Chapter 5.3: Network Design

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

Outline

- Physical Network Design
  - Select technologies and devices for campus networks
  - Select technologies and devices for enterprise networks
- Testing, Optimizing, and Documenting the Network Design

Selecting Technologies and Devices

- We now know what the network will look like.
- We also know what capabilities the network will need.
- We are now ready to start picking out technologies and devices.

Campus Network Design Steps

- Develop a cabling plant design
- Select the types of cabling
- Select the data-link-layer technologies
- Select internetworking devices

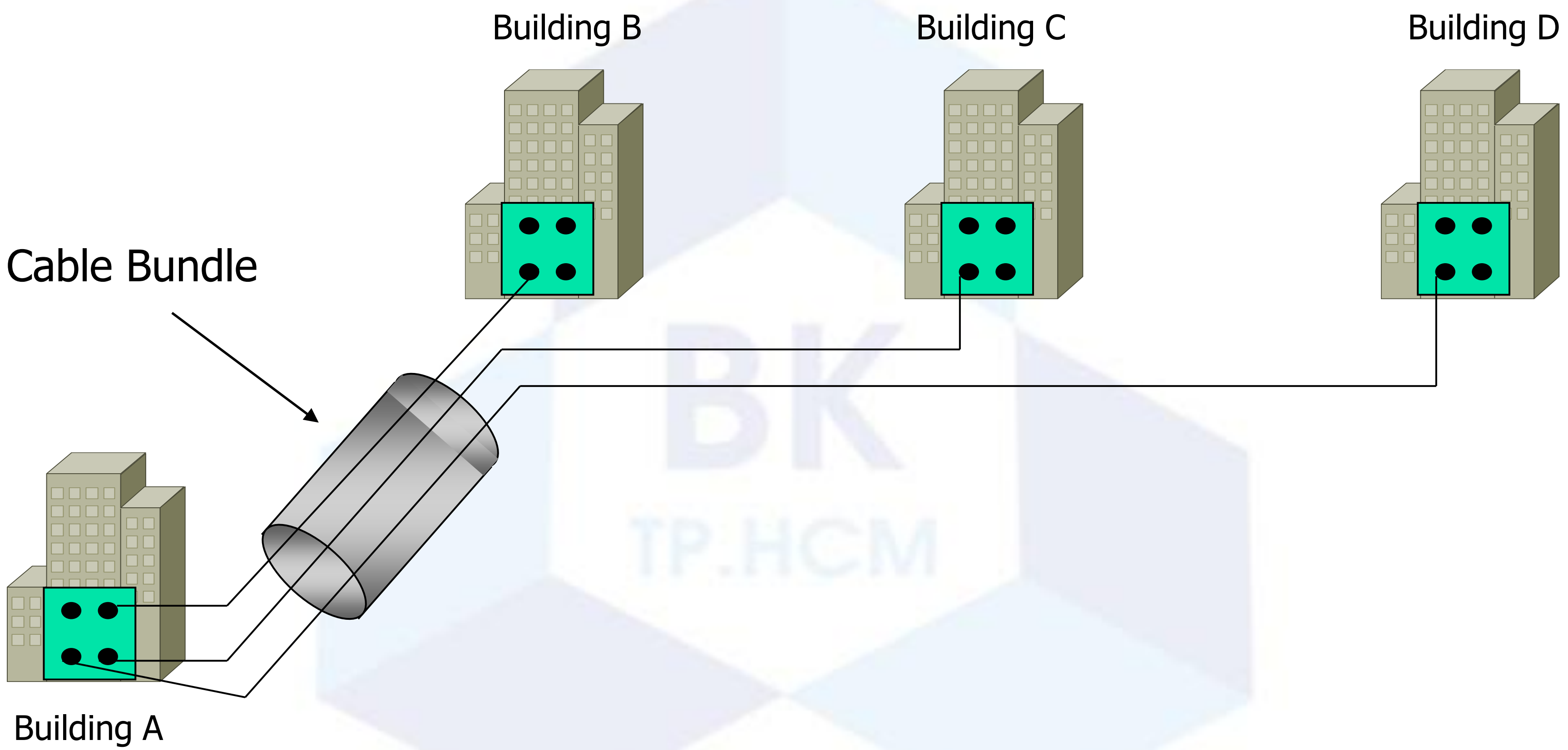
Cabling Plant Design Considerations

- Campus and building cabling topologies
- The types and lengths of cables between buildings
- Within buildings
  - The location of telecommunications closets and cross-connect rooms
  - The types and lengths of cables for vertical cabling between floors
  - The types and lengths of cables for horizontal cabling within floors
  - The types and lengths of cables for work-area cabling going from telecommunications closets to workstations

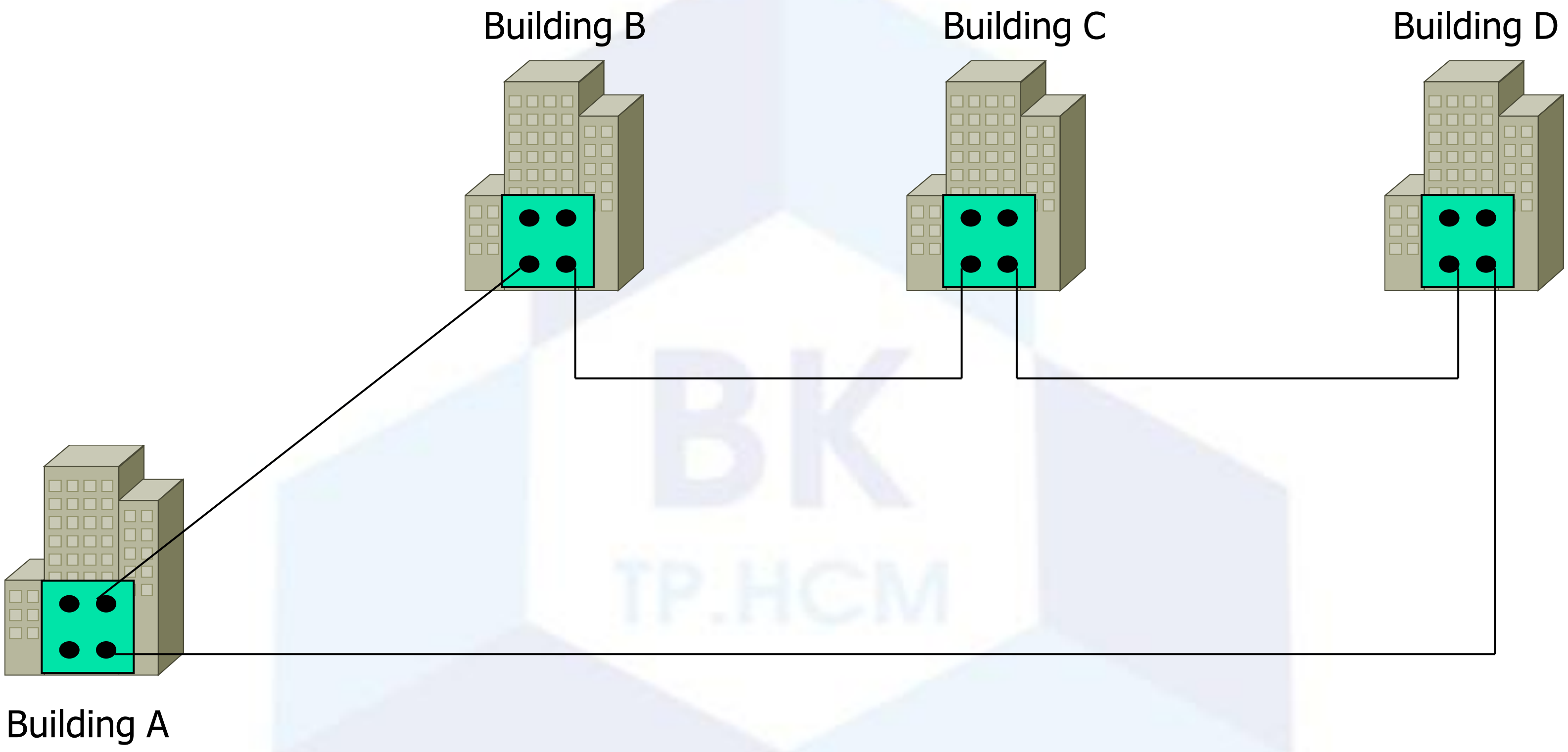
Centralized Versus Distributed Cabling Topologies

- A centralized cabling scheme terminates most or all of the cable runs in one area of the design environment. A star topology is an example of a centralized system.
- A distributed cabling scheme terminates cable runs throughout the design environment. Ring, bus, and tree topologies are examples of distributed systems.

Centralized Campus Cabling

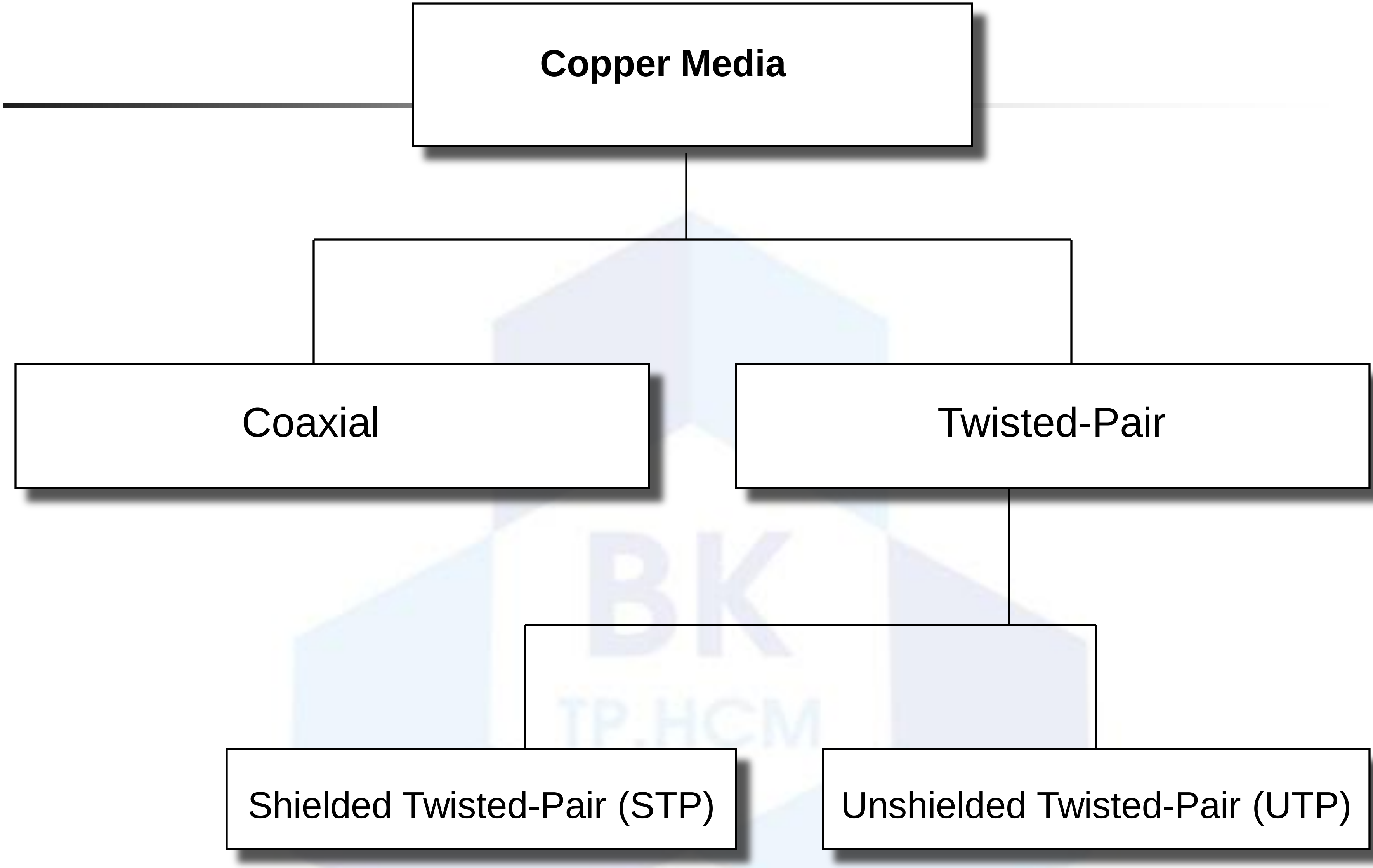


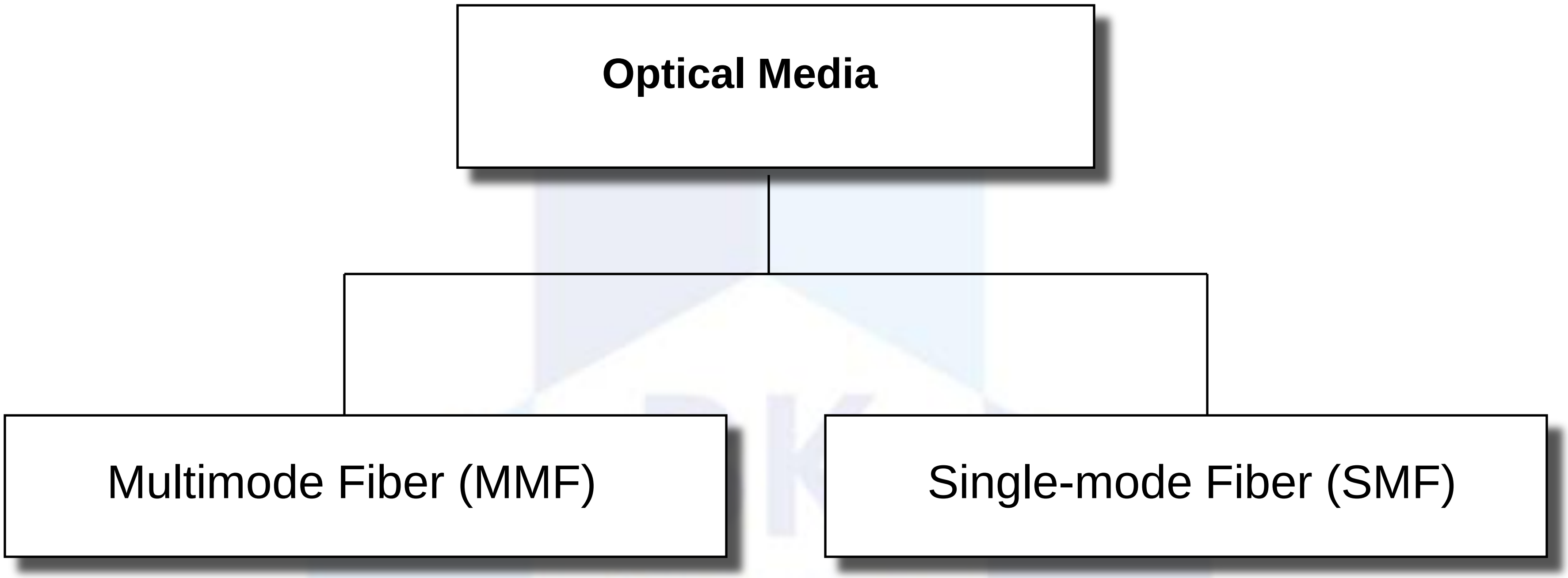
Distributed Campus Cabling



Types of Media Used in Campus Networks

- Copper media
- Optical media
- Wireless media


Copper Media
Coaxial
Twisted-Pair
Shielded Twisted-Pair (STP)
Unshielded Twisted-Pair (UTP)


Optical Media
Multimode Fiber (MMF)
Single-mode Fiber (SMF)

Copper Vs Fiber-Optic Cabling

- Twisted-pair and coax cable transmit network signals in the form of current
- Fiber-optic cable transmits network signals in the form of light
- Fiber-optic cable is made of glass
  - Not susceptible to electromagnetic or radio frequency interference
  - Not as susceptible to attenuation, which means longer cables are possible
  - Supports very high bandwidth (10 Gbps or greater)
  - For long distances, fiber costs less than copper

Cabling Guidelines

- At the access layer use
  - Copper UTP rated for Category 5 or 5e, unless there is a good reason not to
  - To future proof the network
    - Use 5e instead of 5
    - Install UTP Category 6 rated cable and terminate the cable with Cat 5 or 5e connectors
    - Then only the connectors need to be changed to move up in speed
  - In special cases
    - Use MMF for bandwidth intensive applications
    - Or install fiber along with the copper

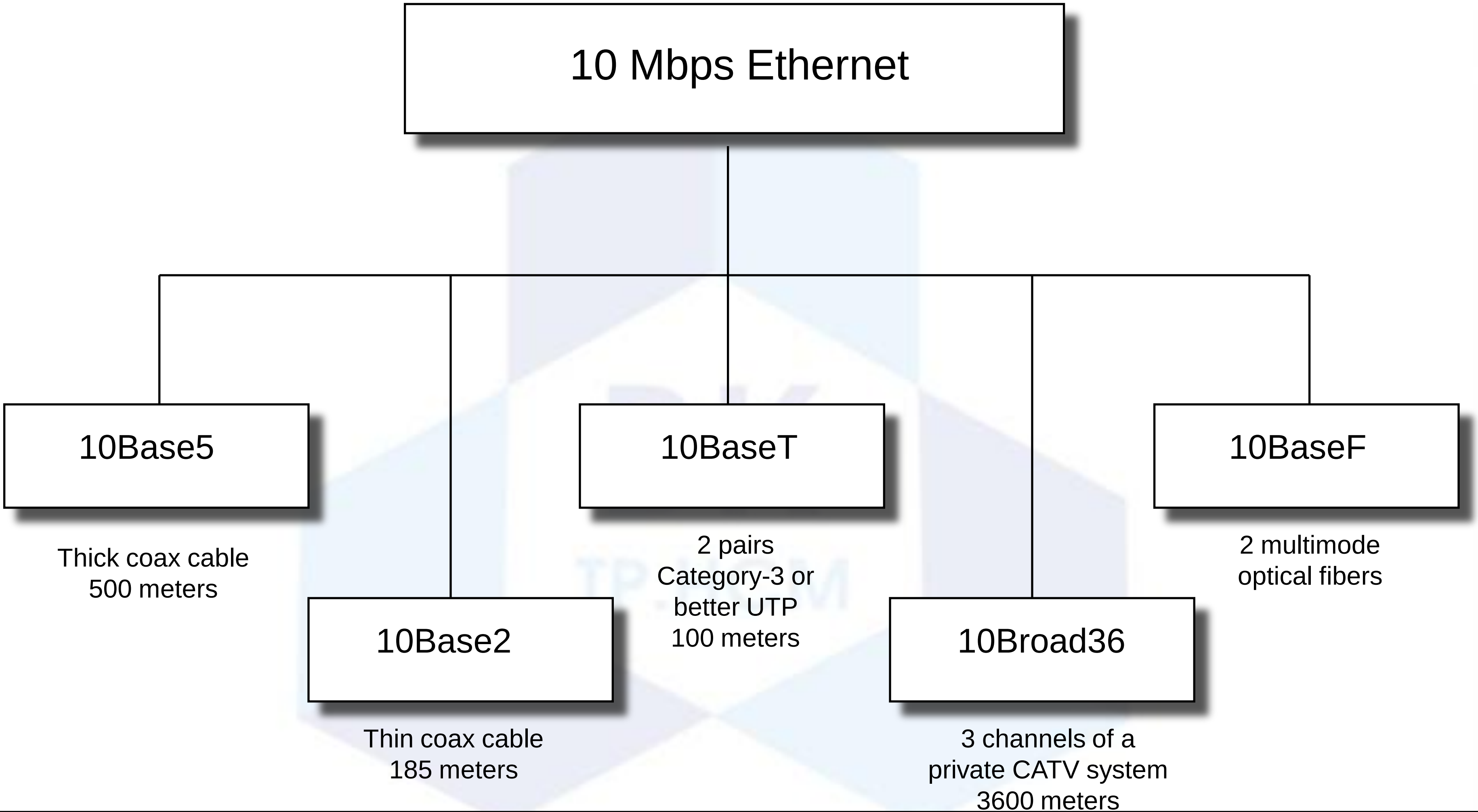
Cabling Guidelines

- At the distribution layer use
  - MMF if distance allows
  - SMF otherwise
  - Unless unusual circumstances occur and cable cannot be run, then use a wireless method
  - To future proof the network
    - Run both MMF and SMF

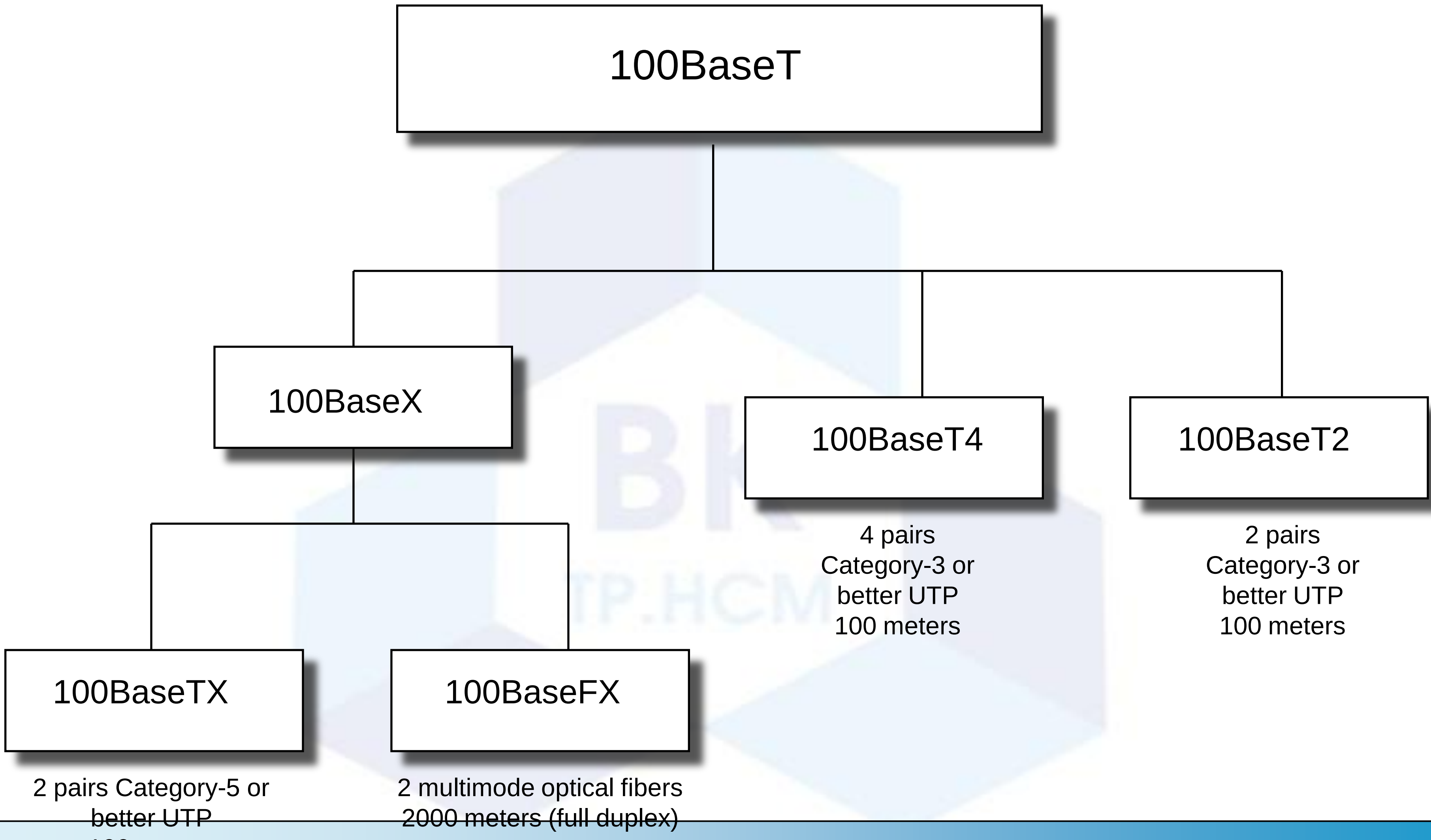
LAN Technologies

- Half-duplex Ethernet (becoming obsolete)
- Full-duplex Ethernet
- 10-Mbps Ethernet (becoming obsolete)
- 100-Mbps Ethernet
- 1000-Mbps (1-Gbps or Gigabit) Ethernet
- 10-Gbps Ethernet
- Metro Ethernet
- Long Range Ethernet (LRE)
- Cisco’s EtherChannel

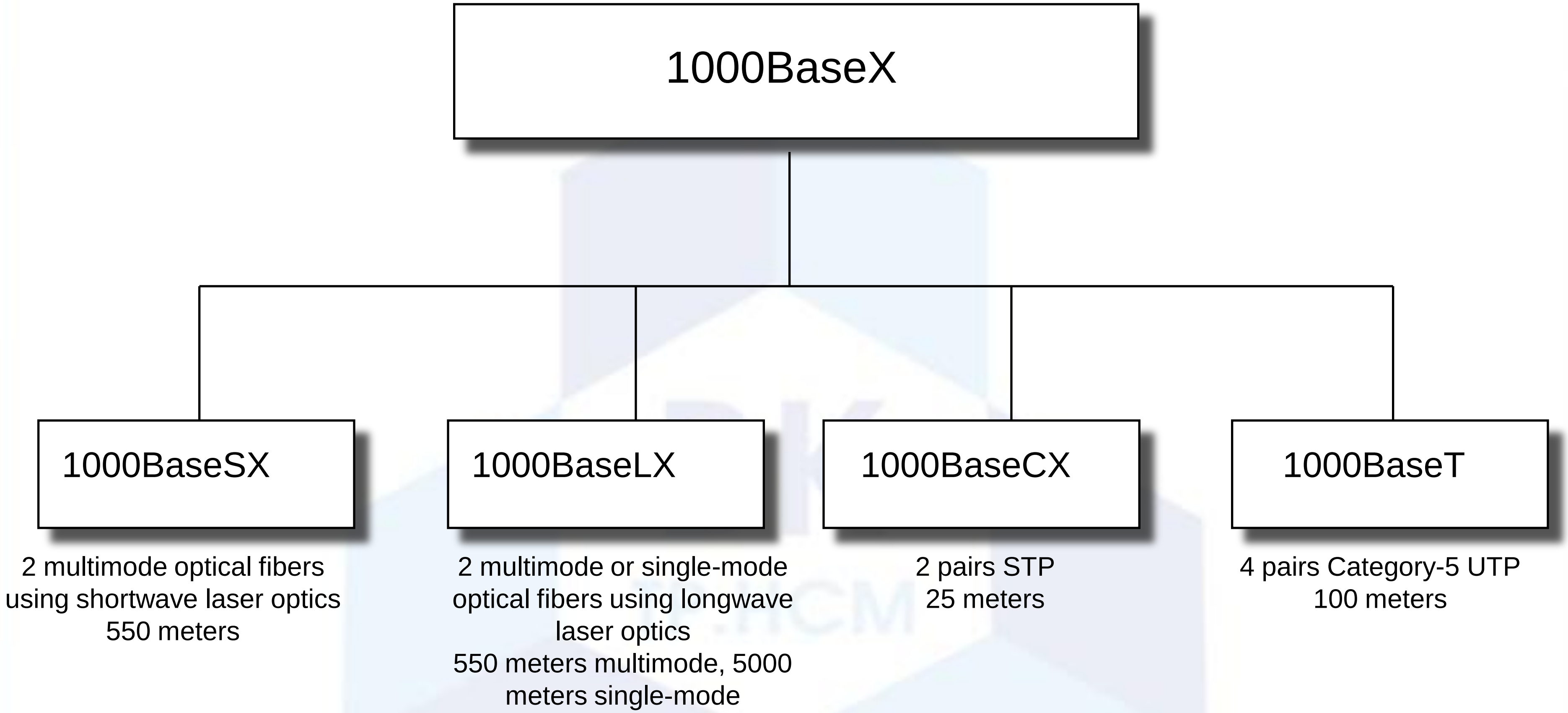
IEEE 802.3 10-Mbps Ethernet



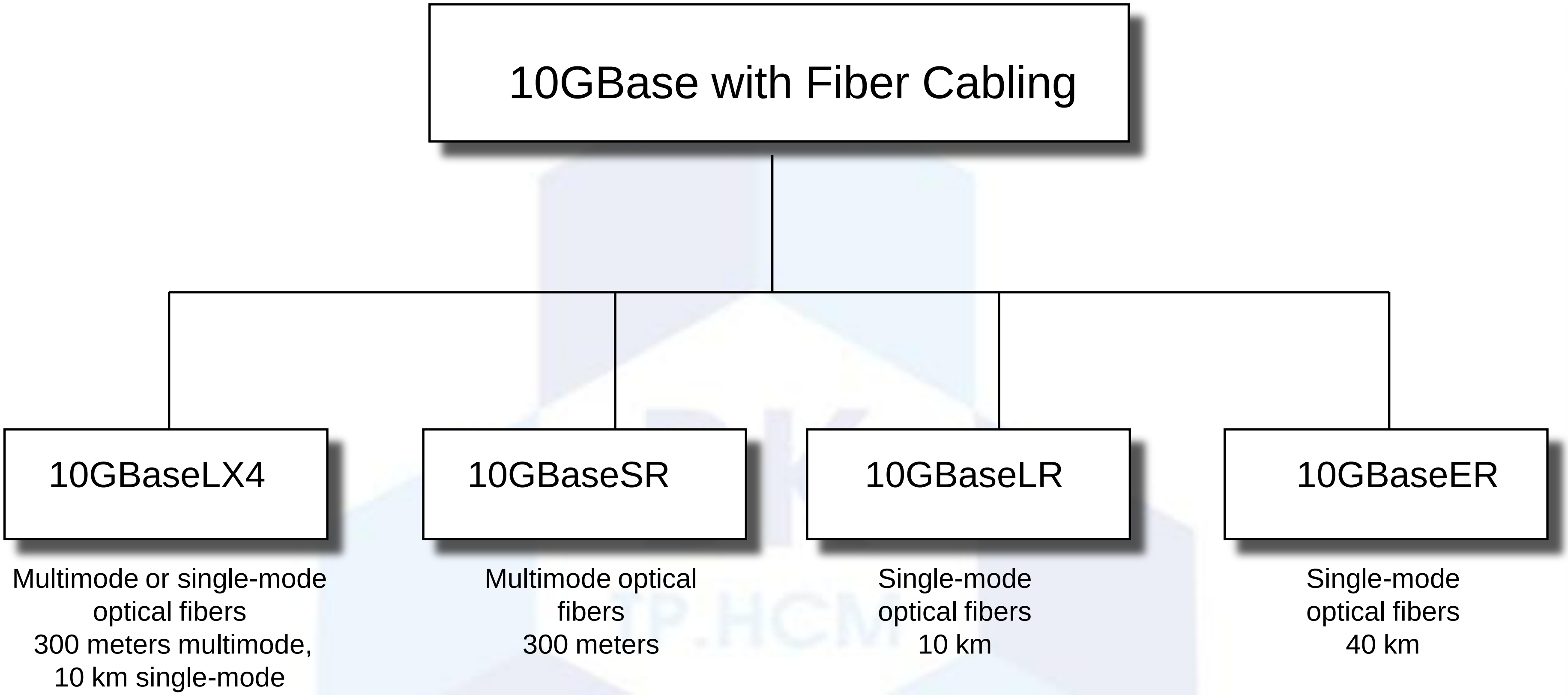
IEEE 802.3 100-Mbps Ethernet



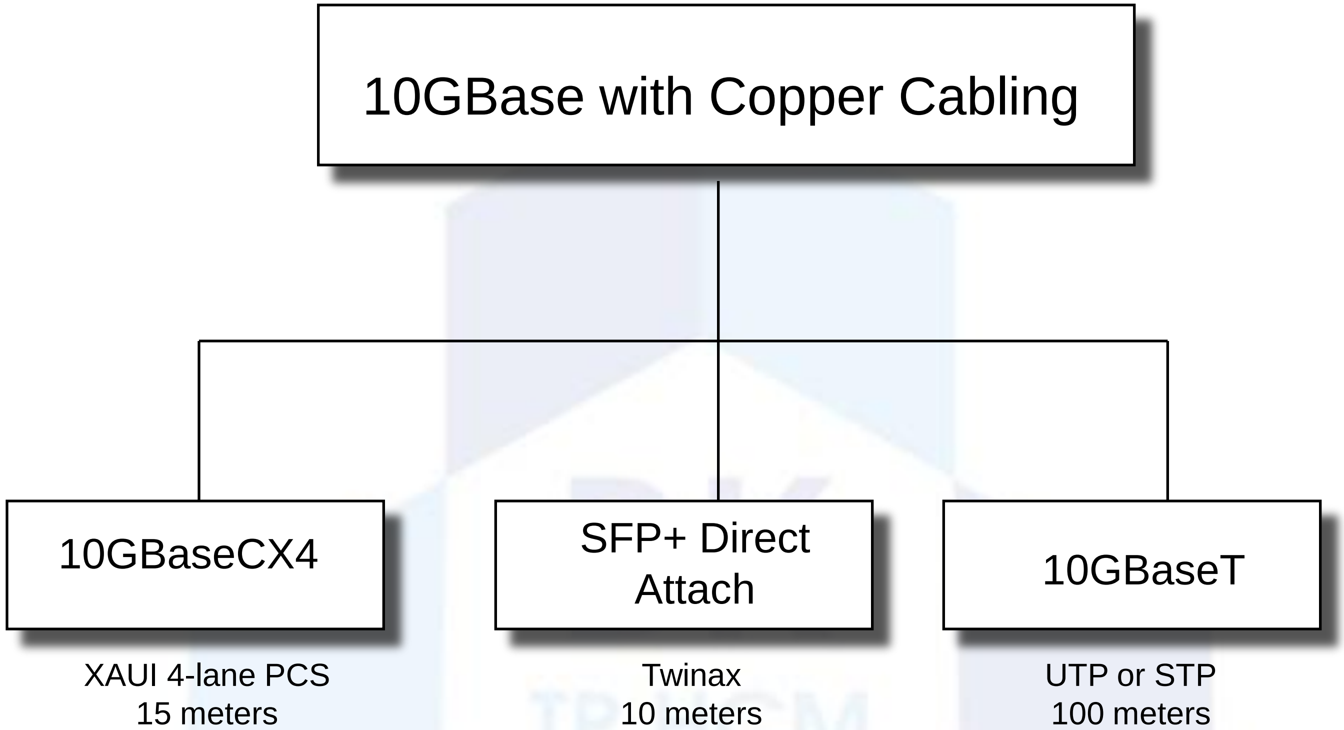
IEEE 802.3 Gigabit Ethernet



IEEE 802.3 10-Gbps Ethernet



IEEE 802.3 10-Gbps Ethernet



Metro Ethernet

- Service offered by providers and carriers that traditionally had only classic WAN offerings
- The customer can use a standard Ethernet interface to reach a MAN or WAN
- The customer can add bandwidth as needed with a simple configuration change

Long-Reach Ethernet

- Enables the use of Ethernet over existing, unconditioned, voice-grade copper twisted-pair cabling
- Used to connect buildings and rooms within buildings
  - Rural areas
  - Old cities where upgrading cabling is impractical
  - Multi-unit structures such as hotels, apartment complexes, business complexes, and government agencies

Internetworking Devices for Campus Networks

- Switches
- Routers
- Wireless access points
- Wireless bridges

Selection Criteria for Internetworking Devices

- The number of ports Dễ dàng vận hành, sửa chữa, dự phòng
- Processing speed
- The amount of memory
- Latency when device relays data
- Throughput when device relays data
- LAN and WAN technologies supported
- Media supported

More Selection Criteria for Internetworking Devices

- Cost
- Ease of configuration and management
- MTBF and MTTR
- Support for hot-swappable components
- Support for redundant power supplies
- Quality of technical support, documentation, and training
- Etc.

Outline

- Physical Network Design
  - Select technologies and devices for campus networks
  - Select technologies and devices for enterprise networks
- Testing, Optimizing, and Documenting the Network Design

Enterprise Technologies and Devices

- Remote access networks
- Wide area networks (WANs)
- Devices
  - End user remote access devices
  - Central site remote access devices
  - VPN concentrators
  - Routers

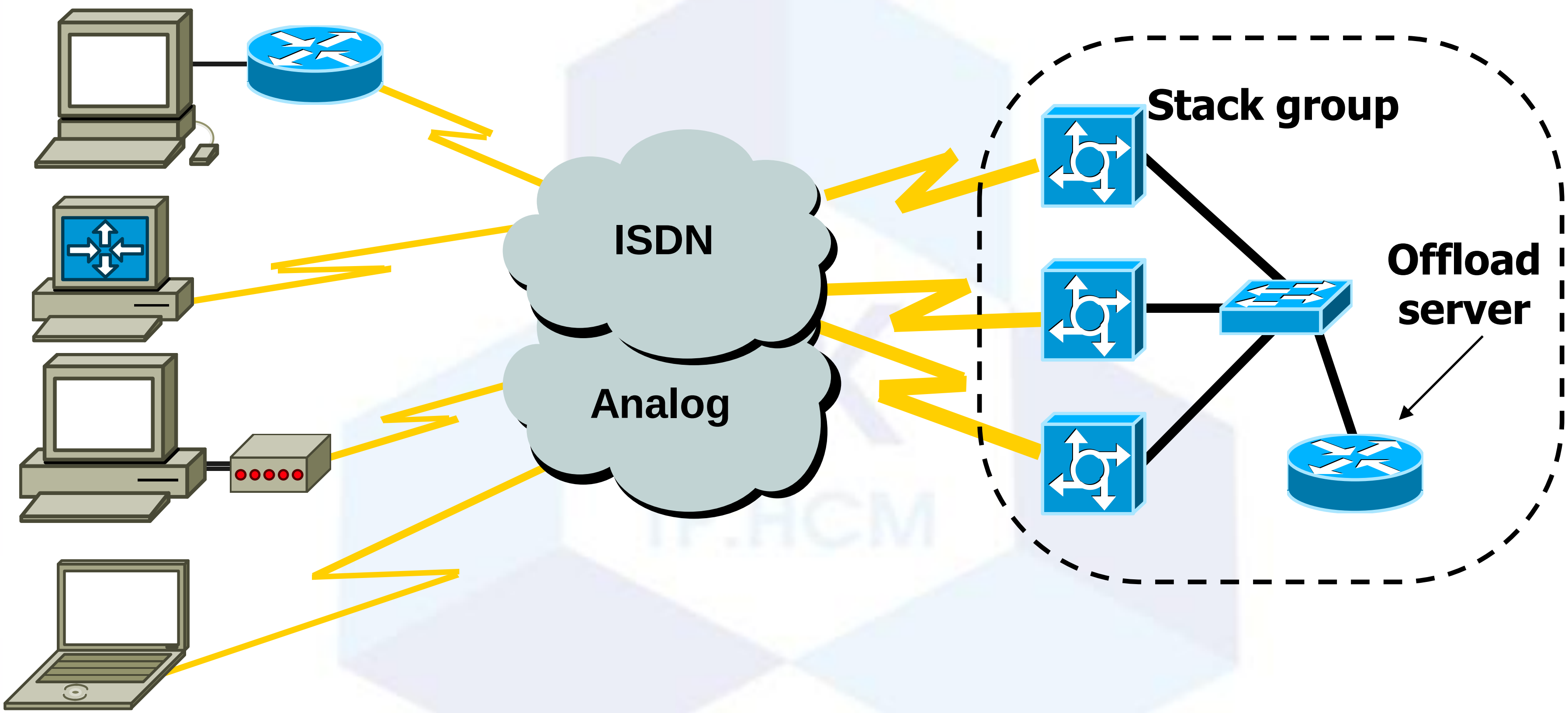
Selection Criteria

- Business requirements and constraints
- Cost
- Technical goals
- Bandwidth requirements
- QoS requirements
- Network topology
- Traffic flow and load
- Etc.

Remote Access Technologies

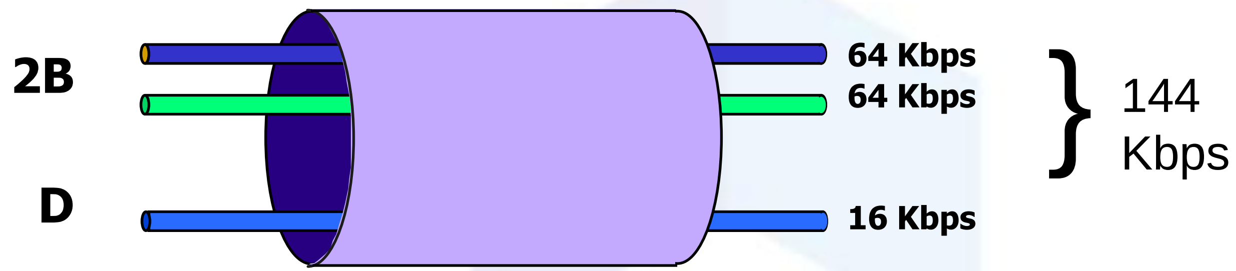
- The Point-to-Point Protocol (PPP)
- Integrated Services Digital Network (ISDN)
- Cable modems
- Digital Subscriber Line (DSL)

Multichassis Multilink PPP

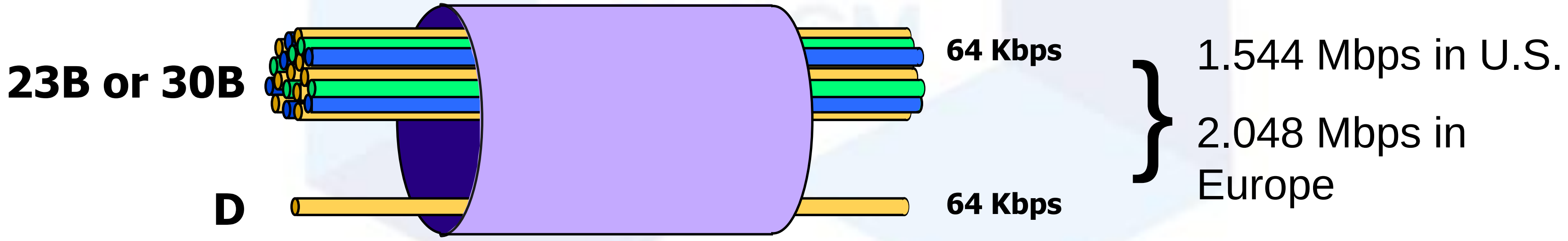


ISDN Interfaces

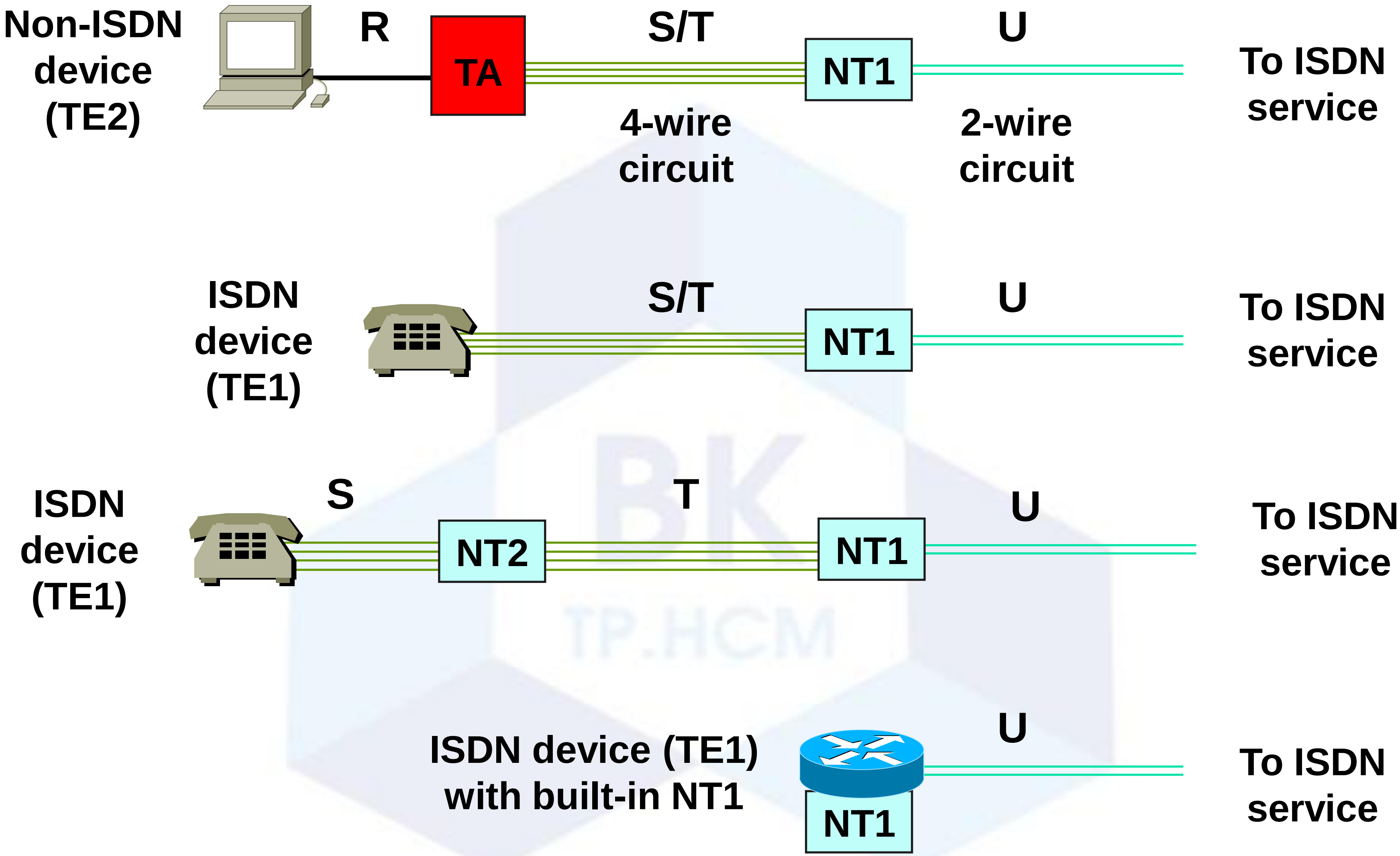
Basic Rate Interface (BRI)



Primary Rate Interface (PRI)



ISDN Components



Cable Modem Service

- Operates over the coax cable used by cable TV
- Much faster than analog modems, and usually much faster than ISDN (depending on how many users share the cable)
  - 25 to 50 Mbps downstream from the head end
  - 2 to 3 Mbps upstream from end users
- Standard = Data Over Cable Service Interface Specification (DOCSIS)

DSL

- High-speed digital data traffic over ordinary telephone wires
- Sophisticated modulation schemes mean higher speeds than ISDN
  - Speeds range from 1.544 to 9 Mbps
- Actual bandwidth depends on type of DSL service, DSL modem, and many physical-layer factors
- Asymmetric DSL (ADSL) very popular
  - Downstream faster than upstream

WAN Technologies

- Leased lines
- Synchronous Optical Network (SONET)
- Frame Relay
- Asynchronous Transfer Mode (ATM)

Leased Lines

- Dedicated digital, copper circuits that a customer leases from a carrier for a predetermined amount of time, usually for months or years
- Speeds range from 64 Kbps to 45 Mbps
- Enterprises use leased lines for both voice and data traffic

The North American Digital Hierarchy

Signal	Capacity	Number of DS0s	Colloquial Name
DS0	64 Kbps	1	Channel
DS1	1.544 Mbps	24	T-1
DS1C	3.152 Mbps	48	T-1C
DS2	6.312 Mbps	96	T-2
DS3	44.736 Mbps	672	T-3
DS4	274.176 Mbps	4032	T-4
DS5	400.352 Mbps	5760	T5

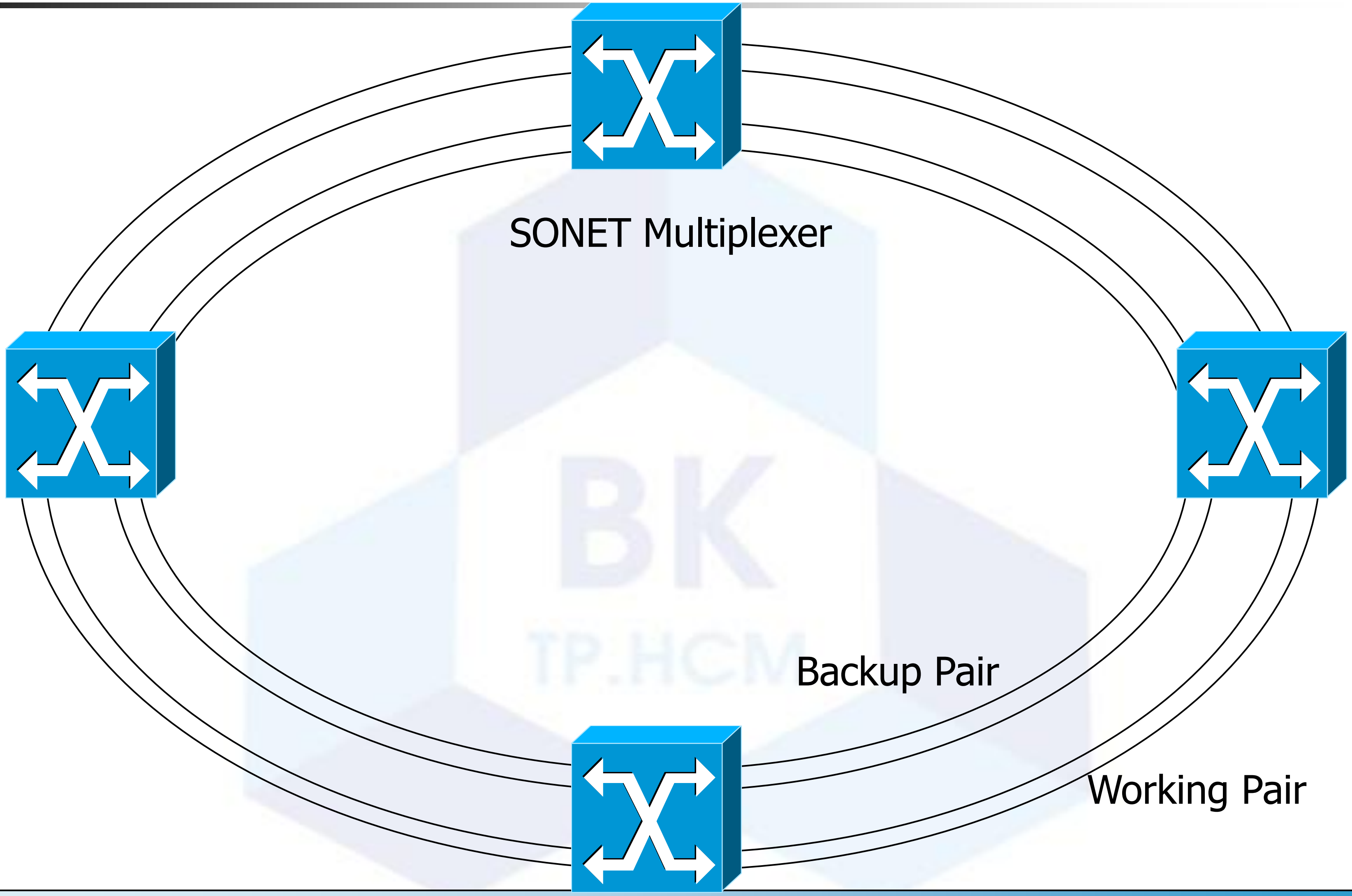
Synchronous Optical Network (SONET)

- Physical-layer specification for high-speed synchronous transmission of packets or cells over fiber-optic cabling
- Service providers and carriers make wide use of SONET in their internal networks
- Gaining popularity within private networks

SONET Optical Carrier (OC) Levels
aka Synchronous Transport Signal (STS) Levels

STS Rate	OC Level	Speed
STS-1	OC-1	51.84 Mbps
STS-3	OC-3	155.52 Mbps
STS-12	OC-12	622.08 Mbps
STS-24	OC-24	1.244 Gbps
STS-48	OC-48	2.488 Gbps
STS-96	OC-96	4.976 Gbps
STS-192	OC-192	9.952 Gbps

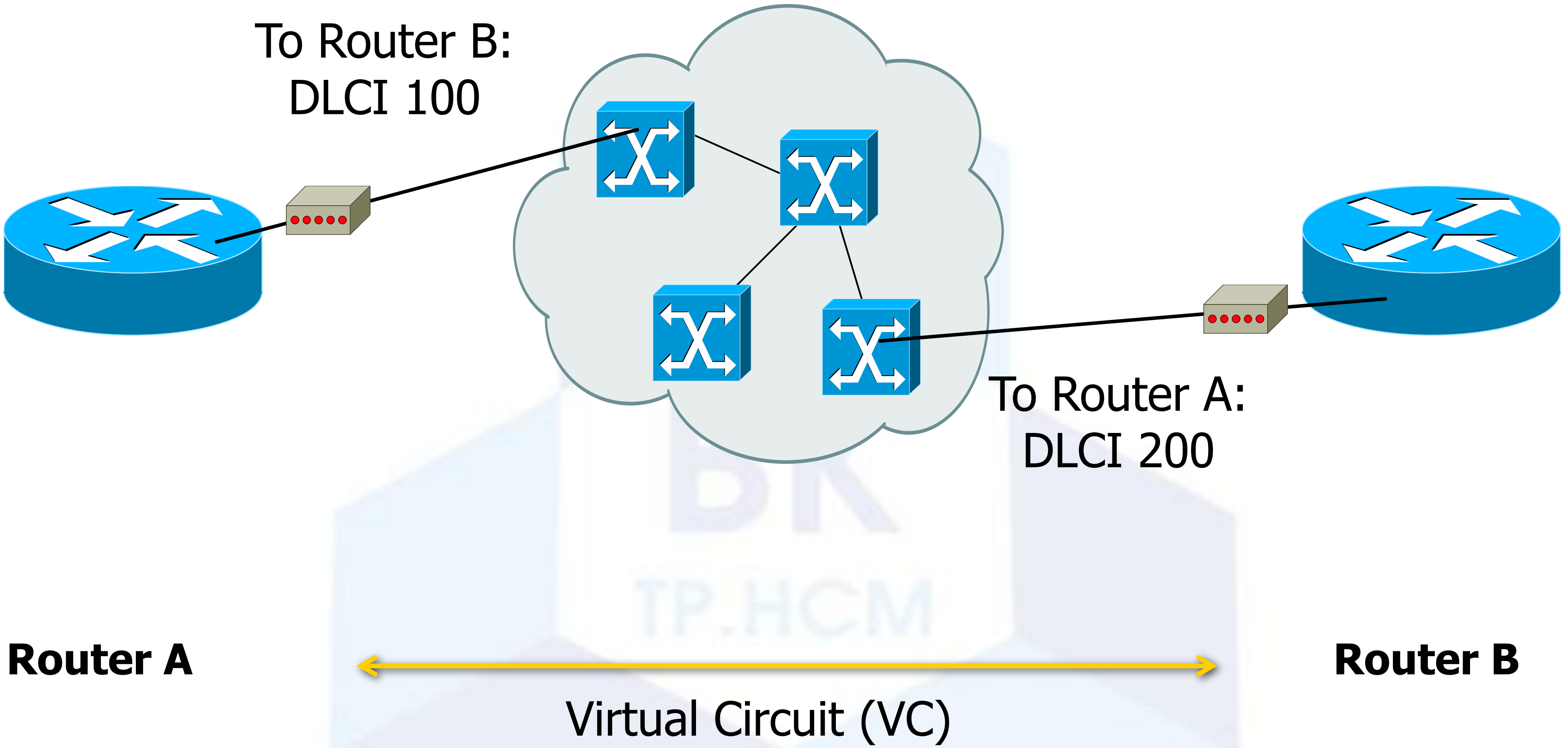
Typical SONET Topology



Frame Relay

- Industry-standard data-link-layer protocol for transporting traffic across wide-area virtual circuits
- Optimized for efficiency on circuits with low error rates
- Attractively-priced in most parts of the world
- Carriers agree to forward traffic at a Committed Information Rate (CIR)

Frame Relay (continued)



Asynchronous Transfer Mode (ATM)

- Used in service provider internal networks
- Gaining popularity within private networks, both WANs and sometimes LANs
- Supports very high bandwidth requirements
  - Copper cabling: 45 Mbps or more
  - Fiber-optic cabling: OC-192 (9.952 Gbps) and beyond, especially if technologies such as wave-division multiplexing (WDM) are used

Ethernet over ATM

- ATM router interfaces are expensive
- Some providers allow a customer to use an Ethernet interface to access the provider's ATM WAN
- May require a converter
- Expected to gain popularity because it has the advantages of both worlds
  - Easy-to-use LAN
  - QoS-aware WAN

Selection Criteria for Remote Access Devices

- Support for VPN features
- Support for NAT
- Reliability
- Cost
- Ease of configuration and management
- Support for one or more high-speed Ethernet interfaces
- If desired, wireless support
- Etc.

Selection Criteria for VPN Concentrators

- Support for:
  - Tunneling protocols such as IPSec, PPTP, and L2TP
  - Encryption algorithms such as 168-bit Triple DES, Microsoft Encryption (MPPE), RC4, AES
  - Authentication algorithms, including MD5, SHA-1, HMAC
  - Network system protocols, such as DNS, RADIUS, Kerberos, LDAP
  - Routing protocols
  - Certificate authorities
  - Network management using SSH or HTTP with SSL
  - Etc.

Selection Criteria for Enterprise Routers

- Number of ports
- Processing speed
- Media and technologies supported
- MTTR and MTBF
- Throughput
- Optimization features
- Etc

Selection Criteria for a WAN Service Provider

- Extent of services and technologies
- Geographical areas covered
- Reliability and performance characteristics of the provider's internal network
- The level of security offered by the provider
- The level of technical support offered by the provider
- The likelihood that the provider will continue to stay in business

Selecting a Provider (continued)

- The provider's willingness to work with you to meet your needs
- The physical routing of network links
- Redundancy within the network
- The extent to which the provider relies on other providers for redundancy
- The level of oversubscription on the network
- QoS support
- Etc.

Outline

- Physical Network Design
- Testing, Optimizing, and Documenting the Network Design
  - Test the network design
  - Optimize the network design
  - Document the network design

Reasons to Test

- Verify that the design meets key business and technical goals
- Validate LAN and WAN technology and device selections
- Verify that a service provider provides the agreed-up service
- Identify bottlenecks or connectivity problems
- Determine optimization techniques that will be necessary

Testing Your Network Design

- Use industry testing services
- Build and test a prototype system
- Use tools

Industry Testing Services

- The Interoperability Lab at the University of New Hampshire (IOL)
- ICSA Labs
- Miercom Labs
- AppLabs
- The Tolly Group

Scope of a Prototype System

- It’s not generally practical to implement a full-scale system.
- A prototype should verify important capabilities and functions that might not perform adequately.
- Risky functions include complex, intricate functions and functions that were influenced by the need to make tradeoffs.

Components of a Test Plan

- Test objectives and acceptance criteria
- The types of tests that will be run
- Network equipment and other resources required
- Testing scripts
- The timeline and milestones for the testing project

Test Objectives and Acceptance Criteria

- Specific and concrete
- Based on business and technical goals
- Clear criteria for declaring that a test passed or failed
- Avoid biases and preconceived notions about outcomes
- If appropriate, reference a baseline

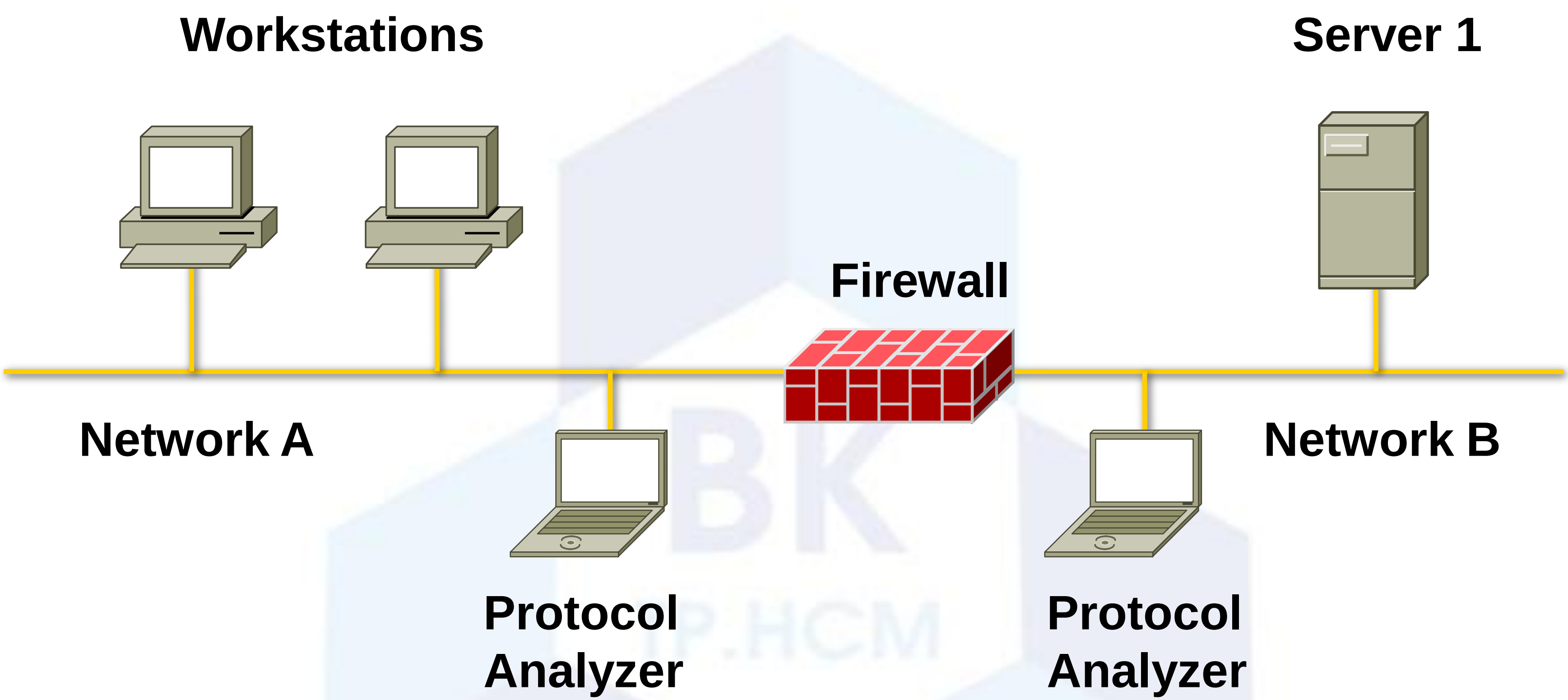
Types of Tests

- Application response-time tests
- Throughput tests
- Availability tests
- Regression tests

Resources Needed for Testing

- Scheduled time in a lab either at your site or the customer's site
- Power, air conditioning, rack space, and other physical resources
- Help from coworkers or customer staff
- Help from users to test applications
- Network addresses and names

Example Test Script



Example Test Script (continued)

- Test objective. Assess the firewall's capability to block Application ABC traffic, during both light and moderately heavy load conditions.
- Acceptance criterion. The firewall should block the TCP SYN request from every workstation on Network A that attempts to set up an Application ABC session with Server 1 on Network B. The firewall should send each workstation a TCP RST (reset) packet.

Example Test Script (continued)

1. Start capturing network traffic on the protocol analyzer on Network A.
2. Start capturing network traffic on the protocol analyzer on Network B.
3. Run Application ABC on a workstation located on Network A and access Server 1 on Network B.
4. Stop capturing network traffic on the protocol analyzers.

Example Test Script (continued)

5. Display data on Network A's protocol analyzer and verify that the analyzer captured a TCP SYN packet from the workstation. Verify that the network layer destination address is Server 1 on Network B, and the destination port is port 1234 (the port number for Application ABC). Verify that the firewall responded to the workstation with a TCP RST packet.
6. Display data on Network B's protocol analyzer and verify that the analyzer did not capture any Application-ABC traffic from the workstation.

Example Test Script (continued)

7. Log the results of the test in the project log file.
8. Save the protocol-analyzer trace files to the project trace-file directory.
9. Gradually increase the workload on the firewall, by increasing the number of workstations on Network A one at a time, until 50 workstations are running Application ABC and attempting to reach Server 1. Repeat steps 1 through 8 after each workstation is added to the test.

Tools for Testing a Network Design

- Network-management and monitoring tools
- Traffic generation tools
- Modeling and simulation tools
- QoS and service-level management tools
- http://www.topdownbook.com/tools.html

Outline

- Physical Network Design
- Testing, Optimizing, and Documenting the Network Design
  - Test the network design
  - Optimize the network design
  - Document the network design

Reasons to Optimize

- Meet key business and technical goals
- Use bandwidth efficiently
- Control delay and jitter
- Reduce serialization delay
- Support preferential service for essential applications
- Meet Quality of Service (QoS) requirements

IP Multicast Helps Optimize Bandwidth Usage

- With IP multicast, you can send a high-volume multimedia stream just once instead of once for each user
- Requires support for
  - Multicast addressing
  - Multicast registration (IGMP)
  - Multicast routing protocols

IP Multicast Addressing

- Uses Class D multicast destination address
  - 224.0.0.0 to 239.255.255.255
- Converted to a MAC-layer multicast destination address
  - The low-order 23 bits of the Class D address become the low-order 23 bits of the MAC-layer address
  - The top 9 bits of the Class D address are not used
  - The top 25 bits of the MAC-layer address are 0x01:00:5E followed by a binary 0

Internet Group Management Protocol (IGMP)

- Allows a host to join a multicast group
- Host transmits a *membership-report* message to inform routers on the segment that traffic for a group should be multicast to the host's segment
- IGMPv2 has support for a router more quickly learning that the last host on a segment has left a group

Multicast Routing Protocols

- Becoming obsolete
  - Multicast OSPF (MOSPF)
  - Distance Vector Multicast Routing Protocol (DVMRP)
- Still used
  - Protocol Independent Multicast (PIM)
    - Dense-Mode PIM
    - Sparse-Mode PIM

Reducing Serialization Delay

- Link-layer fragmentation and interleaving
  - Breaks up and reassembles frames
  - Multilink PPP
  - Frame Relay FRF.12
- Compressed Real Time Protocol
  - RTP is used for voice and video
  - Compressed RTP compresses the RTP, UDP, and IP header from 40 bytes to 2 to 4 bytes

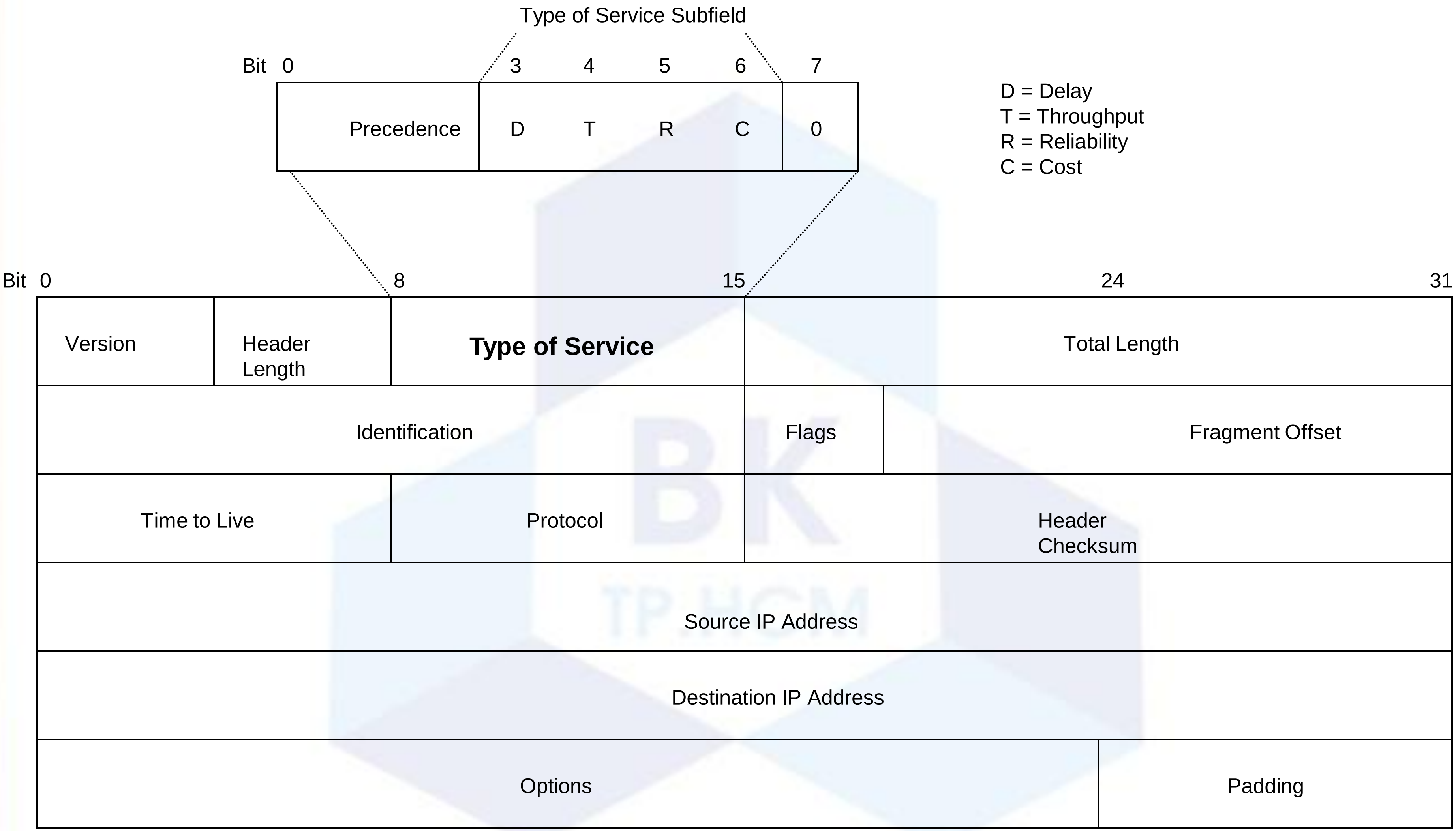
A Few Technologies for Meeting QoS Requirements

- IETF controlled load service
- IETF guaranteed service
- IP precedence
- IP differentiated services

IP Type of Service Field

- The type of service field in the IP header is divided into two subfields
  - The 3-bit precedence subfield supports eight levels of priority
  - The 4-bit type of service subfield supports four types of service
- Although IP precedence is still used, the type of service subfield was hardly ever used

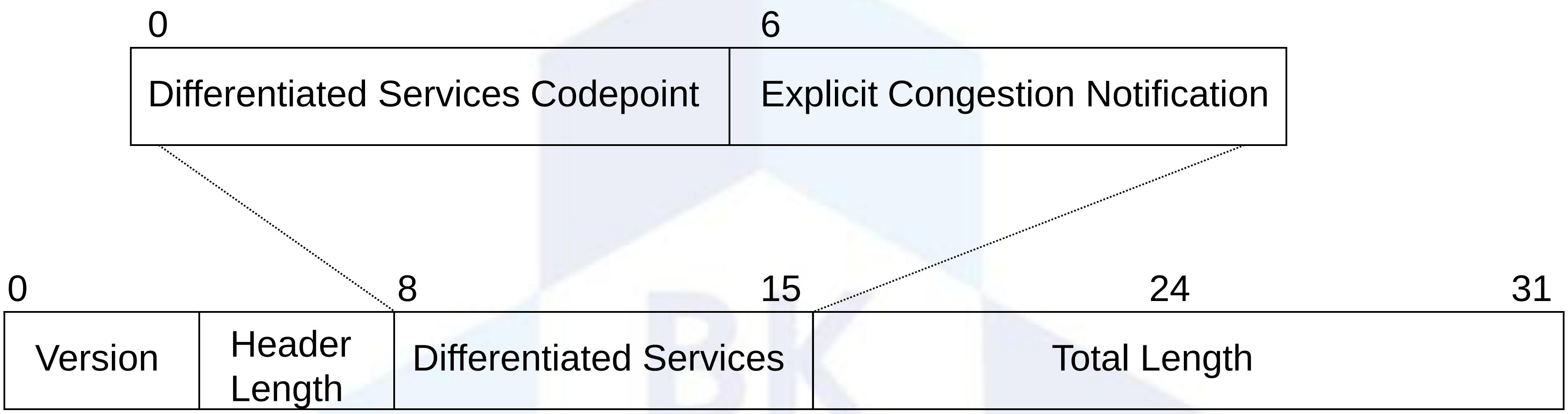
IP Type of Service Field



IP Differentiated Services (DS) Field

- RFC 2474 redefines the type of service field as the Differentiated Services (DS) field
  - Bits 0 through 5 are the Differentiated Services Codepoint (DSCP) subfield
    - Has essentially the same goal as the precedence subfield
    - Influences queuing and packet dropping decisions for IP packets at a router output interface
  - Bits 6 and 7 are the Explicit Congestion Notification (ECN) subfield

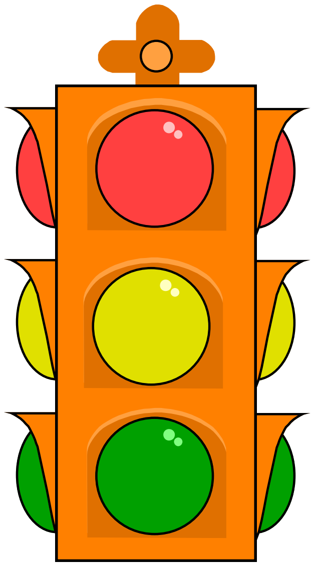
IP Differentiated Services (DS) Field



Classifying LAN Traffic

- IEEE 802.1p
- Classifies traffic at the data-link layer
- Supports eight classes of service
- A switch can have a separate queue for each class and service the highest-priority queues first

Low-Latency Queuing



- One queue always gets the green light
  - Use this for voice
- Combine this with class-based weighted fair queuing
  - Define traffic classes based on protocols, access control lists, and input interfaces
  - Assign characteristics to classes such as bandwidth required and the maximum number of packets that can be queued for the class

Random Early Detection (RED)

- Congestion avoidance rather than congestion management
- Monitors traffic loads and randomly discards packets if congestion increases
- Source nodes detect dropped packets and slow down
  - Works best with TCP
- Weighted Random Early Detection
  - Cisco's implementation uses IP precedence or the DS field instead of just randomly dropping packets

Traffic Shaping

- Manage and control network traffic to avoid bottlenecks
- Avoid overwhelming a downstream router or link
- Reduce outbound traffic for a flow to a configured bit rate
  - Queue bursts of traffic for that flow

Outline

- Physical Network Design
- Testing, Optimizing, and Documenting the Network Design
  - Test the network design
  - Optimize the network design
  - Document the network design

Documenting Your Design

- If you are given a request for proposal (RFP), respond to the request in the exact format that the RFP specifies
- If no RFP, you should still write a design document
  - Describe your customer's requirements and how your design meets those requirements
  - Document the budget for the project
  - Explain plans for implementing the design

Typical RFP Response Topics

- A network topology for the new design
- Information on the protocols, technologies, and products that form the design
- An implementation plan
- A training plan
- Support and service information
- Prices and payment options
- Qualifications of the responding vendor or supplier
- Recommendations from other customers
- Legal contractual terms and conditions

Contents of a Network Design Document

- Executive summary
- Project goal
- Project scope
- Design requirements
- Current state of the network
- New logical and physical design
- Results of network design testing
- Implementation plan
- Project budget

Design Requirements

- Business goals explain the role the network design will play in helping an organization succeed
- Technical goals include scalability, performance, security, manageability, usability, adaptability, and affordability

Logical and Physical Design

- Logical design
  - Topology
  - Models for addressing and naming
  - Switching and routing protocols
  - Security strategies
  - Network management strategies
- Physical design
  - Actual technologies and devices

Implementation Plan

- Recommendations for deploying the network design
- Project schedule
  - Including any dates and times for service provider installations
- Any plans for outsourcing
- Training
- Risks
- A fallback plan if the implementation should fail
- A plan for evolving the design as new requirements arise

Possible Appendixes

- Detailed topology maps
- Device configurations
- Addressing and naming details
- Network design testing results
- Contact information
- Pricing and payment options
- More information about the company that is presenting the design
  - Annual reports, product catalogs, press releases
- Legal contractual terms and conditions