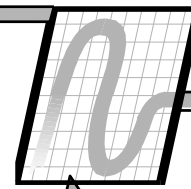


Fundamentals of DDC



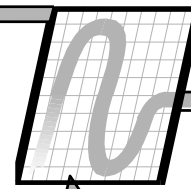
Some IT Considerations

Acronyms



- IP – Internet Protocol: the **key** Internet technology
- TCP – Transmission Control Protocol
- UDP – User Datagram Protocol
- HTTP – HyperText Transport Protocol
- HTML – HyperText Markup Language
- XML – eXtensible Markup Language
- SOAP – Simple Object Access Protocol
- DHCP – Dynamic Host Configuration Protocol
- DNS – Domain Name Service
- NTP – Network Time Protocol
- SMTP – Simple Mail Transport Protocol
- SNMP – Simple Network Management Protocol
- PEBCAK – Problem Exists Between Chair And Keyboard
- ID-Ten-T.....

Data Packets



- Packet is chunk of data with additional information
- Header
 - Source Address
 - Destination Address
 - Size of data packet
 - Encryption information
 - Sequence or ID Number
 - Priority
- The actual data, sometimes called the “payload”
- Different protocols have different packet definitions

IP vs Ethernet vs Media



- IP is an addressing scheme (e.g. “192.168.1.23”)
- **Many** different protocols run on IP
- Doesn't depend on the wire
- Runs on **many** media types
 - **Ethernet**, ATM, SONNET, PPP, VPN, WiFi, WiMax, etc.
- Ethernet is a collection of wire and media types
- Includes it's own addressing
 - MAC address (of your desktop Ethernet card.... Not the same as WiFi MAC address – WiFi has it's own MAC addressing)
- Covers multiple media types
 - Cat 5 / Cat 6, Fiber Optic, etc.
- We often equate IP == Ethernet... but they're not the same

Ethernet architecture

Ethernet LAN

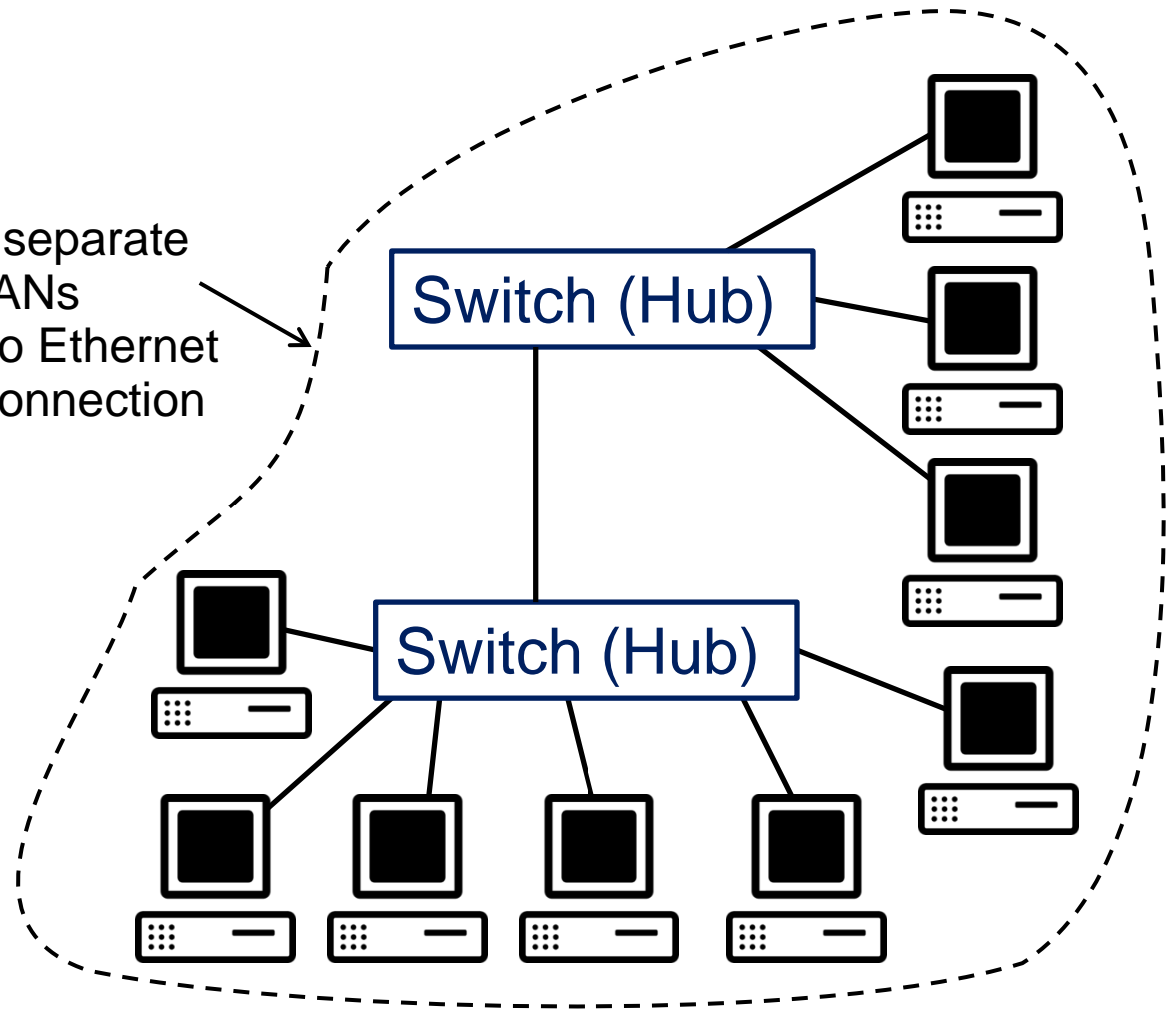
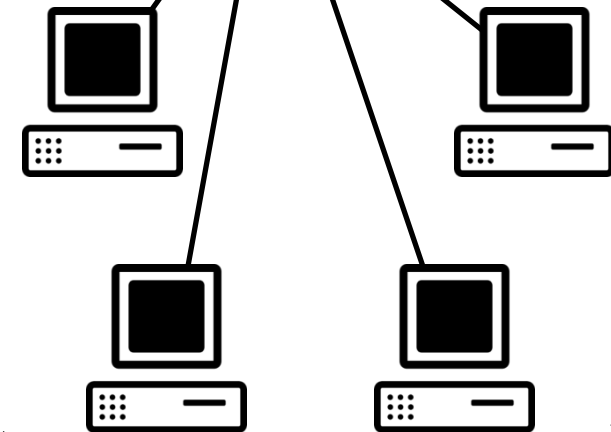
Ethernet LAN

2 separate
LANs
No Ethernet
Connection

Switch (Hub)

Switch (Hub)

Switch (Hub)



Virtual LAN (VLAN)

Still no connection between the 2 VLANs
Switch is configured in software to be 2 switches

Ethernet VLAN

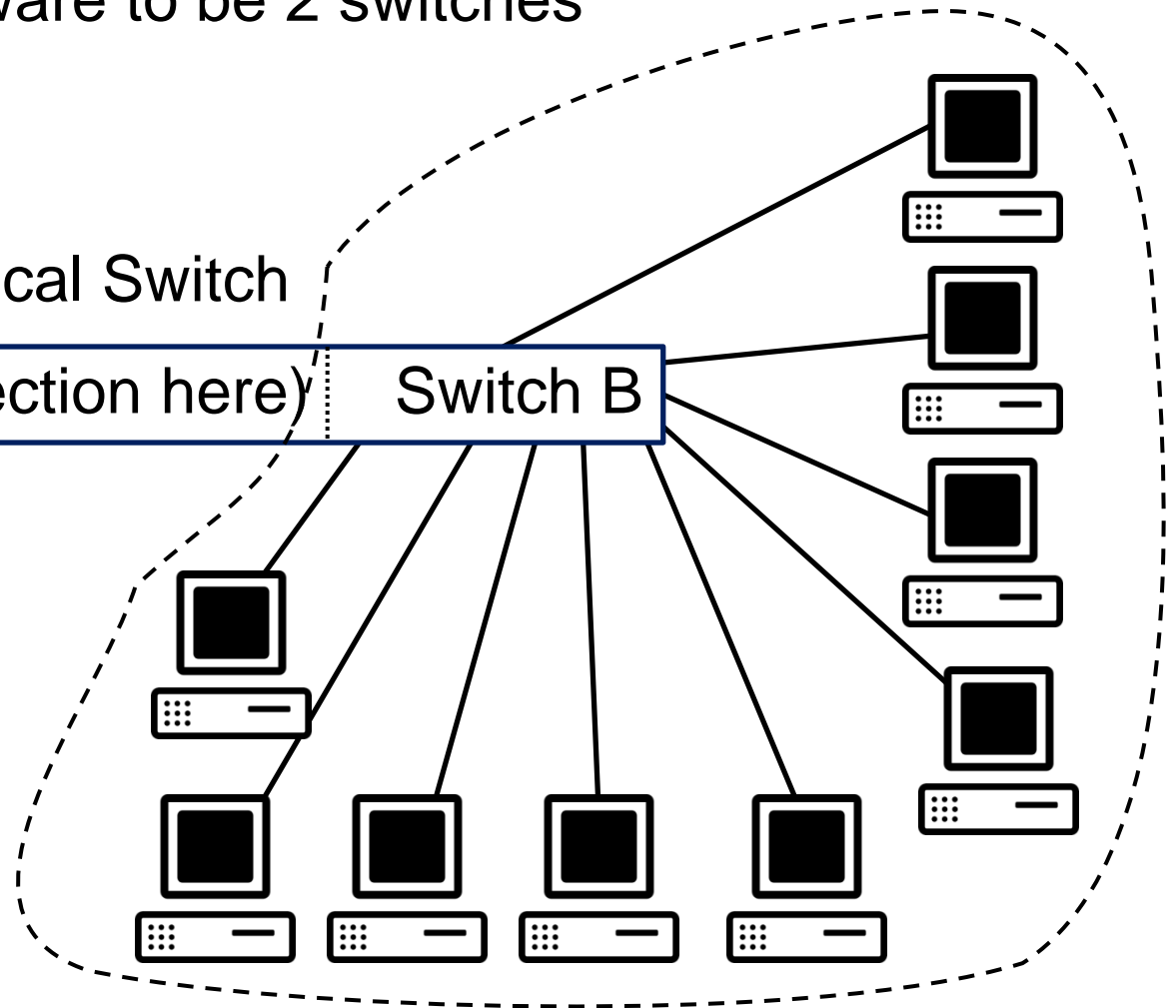
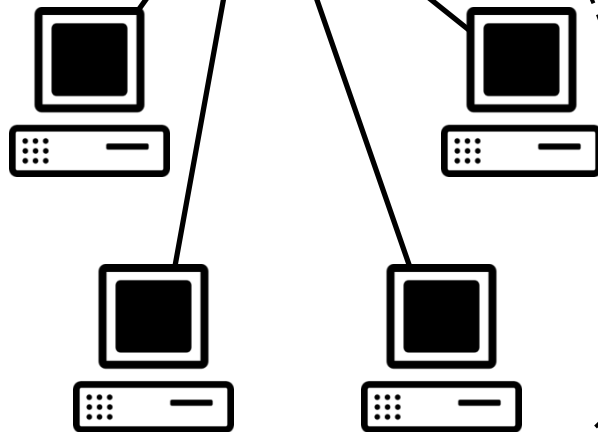
Ethernet VLAN

One Physical Switch

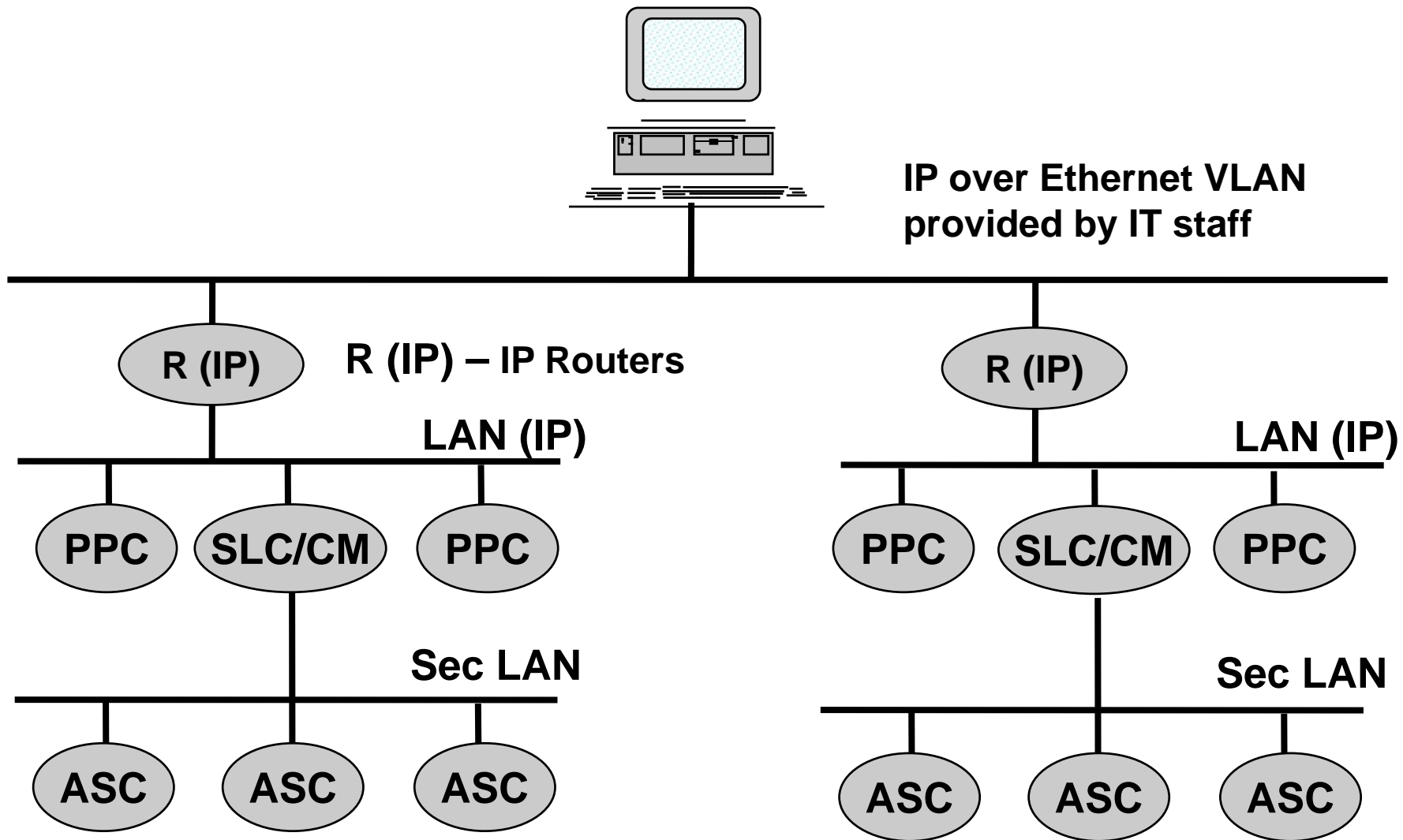
Switch A

(no connection here)

Switch B

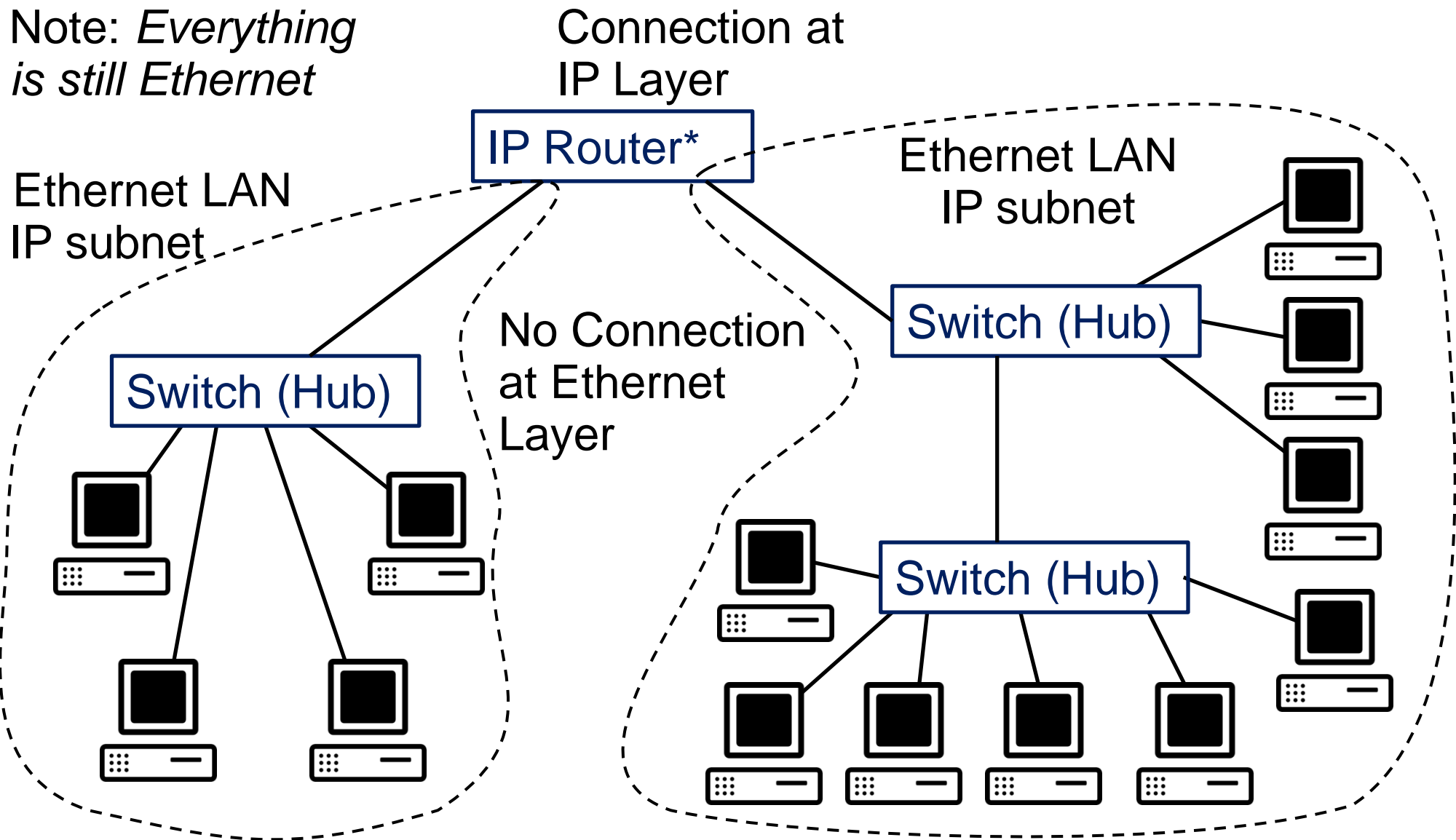


Typical Campus BAS

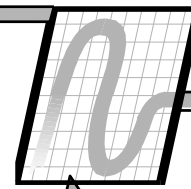


IP / Ethernet architecture

Note: *Everything is still Ethernet*



Protocol Stack



- Break a process down into simple steps
 - Example: mailing something

Application – send a birthday party invitation to a friend

Write it: letter, Christmas card, invitation, ...

Put in envelope: letter, photo, bill to pay....

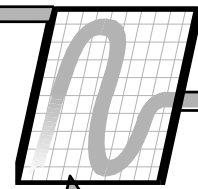
Address it: letter, package,

Mail it: USPS, UPS, FedEx



To network for delivery

Protocol Stack



Getting something in the mail

Application – act on the invitation

Read it: letter, Christmas card, invitation, ...

Open it: envelope or package

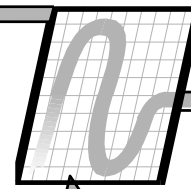
Check address: to me?

Deliver it: to my address

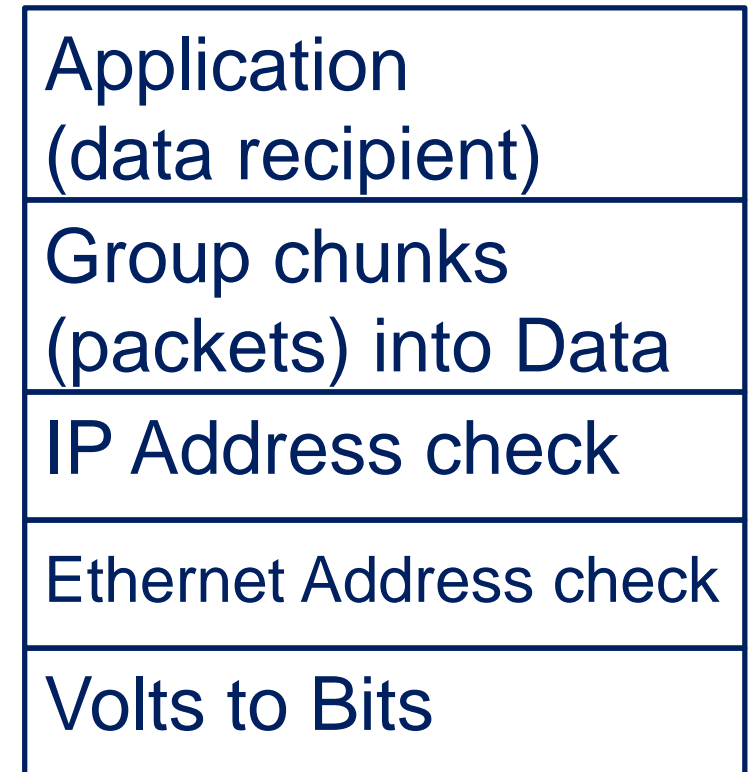
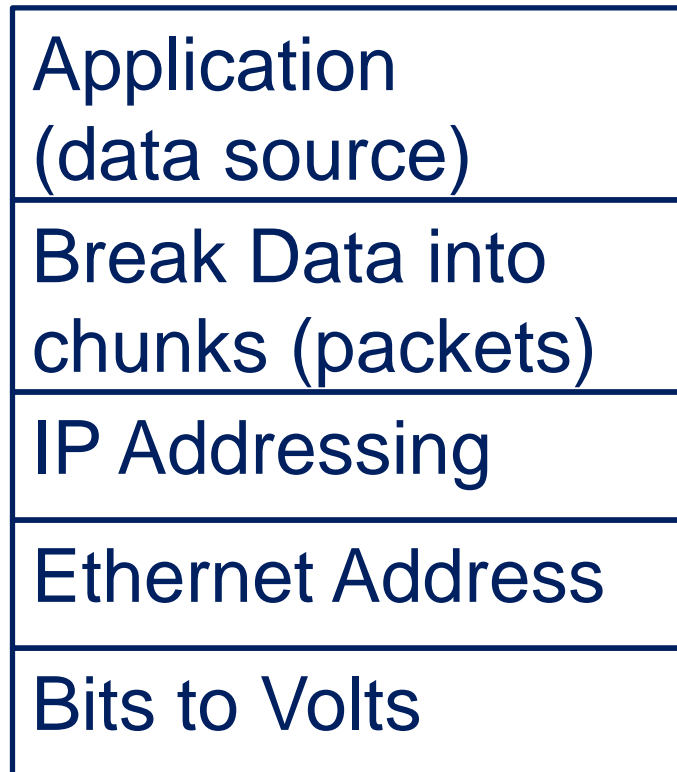


From network

Protocol Stack

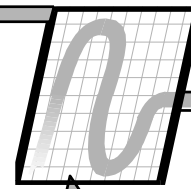


Sending BAS data over the network



Voltage signals over the wire

Protocol Stack



- Each layer provides an interface to the layer above it
 - IP to Application: “Here’s how to send data using IP”
- Each layer uses the interface of the layer below it
 - IP to Ethernet: “Hey Ethernet, send this data to that Ethernet address”
- Each layer performs a specific function
- No layer knows the details about what is above or below it
 - Layers above IP look down and just see “a network”
 - IP layer handles data packets provided by layers above -- has no idea what the **content** is

Envelopes inside Envelopes



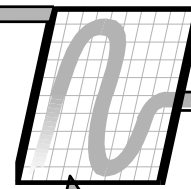
Ethernet packet: For MAC 00:F1:23:00:23:23:01:4D

IP Layer: IP packet: For 192.168.1.5

Application Header:
For PI loop, AHU-15

Data:
SA-T = 65

More Envelopes



Ethernet packet: For MAC 00:F7:44:DB:08:79:4D:12

IP Layer: IP packet: For 243.21.8.234

To IP Layer: "I'm just an Application

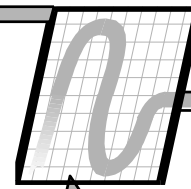
Tunnel IP Layer: VPN packet

To Application: "I'm the IP Layer"

Application Header:
For PI loop, AHU-15

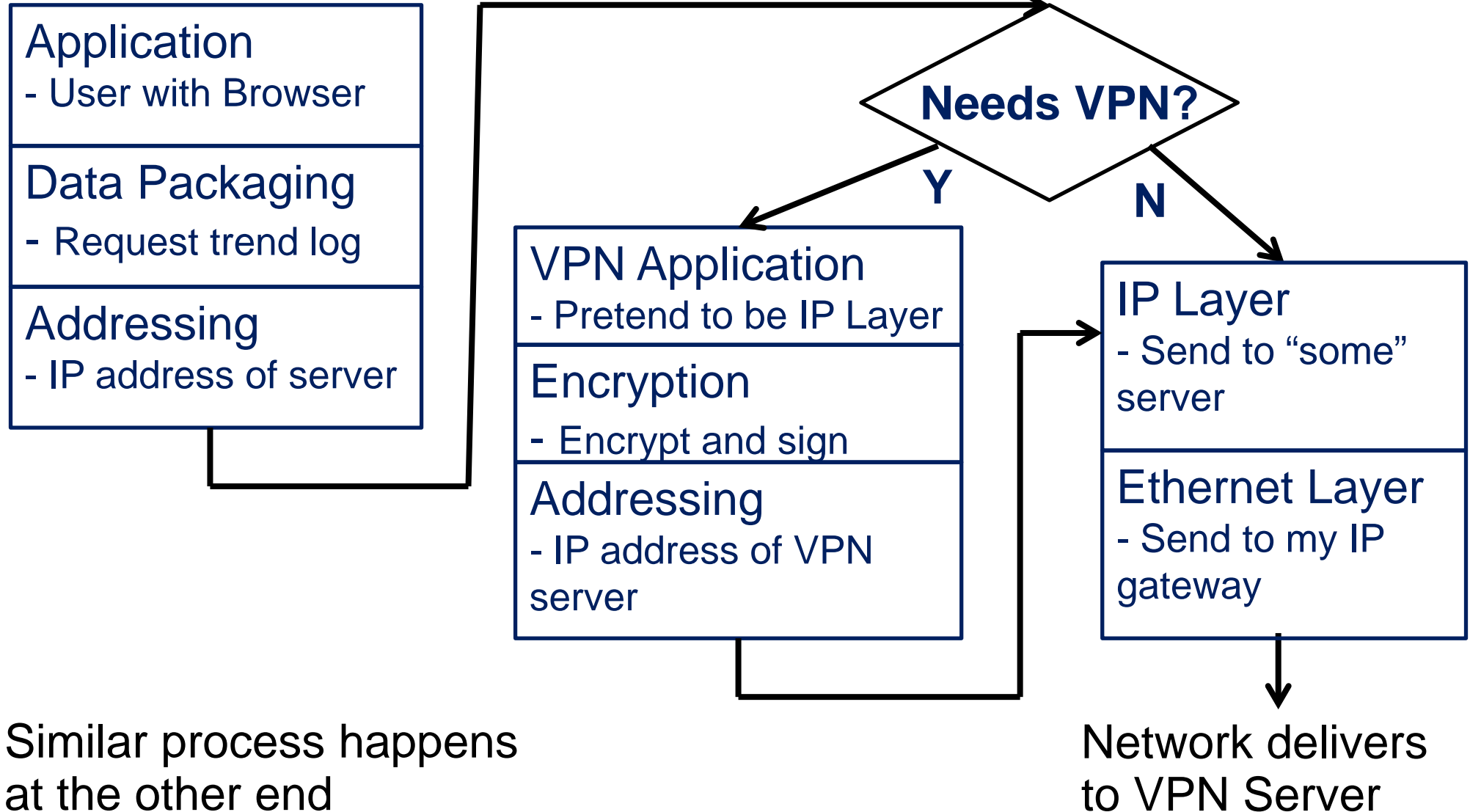
Data:
SA-T = 65

So What?



- Applications that ***can't*** run on the Internet
 - Some applications, for technical reasons, won't work over the Internet
 - This “Tunnel Layer” hides the Internet from the Application, so it can run
- Applications that ***shouldn't*** run on the Internet
 - Insecure ones
 - Maybe ***YOUR*** BAS with Admin Password = “Admin”
 - This “Tunnel Layer” can provide encryption and security.

Browse BAS via VPN

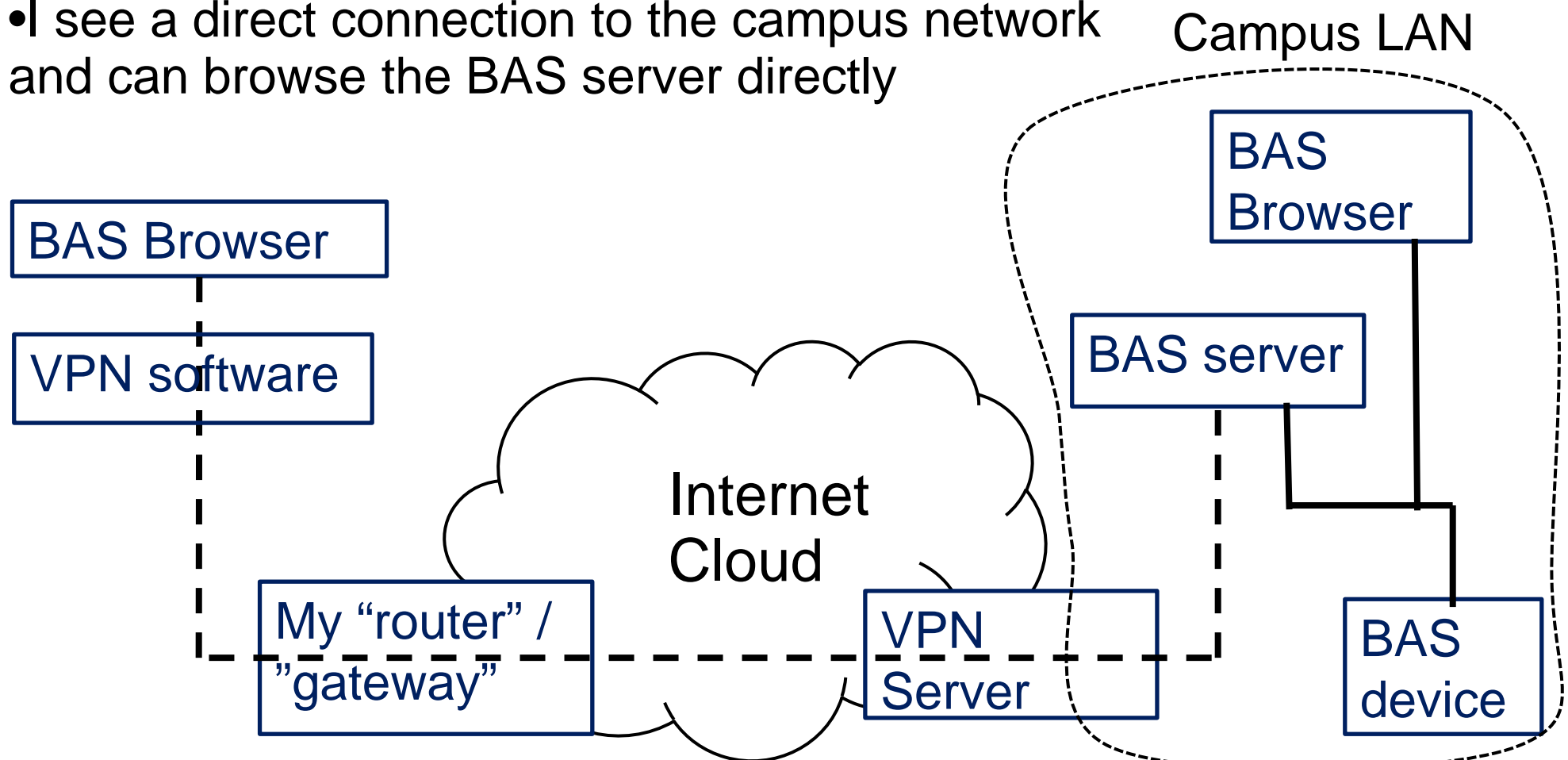


Similar process happens
at the other end

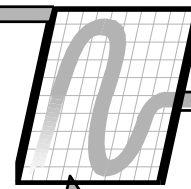
Network delivers
to VPN Server

VPN via Tunneling

- The VPN client and VPN server hide the Internet
- Dashed line looks like a direct wired connection
- I see a direct connection to the campus network and can browse the BAS server directly

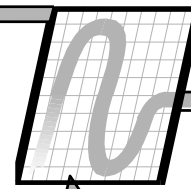


BAS to IT Dictionary



- Router vs. IP Router
 - (General) Performs sorting (filtering) based on address
 - Post office mail sorter is a router
 - Ethernet Switch is really a router
 - (IT) “All routers are IP routers”
- Servers and Desktop machines
 - (BAS) Our front end machine is a Server
 - (IT) A Server machine has specific hardware / software
 - Our “Server” may run on their “Desktop” PC

BAS to IT Dictionary



- Gateway vs. Gateway
 - (BAS) protocol translator (e.g. Lon –to- BACnet)
 - (IT) Router in the architecture
 - The Router that connects your PC to other networks
- Application vs. System
 - (BAS) We have a Building Automation **System**
 - (IT) Your “system” is an Application on our Network
- IP vs. Serial Protocol
 - (BAS) Lon over TP/FT-10, BACnet over MS/TP, etc.
 - (IT) If it’s not IP.... it is a “serial” protocol

Other areas of confusion



- Product Lifecycle
 - IT Equipment often purchased with service contract
 - IT Equipment is obsolete in 3 – 5 years
 - “Patch by replacement”
 - BAS systems have 20+ year lifetimes
 - Most of our systems can’t be patched and can’t be replaced
- Sole Source is the Rule: Microsoft, Cisco, Dell/HP/Lenovo
- Virtual World vs. Real World
 - A hacker can do “anything” with your IT data
 - A hacker can’t blow up your boiler (actual concern from IT)
 - SCADA systems may have real dangers, HVAC generally doesn’t

Areas of concern to IT staff



- Old systems that can't be patched
 - Isolate in stand-alone mode whenever possible
- Connections to critical systems
 - Design with limited access / remote functionality
- Remote Access
 - Talk to IT about how to secure this
 - Be careful with using WiFi without talking to IT
 - Do **NOT** install commercial cable modem / DSL
- Default passwords & Vendor back-doors
 - Make sure they are changed / closed

Conclusion



- The World is moving towards IT
- HVAC is moving towards IT
 - Controllers on IP
 - Web-based front ends
 - Access from home via VPN and browser
 - Enterprise systems
- Get your IT staff involved up front!
 - Anticipate problems
 - Learn to speak their language