifies addressing and makes it easier to configure packet filters
- Require all wireless (and wired) laptops to run personal firewall and antivirus software
- Disable beacons that broadcast the SSID, and require MAC address authentication
  - Except in cases where the WLAN is used by visitors

WLAN Security Options

- IEEE 802.11i
- Wi-Fi Protected Access (WPA)
- IEEE 802.1X Extensible Authentication Protocol (EAP)
  - Lightweight EAP or LEAP (Cisco)
  - Protected EAP (PEAP)
- Virtual Private Networks (VPNs)

VPN Software on Wireless Clients

- Safest way to do wireless networking for corporations
- Wireless client requires VPN software
- Connects to VPN concentrator at HQ
- Creates a tunnel for sending all traffic
- VPN security provides:
  - User authentication
  - Strong encryption of data
  - Data integrity

Outline

- Logical Network Design
  - Design a network topology
  - Design models for addressing and naming
  - Select switching and routing protocols
  - Develop network security strategies
  - Develop network management strategies

Network Management

- Helps an organization achieve availability, performance, and security goals
- Helps an organization measure how well design goals are being met and adjust network parameters if they are not being met
- Facilitates scalability
  - Helps an organization analyze current network behavior, apply upgrades appropriately, and troubleshoot any problems with upgrades

Network Management Design

- Consider scalability, traffic patterns, data formats, cost/benefit tradeoffs
- Determine which resources should be monitored
- Determine metrics for measuring performance
- Determine which and how much data to collect

Proactive Network Management

- Plan to check the health of the network during normal operation, not just when there are problems
- Recognize potential problems as they develop
- Optimize performance
- Plan upgrades appropriately

Network Management Processes According to the ISO

- Fault management
- Configuration management
- Accounting management
- Performance management
- Security management