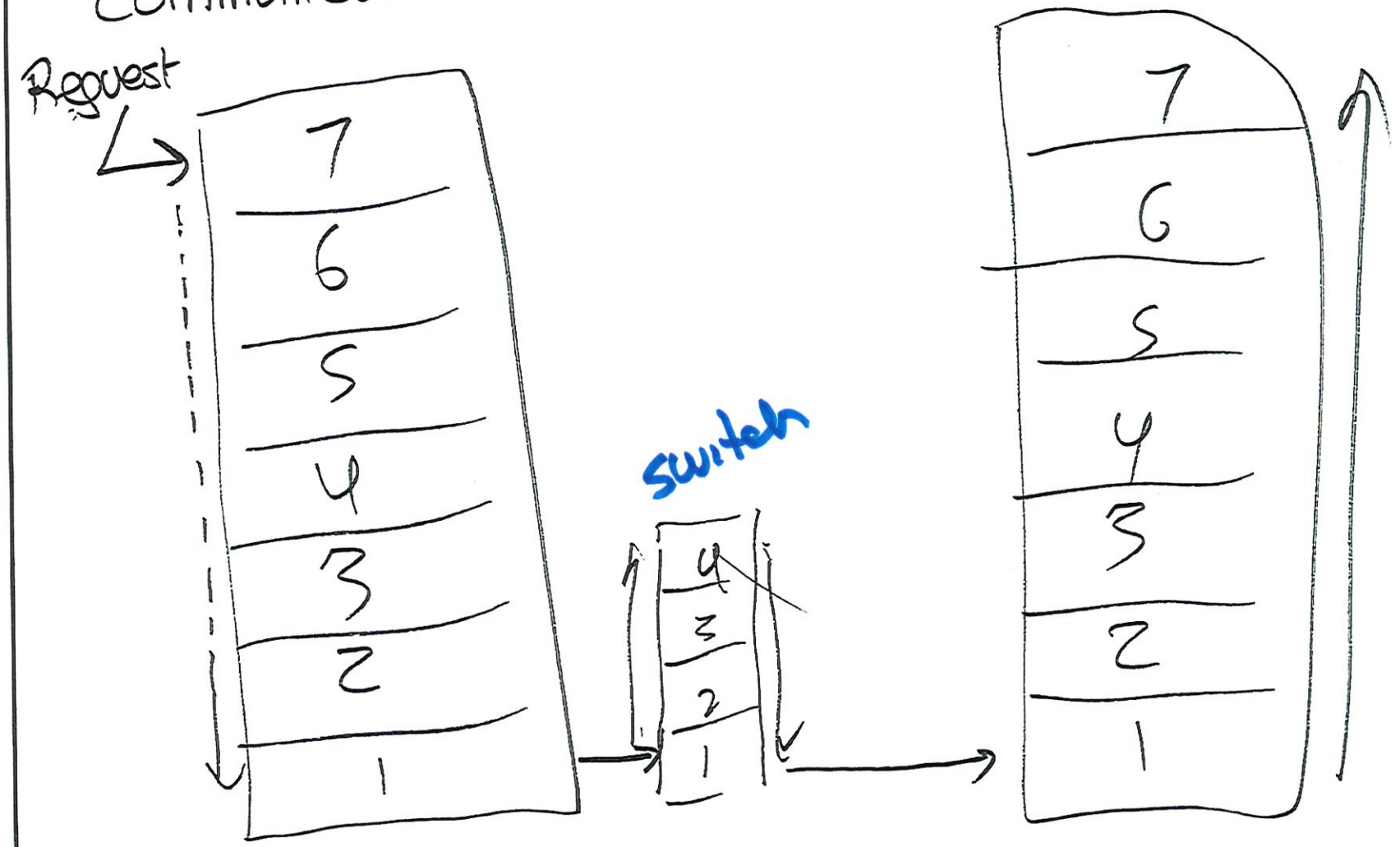
University of Idaho

ECE 444 / ECE 544 / CS 444 / CS 544 Supervisory Control and Critical Infrastructure Systems

Session 17

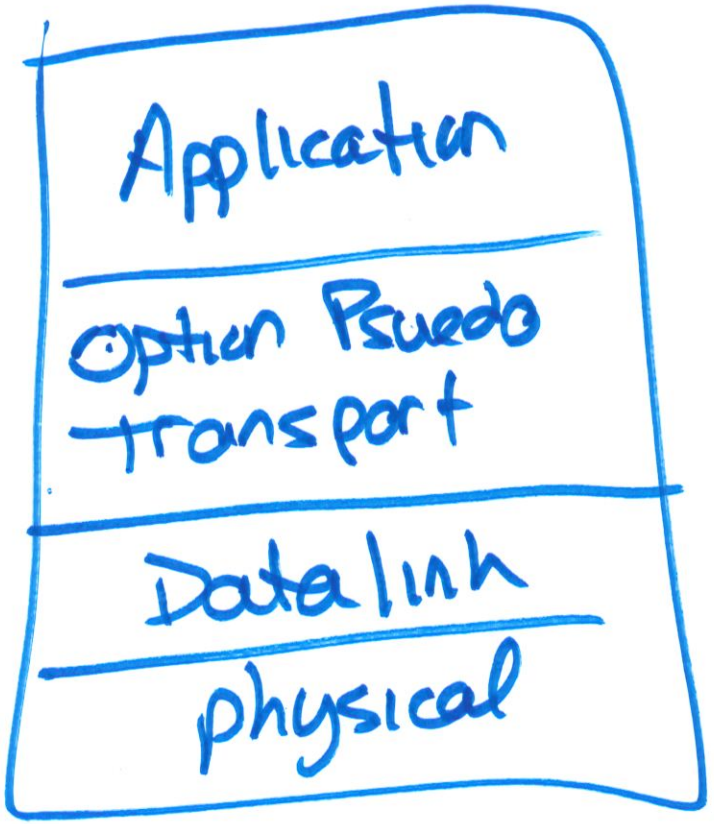
L17 1/n ~~L16 11/14~~

Communication between devices



LH 2/12

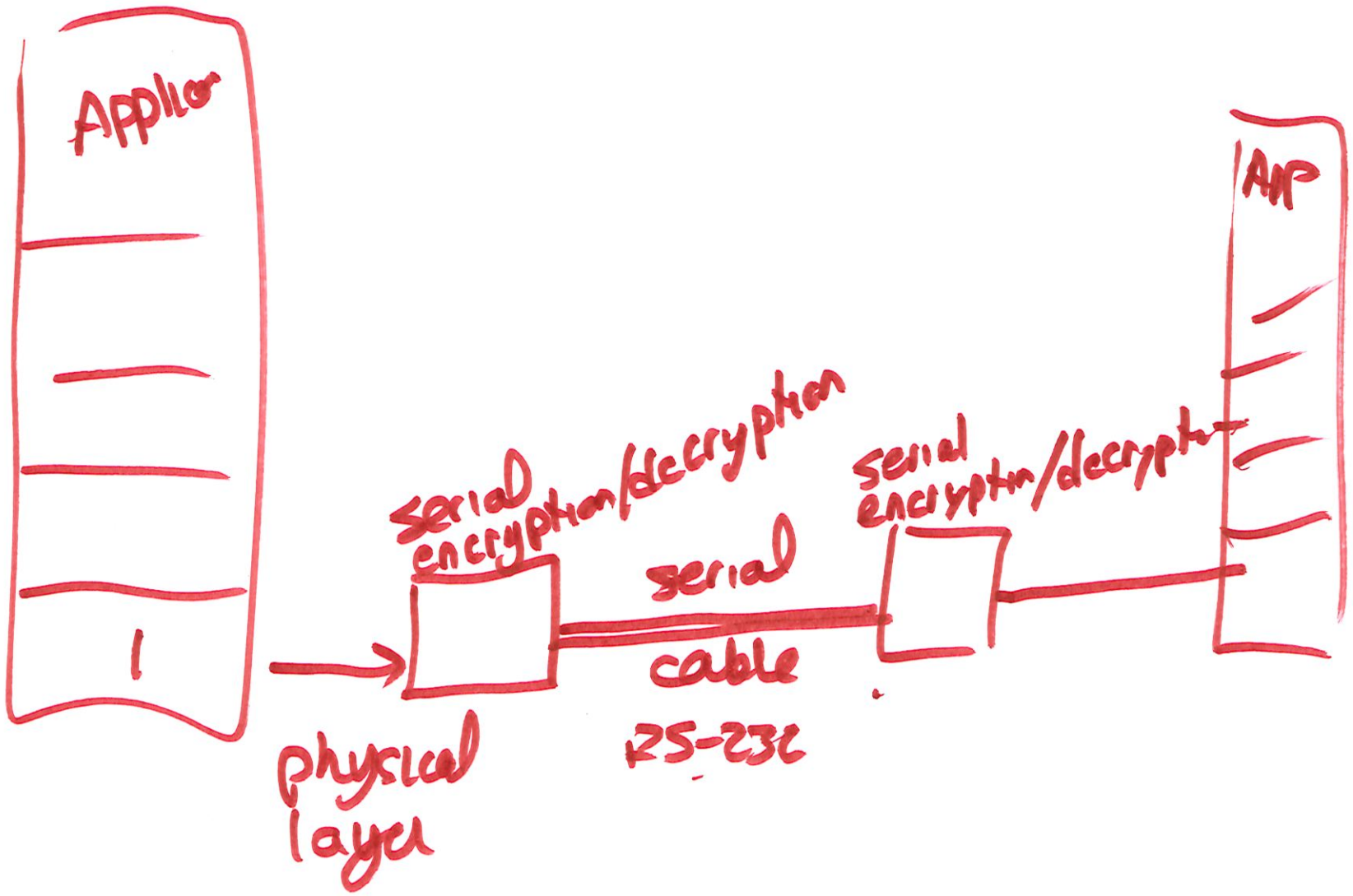
IEC Enhanced Performance Architecture



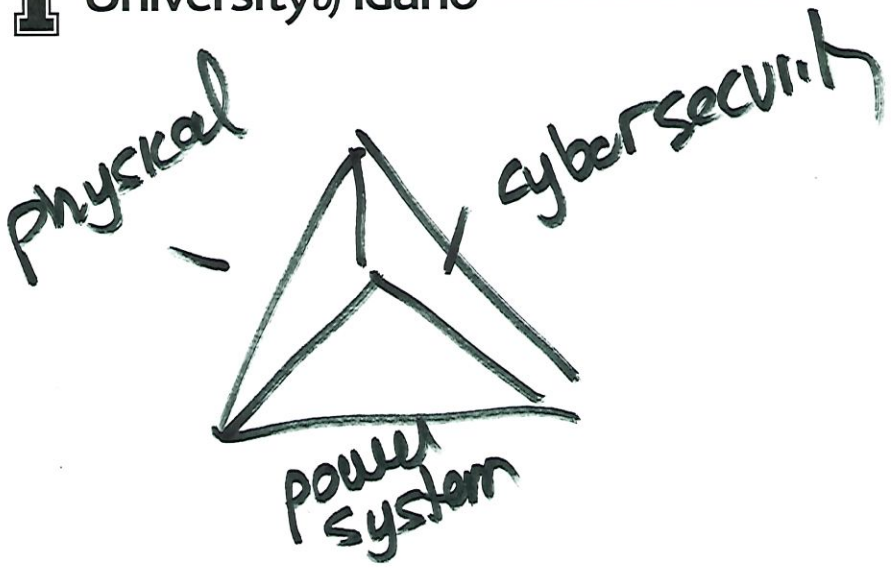
more common with serial data systems using RS-232 or RS-485

- For IEC 61850 use all 7 layers → TCP/IP

L17 3/12


Applic
AP
serial encryption/decryption
serial encryption/decrypt
serial
cable
RS-232
physical layer

L17 4/12



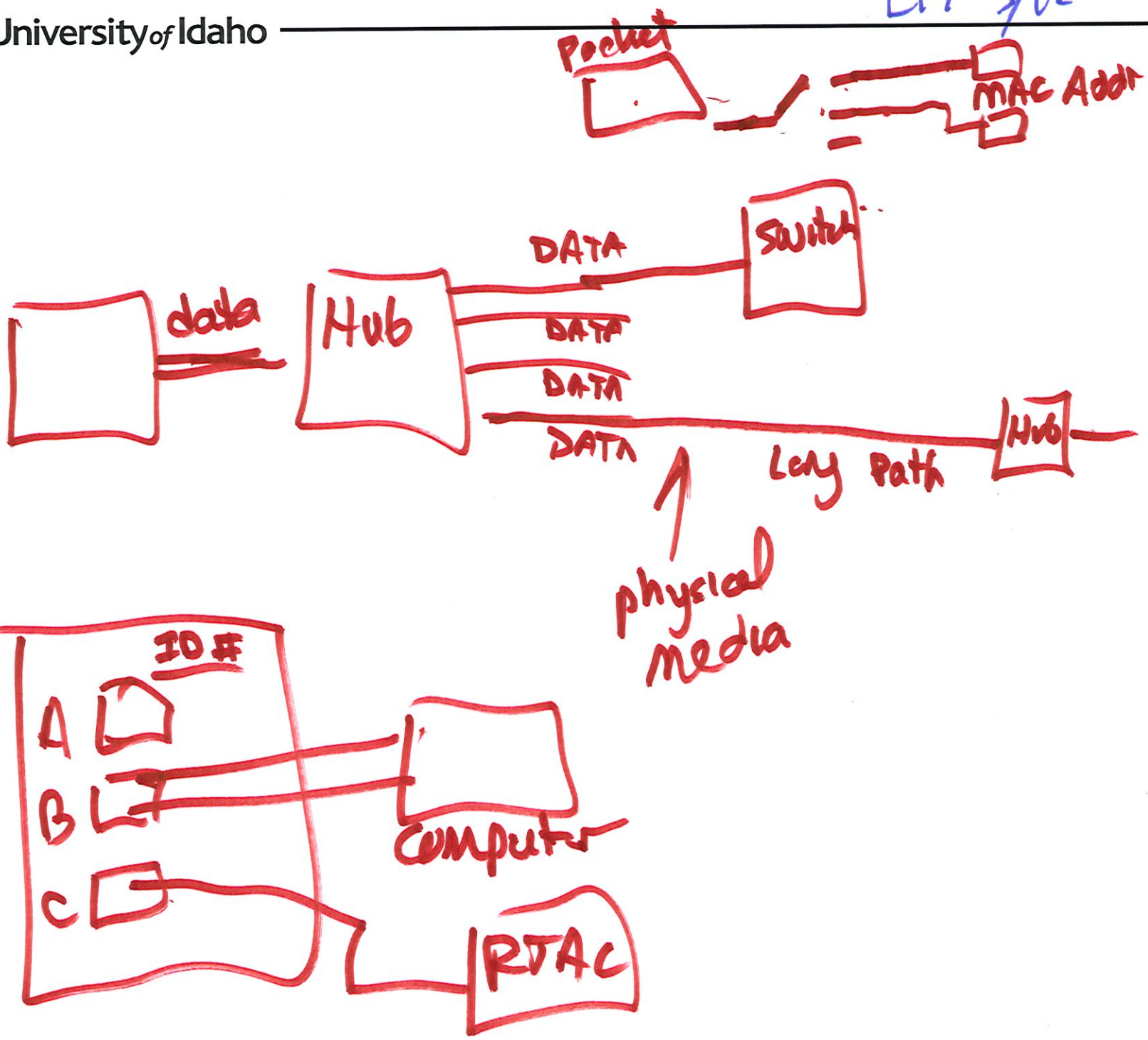
NERC Critical Infrastructure Protection (CIP)

- set of criteria
- audited
- fines

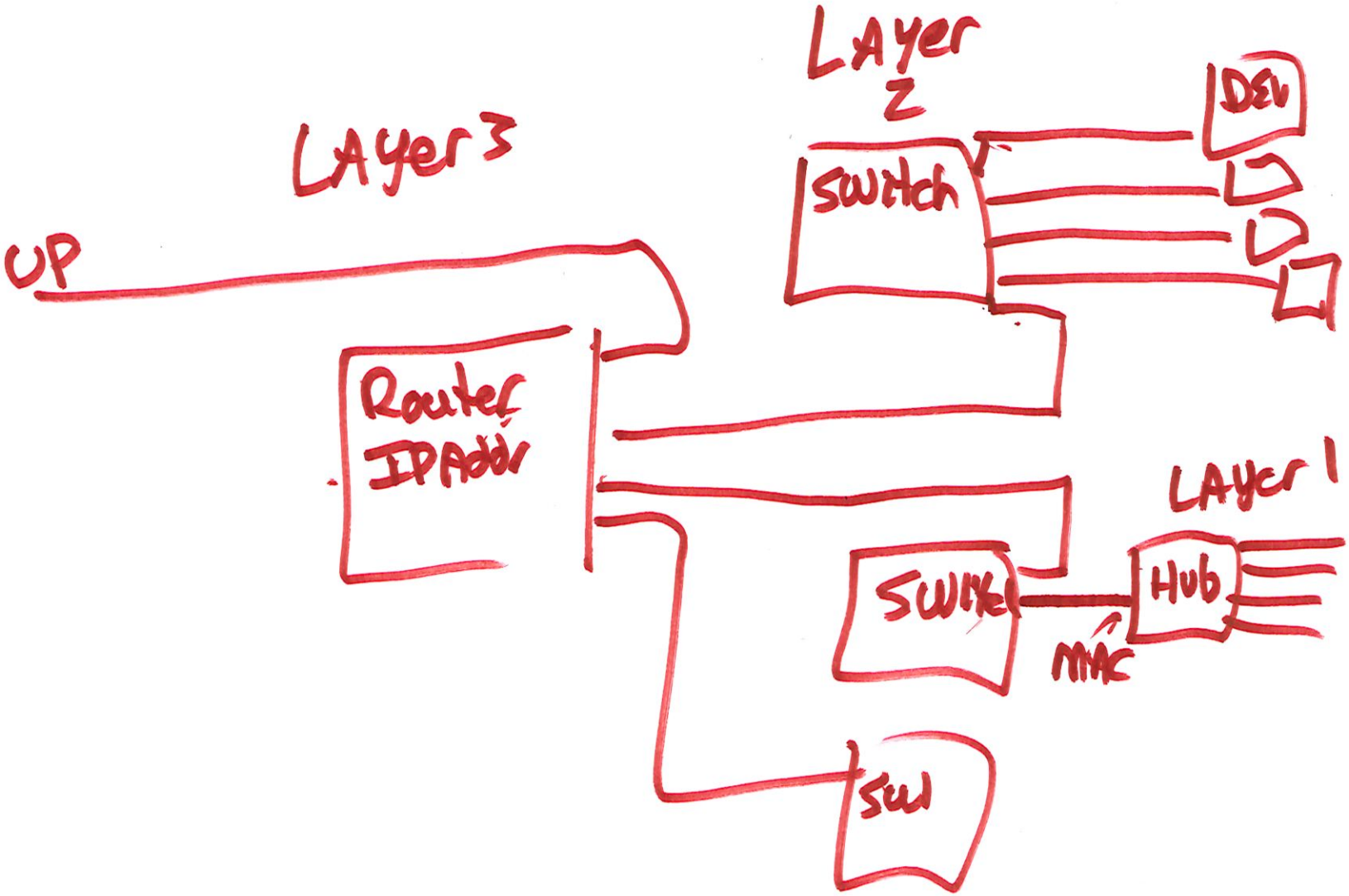
→ Power Industry organization

FERC - Federal Energy Regulatory Commission } stepped in on cybersecurity

L17 S/12


Packet
MAC Addr
DATA
Switch
data
Hub
DATA
DATA
DATA
Hub
Long Path
physical media
IO #
A
B
C
Computer
RTAC

L17 6/12



Network Connectivity Devices

- Hub (repeater hub): hardware device for connecting ethernet devices together
  - Layer 1 device
  - Data received in a port broadcast out all of the other ports
  - Devices depend on identifier in the data packets to choose what to read or respond to
  - Can be used a repeaters
  - For analyzing network traffic, protocol analyzers can be connected to a port on a hub as an alternative to a network tap, span port or port mirror

Network Connectivity Devices

- Network Switch (switching hub, bridging hub, IEEE MAC bridge)
  - Layer 2 (data link layer) device
    - Uses Media Access Control (MAC) addresses to forward data
    - Layer 2 bridging
    - Data is transmitted only out the port that is addressed
  - Trend for switches to include routing capabilities
    - Adds Layer 3 (network layer capabilities)
    - Might be referred to as layer 3 switches (multilayer switches)
  - Network segmentation to reduce collision domains
  - Can enable/disable ports
  - MAC filtering and other access control

Network Connectivity Devices

- Router: a networking device that forwards data packets between internetwork protocol-based networks
  - Network layer (layer 3)
  - Reads address in header
  - Routing table to direct packets to the right network
  - Modern routers may include firewall or VPN
    - Blurring with switches

Network Connectivity Devices

- Modem (modulator/demodulator)
- Used to convert between analog format (telephone, radio for example) and digital format
  - Transmits by modulating carrier wave signal to encode digital data in an analog transmission format
  - Receives by demodulating the analog carrier wave
- Early systems had audible sounds on phone lines
- Frequency raised to increase speed/performance

L17 9/12

Types of Switches

- Unmanaged switches
  - No configuration, essentially plug and play
- Managed switches
  - Configuration Interface
    - Serial console, telnet, secure shell
    - Simple network management protocol (SNMP) agent
    - Web interface, etc.
  - Features available with switches
    - Reconfiguration protocols
    - Port mirror
    - Port configuration
    - Packet filtering
    - Creating VLAN (virtual local area networks)

Types of Switches

- Enterprise managed switches
  - Additional features • Layer 3
- Software Defined Network (SDN) switches
  - Start out no paths defined
  - To configure the switch, one defines functional paths
  - This is opposite of a managed or unmanaged switch where path functions are largely on by default and then limited through configuration

L17 10/12

Network Performance Measures

For ICS reliability is important
- especially ones that impact safety

Power system
→ Performance of power system is the goal

⇒ ICS is a means to that goal

⇒ cost center, not a revenue generator

- communication network is fairly sparse
  - → not a lot of redundancy in connectivity
    - → either inside a substation
    - → or between stations and control centers
    - - often more redundancy in power network itself

L17 12/12

To Improve Reliability:

→ Physical design
- more switches (etc.)
- more paths (physical media)
- Backup structures
(Backup power for communication equipment)

- Logical design

Measures of reliability
→ evaluate designs