1.264 Lecture 37

Telecom: Enterprise networks, VPN

Enterprise networks

- Connections within enterprise
- External connections
  - Remote offices
  - Employees
  - Customers
  - Business partners, supply chain partners
  - Patients…and other actors with special requirements
- Principles of enterprise network design
  - Standards based
  - Secure
  - Reliable: disruptions affect all external connections
  - Quality of service: latency, throughput, services, …

Building blocks of enterprise network

- Local area networks
- Wide- or metro-area networks: include 1 or more of:
  - Private lines (point to point circuits)
  - “Carrier Ethernet” MAN over carrier fiber in metro areas
  - Virtual private net (VPN) over Internet
  - Private or carrier-provided networks separate from Internet
    - Frame relay (pre-Internet, still used but being superseded)
    - Label switched (MPLS), over carrier IP network
    - Covered later in this lecture
- Voice network: includes one or more of:
  - Integrated with data network
  - Private lines shared between data and voice
  - Voice carried over IP or MPLS network
- Video network
  - Usually carried as service over data network

Virtual private networks (VPN)

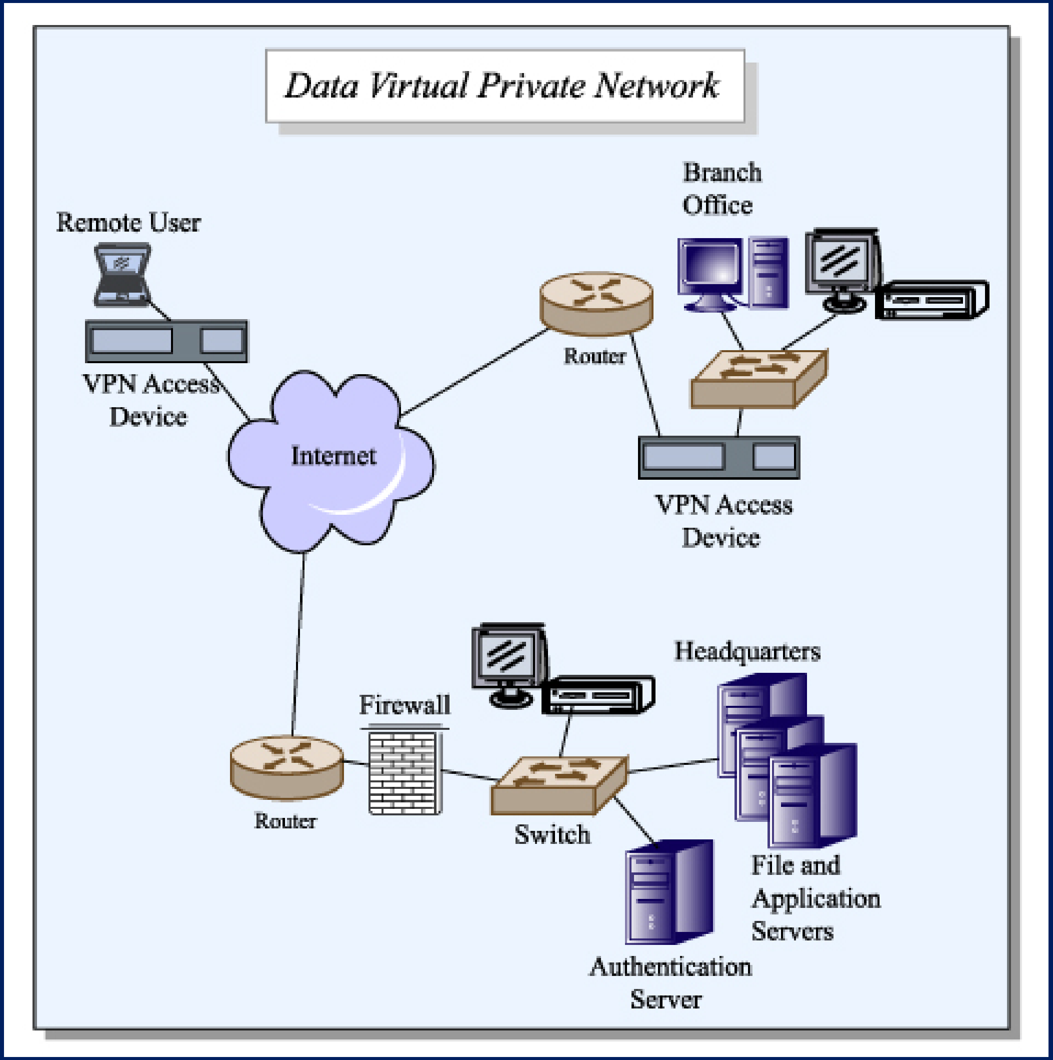


Image by MIT OpenCourseWare.

Virtual private networks (VPNs)

- Definition: VPN is set of sites that
  - Communicate over the open Internet but
  - With the security and management capabilities of dedicated circuit or frame relay network
  - Supporting applications without modification
  - With simple management for admins and users
  - And with low overhead and good communications performance
  - Typically handle data only but can handle voice, video
- VPN basic functions
  - Authentication (identity), authorization (privileges)
  - Establishment of secure tunnel (path) in network

VPN technology

- VPN tunnel encapsulates data of one protocol inside the data field of another protocol
  - VPN encrypts corporate data inside IP packet data field (which is managed by TCP, which is called by HTTP)
    - HTTP and TCP data is inside the IP packet and is encrypted
  - The corporate data is encrypted via the VPN’s security protocol (symmetric, asymmetric keys, message digests)
    - SSL is frequently used; Kerberos-like options also available
- VPNs operate at layer 2 (Ethernet) or layer 3 (IP)
  - Layer 3: Routers use IP information to route
    - Most common: Easier to manage, but lower performance
  - Layer 2: uses Ethernet addresses; corporation responsible for routing packets across WAN and LANs
    - Harder to manage, but better performance
- VPNs operate over DSL, cable, etc.
  - Simple network topology (all links to/thru central point)
  - Limited redundancy, resiliency

VPN tunnel

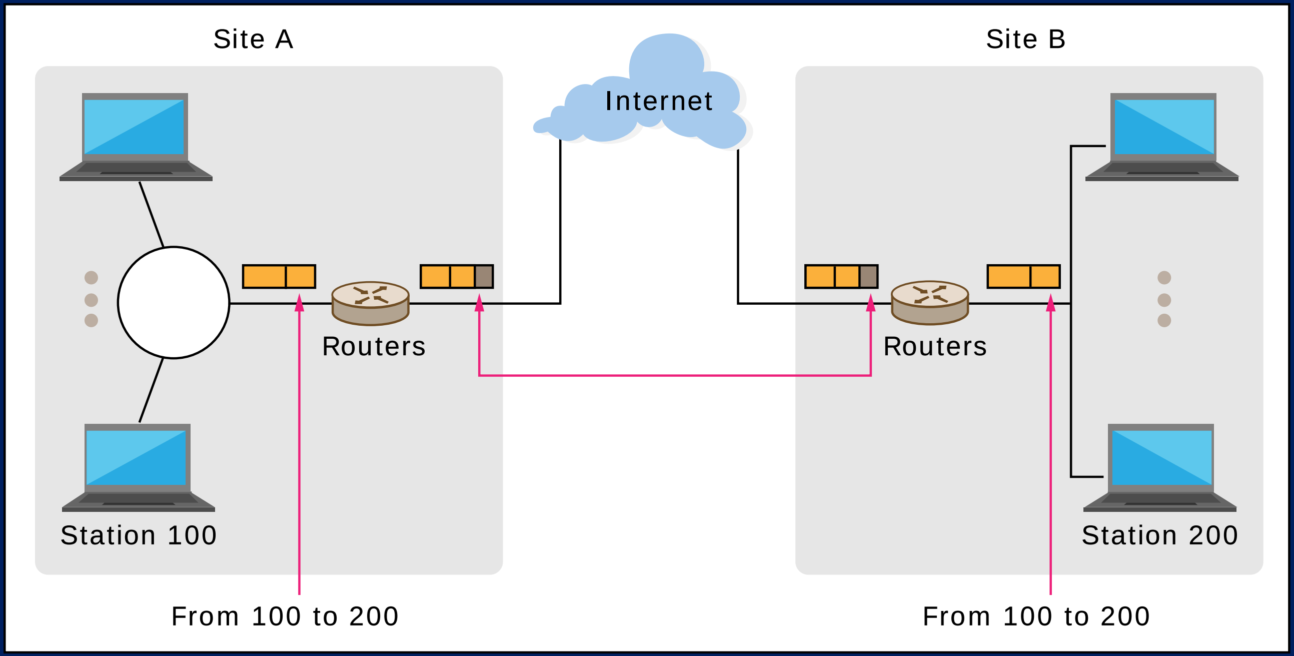


Image by MIT OpenCourseWare.

- Internet carries packet between routers R1 and R2
- Packet is encrypted, and intruder only sees R1 and R2 IP addresses
- Actual IP addresses (100 and 200) cannot be seen, nor the packet contents

VPN terminology

- Intranet
  - Portion of VPN connecting internal sites
- Extranet
  - Portion of VPN connecting external sites
- Security protocols
  - Secure Sockets Layer (SSL)
  - IPsec (secure IP standard) at layer 3
    - Can encrypt entire packet (tunnel mode) or just the data field (transport mode)
    - All devices must share a common (public) key, in digital certificate
    - Devices negotiate secure tunnel using Internet Key Exchange (IKE) protocol
  - Layer 2 tunneling protocol (L2TP)
    - Requires pre-arranged paths between devices or to/from secure server

Enterprise routing: IP and other protocols

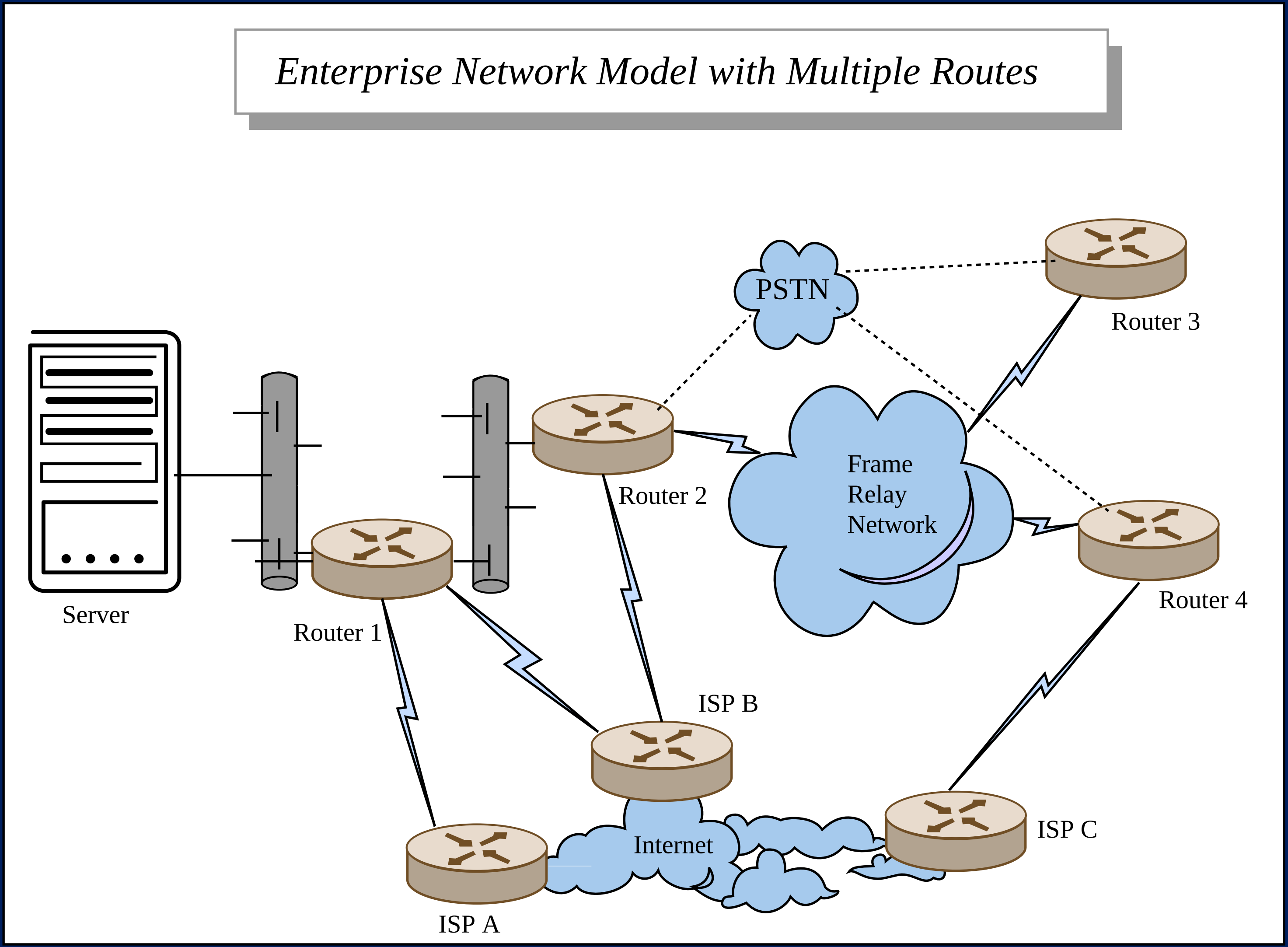


Image by MIT OpenCourseWare.

Multiprotocol Label Switching (MPLS)

- Label edge routers (LERs) assign a label that defines the path the packet will take through the IP network
  - Routing happens only once, at edge
  - Routing at interior routers (label switched routers, or LSRs) is done in hardware, not a software lookup of IP routing tables
    - Much faster, cheaper
    - A stack of labels allows complex, hierarchical networks
  - Label distribution protocol (LDP) used to distribute labels to all LSRs and LERs, using TCP/IP
  - MPLS allows QoS, security (strict traffic rules)
    - MPLS VPNs operate at layer 2 or layer 3
    - Corporate routers don’t need to support MPLS; they connect to LER via IP
  - MPLS is a fiber-only technology, national but not global scope (yet), complex network, “Ethernet-like” operation

Multiprotocol Label Switching

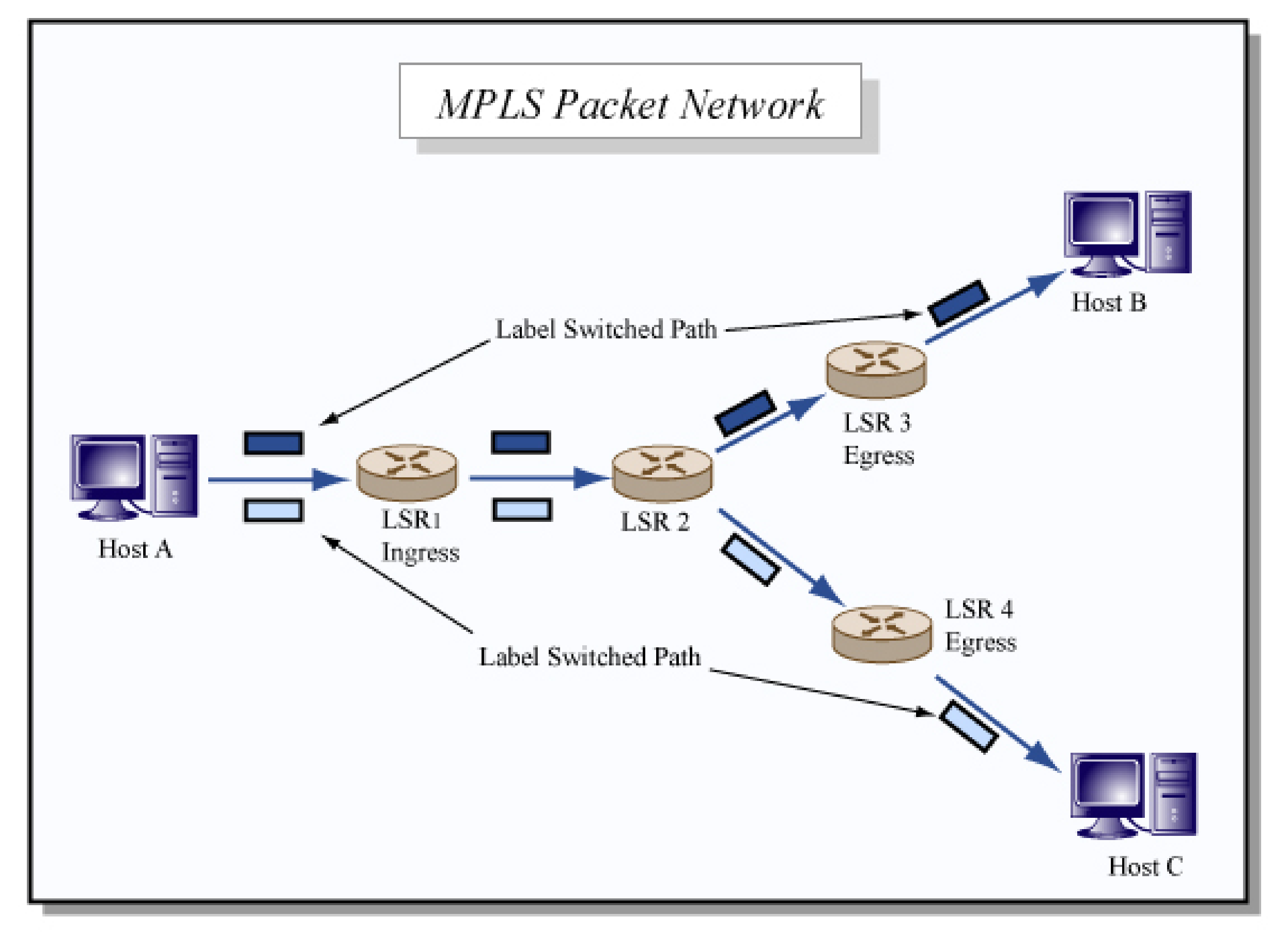


Image by MIT OpenCourseWare.

Network neutrality debate…

Virtual LANs

- MPLS is sometimes described as implementing a virtual LAN, or VLAN: set up LANs in software

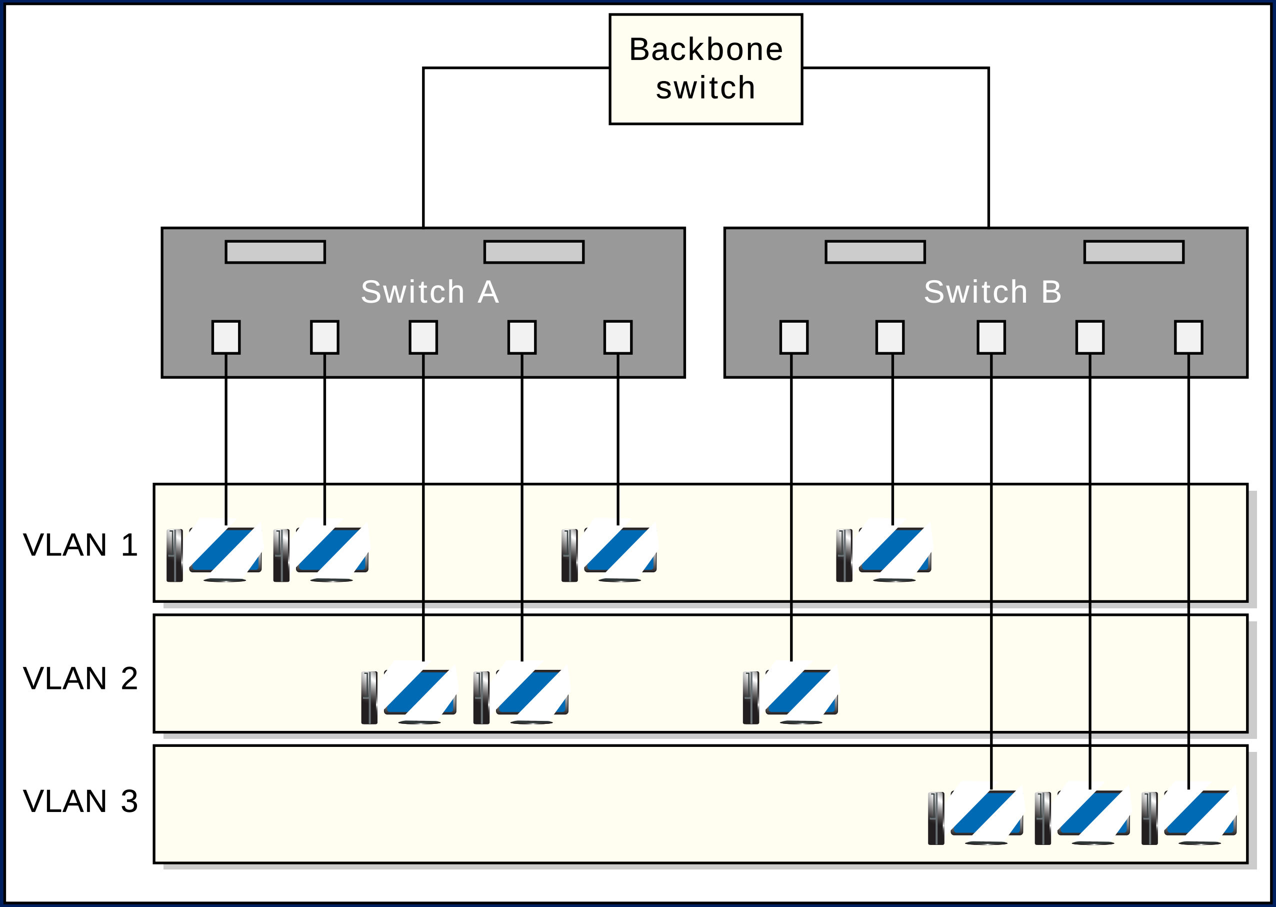
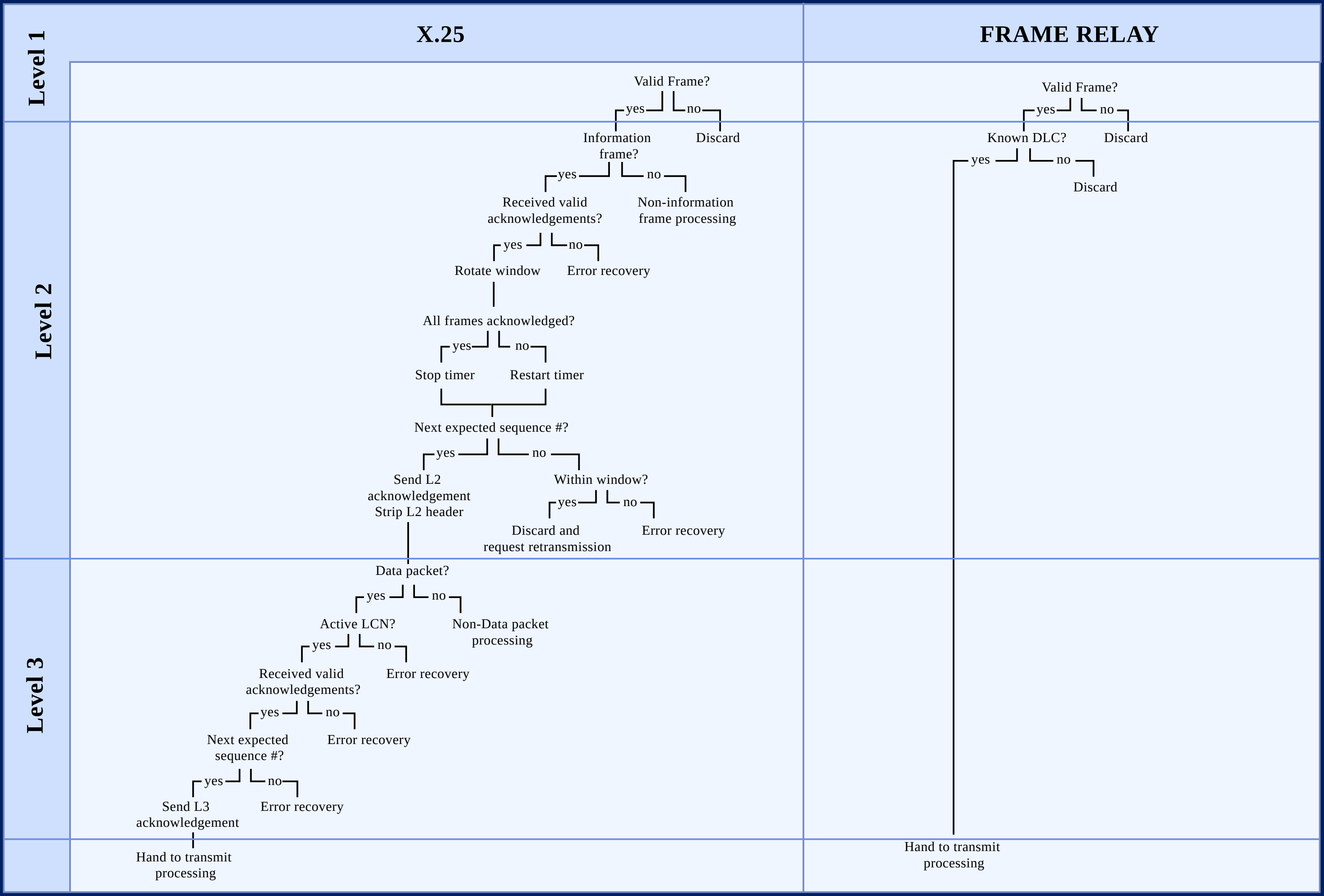


Image by MIT OpenCourseWare.

Technology changes

- Next slide compares X.25 and frame relay
  - X.25 was developed for copper or radio long-haul networks with high error rates
  - Link-by-link error correction as a message travels across the network
  - Assumes ‘dumb’ equipment at the edges, so the X.25 protocol takes full responsibility for delivering messages correctly
- Frame relay (or any other protocol carried on fiber optics such as TCP/IP)
  - Relies on low fiber optic error rate. No link-by-link error correction, just a retransmission triggered by end node if message not correctly received
- A wireless long haul net would need roughly the same protocols as X.25
  - Smart edge devices make it easier than X.25

Frame relay vs X.25



X.25

FRAME RELAY

Level 1

Level 2

Level 3

Valid Frame?
yes
no
Information frame?
Discard
yes
no
Received valid acknowledgements?
Non-information frame processing
yes
no
Rotate window
Error recovery
All frames acknowledged?
yes
no
Stop timer
Restart timer
Next expected sequence #?
yes
no
Send L2 acknowledgement Strip L2 header
Within window?
yes
no
Discard and request retransmission
Error recovery
Data packet?
yes
no
Active LCN?
Non-Data packet processing
yes
no
Received valid acknowledgements?
Error recovery
yes
no
Next expected sequence #?
Error recovery
yes
no
Send L3 acknowledgement
Error recovery
Hand to transmit processing

Valid Frame?
yes
no
Known DLC?
Discard
yes
no
Discard
Hand to transmit processing

Image by MIT OpenCourseWare.

Frame relay/Internet vs. X.25

- Difference between reliable and unreliable networks
  - Fiber has error rate of 1 bit in 10^{14}; can correct end-to-end
  - Wireless has error rate of 1 bit in 10^{6}; must correct link-by-link
- Difference between smart and dumb terminals
  - Formerly, terminals had no CPU and just displayed what the communications line sent to them
    - Could not detect or correct errors
  - PCs, servers, smart phones as terminals can correct and detect errors
- “Hollowing out of the network”
  - Network (switches, etc.) used to have all the intelligence
  - Now network is just a set of ‘bit pipes’
  - Edge devices have the intelligence

Telecom convergence

- Convergence: Moving all voice, data and video traffic onto Internet
  - Consumer service reasons:
    - Smart cards and mobile phones: browsers, phone as payment medium, smart posters, cameras
    - E-commerce generally
  - End of the personal computer (PC) as we know it, for most users
  - Cost reduction: one network versus many
    - Private nets morph into carrier nets with Internet protocols
  - Increased mobility services
    - Tying wireless access to fiber optic backbone flexibly
  - Barriers:
    - Low quality, chaos of open Internet to reach customers
    - Security to reach customers
    - Broadband in the ‘last mile’ to reach businesses and homes

Glossary

- VPN: Virtual private network
- IPsec: Secure IP (layer 3 security used in VPNs)
- L2TP: Layer 2 tunneling protocol (VPN)
- PSTN: Public switched telephone network, or carrier network
- MPLS: Multiprotocol Label Switching, a WAN technology to connect LANs transparently
  - LER: MPLS Label Edge Router
  - LSR: MPLS Label Switched Router (interior)
  - LDP: MPLS Label Distribution Protocol
- QoS: Quality of service

Steps and skills for building these systems are same as we’ve covered in class this semester

- Software engineering and project management
  - People, process, product, technology dimensions
  - Select development method (often spiral model)
  - Requirements, design, resource estimation, implementation, QA
- Process modeling
  - UML: describe use cases, states, activities, classes, components
  - Used in requirements, scoping, design early; architecture late
- Data modeling
  - Model business rules, verify with users (internal, customers, …)
  - Normalization, referential integrity
- Database
  - Relational databases, SQL at core of applications, Web
  - Databases read/write XML

Steps, continued

- World Wide Web:
  - Connect clients and servers: HTTP, XML, Web services
  - Use HTTP, XML as universal data access
  - XML allows human, machine and document interpretation
  - XML documents include business rules, database schema
- Security
  - Protocols codify rules, principals, risks, …
  - TLS and Kerberos
  - TLS encryption, certificates, digital signatures
  - People, process, product, technology dimensions again
- Networks
  - Multi tier : Web, application, database
  - 7 layer data comm model: HTTP (7), TCP/IP (4/3), Ethernet (2)
  - LANs, MANs, WANs: LANs, MANs are Ethernet, WANs vary
  - Fiber optic core, wireless/copper/CATV for access
  - Use private/carrier network, not open Internet in many cases

Course summary: process

- If you spent 12 hours per week for 14 weeks, that's 168 hours, or 4 40 hour weeks
- Ready for second spiral after 8 person weeks of work (4 person weeks times 2 people)
  - This can be done in the wasted “up-front” time to prepare for an anticipated project
  - It will usually take this long because you'll usually be learning a new domain and/or new technology
- By using the spiral model and being able to do requirements, UML, data models, SQL, Web sites, initial security approach and initial telecom approach, you can:
  - Work effectively with IT staff
  - Manage engineering or logistics projects with IT components
- By knowing technical areas covered in class, you can:
  - Specify, design and build databases, Web sites, etc. as a consultant