System Architecture

Block Objective

- Describe the key application and data processing functions of a DDC system.
- Identify the key physical components that make up a DDC system.
- Describe the WAN/LAN structure for building a DDC system.
- Describe the enterprise level system for operator interaction with a DDC system.
- Mention some considerations for security

Basic DDC Functions

- Process Control
- Supervisory Logic Control
- Time Based Control
- Dynamic Data Reporting
- Alarm Handling
- Operator Access to Application Parameters
- Data Collection and Reporting

Process Control

- Process Control: Measuring process variables, executing logic and issuing commands to end devices.
  - Measuring the Supply Air Duct Static Pressure
  - Executing a Control Loop
  - Issuing a command to the Supply Fan VFD
- ***This is the essence of control and has to work!***
  - Make sure your vendor understands HVAC!
  - Some – with IT backgrounds – do NOT!

Supervisory Logic Control

- Supervisory Logic Control: Gathering data from process control loops, executing logic and issuing instructions to one or more process control loops.
  - Get damper positions from VAV controllers
  - Select the highest value.
  - Calculate a discharge air static pressure set point that will drive the highest damper position value to 90%.
  - Send the new static pressure set point to the air handling unit control device to adjust its process control loop.

Time Based Control

- Time based control is fundamental to DDC systems.
- At some location within a DDC system we must keep track of the time, compare the time to a specific schedule and execute occupied/unoccupied or start/stop commands per the schedule.
- We also need the flexibility to allow our system operators to quickly change time schedules for efficient system operation.

Dynamic Data Reporting

- The presentation of both fixed and variable data from the applications to the operator.
- Operators need to see the values of the sensors and the commands sent to the end devices.
- Operators need to see the values of the application parameters that are adjustable.
  - Set Points (often!)
  - Tuning parameters
  - Calibration offsets (maybe not so often)
  - Reset schedule parameters

Alarm Handling

- With DDC systems we can be alerted when system performance is not normal.
- Within our hardware device logic we can create binary indicators of an alarm condition.
  - When the mixed air temperature falls below 42F, assign a value of 1 to a variable called the Mixed Air Low Limit Alarm.
- When an alarm indicator transitions from a value of 0 to a value of 1, we want the system to transmit an informative message to the system operators.

Operator Adjustable Parameters

- Within the applications there may be a number of parameters that may need to be changed over time to achieve optimum control.
- Parameters can be hard coded within the applications. In order to change the value, the program must be opened, the value changed, the program compiled and then downloaded…not very flexible.
- Parameters can be “exposed” to the GUI such that the operator can make a simple change to the value without touching the application file.

Data Collection and Storage

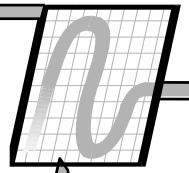
- DDC systems give us the ability to collect data about system performance over time.
- This data is extremely valuable to system operators and management.
- This data is referred to a trend log data and it can be stored at the hardware level, at the IP / front end level (computer) of a DDC system or in both places.
  - Historical data collection
  - Temporary performance data collection

Interim Summary

- Key performance elements of a DDC system are:
  - Process Control
  - Supervisory Logic Control
  - Time Based Control
  - Dynamic Data Reporting
  - Alarm Generation and Message Transmission
  - Application Parameter Adjustability
  - Data collection, Storage and Presentation
- As we study the different components that make up a DDC system, we will identify where each of these key elements are accomplished.

Process Controllers

Process Controller



- A process controller is an electronic device to which we connect sensors and actuators.
- It has the ability to execute control logic in accordance with a sequence of control.
- A typical process controller will have multiple physical inputs (analog and binary) and multiple physical outputs (analog and binary).
- With multiple I/O, multiple process control loops can be executed by a single process controller.

Process Controller-Data Flow

- A process controller can exchange data with other devices on the network.
  - A controller has an outdoor air temperature (OA-T) sensor. OA-T is broadcast on the network for use by other process controllers.
- A process controller can exchange data with User Interfaces (UI), either networked or local
  - All inputs and outputs
  - Internal calculated values
  - Set point or manual start/stop commands
  - Calibration and tuning parameters

Process Controller-Time

- A process controller may or may not have embedded time schedules.
  - If they do, the system operator should have the ability to change the schedule parameters.
  - If they do not, they must receive the time based start stop command from another device over the network.
  - May need to adjust start/stop – e.g. optimum start/stop

Process Controllers-Dynamic Data

- The values of the measured variables and the logical commands to the end devices are published to the network for presentation to the GUI.
- The same can be said for the values of internal points and application parameters.
- What gets published and how is critical when multiple vendors are involved
- Are points read-only, or are they writeable?
    - How?

Process Controller-Alarms

- Application logic within a process controller can easily create binary indicator of alarm conditions.
- A process controller may or may not have the ability to assign a message to an alarm indicator and forward that message to the system operator.
- If the ability to send a message exists, great.
- If the ability to send a message does not exist, another device must monitor the binary indicator and assign and forward the message

Process Controller-Trend Data

- A process controller may or may not have the ability to locally store trend data for periodic uploading to a computer.
  - If they do, the data will be sent to the computer in batches (e.g. upload when the local storage is 80% full)
  - If they do not, the data may be sent over the network to another device for trending or all trending may be accomplished by a computer that is polling the controller for the data (not desirable).

Process Controllers-Operator Control

- Specific application parameters shall be published to the network such that the operator shall be able to modify the value from time to time without interrupting the control processes and without downloading a new file.

Process Controllers

- Key characterizations of process controllers are:
  - Application specific versus programmable
  - Primary versus secondary
  - Peer to peer versus managed communication support

Application Specific Controllers

- The application is installed in the device at the factory.
- There are a number of application configuration parameters that must be set by the engineer to create the specific application desired.
  - Does the VAV unit have a fan? Series or parallel?
  - What is the cooling set point? Heating set point?
- Sometimes these controllers are referred to as “configurable” versus “programmable”

Programmable Controllers

- The controller is shipped “empty”
- The engineer will use a Programming Tool to create and download a application to the controller.
- There is no universal programming tool. Each vendor creates their own tool.
  - One of the liabilities of operating a multi-vendor system is the requirement to master multiple programming tools.
  - Open protocols does not change this issue!
  - There are work-arounds, but they have a cost

Application Programming Tools

- Two types of application programming software tools dominate the industry.
- Line programming tools
  - Very flexible
  - Somewhat difficult to master
  - Typically do not include simulation capabilities
- Graphical programming tools
  - Much easier to master
  - May include off-line simulation capabilities

Controller Types

- Different DDC controllers are designed for different purposes.
- Some controllers are designed for more robust applications while others are intended for simple unitary applications.
- For our purposes we will characterize DDC controllers as “Primary” or “Secondary”.

Primary Controllers

- Programmable
- Full software compliment/features/built-in functions
- Large point capacity
- High resolution Analog Inputs
- Lots of memory and CPU power
- Real Time Clock
- Buffer for Alarms and Trends
- Peer-to-Peer Communication
- Suitable for Process Control or Supervisory Logic Control

Secondary Controllers

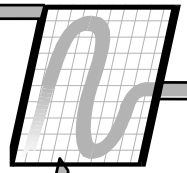
- Process Control Only
  - Typical application is terminal equipment or small central station equipment
  - Time based control typically not included
  - Limited software compliment
  - Smaller total point count
  - Typically application specific but may be programmable
  - Typically lower analog to digital converter resolution
  - Trend data not typically stored at this level
  - May be polling (not peer-to-peer communication)

Application of Controllers

- A good installation will use controllers for their designed purpose.
- Central Station Equipment
  - Primary Controllers
- Small AHUs
  - Primary or Secondary Controllers
- Unitary Equipment – VAV, HPs, Fan Coils, Portal Controllers in Security systems
  - Secondary Controllers

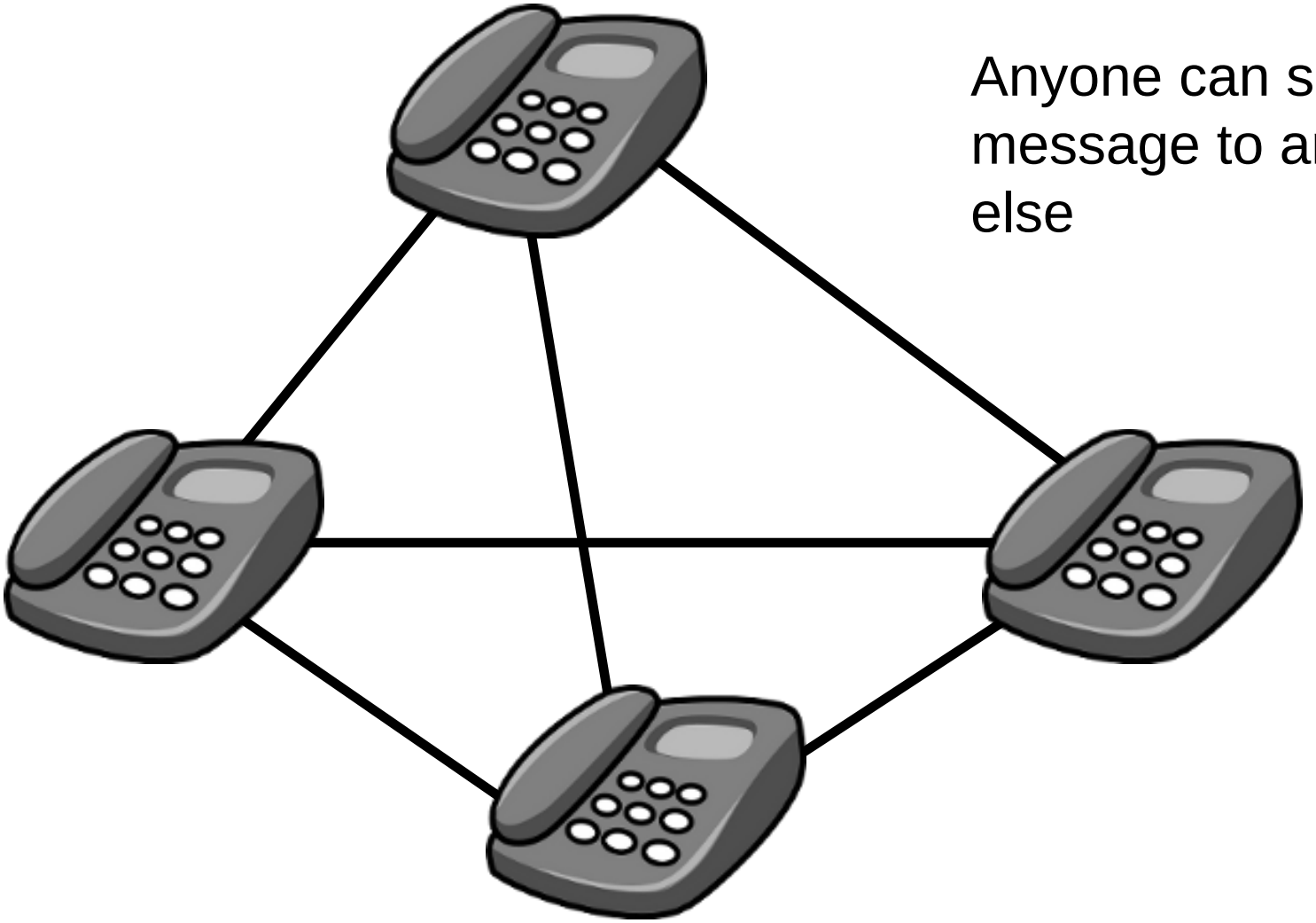
Communications and Networking

Communication Concepts



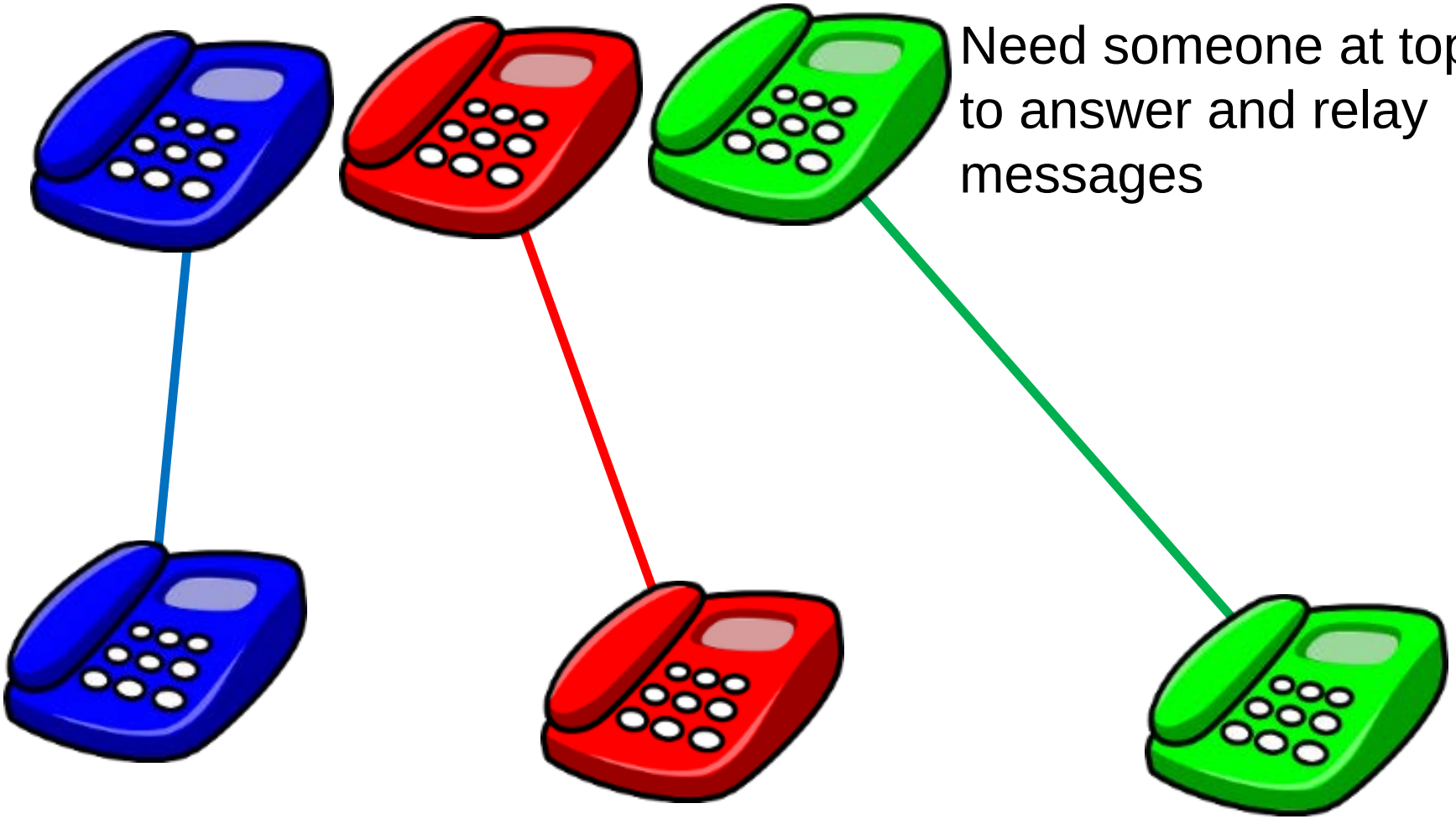
- Communication between devices on a network can be characterized as peer to peer or managed.
  - With peer to peer communication all devices are considered equal and any device can communicate directly with any other device.
  - With managed communication, there is a communication manager that sends and receives data to and from a collection of devices. The devices can only communicate with the manager. As a result, to get data from one device to a second device the data must go from the first device to the manager and then out to the second device.
  - Will get confusing when we talk BACnet!

Peer-to-Peer Communication



Anyone can send a message to anyone else

Managed Communication



Need someone at top to answer and relay messages

Communication Concepts

- In addition to peer to peer versus managed communication we also need to discuss event driven versus polled communication.
- Event Driven Communication: The sending devices determines when the data is sent
    - Only send it when there's a change
    - Often called “COV” (Change Of Value)
- Polled Communication: The receiving device asks the sending device for the data.

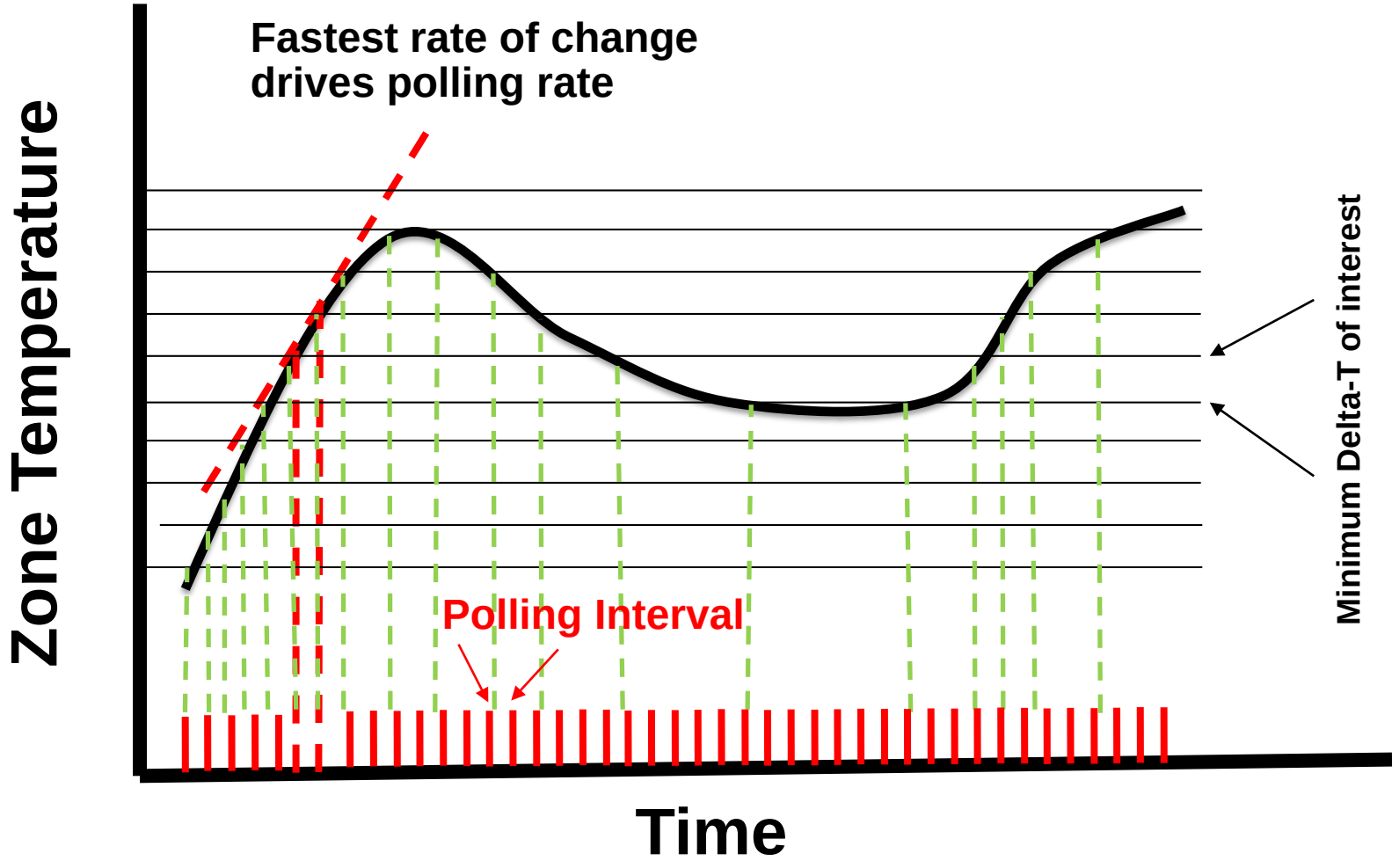
Event Driven Communication

- Initiated by device originating data, the transmitter
- There are important communication parameters in any controller that control event driven communication.
- Send on Delta: Send if the variable changes by this amount or more.
- Minimum Send Time: Send at most this often.
- Maximum Send Time: Send at least this often.
- Efficient use of network bandwidth.

Polling Communication

- The receiving controller will periodically send a request to the sending controller for the latest value associated with a particular variable.
- A polling rate must be set.
- Polling based communication is not a good steward of bandwidth
- Polling may make sense for OWS graphics
    - Receiver only asks for what it needs

Event Driven vs Polling



What's a Protocol

- Is a set of rules that define a method of communication
- The English language is a protocol.
- French is a different protocol.
- The Roman alphabet is a protocol.
- To communicate, devices must use the same protocol.
  - "We use the Roman alphabet"
  - English and French both use the Roman alphabet – but still can't communicate.

Equipment level Gateways

- Packaged equipment comes with its own controls
  - AHUs, Chillers, Boilers
- The equipment is way more important than the protocol used by the packaged controls
- Most DDC vendors have canned gateway applications for common equipment.
- Determining which points and functionality to expose to the DDC system is critical.
- (We'll discuss "Building Level Gateways" later)

The Physical Network

- *You can not spend too much money on the physical aspects of your network*
- Comments from the vendor along the line of, “Oh, we will just use the cable left behind after we rip out the old DDC system” should set off alarm bells in your head.
- A quality physical network is worth its weight in gold when it comes to reliability of data transmission.

Communication Cable

- Twisted pair by far the most common
  - May be shielded (common) or unshielded (Ethernet)
- Fiber Optics often used to connect multiple twisted pair networks in different buildings.
- DDC Vendor's Requirements vary and are important
  - Mutual Capacitance
  - Characteristic Impedance
- Higher LAN speeds accentuate problems
- Some systems are polarity sensitive, others are not

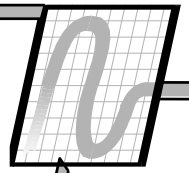
Network Media/Wiring

- At the IP level, it is usually the IT department's responsibility to maintain the network infrastructure. DDC vendors typically connect to an existing IP system.
- The physical aspects of your network are extremely important.
- At the 2nd and 3rd levels, the DDC vendor has prime responsibility for the physical network.

The IP Layer

- Working with a corporate IT department can bring some challenges.
  - They speak a different language
  - Getting permission to get on the network: ***SECURITY***!
  - Proving that the DDC system is not a security risk
  - Being a good IT client: filtering and limiting traffic.
  - Poor quality networks: What is the IP network downtime? Can the DDC system live with the answer?
  - Crossing through firewalls for internet connectivity
    - What ports need to be open?
    - Location of web servers?

The IP Layer

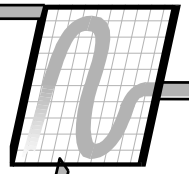


- Availability of ports to connect PCs and routers must be considered.
- If they do not exist, dollars will be required.
- Location of routers and PCs with respect to IT switches must be evaluated. You may need a new “comm closet”.
- Can the vendor provide a network diagnostic tool for measuring bandwidth on the IP layer?
- Project planning must include a member of the IT group. ***Surprises are painful.***

Some Basic Concepts

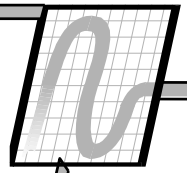
- Daisy Chain wiring
  - Wiring goes from device to device without tees or stubs
  - Most forgiving wiring concept for data communications
  - Probably most common for non-IP networking
- Star topology (e.g. Ethernet)
  - Everything comes back to center hub device
  - Role of hub in managing network?
- Free topology (uncommon)
  - No restrictions. Wire it up however is “easiest”
  - Not recommended – even when it is supported

Some Basic Concepts



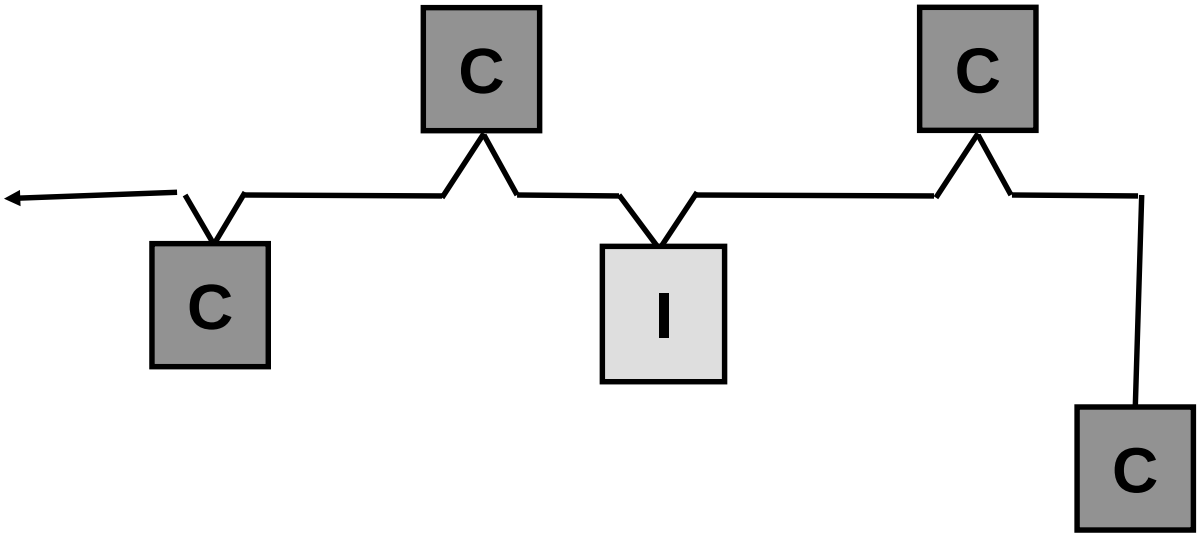
- The use of stubs
  - A stub is a short length of wire to a device off of a tee.
  - Some networks permit them, some don't
  - Typically 10 feet or less
  - Used improperly, stubs can create signal reflections & collisions
- Termination devices or load devices
  - Small devices made up of resistive and capacitive circuitry
  - Installed at specified locations on the LAN.
  - If required consider them mandatory

Some Basic Concepts

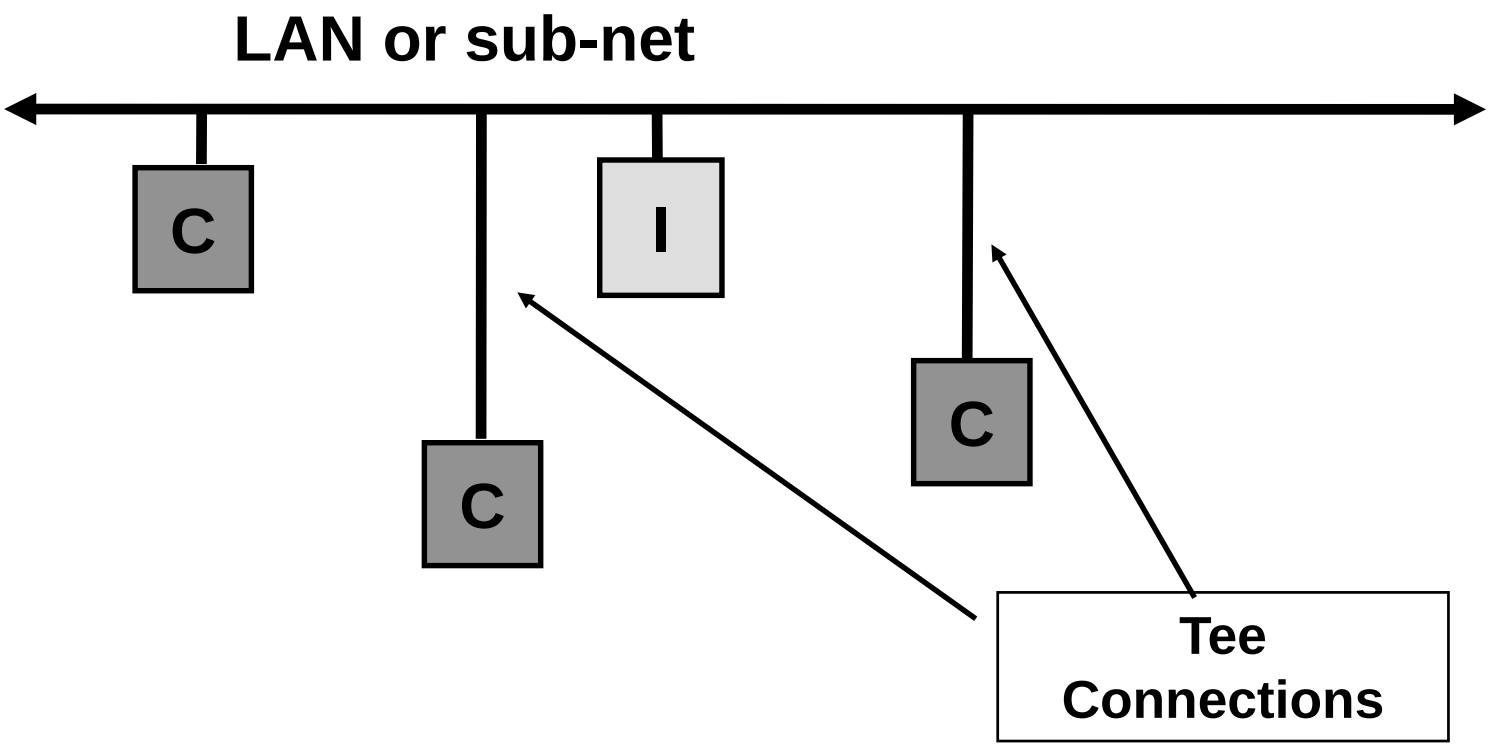


- Surge suppressors
  - Installed when the LAN leaves the building
  - Designed to absorb voltage surges (lightning)
  - May use optical fiber for isolation instead
- Repeaters
  - Physical device
  - Logically transparent
  - Allows for additional length of cable or number of devices
  - Introduce millisecond delays on message transmission
  - Multiple repeaters per LAN not recommended

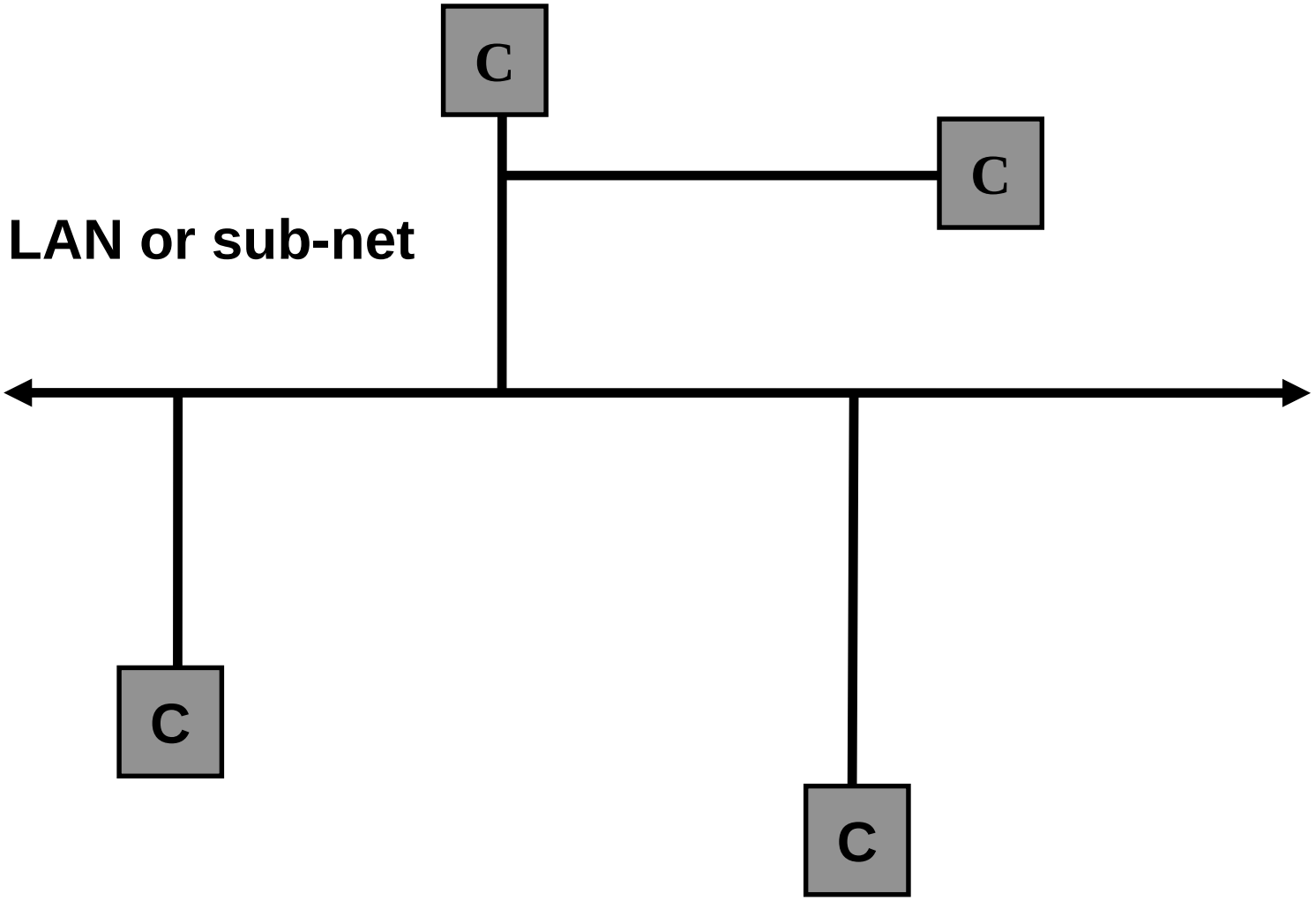
Daisy Chain or Bus Design



Tees or Stubs



Free Topology

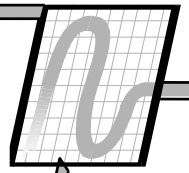


Network Planning

- One of your submittal requirements must be the “engineering guidelines” for the installation of all cabling.
- These guidelines must be published or certified by the vendor (not the contractor).
- The requirements in the guideline must be part of the startup testing requirements.

Architecture

Summary



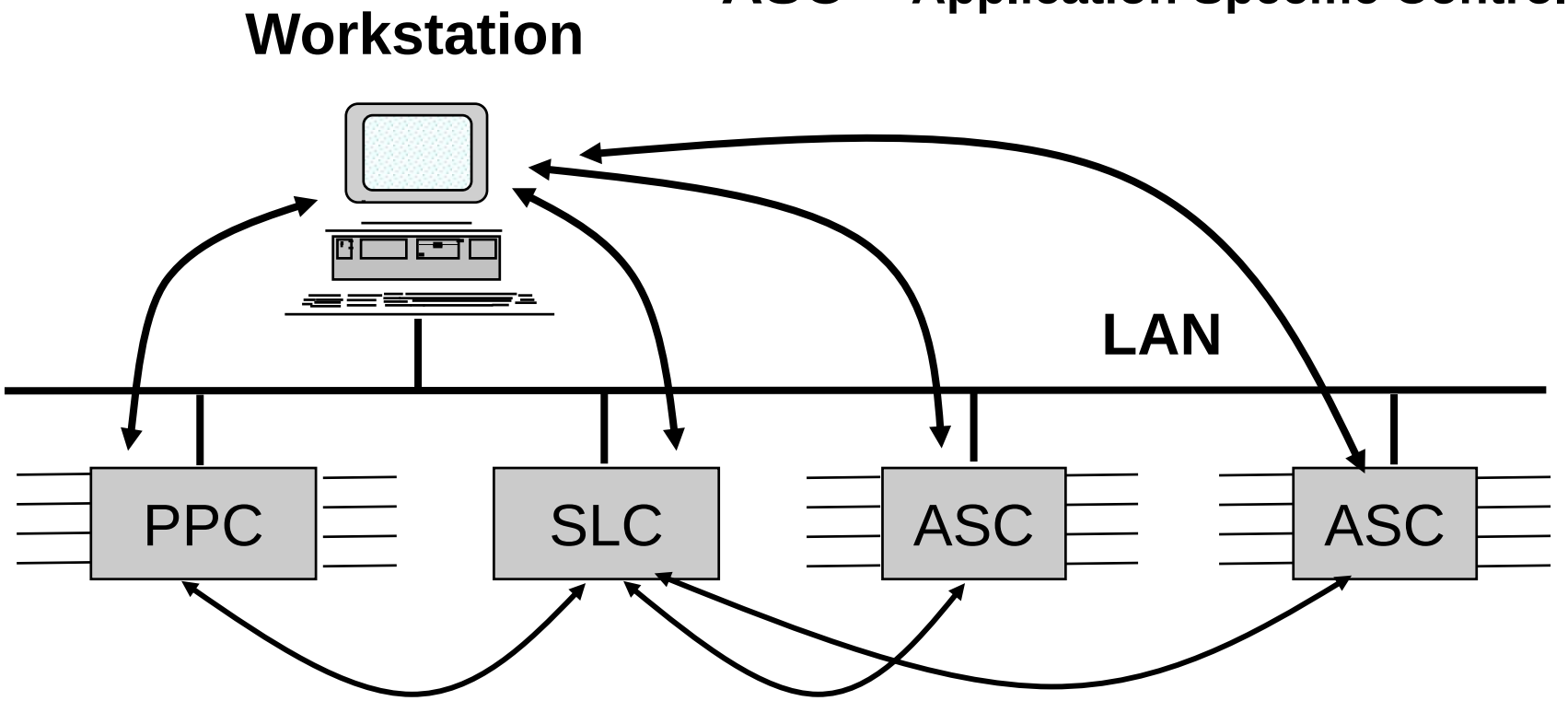
- Now that we have some basics covered, let’s start to build up a network.
- We will begin with a very small network and grow into larger networks.
- We will discuss both the hardware side and software side of networks.

Review: Controller types

- PPC: programmable process controller
- SLC: supervisory logic controller
- ASC: application specific controller
- Router: device to route information as required
- CM: communication manager

A Simple Network

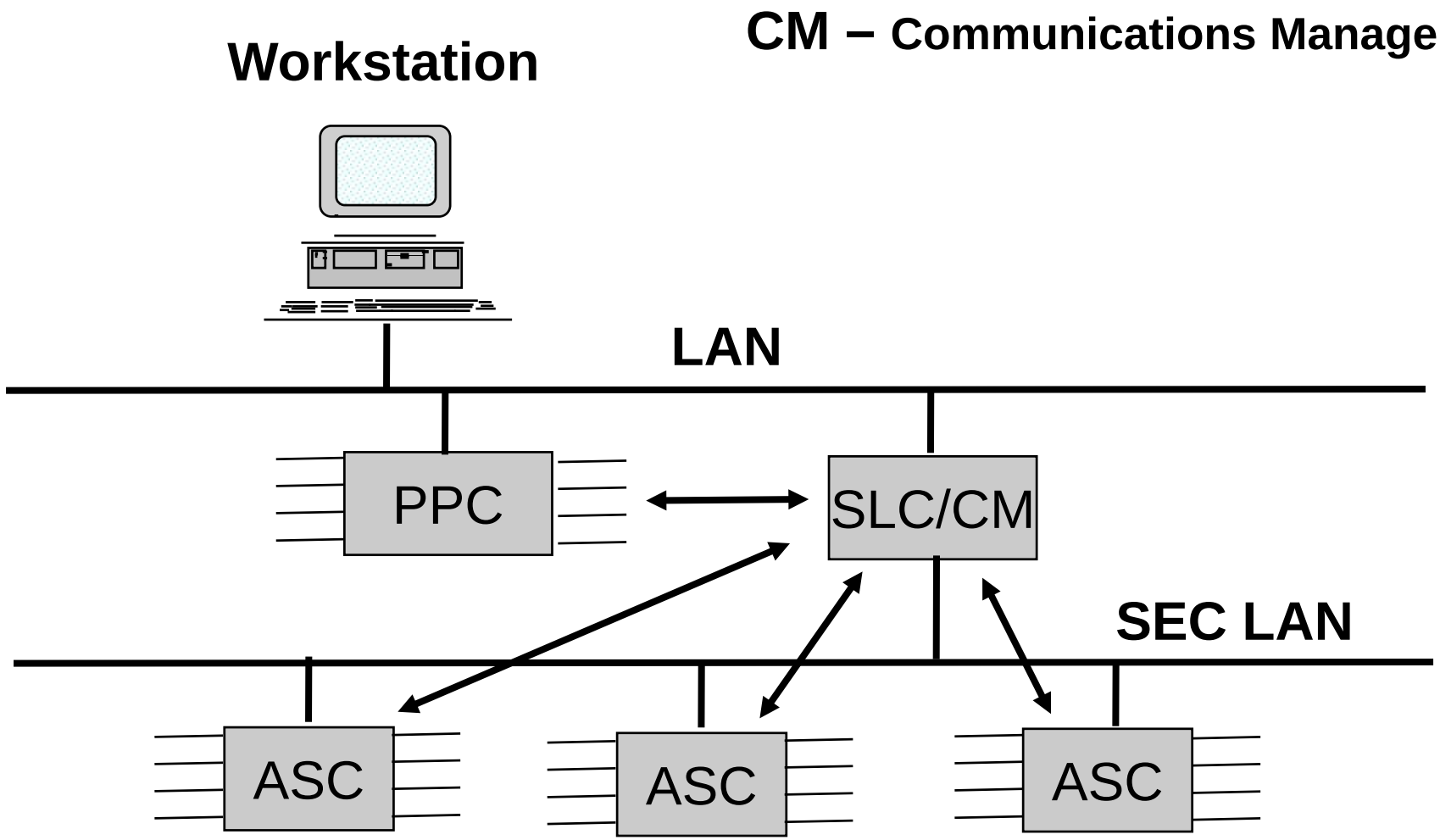
PPC – Primary Process Controller
SLC – Supervisory Logic Controller
ASC – Application Specific Controller



A Simple Network-Typical

- The PPC controls the central station AHU
  - Process control
  - Trending for AHU variables
  - Alarm handling for AHU
- The ASCs control the VAV terminals
- The SLC:
  - Time Schedules for the system
  - Trending for the ASCs
  - Alarm handling for the ASCs
  - Supervisory logic for the system

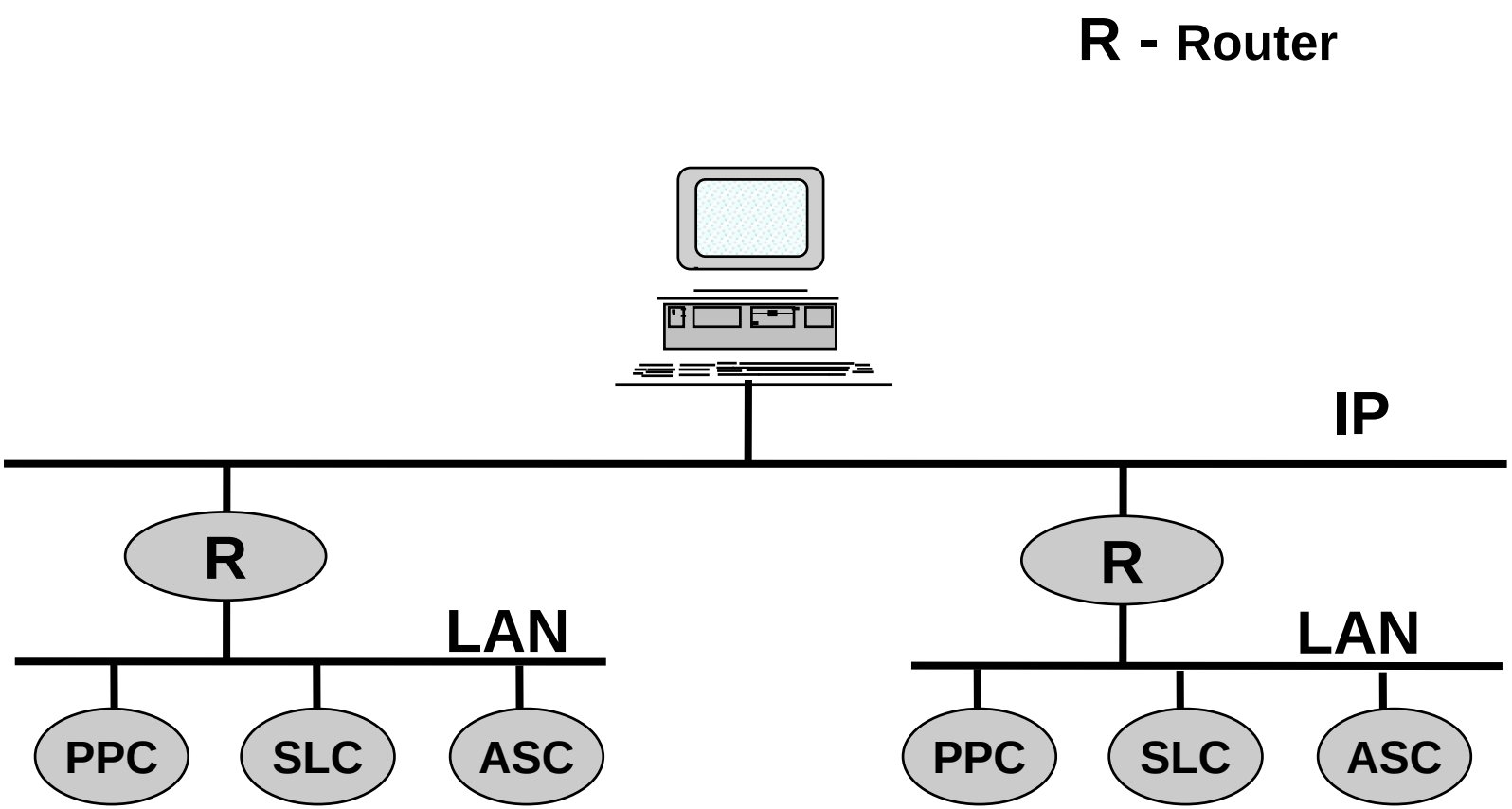
Primary LAN w/Secondary LAN



Primary LAN w/Secondary LAN

- The ASCs are moved to a secondary LAN that comes off of the SLC which also serves as a Communication Manager in this architecture.
- Communication from the PPC to the SLC/CM is peer to peer while communication from the SLC/CM to the ASCs is managed communication.
- In both of the previous diagrams, we did not have a TCP/IP layer in the architecture.

Add a TCP/IP Layer



IP Layer

- We have added the TCP/IP layer to the network architecture.
- This allows us to connect multiple LANs into a single network.
- Data can flow from any device on the left over the IP to any device on the right.
- The Workstation can monitor both LANs.
- We have also introduced a new component, the “Router” which connects the IP layer to the LAN layer.

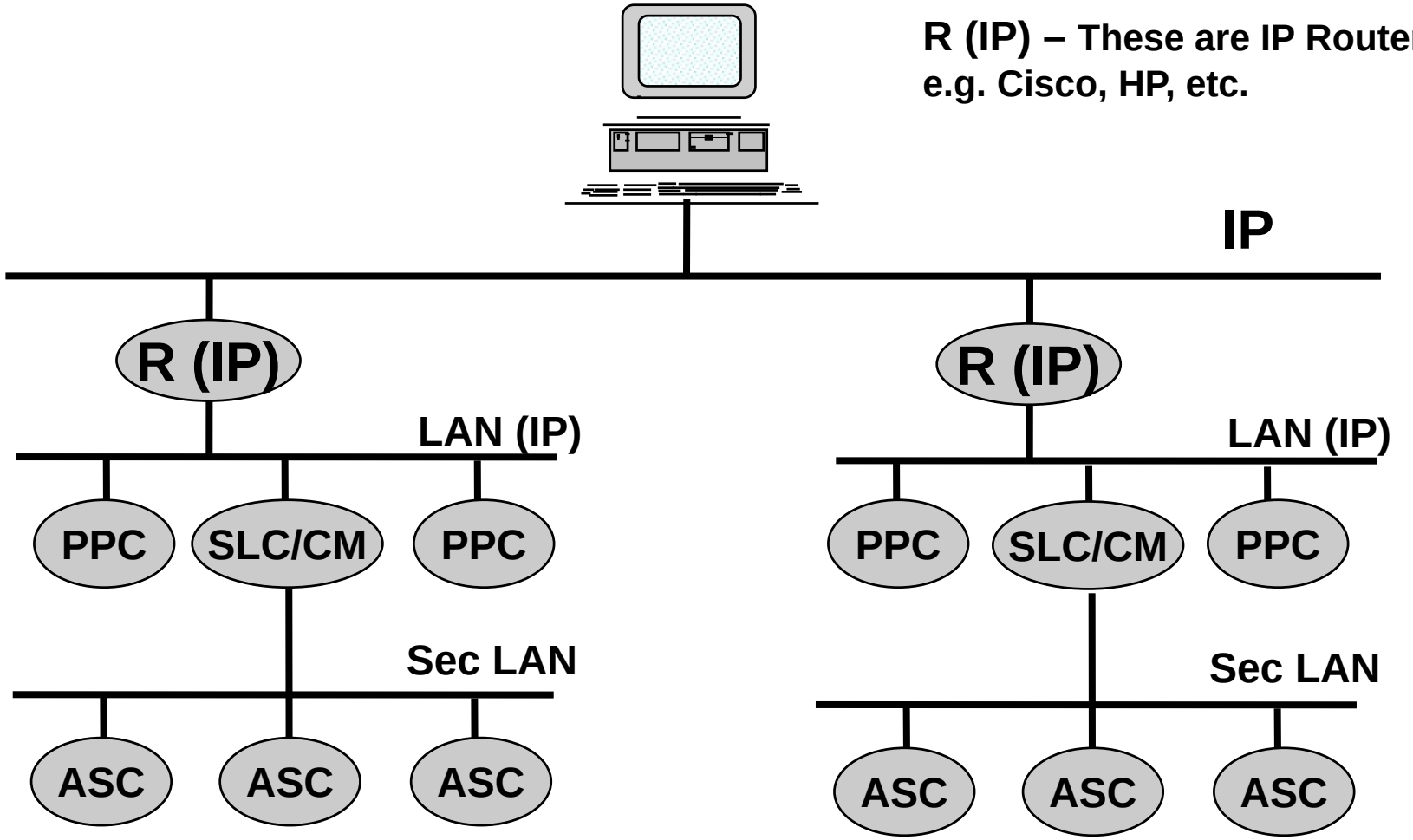
The Router

- The router accomplishes several different functions.
- It packs and unpacks IP packets with data associated with the controllers.
- It allows all data intended for the workstation to pass to the IP layer from the LAN.
- It only passes data that needs to go from LAN to IP (or IP to LAN) and blocks all other data -- important for bandwidth control on the IP layer.

The Router - continued

- Routers are used at various levels in the architecture – not just “Router to IP”
  - Lon allows routers within the Lon “field bus”
- These are **NOT IP ROUTERS!!!!!**
  - Be very careful when talking to IT staff
- They do packet filtering by destination address
  - Useful within field bus for this purpose
- Not a Communications Manager, or protocol converter (Gateway)
  - Forwards based on address, not on content

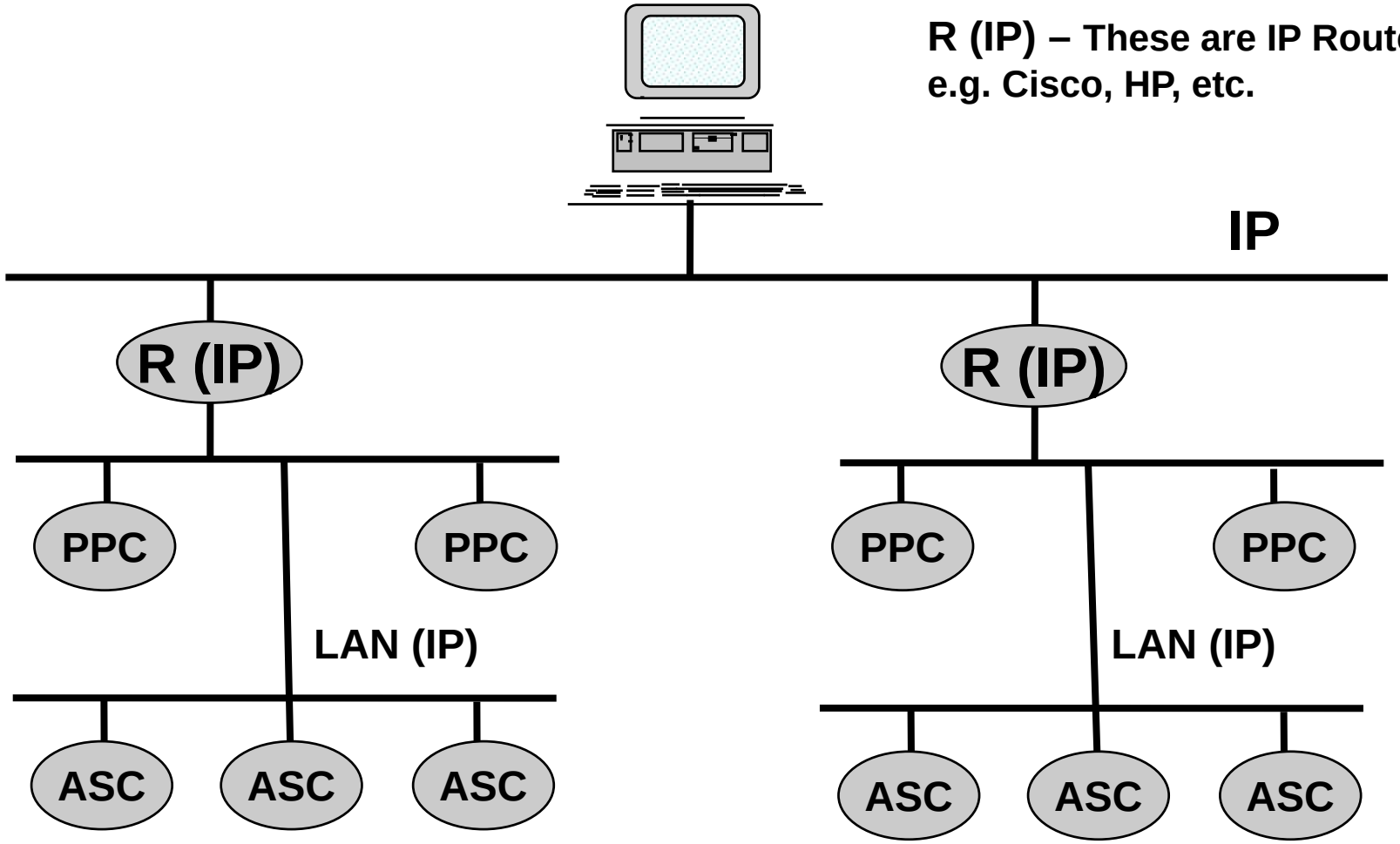
TCP/IP and Sec. LAN



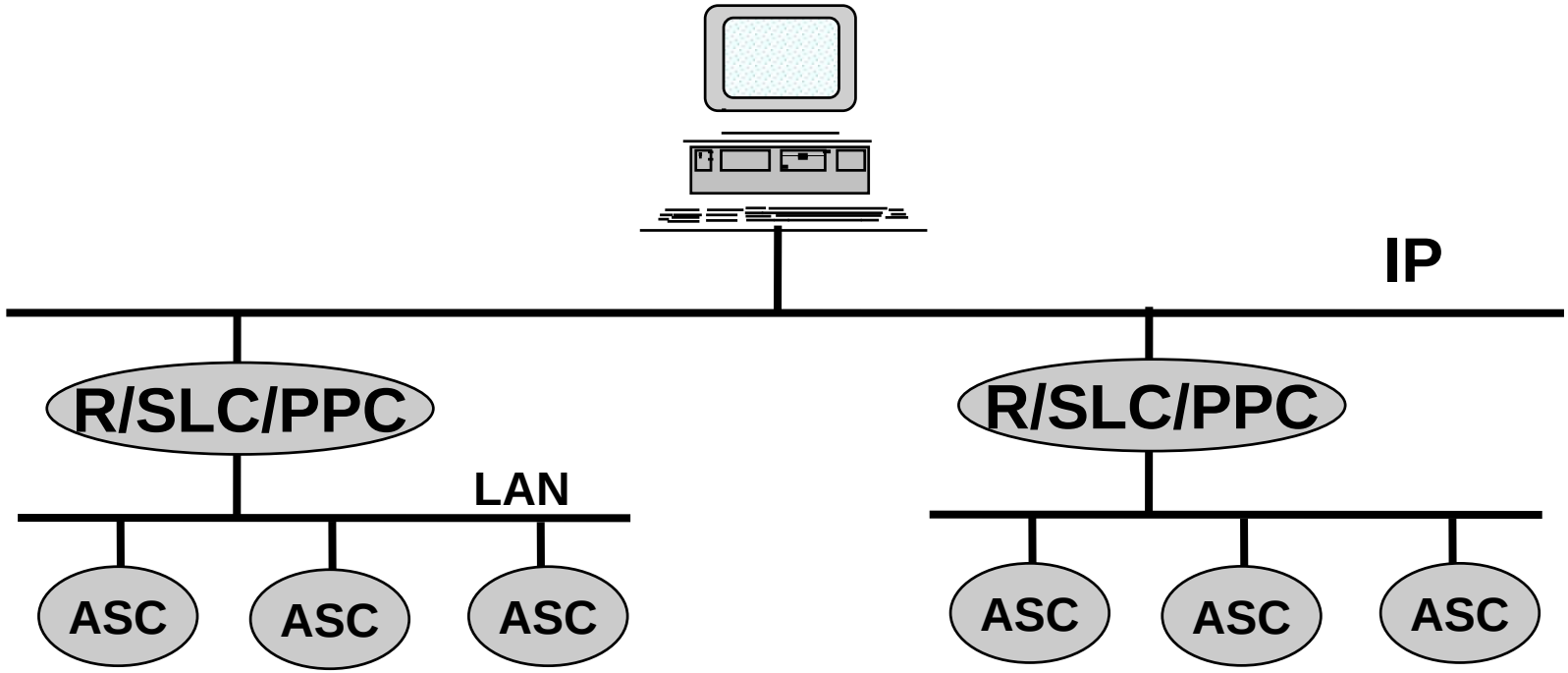
TCP/IP Plus Sec LAN

- The LAN now has only PPCs and SLC/CMs connected to it.
- All of the small secondary controllers that are typically ASCs have been moved to the secondary LAN.
- The SLC/CM manages the communication with the ASCs and provides the supervisory logic, time schedule, trend logging and alarm handling support for the ASCs.

TCP/IP ONLY


R (IP) – These are IP Routers
e.g. Cisco, HP, etc.
IP
R (IP)
R (IP)
PPC
PPC
PPC
PPC
LAN (IP)
LAN (IP)
ASC
ASC
ASC
ASC
ASC
ASC

Other Combinations



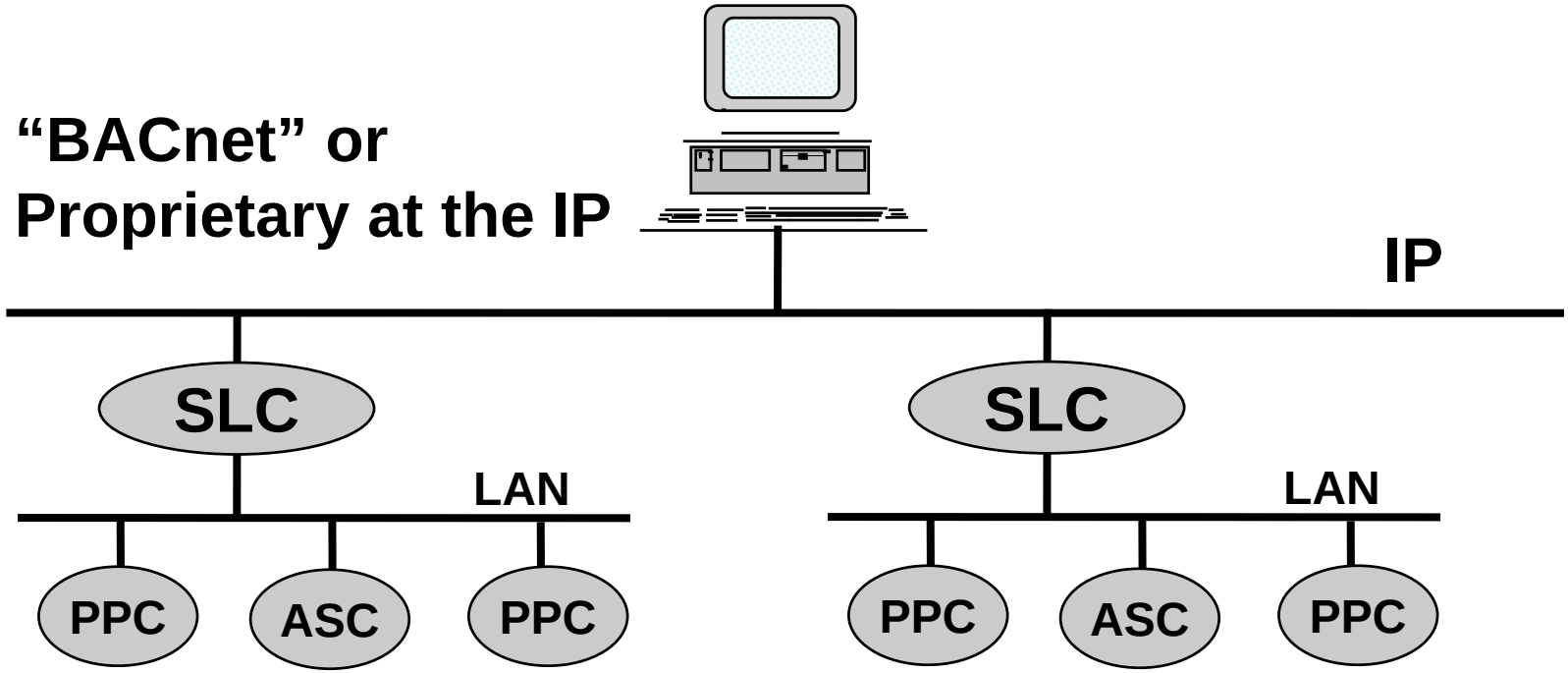
Other Combinations

- In this architecture the vendor has combined the router functionality, the supervisory logic controller functionality and a programmable process controller functionality into one device.
- The PPC functionality is typically used for the central station equipment.
- On the LAN we will typically see only small secondary ASCs for control of unitary equipment and portal control (security).
- Common BACnet architecture

Mixed Protocols

- There are several vendors that deliver control systems that use different protocols at the different layers in the system architecture.
- Typically, this is either Lon or BACnet at the LAN level and a mixture of proprietary and “BACnet” at the IP level.
- May also have proprietary at the equipment level
- Can also be used for integration of legacy buildings where the legacy protocol is “other”

Building Level Gateway



LonTalk, BACnet, or proprietary at the LAN

SLC does not act as a Router. Instead, it is a Communications Manager, or Gateway

Building Level Gateway

- The LAN below the new device has PPCs as well as ASCs executing process control.
- In this architecture the vendor has the connection to IP via a Gateway / supervisory logic controller:
  - SLC: Programmable control logic functionality for supervisory control, time based control, trend logging and alarm handling
  - Gateway: data arrives via LonTalk, BACnet, or proprietary from the LAN and can be transmitted over the IP via proprietary protocol.

Building Level Gateway

- The controllers on the LAN are reduced to simple PPCs and ASCs.
  - Occupancy commands are input network variables
  - Data requiring trending is transmitted from the LAN device to the IP level device.
  - Binary alarm variables are transmitted from the LAN devices to the IP level device where a message is attached and transmitted to various workstations.
- Tridium JACE
- Johnson NAE

Summary

- The key to understanding network architecture is to think “functionally” and not “physically”.
- You know all the key functions that have to exist.
  - PPC: programmable process controller
  - SLC: supervisory logic controller
  - ASC: application specific controller
  - Router: device to route information as required
  - CM: communication manager
- The different vendors will package these functions in different ways.

Mastering the Business

- Your next task is to gather information from the vendors that you wish to work with.
- Ask them to go over their architecture.
  - Describe the physical layout
  - Define each component
  - List the functions accomplished within each component
  - At the controller level, characterize the applications for which the PPC or ASC was developed.
  - Review datasheets for each device…learn to read the datasheets.
  - Talk about numerical limits.

Meet with your vendor

- If a device supports trend log storage..how many different variables and how many samples each before an upload is mandatory?
- Where is alarm handling done?
  - Text messages assigned to specific alarms
  - Routing of alarms
- Where do time schedules reside?
- Device to device communication
  - Where is it peer to peer vs. managed?
  - Where is event driven vs polling based communication used?

Small Secondary Controller

- Are they application specific or programmable?
- If programmable do they use standard applications?
- If programmable, what is the programming tool?
- Is the programming tool line based or graphical?
- Is there an application simulation capability?
- Is it the ***same*** programming tool as for the larger Primary Controllers?

The Front End

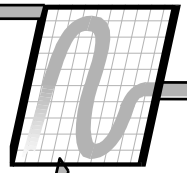
The IP network Level

- We now need to look more closely at the IP network level of our architecture.
- It consists of:
  - Servers
  - Workstations
  - Web Servers
  - Webclients

The Server PC

- In the DDC world we refer to the PC that is responsible for managing the communication with the hardware devices as a server.
- This is a definition that will greatly confuse an IT person…so be careful when you use this term with the IT people. Sometimes it is better to refer to a DDC server as a “Primary Workstation”.
- This PC will communicate with the hardware, collect information and store that information in a database on the PC.

System data at the Server

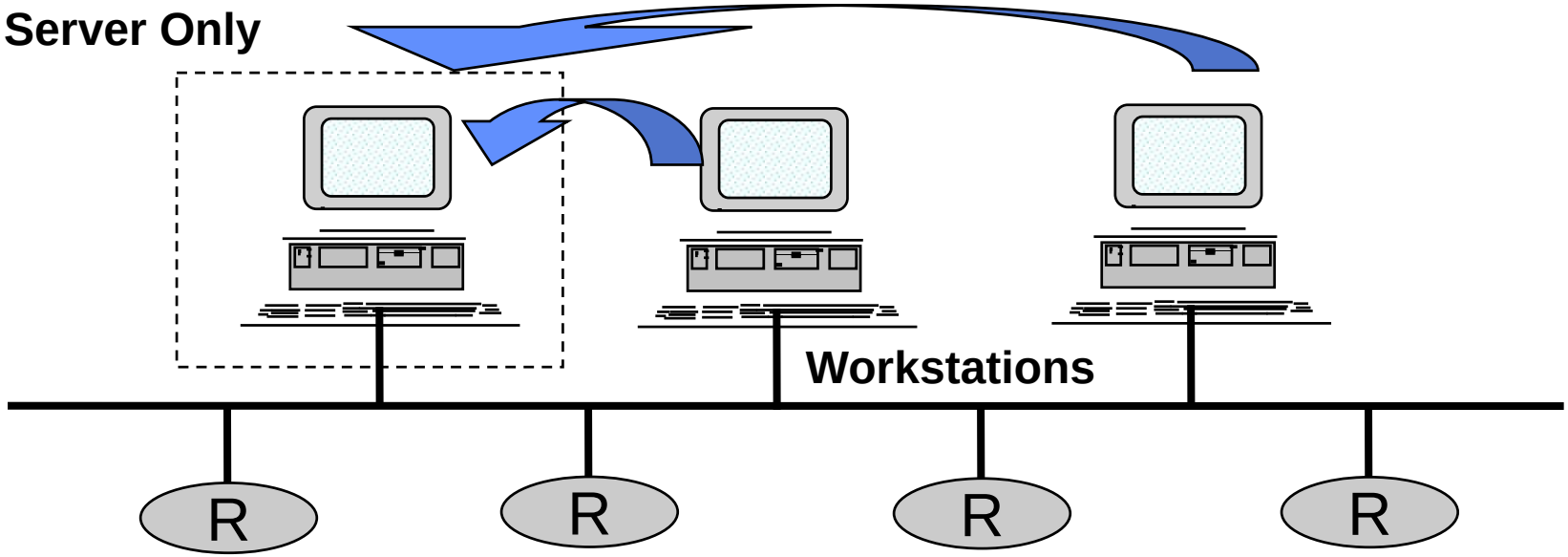


- The server has “all” the system information – usually in several different locations.
- Part of the data should be stored in a standard database (e.g. Oracle, MySQL, MS-SQL).
  - Trend data
  - Event data
  - Personnel data when security systems are involved.
  - Note the data is likely ***still*** in a proprietary format.
- The rest of the data will (likely) be stored in some unknown format -- which is not a problem
  - But ***is*** a problem with multi-vendor systems.

Workstation Software

- Once the Server has all of the information, we need a way for the operator to access the data.
- We refer to this as Workstation capability.
- This is ***generally*** a web browser

PC Structure



- The workstations present data to the operators.
- The server is locked in a “closet”.
- Workstations use web browser, or have vendor unique software.

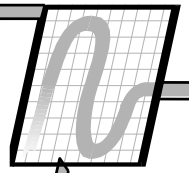
Workstations

- What is a workstation?
  - (aka UI, GUI, MMI, HMI, OWS……)
- It is a “Point of Entry” for human interaction with the system.
- We need to break down our human interaction into two types of tasks.
  - Operation (this is generally the “workstation”)
  - Engineering
  - This distinction will be particularly important in multi-vendor systems

Operator tasks

- View point data in lists and on graphics
- View live trend data
- View historical trend data
- Acknowledge alarms
- Run pre-prepared reports
- Adjust application parameters (typically setpoints)
- Manually override logic and force actions
- Edit time schedule parameters

Engineering Tasks



- Building the system
- Adding devices
- Addressing devices
- Initial application programming
- Downloading programs
- Modifying programs
- Configuring application specific controllers
- Setting up trends
- Creating reports
- Creating graphic displays
- Point calibration

Workstation Software

- Workstation software in the DDC industry has migrated from a single package with a single user license to a very modular approach with complex licensing concepts.
- With software licenses you must also address the number of users that can execute a particular task at the same time .. “seats at the table”
  - “Only one workstation at a time can be used to create a new graphic page, with the current licensing.”

Mastering the Business

- Very important to understand the structure and licensing concepts that they offer.
  - Server software
  - Database structure (standard, proprietary…etc.)
  - Operator software
  - Report viewing software (might be Excel or Access)
  - Engineering software:
    - Addressing
    - Application programming
    - Graphics
    - Report generation

Your Operational Requirements

Task	PC1	PC2	PC3	Simultaneous
Server	X			
View Data	X	X	X	YES
Ack Alarms	X	X	X	YES
View Reports	X	X	X	YES
Ovrd Points	X	X	X	YES
View Trends	X	X	X	YES
Edit Schedules	X	X	X	YES
Etc.				

Your Engineering Requirements

Task	PC1	PC2	PC3	Simultaneous
Server	X			
Add devices	X	X		NO
Address Devices	X	X	X	NO
Create Applications	X			NO
Download Apps	X	X	X	NO
Configure ASCs	X	X	X	YES
Setup Trends	X	X	X	YES
Setup Reports	X	X	X	NO
Etc.				

Mastering the Business

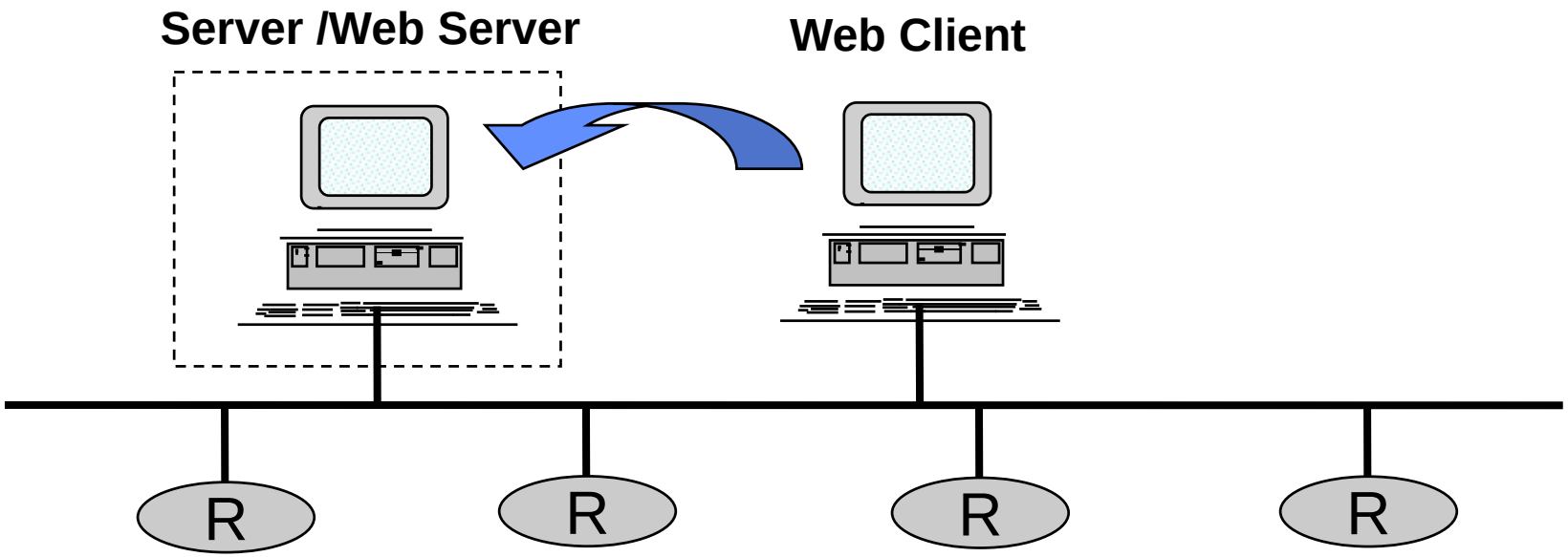
- It is very important to define the capability to be delivered at the IP level of the system.
- Define your “Points of Entry”
- Define the tasks to be executed at each point of entry.
- Be sure to consider the issue of “simultaneous”
- Be aware that software costs will increase as you ask for more functionality at more points of entry and you require a lot of simultaneous functionality.

Web Serving

- For most task, the workstation needs nothing more than a web browser.
- For workstations to use browser software only, there has to be a web server software package.
- The web serving software takes the data from the database and converts it for presentation in an HTML format.
- May only include Operational tasks

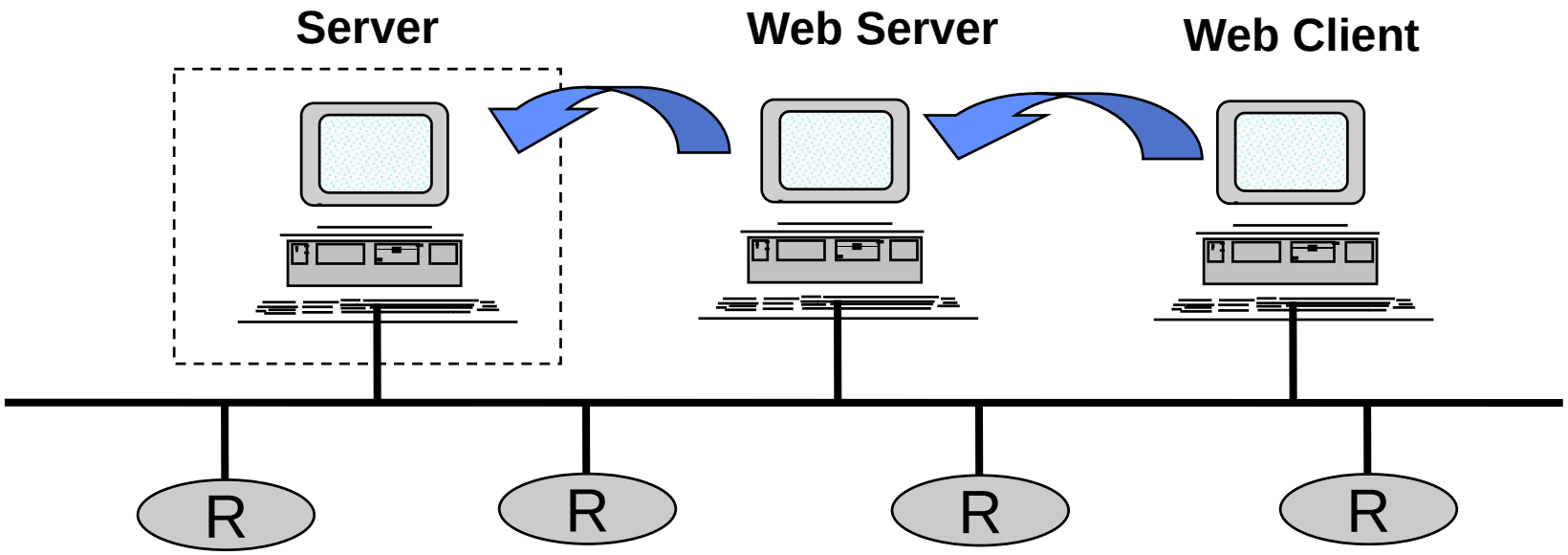
Web Serving

- The Web Server software is typically on the same PC as the database.
- Web server is likely a standard IT application



Web Serving

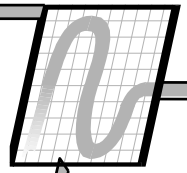
- The Web Server software may not be on the same PC as the system database.
- The Web Server goes to the server and gets the data it needs to convert to HTML format.



Web Server PC

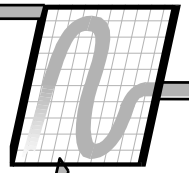
- Web server on separate PC from DDC “server”
- IT staff can permit access to Web server while blocking access to DDC server
- Useful for securing BAS
- May be useful for allowing access from anywhere on corporate int***ra***net
- Useful (but not generally sufficient) when allowing access from Internet.
- (more sophisticated solution: VPN from outside)

Web Clients



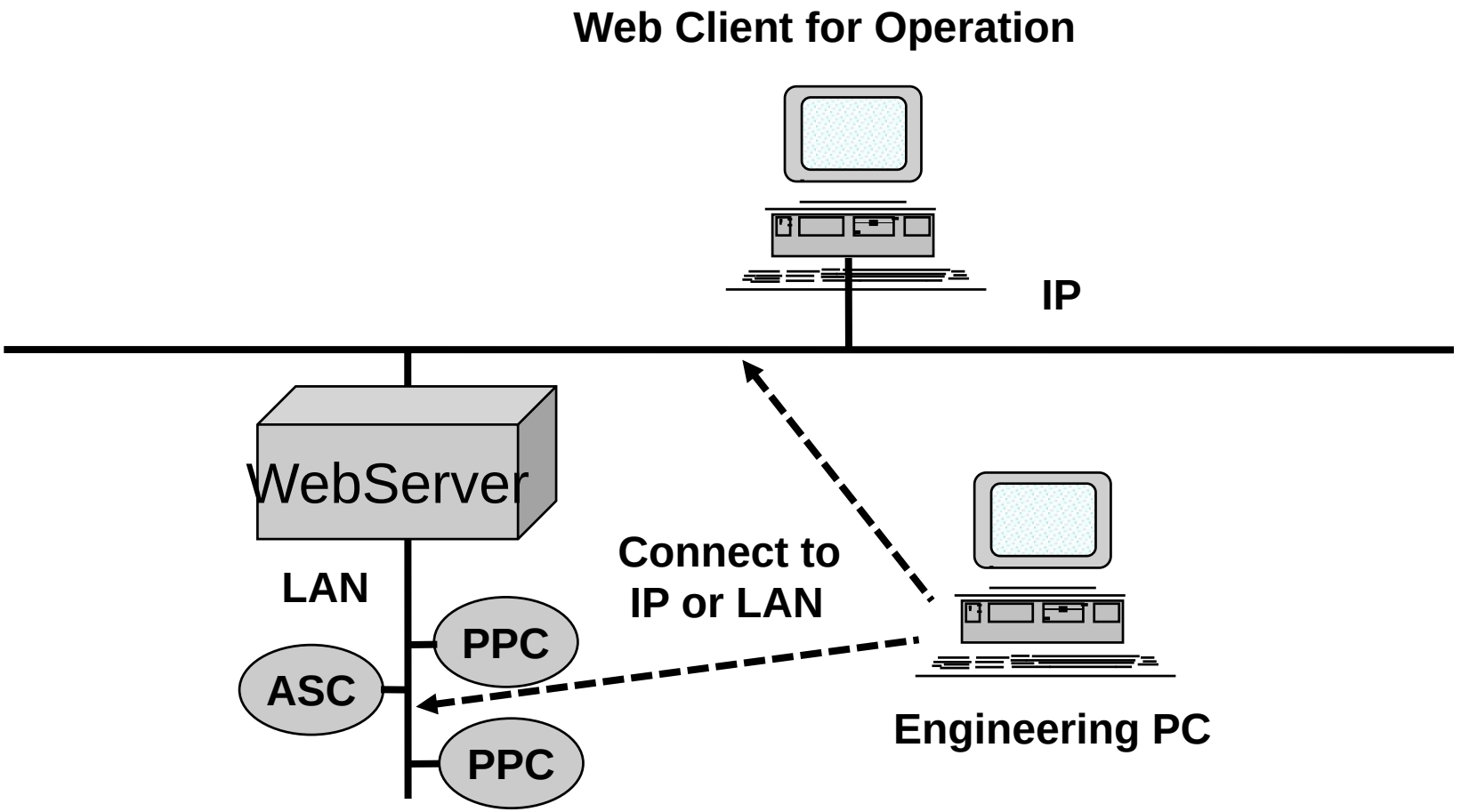
- Once we have a web server, we can then have multiple web clients.
- Web Clients are PCs that use a standard browser to access the data from the Web Server.
- Within the Web Server there is a license management package that controls how many web clients are allowed to access the web server at the same time.
- You still have to purchase the “seats at the table”

Non-PC Web Servers



- The Web Server is just a software package.
- It can reside on a hardware device that is connected to the IP network.
- May include router functionality.
- IT staff may have fits with these devices.
  - They may have vulnerabilities like a normal PC
  - The web server itself may be vulnerable
  - May run some “IT-ish” OS, sometimes Windows
  - But can’t be managed like a normal PC

Hardware Web Server



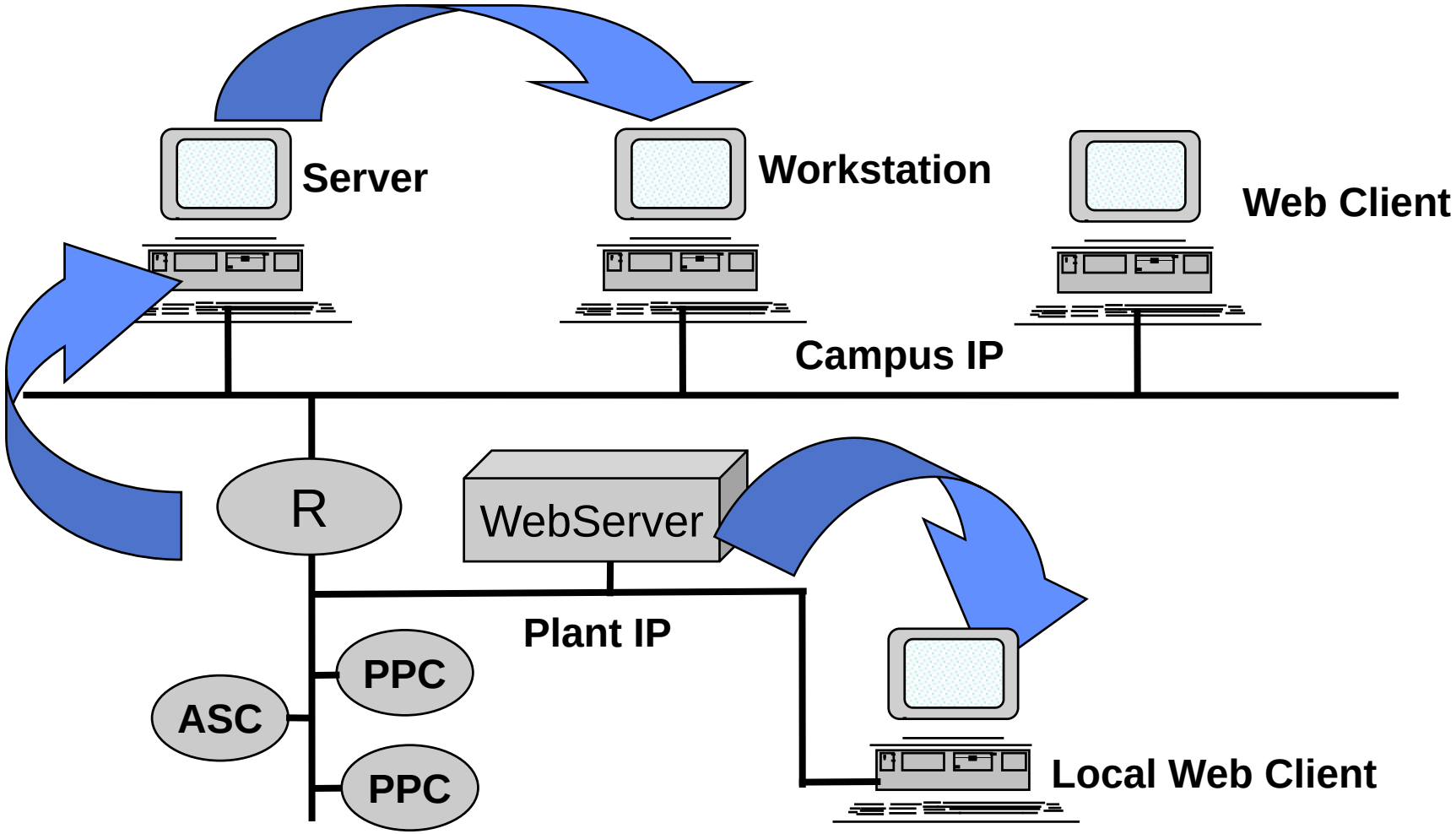
Hardware Web Server

- The IP level hardware device is both a server and web server. It holds a database for presentation to the web client.
- It may be possible to run vendor unique engineering software on the client to execute engineering tasks or you may have to connect locally to the LAN in order to execute engineering tasks.

Dual Web Server Systems

- It is possible to have both a PC based server and a hardware based web server.
- The system just has to have all of the hardware and software components in place to support both structures simultaneously.
- Example might be a central plant that needs it’s own local web server to support a 24/7 O&M staff

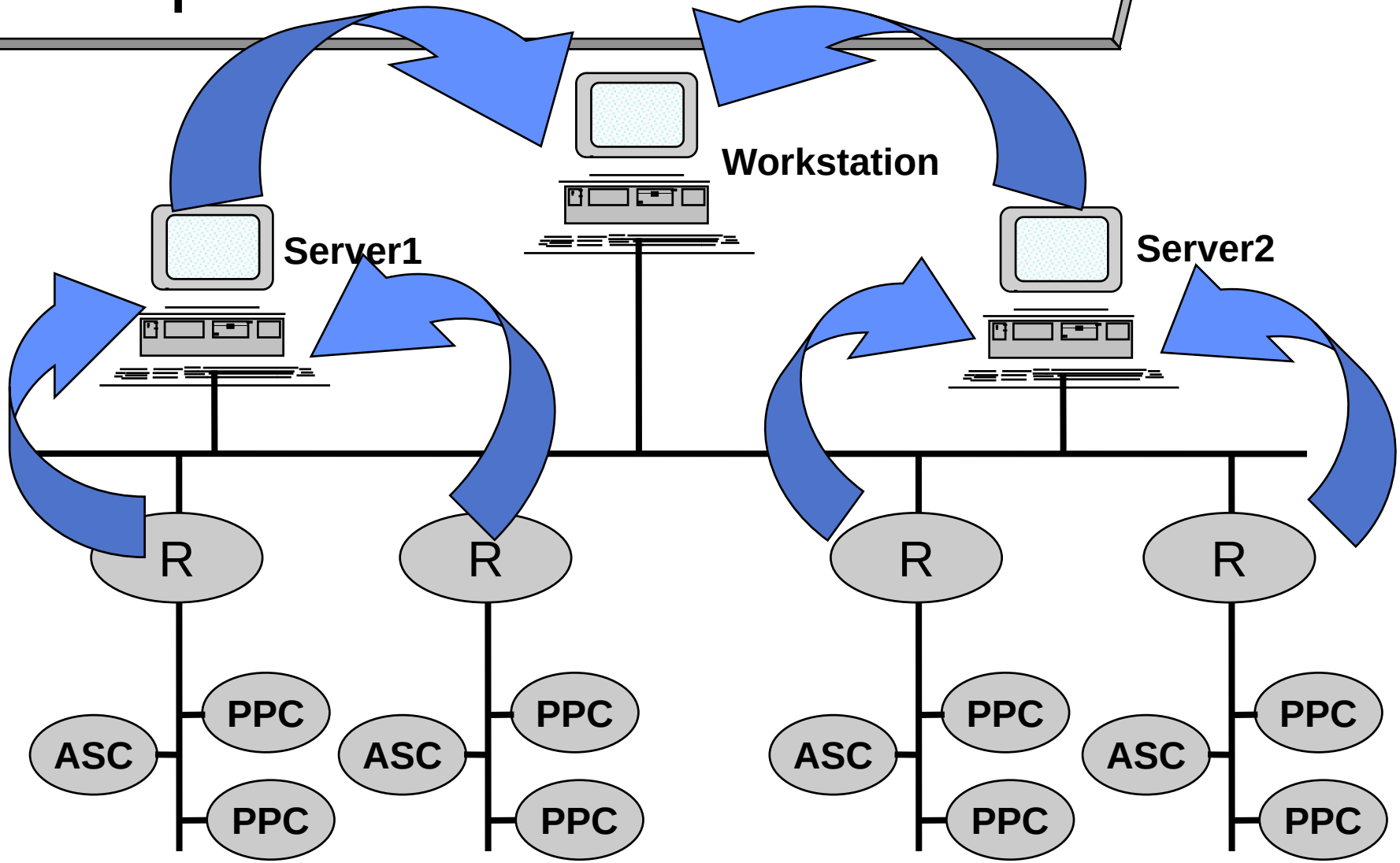
Dual Web Server Systems



Enterprise Level Integration

- As systems get larger, it may be advantageous to have multiple independent systems (servers, databases, networks) with workstations that can present data from the multiple systems to a single operator workstation.
- This, particularly when multiple vendor's servers are involved, is commonly referred to as Enterprise level integration.
  - Front end servers sharing data, not field level devices sharing data

Multiple Server Environments



Multiple Server Environments

- The same issues that applied to single server environments also apply here.
- You need to define where all functionality resides and what capability is presented at each point of entry into the system.
- In this case you also need to evaluate whether data from one server/network can flow to a second server/network for the purposes of effecting control logic.
  - This is not typically required on such large systems.
  - The purpose of the multi-server system is to aggregate data at one workstation.

Summary

- We have now concluded a big picture look at system architecture.
  - Focus on structure
  - Focus on functionality
  - Recognize that the vendors have a lot of freedom to deliver all the required functionality in many different ways.
- Your challenge is to understand how your needs are being met by a specific structure and what are the performance factors for the specific structure begin delivered.

Summary

- There is no “Standard Architecture” for a DDC system, however each system will combine some or all of the elements described.
- All systems will use a LAN or sub-net and typically some form of a site LAN or WAN if the system size requires it.
- The structure of the enterprise level of the system is very important.
  - Servers
  - Workstations
  - Web Servers
  - Web Clients

A note on BAS Security

Securing the BAS

- Attacks on infrastructure very much in the news
- What is the risk to me from my BAS?
- ***Risk*** is made up of ***vulnerability*** and ***consequences***
  - My shed is unlocked (vulnerability = HIGH) but there's nothing of value there (consequence = LOW)
  - My house is locked (vulnerability = LOW) but there's high value things there (consequence = HIGH)
    - Which is the higher risk?
    - Which do I add security to first?
- Risk is what insurance companies deal with:
  - How much is your house worth?
  - Do you have smoke detectors?

Target: IT Security Failure

- HVAC vendor has corporate IT password to support BAS from outside
- Password is stolen
- Attackers hack Target's Point Of Sale system
  - Never touched the BAS
  - Why does HVAC password get you to POS system?

- My toilet is broken
- I give plumber my house keys -- and car keys
- Plumber looses keys and my car gets stolen
- The security fix: A padlock on my toilet

Most BAS is LOW risk

- ***Most*** building aren't worth attacking.
  - Turn off heat to classroom or admin building
  - Go turn heat back on, manually if necessary
  - Mechanical design (and physics!) limit consequences
- Often easier to attack mechanical system directly
- There are ***critical*** exceptions:
  - Turning off cooling to a data center
  - Turning off airflow in a bio containment lab
  - Turning off power
- Often not cost-effective to protect the whole BAS
  - Protect critical systems from the BAS

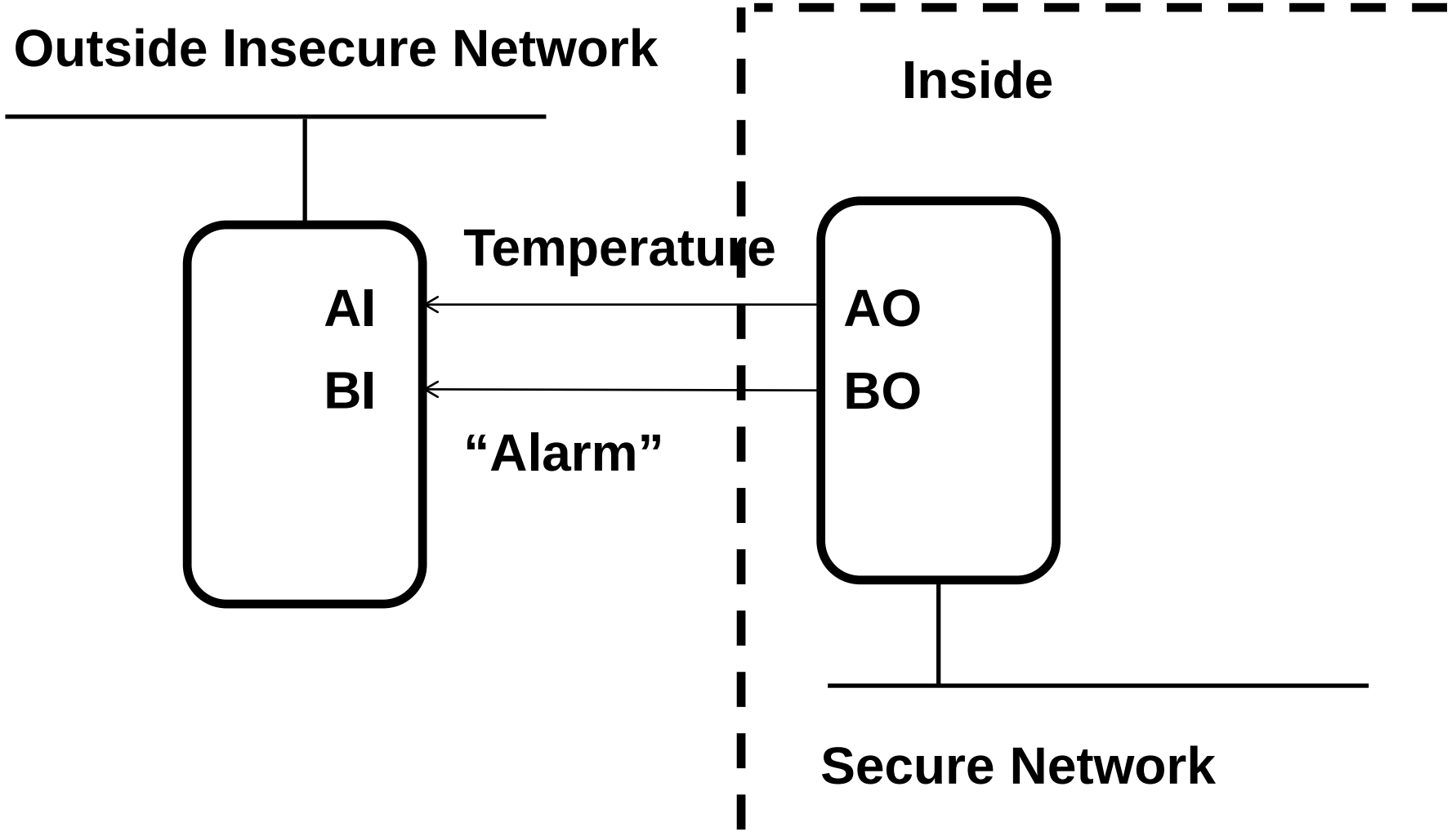
Limit OWS Functionality

- Normally, our goal is: Make sure we can do **<*x*>** from the front end.
- Now, our goal is: Make sure ***no one*** can do **<*x*>** from “outside”
  - “outside” usually being some physical perimeter
- Seems counter-intuitive… but
  - Critical systems may need more monitoring
  - They seldom need more outside control
    - When do you change the setpoint on the data center?
    - When do you ***remotely*** change airflow in the lab?
    - When do you turn off the A/C for the UPS?
    - When do you want to stop a generator remotely?

How to Limit

- Hardware only interface: AO/BOs talking to AI/BIs
  - BO on inside device providing alarm contact to outside BI
- Use a different protocol for the critical system and a limited gateway to connect to BAS
  - Only map through commands / statuses that are absolutely necessary
- May be some custom firewall approach as well to limit traffic between critical system and outside

Hardware I/O Only



Basic Security Steps

- Don’t allow remote access – particularly via vendor backdoors
- Lock down your OWSes: don’t allow standard applications or Internet access from an OWS
- Change passwords regularly
  - Limit access by user
- Turn on auditing: track operator actions
- Keep mechanical rooms locked
  - How to secure terminal equipment?
  - Whole bunch of non-cyber security things…..

System Architecture Summary

- The proper application of controllers is essential for a quality system.
- Information sharing between controllers and centralized data collection and presentation are two of the major advantages of DDC systems.
- The DDC network or “System Architecture” is the backbone that provides these capabilities.
- Your system architecture is your “Master Plan” and it deserves a lot of thought and investigation.
- More later on BACnet and Lon architectures