Development of Communication Solutions

Erich W. Gunther

EnerNex Corporation

Knoxville, Tennessee

erich@enernex.com

EnerNex CORPORATION

Purpose of Presentation

- Overview of basic communication principles
- History of utility communications
- Introduction to modern communication concepts

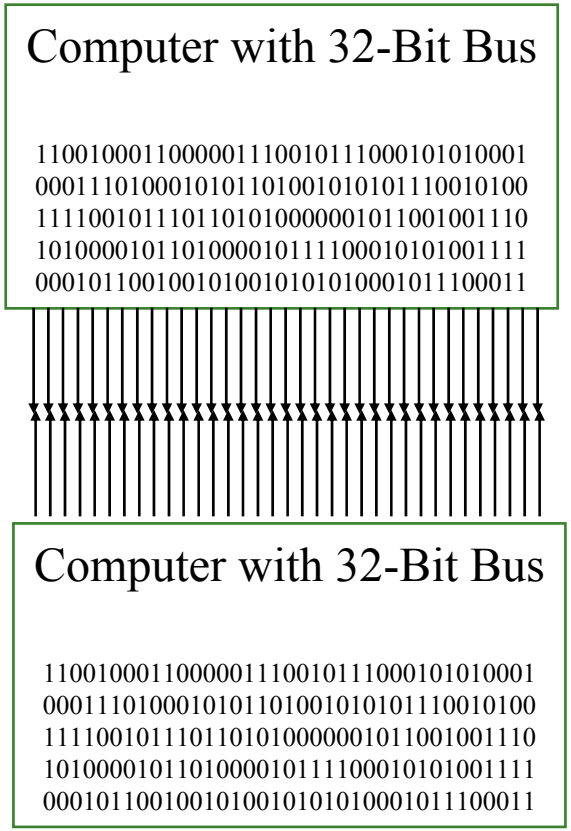
Communication Basics

Computers need to “talk” because they need to share data and resources.

In the good old days we carried data between computers on spools of magnetic tape and with decks of punched cards (“SneakerNET”)

Computer communications has to do with enabling two computers to copy information from the memory of one to the memory of the other, without human aid and without errors…

Communication Technologies

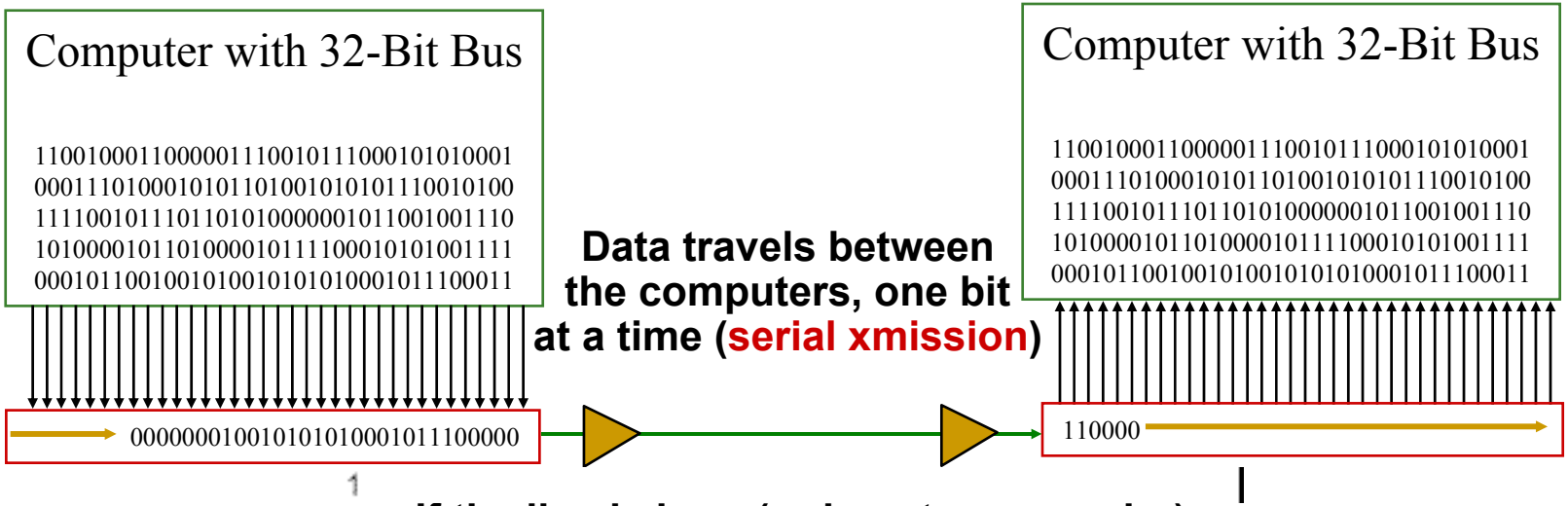


The logical way to connect computers to each other is to extend their data bus to each other and send data across this connection at speeds equal to those used internally to the computer.

Unfortunately, electrical properties of signal transmission make this infeasible except over very short distances (meters, not kilometers)

Such a connection is called a Parallel interface because all data bits transfer between the computers in parallel, at the same time.

Communication Technologies



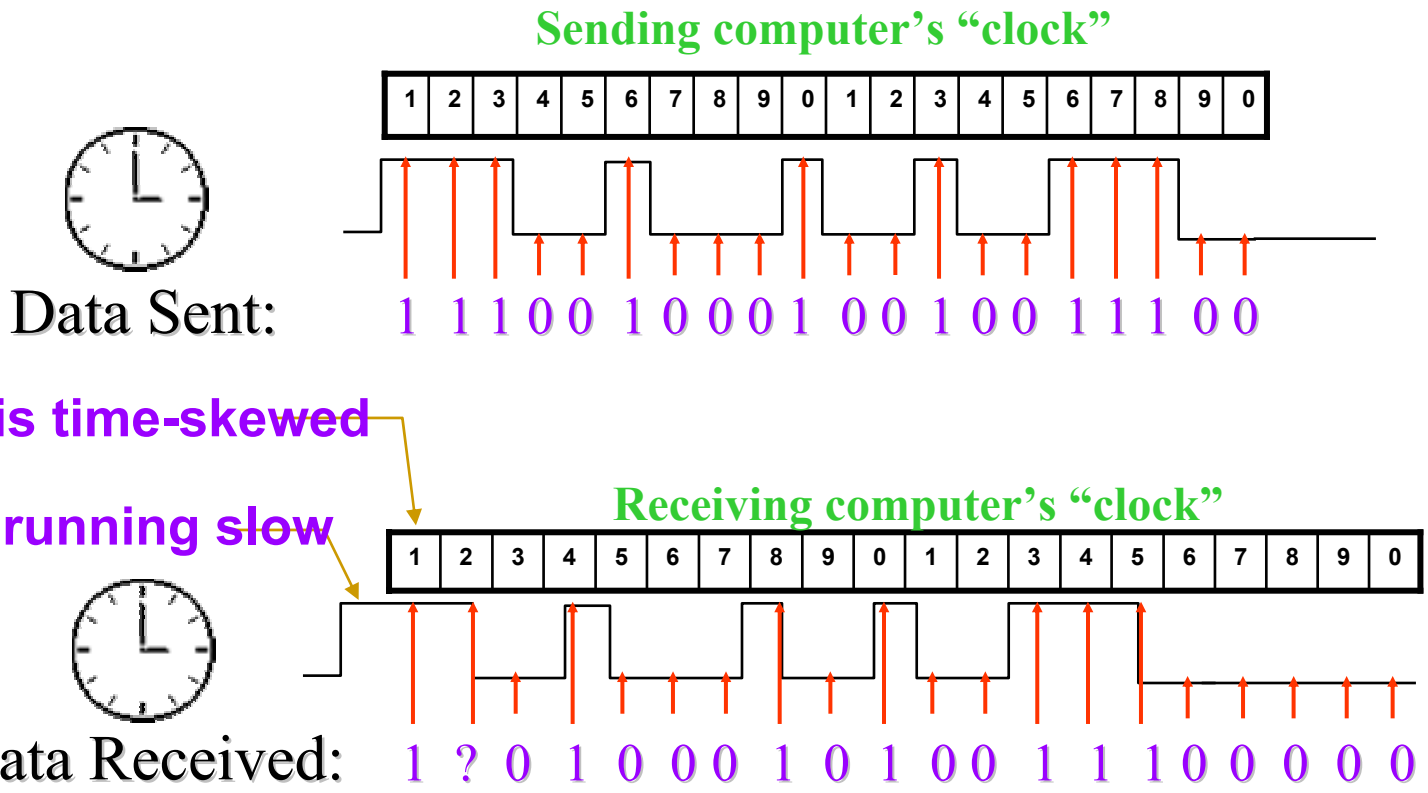
Data travels between the computers, one bit at a time (serial xmission)

If the line is long (or is not a mere wire) we may use special devices (modems) to boost and condition the signal.

Most/All long-distance communication systems used "serial" transmission schemes….telegraph, radio, telephone, telex

The faster we can shove bits down the line (baud rate) the more rapidly we can get the data from one computer to the other (data transfer rate). The line's electrical characteristics generally limit the top speed (bandwidth).

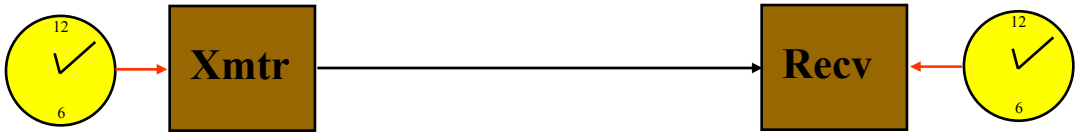
Communication Technologies



The receiving computer is "looking" at the in-coming signal at the WRONG times !! The clocks at both end MUST be synchronized in order to send data accurately…

Communication Technologies

Asynchronous vs. Synchronous transmission



The "Clock" is just a counter that cycles at the agreed rate. A sync just sets it back to a zero value

Serial transmission requires synchronized clocks at both ends so that receiver knows when signal level being received represents each successive bit in the stream.

Async transmission sync's receive clock by putting out a "start" bit to reset clock. This is done for each octet of bits sent.

The BEST efficiency we can get is 80% Often characters aren't packed and so additional efficiency losses occur.

Sync transmission sync's receive clock by putting out a special bit pattern to reset clock. This is done once, and then xmission NEVER stops. Pads sent when link idle.

11011111
00110001110000110110000111001011001…..

The BEST efficiency we can get is near to 100% if the transmission is lengthy NRZI encoding provides continual clocking using bit-stuffing to insure no long run of 1s

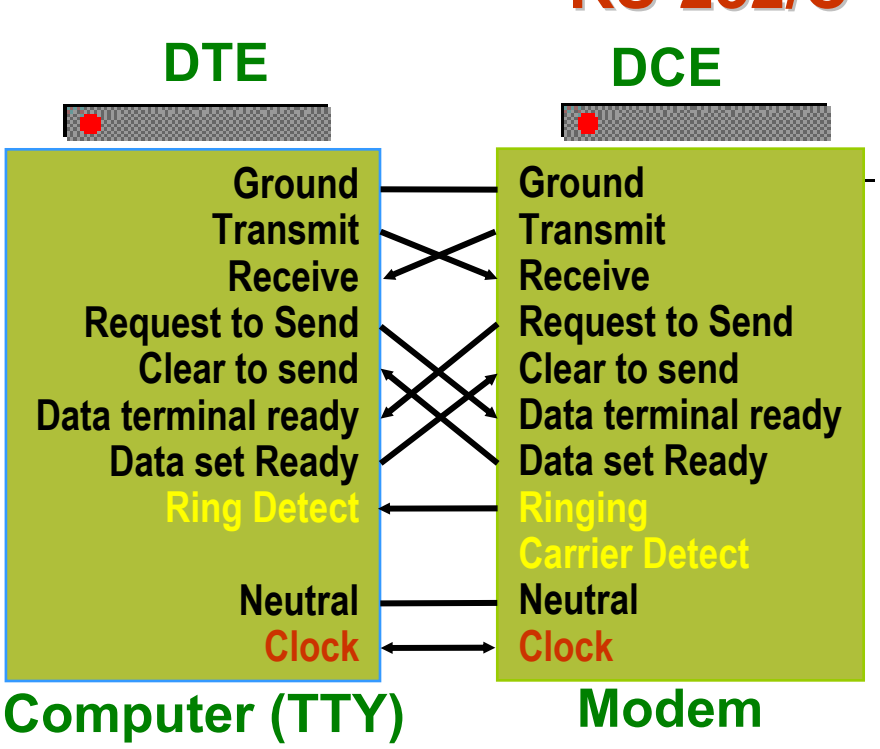
EnerNex CORPORATION

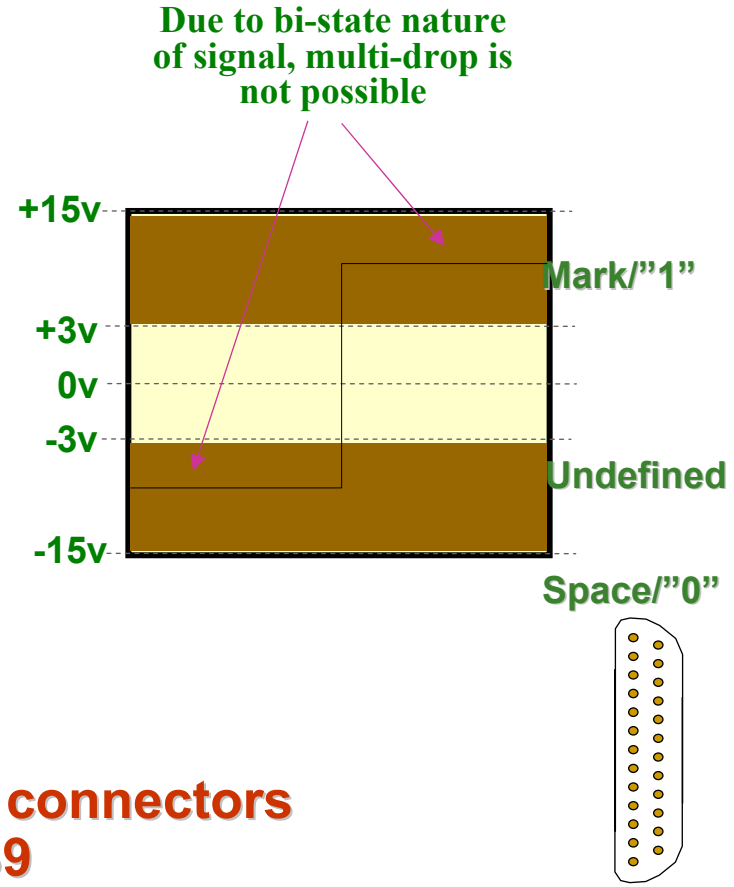
Communication Technologies

Digital Data Communication Hardware Standards

Standards are needed to allow interconnection of equipment

RS-232/C





Standard did NOT define physical connectors but *de facto* is DB25/DB9

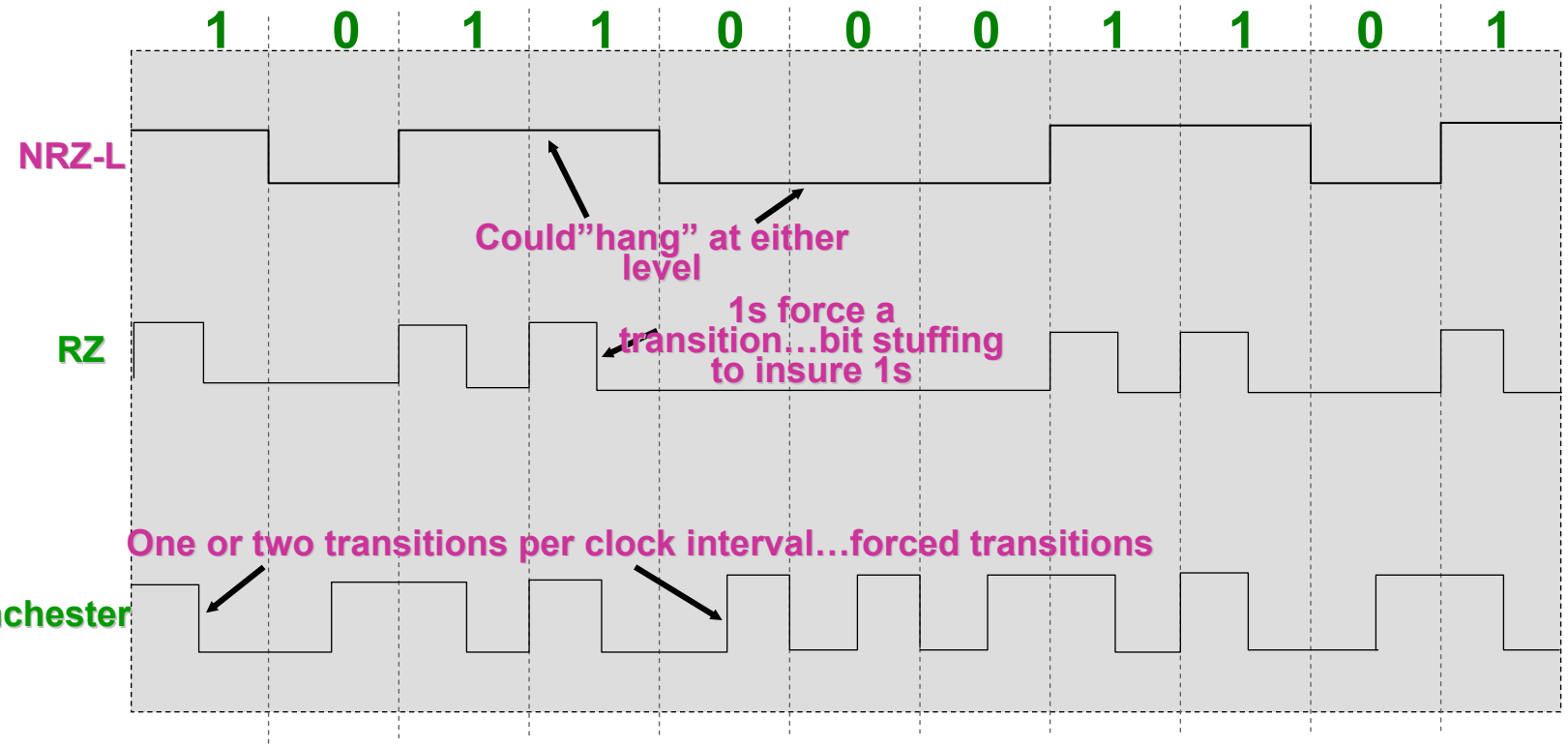
EnerNex CORPORATION

Communication Technologies

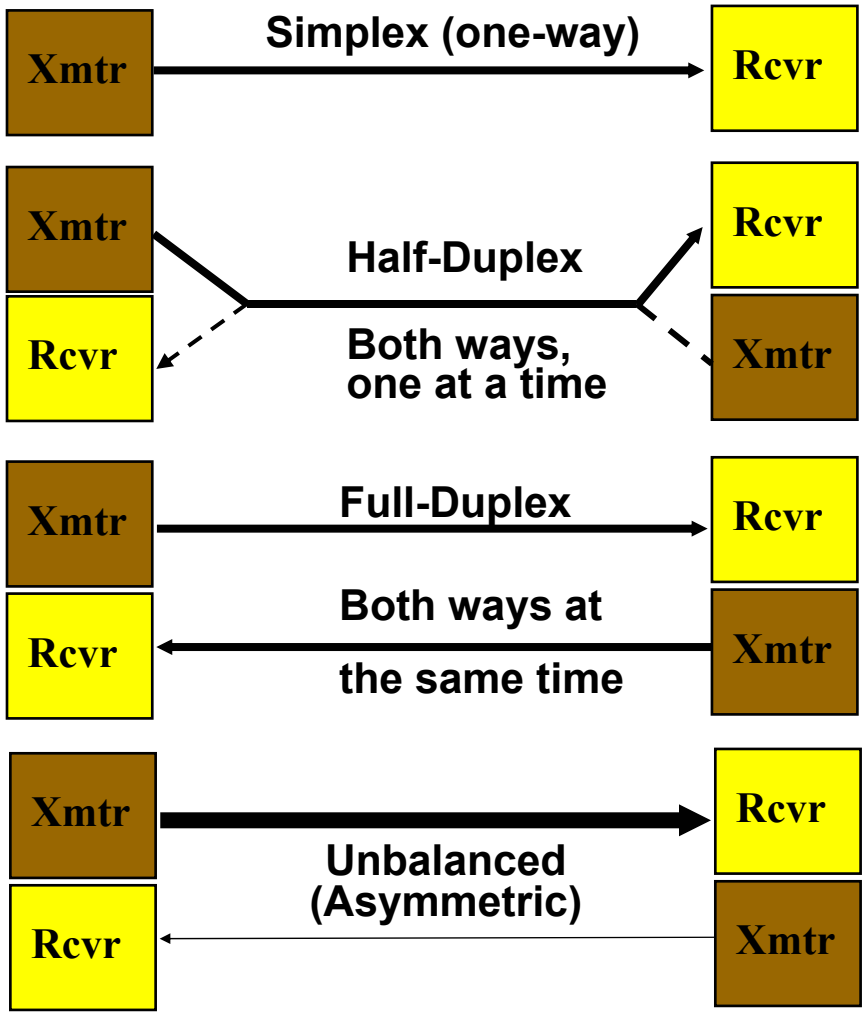
Digital Data Communication Hardware Standards

Serial data needs to be "encoded" onto the transmission media.

- How do you tell "dead" from sending lots of '0's or '1's ?
- How to keep clock synchronization at both ends ?
- How to detect errors in encoding ?



Communication Technologies

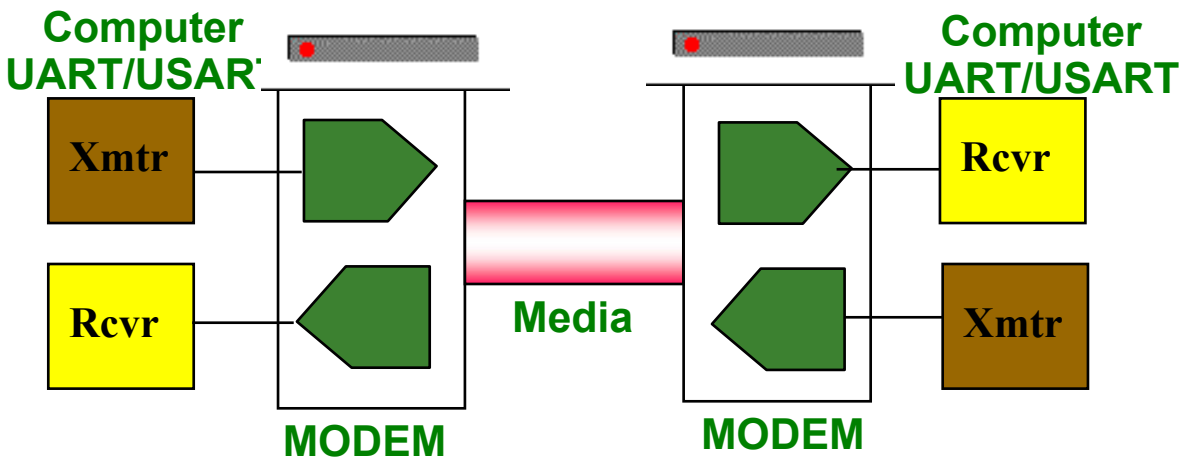


Wide-area technologies

- Public telephone
  - High performance modems
    - V.34(E)
  - High performance lines
    - T1, ISDN, xDSL,etc.
  - Wireless technologies
    - Cellular
    - PCS & CDPD
- Private telecom
  - Microwave based
  - Fiber Based (SONET)
- Internet
- Cable TV
  - Baseband/Broadband
- Satellite
  - Base station
  - Telephone
  - Pager
- Radio
  - Licensed
    - MAS radios
  - Unlicensed
    - Spread Spectrum
    - Very low power
    - Packet/CDPD

EnerNex CORPORATION

Communication Technologies



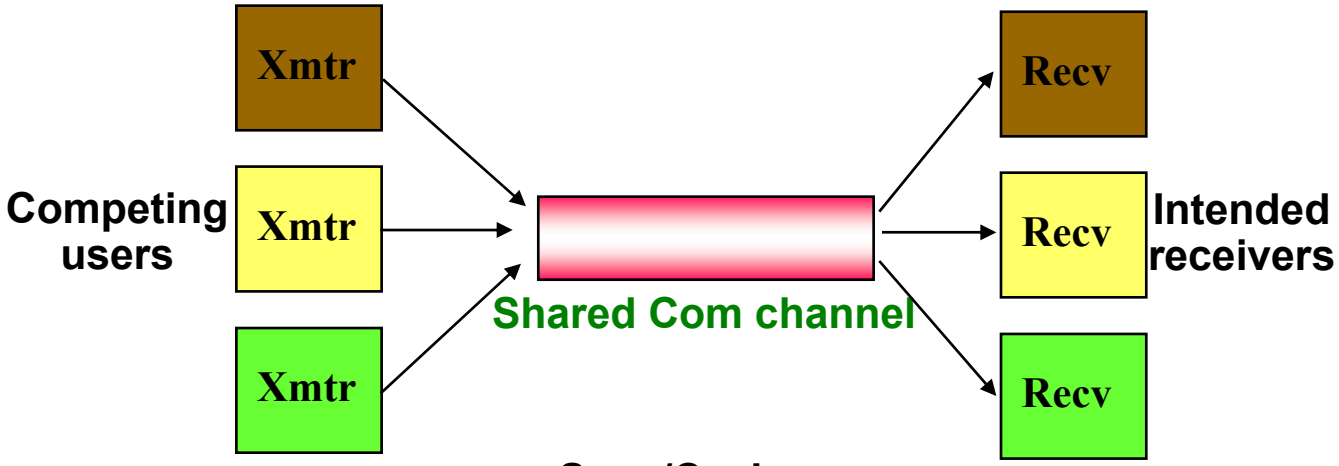
MO Modulator
DEM Demodulator

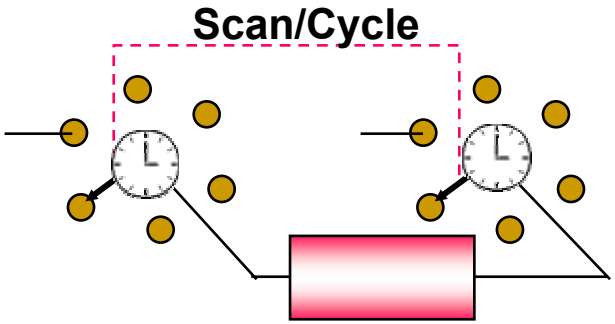
Wire/metallic cable	Modulated voltage/current signal
Telephone circuit	Audio signal within band of channel
Electromagnetic radiation	Modulated radio signal
Fiber Optic cable	Modulated Light source
Coax cable	Modulated radio signal
Infrared light	Modulated light source

Beyond basic Mo&Dem function, modern modems do encoding, line compensation, data compression and even data encryption functions !

Communication Technologies

Channel Sharing (Multiplexing)





Time-division multiplexing TDM

Occasional use of whole channel

This is how the Modern (FO) telephone system works

Frequency-division multiplexing FDM

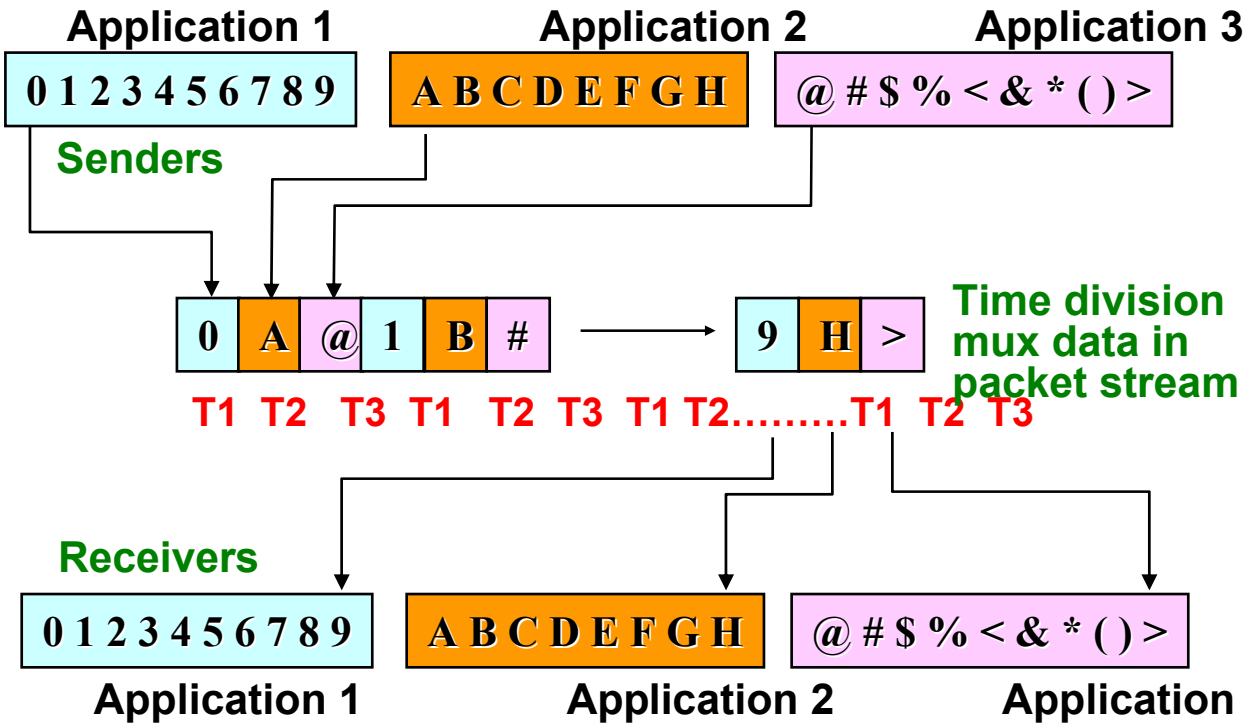
Continuous use of fractional channel

This is how radio and TV work…

EnerNex CORPORATION

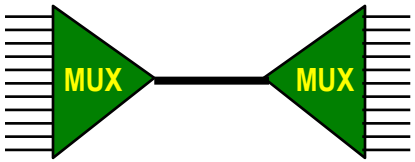
Communication Technologies

Channel Sharing (Multiplexing)



Time Division Multiplexing (TDM) is the most common way in which digital signals are put across a shared channel..

Time division MUX makes it seem as if separate channels are available ….



Frequency-division multiplexing is how TV and Radio work…separate “channels” (frequency bands) for each pair of communicating tasks...

Protocols

Protocols enable inter-computer communications

They define:

- How to establish/end communications
- Who manages the communications
- How to direct/route messages
- How data is represented/protected
- Performance mechanisms
- The types of data supported
- Supported “commands”
- How to detect errors
- How to recover from errors

Protocols

- **How to establish/end communications**
  - Special messages, Sync codes
  - Master must initiate
  - Anyone may initiate if channel is idle (CSMA/CD)
  - Token passing
- **Who manages the communications**
  - Centralized, distributed (peer),Master-Slave
- **How to direct/route messages**
  - ISO/OSI type architecture
  - Packet header information, Datagrams
- **How data is represented/protected**
  - ASCII, Binary, Packed, Encrypted
  - CRC-codes, checksums
  - Special error-detecting codes

Protocols

- **The types of data supported**
  - Integers, floats, text, IEEE, Unicode, time/date
  - Data structures (compound)
  - Arrays, vectors, files
  - Executable program code
- **Supported “commands”**
  - Protocol management
  - Computer OS (i.e. set time, run task, etc.)
  - Special purpose (RTU style i.e. Close contact)
- **How to detect errors**
  - Violation of protocol “rules”
  - CRC error
  - Invalid codes, IDs, command
  - Hardware faults
  - Timeout counters

Protocols

- **How to recover from errors**
  - ‘Fix’ correctable errors
  - Retry ‘packet’
  - Retry of message
  - Re-initialize communications
- **Performance mechanisms**
  - Priority assignments
  - Bandwidth allocation
  - ‘Slot’ allocation
  - Packet size limits
  - Virtual circuit switching
  - Best path optimization

Human-Human Protocol

Via telephone

Caller:
Hello, is this Mr. X ?

Answerer:
Hello, yes this is X.

Caller:
Great, do you have a minute?

Answerer:
Sure, what do you want?

Caller:
I sell Insurance

…etc….
…etc….

Caller:
Well, that’s all I wanted to say

Answerer:
Thanks, fine, Goodbye

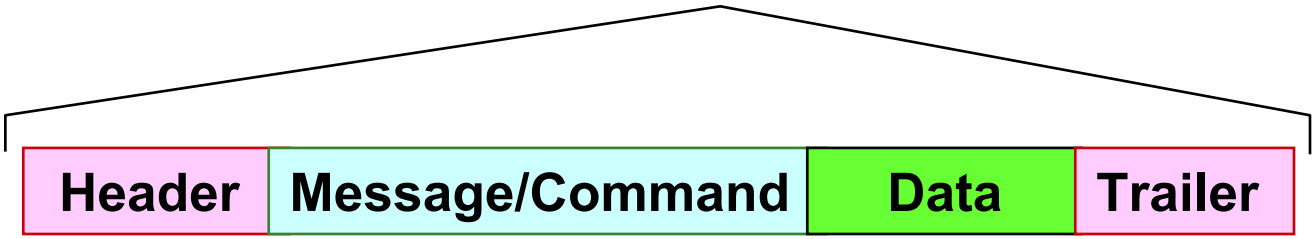
Caller:
Hey, can I call you again ?

Answerer:
No, thanks anyway.

Caller:
Oh, well, goodbye then.

Protocols

Message Packet (Typical)



- •Syncs
- •Source ID
- •Destination ID
- •Priority
- •Etc.

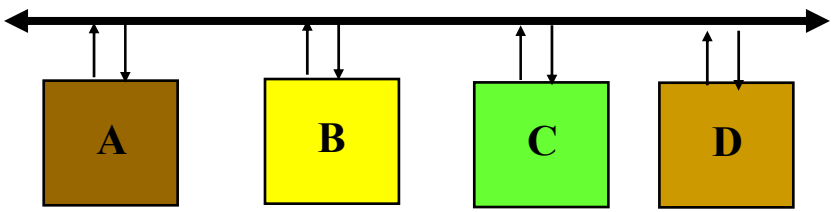
- •Message type
- •Size
- •Codes
- •Authority
- •Etc.

Data used to perform the command (if needed) May be very large and have internal CRCs.

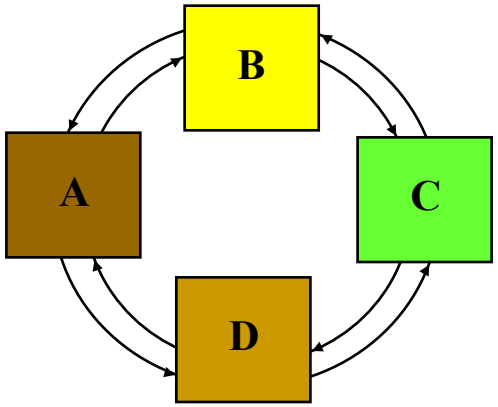
- •Packet CRC
- •Token

- •Protocol message structures can vary widely based on their specialization and performance requirements.
- •Architecture impacts protocol message complexity.

Network Architectures

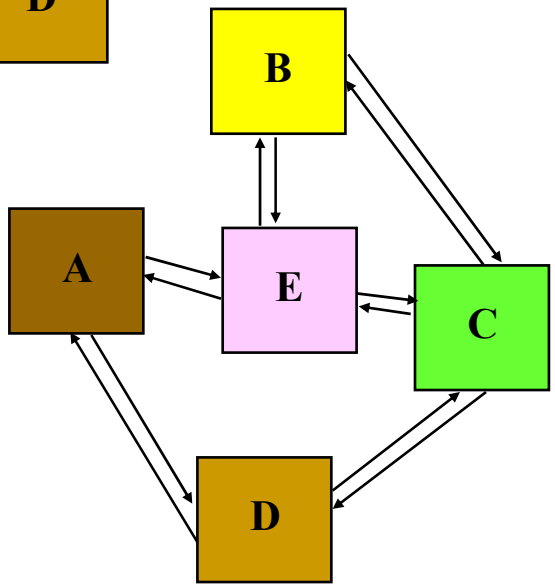


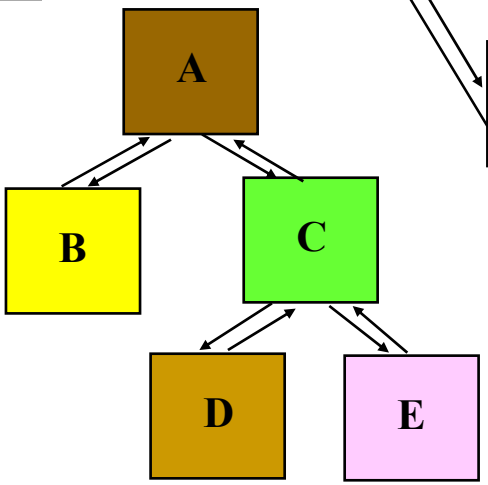
Bus Architecture



Ring or dual, counter-rotating "self-healing" rings

Web or mesh Architecture





Tree Architecture (extended star)

Local-Area Technologies

ETHERNET variations

- 10/100/1000 cable/fiber
- FDDI
- ATM Switches
- Frame-Relay
- 802.11 Wireless

Vendor-Specific

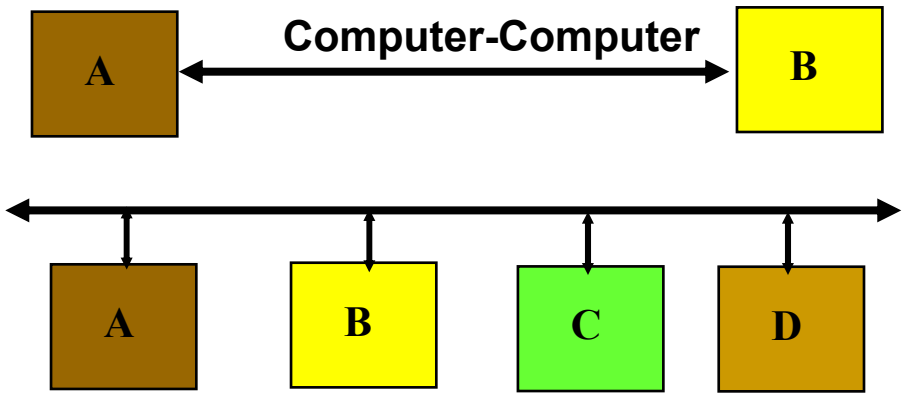
- IBM Token Ring
- Novell Net
- DECNet/ETHERNET

Specialty Networks

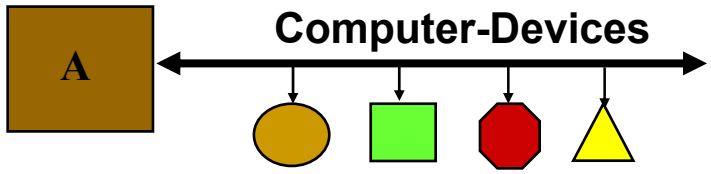
- Echelon/LONtalk
- Profibus
- Modbus+
- WorldFIPS/Fieldbus
- FiberChannel
- FireWire
- SCSI

Hybrid Networks (LAN & WAN) are very commonplace.

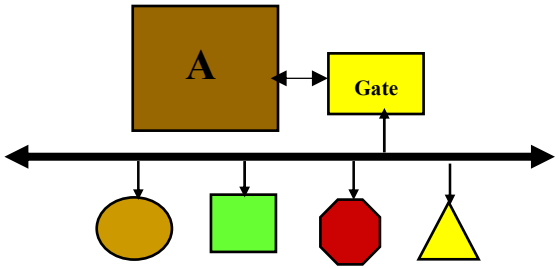
LAN Types



Computers-Computers



Devices-Devices/w Computer gateway

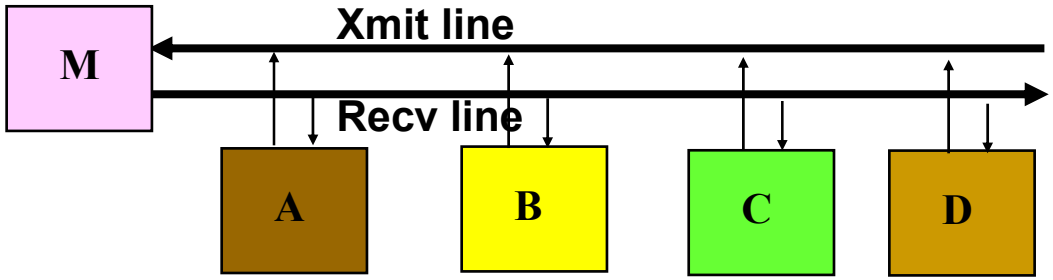


Local-Area Technologies

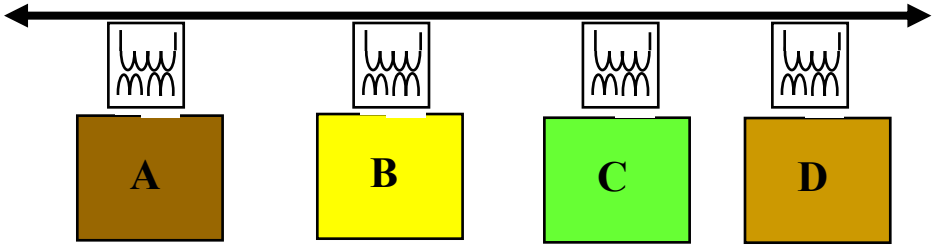
- ETHERNET variations
  - 10/100 cable/fiber
  - FDDI
  - ATM Switches
  - BOD Switches
  - 802.11 Wireless
- Vendor-Specific
  - IBM Token Ring
  - Novell Net
- Specialty Networks
  - Echelon/LONtalk
  - Profibus
  - Modbus+
  - WorldFIPS/Fieldbus
  - FiberChannel
  - FireWire
  - SCSI

LAN's are used in limited geographic areas and generally provide high band-width interconnection among / between nodes.

LAN Types



Some bus architectures require a "master" that acts as a switch-board. No peer-to-peer possible since only master can hear and talk to others.



A peer-to-peer bus mixes Xmt & Rcv so all hear all messages and can talk to each other. A Party-line style communications scheme. Access control vital..

LAN Types

3.7 LAN Standards

In the beginning, every computer manufacturer invented their own proprietary LANs. The development of standards enable multiple vendors to make equipment which can be interconnected.

A Local Area Network "standard" (such as IEEE 802.3 ETHERNET) defines a range of items:

- **The electrical characteristics of the physical media**
- **The signaling and media access control mechanisms**
- **The physical connectors/plugs used (mechanical specs)**
- **The link-layer protocol used for message exchanges**
- **The basic data format representations**
- **The protocol specifications for the "Network" layer interface**

LAN Standards

General-Purpose LANs

- IEEE 802.3 Ethernet
- IEEE 802.4 Token Bus
- IEEE 802.5 Token Ring
- Frame-Relay
- "X.25" Packet Switches
- ATM
- FDDI (X3T9.5)

Normally used for computer-to-computer communications:

- Data of all sizes and types
- Very flexible configurations
- Traffic levels quite variable
- Interface costs mid to high
- Future uses extensible
- Complex network protocol stack
- Mainly non-deterministic uses
- Huge number of nodes allowed

Special-Purpose LANs

- Profibus
- Modbus+
- Datahighway+
- LONtalk/Echelon
- Interbus-S
- Fieldbus/WorldFIPS

Normally used for computer-device-device communications:

- Data sizes and types limited
- Restricted configurations
- Traffic levels low/constant
- Interface costs low to mid
- Simple network protocol stack
- Mainly deterministic uses
- Limited number of nodes allowed

Special-purpose / Proprietery LAN's

- LONtalk/Echelon
- Modbus+

Simple protocol, can be used for many purposes, low-cost interface, low to moderate bandwidth, flexible topology, can be deterministic, WAN extensions supported.

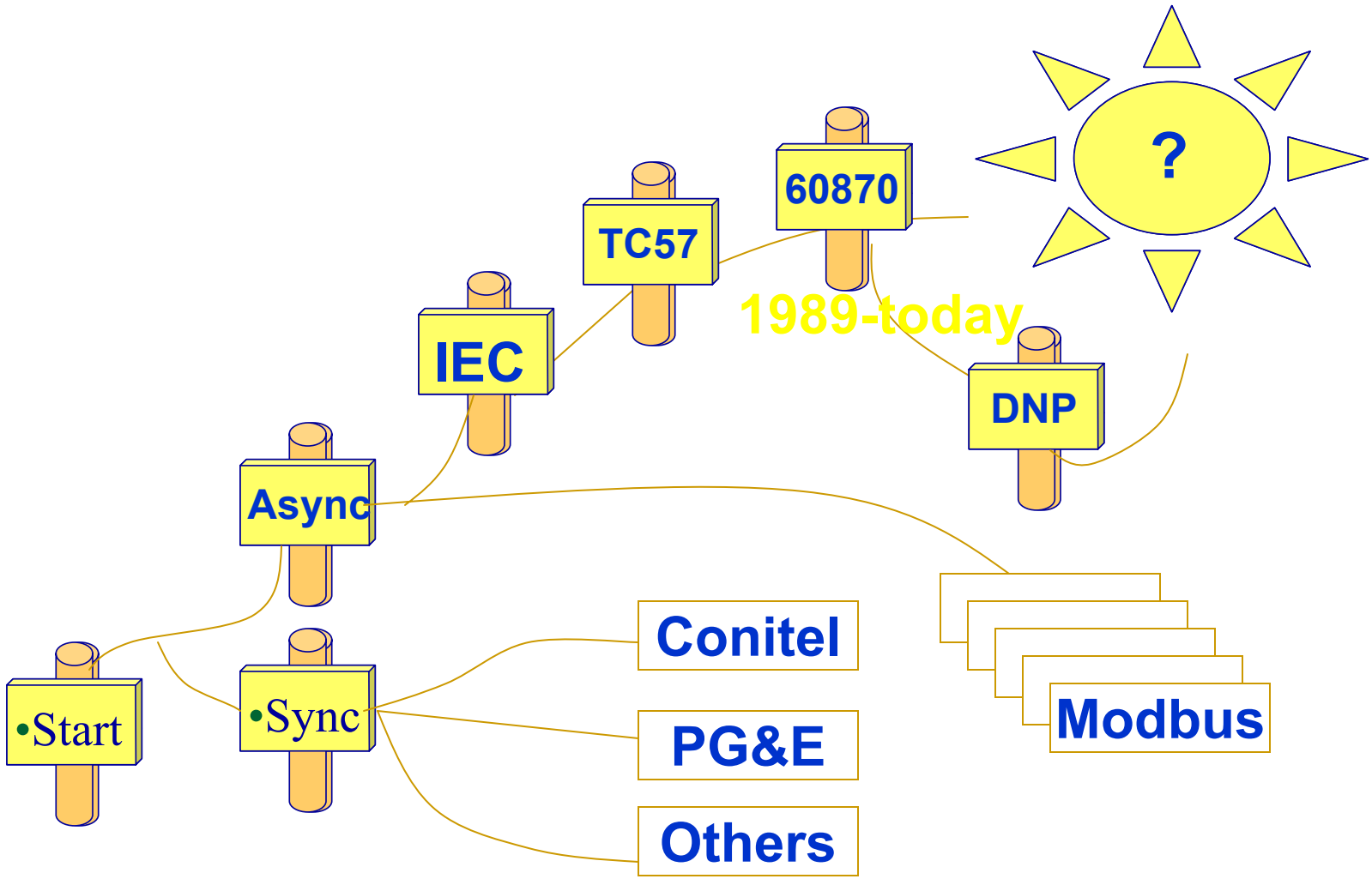
- Profibus
- Interbus-S
- Fieldbus/WorldFIPS
- Datahighway+
- DeviceNet

Generally out of the PLC world and discrete manufacturing applications. For connecting I/O and sensors to PLCs and for inter-PLC and computer data exchange.

- FiberChannel
- SCSI
- FireWire

Intended for connecting peripheral devices to computers. Not general purpose use. High bandwidth, short distances only.

Telecontrol History



Cause and Effect

- Cause
  - Noisy communication channels
  - Low Bandwidth
  - Digital controls in early days
- Effect
  - Protocol check back was mandatory
  - Bit/byte efficiency
  - Small footprints required.

Progression of Initial Technology

- Analog Tones Used (ON/OFF)
- Synchronous Links Used
  - Ability to detect drop-out by receiver of message
- Asynchronous Links Used as digital controls started to be deployed.

SCADA PROTOCOLS

- AEP
- BE-TAC SDLC
- CDC 44-500 TYPE I
- CDC 44-550 TYPE II
- CONITEL 2000
- CONITEL 2100
- CONITEL 2020
- CONITEL 3000
- CONITEL 300
- DNP 3.0
- ESCA MPS 9000S
- FERRANTI VAN-COMM
- GE-TAC 7020 LP
- GE/BE-TAC 7020/4 BCH
- HARRIS 5000
- HARRIS 5500
- HARRIS 6000
- L&G MPS 9000S
- L&G 8979
- L&N NORTHERN STATES POWER
- MODBUS (RTU)
- PG&E 2179
- ICCP /TASE.2
- UCA 2.0 / MMS
- IEC 61850

SCADA PROTOCOLS cont.

- REDAC 70H
- REDAC 80
- ROCKWELL 5010
- SCOM 11.1
- SNW SCOM 111
- SNW SCOM DISTRIBUTION
- SOUTHERN SERVICES SYSTEMS CONTROL 1801
- TLC 11M
- TEJAS SERIES III
- TEJAS SERIES V
- TRW 8000
- TRW 9550
- TRW S9000

And many, many more !

SUBMASTER PROTOCOLS

- CDC 44-500 TYPE I
- GE-TAC 7020 LP
- MODBUS (RTU)
- REDAC 70H
- TEJAS SERIES III
- CONITEL 2020
- GE/BE-TAC 7020/4 BCH
- PG&E
- SNW SCOM 111
- TEJAS SERIES V

IED Protocols

- ABB IMPRS
- ABB MDAR RELAY
- ABB DPU and TPU RELAYS
- COOPER DEVICES (2179 PROTOCOL)
- DNP
- EMS-MAX 1
- POWER MEASUREMENTS ACM 3300 METER
- POWER MEASUREMENTS ACM 3710 METER
- POWER MEASUREMENTS ACM 3720 METER (MODBUS)
- ELECTRO INDUSTRIES DMMS 200 METER
- ELECTRO INDUSTRIES DTAA5 & DTVA 120 METERS
- MODBUS RTU
- QUANTUM 200 METER

IED Protocols cont.

- SCIENTIFIC COLUMBUS JEM I
- SCIENTIFIC COLUMBUS JEM II
- SEL-121 RELAY INTERFACE
- SEL-221 RELAY INTERFACE
- SEL-251 RELAY INTERFACE
- SEL-321 RELAY INTERFACE
- SEL-2020 INTERFACE (MODBUS)
- TRANSDATA MARK V METER
- SIEMENS QUAD-4 METER
- IEC 61850, IEC 61870

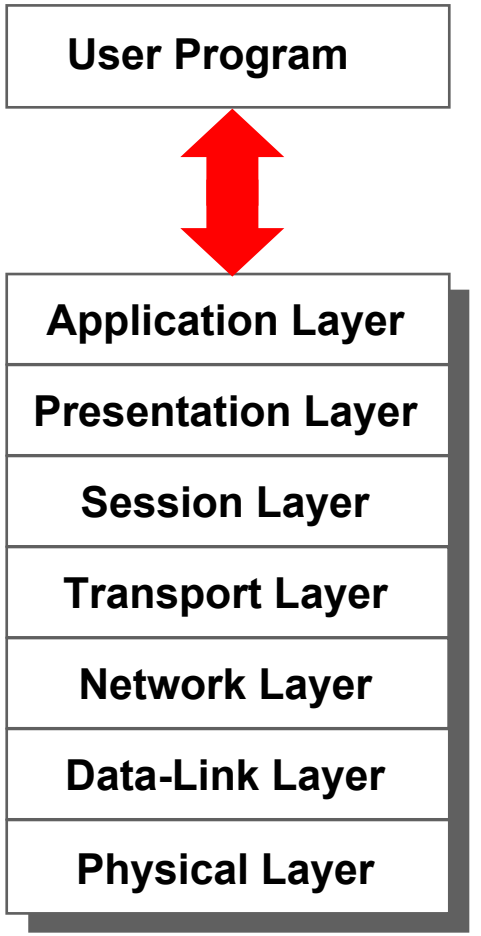
And many, many more !

Modern Communication Concepts

- OSI Model
- Object Models
- Abstract Services

The OSI Reference Model

- The Open Systems Interconnection (OSI) Reference Model is the accepted standard for evaluating and comparing different networking solutions.
- The OSI Model defines seven layers, each with specific functions to support communications between computer systems independent of the vendor.
- A user program accesses network services through the Application Layer with services designed to support the required application.



Benefits of the OSI Model

- The OSI Model provides a foundation and standard set of terms to discuss “network architectures”
- The OSI Model can help clarify and define requirements for specific solutions
- Solutions built consistent with the model can be more easily adapted to address a range of specific requirements

Advantages of Standards

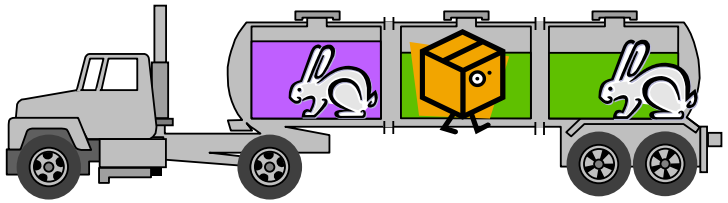
- Using standards, you focus resources on product functions instead of communications services.
- Standards can open closed shops (closed due to an installed proprietary communications solution).
- Using standards, you can leverage commercial products (routers, repeaters, etc....).
- Examples of the leverage of standards:
  - Sun Microsystems leveraged UNIX and TCP/IP.
  - Cisco Systems leveraged Internetwork Protocol.
  - 3Com and Novell leveraged the Ethernet.

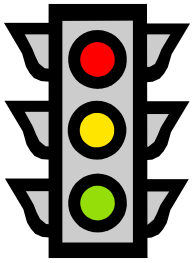
Object Modeling

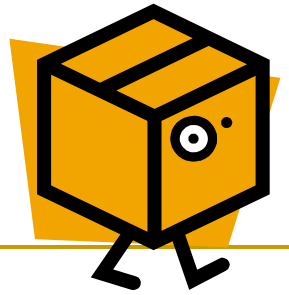
- Object modeling technology has developed within the last few years to become well-established as the most effective method for managing information exchanges.
- Object models for the exchange of information within substations have moved through the standardization process, and are now formally designated as the IEC 61850 International Standard.
- Many of the components of this standard can be reused for object models of other types of devices. Some new components are also needed, but these can follow the rules for creating these new components, thus making them compatible with the existing IEC 61850 standards.

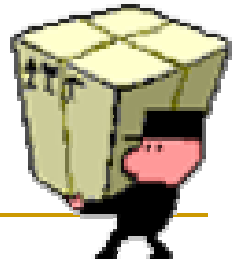
Decomposition of Communication Protocols

- Configuration
  - The roadway
- Transport Profile
  - The vehicle
- Application Profile
  - The rules of the road – verbs
- Object Definitions
  - The objects in the vehicle transported along the roadway according to the rules of the road - nouns



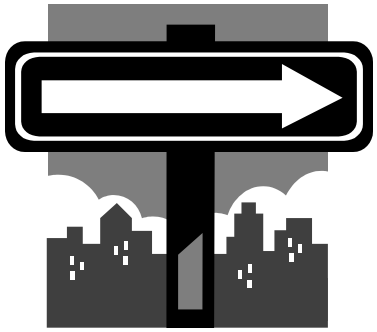


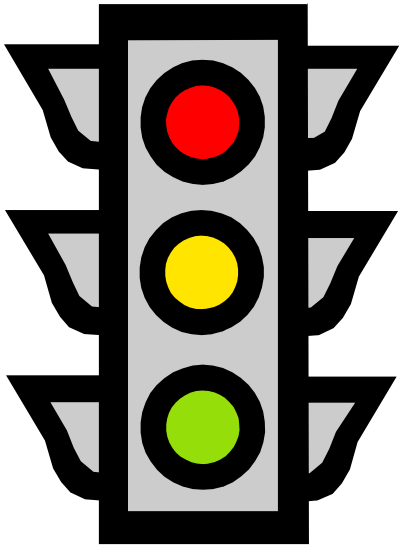




Application Profiles - Verbs

- Rules of the Road: How and When: Verbs
  - Common Application Services Model (CASM)
  - DNP's Application Services
  - Client/Server
  - Publish/Subscribe





Data Objects - Nouns

- Simple, traditional, plain vanilla “objects”
  - Status values
  - Analog values
  - Control points
- Object Models of different flavors
  - Recloser
  - Breaker
  - Voltage regulator
  - LTC Controller
  - Wind Turbine

Process for Developing New Standards

- All communications requirements must reflect the varied ***functional requirements of the domain where communications technology is being applied***
- IEC 61850 has developed many concepts which should be used:
  - Naming conventions
  - Logical Nodes (LN)
  - Common Data Classes (CDC)
- IEC 61850 has specified many components which are directly reusable, extendable, or can act as templates for new components

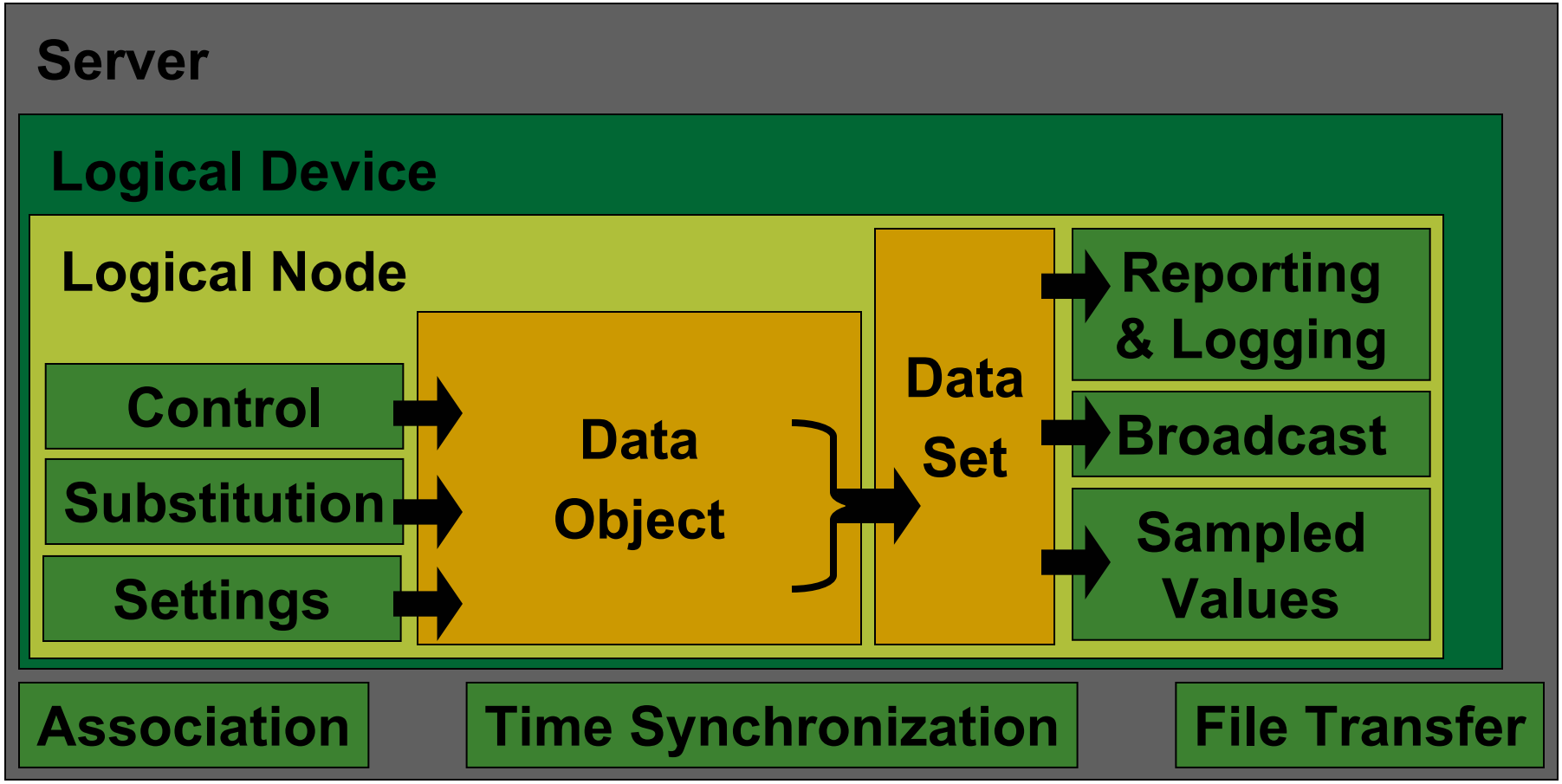
Abstract Services

- Defines services and parameters
- Defines how to build logical devices out of logical nodes
- Defines how to organize data objects derived from logical nodes

Abstract Service Models

- Server
- Association
- Logical Device
- Logical Node
- Data Object
- Data Set
- Broadcast Messages
- Reporting and Logging
- Control Model
- Substitution Model
- Sampled Values
- Time Synch
- File Transfer

Abstract Communication Service Interface (ACSI Model)



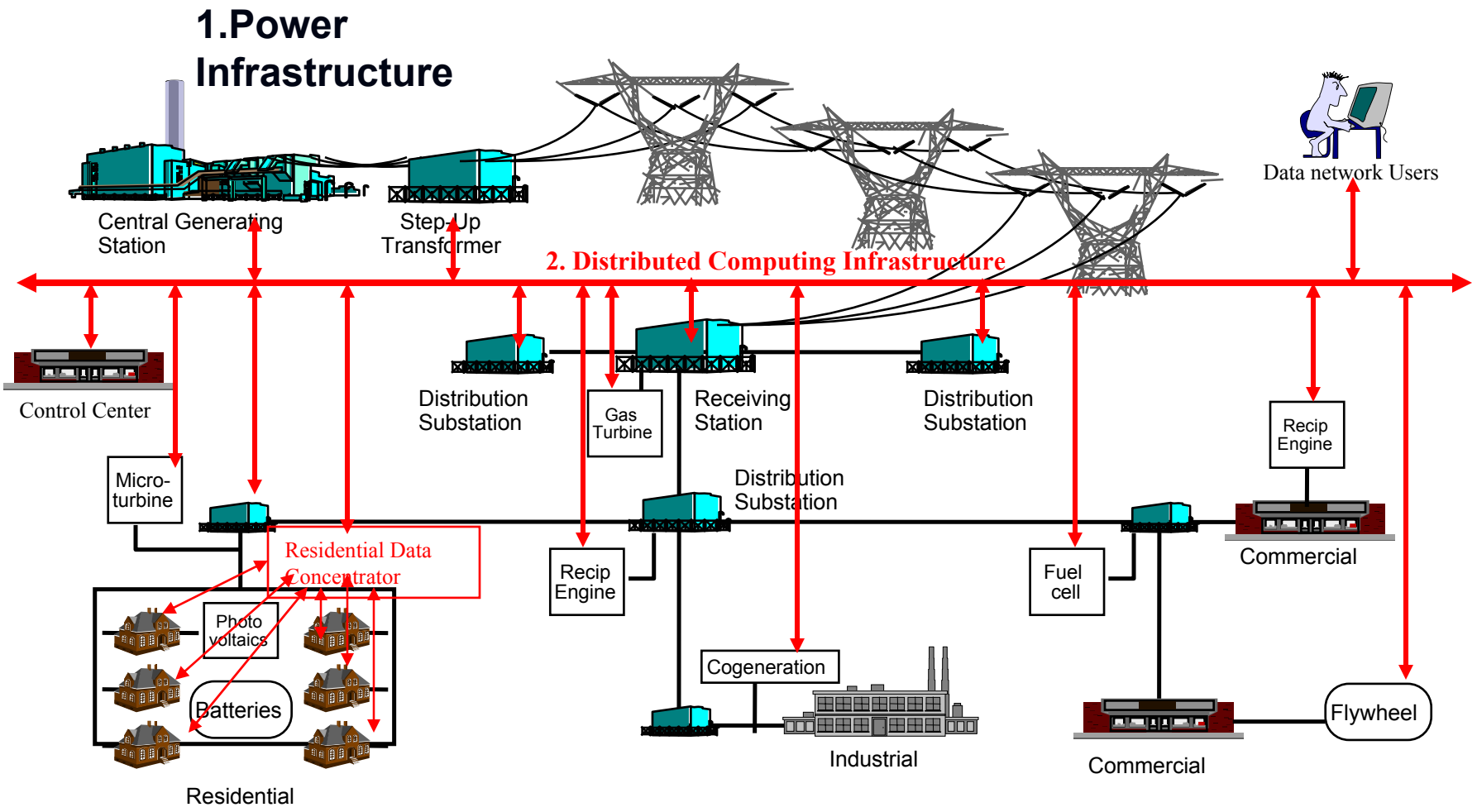
Data Objects

- Represent data within a logical node
  - voltage, current, relay settings. etc.
- Aggregate attributes of defined types
  - measurements, status, controls, configuration, etc.
- have independent access control
- have standardized names, types

Data Sets

- Comprised of references to data objects, accessed with a single name
- May be predefined or dynamic
- may be interrogated by client

Two Infrastructures, Not Just One….



EnerNex CORPORATION