Introduction to Data Communications and Networking for Utility Computing and Control

Carl Hauser
Washington State University

hauser@eecs.wsu.edu

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Funded by the U.S. Department of Energy and the U.S. Department of Homeland Security | cred-c.org

Outline

- Part I: Basic concepts
- Part II: Internet Architecture and Protocols
- Part III: Networks in Utilities

Some Roles of Communication and Computation in Power Grid

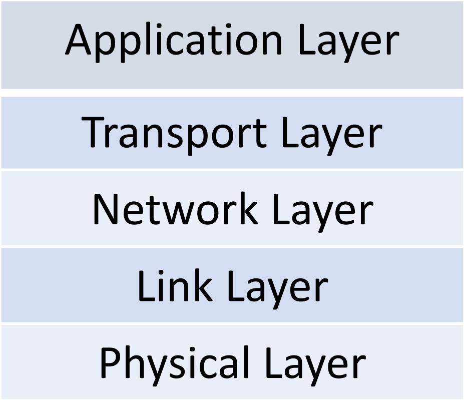
- SCADA systems, AGC example
- EMS, Data Historian
- Protection systems
- Situational awareness - ICCP
- Smart grids
  - Wide-area monitoring and control
  - Smart meters
  - Distributed generation

Part I: Basic Concepts - Performance

- Performance metrics: how much data in how much time
- Bandwidth – bits/second
- Propagation – kilometers/second (speed-of-light limited)
- Queuing – delays due to congestion
- Processing – time data spends “inside” nodes
- Latency
- Loss rates
- Different power grid applications value bandwidth, latency and loss differently

Basic Concepts - Protocols and Layering

- Protocol
  - A set of rules about messages to be sent and what to do with received messages: response messages and local *state changes*
- Layered Protocol Model



- Each protocol layer adds *message headers* to messages from the layer above: encapsulation

Encapsulation

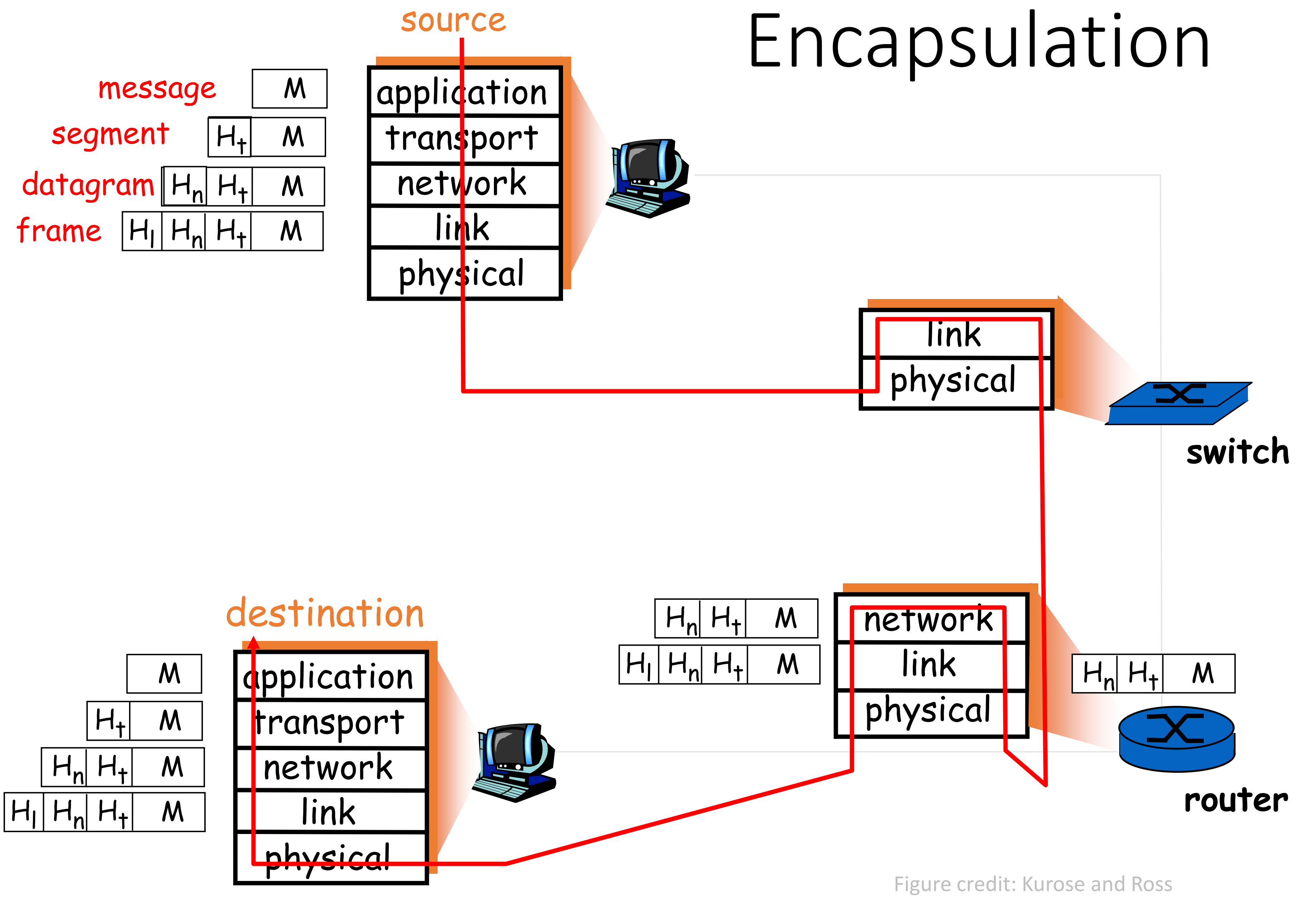


Figure credit: Kurose and Ross

The Internet Looms Large

- Historical protocols – SCADA, point-to-point, point-to-multi-point, link layer
- Internet technologies are ubiquitous, cheap, and at the forefront of cost reduction and functionality improvement technology curves
- Internet technologies bring vulnerabilities to attacks that work in business networks
- What about isolated networks using Internet Protocols?

internet vs The Internet vs Internet Protocols

- internet - network of networks – a concept
- Internet Protocols – a particular set of protocols for internetworking
- The Internet – the world-wide network providing universal connectivity using Internet Protocols
- Private internets – internetworks typically using Internet Protocols but not (intended to be) connected to The Internet
- Virtual Private Networks (VPNs) – use *encapsulation* and *encryption* to create a private internet using The Internet as the link layer of its links

Part II: Internet Architecture and Protocols

- “The Internet” as a thing
  - Hardware: hosts, links, routers
  - Businesses: service providers at local, regional, national and international scales
  - Fundamental service: deliver messages from one host to another, anywhere in the world – the purpose of *the* Internet Protocol (IP)
    - Messages may be *lost,* or delivered *out of order*

IP: fundamental concepts

- Service model:
  - best effort: messages may be lost
  - or reordered
  - Works better if neither happens, but both occur
- Addresses
  - IP addresses are 32 bits, written in *dotted quad* notation
    - 69.166.48.65
  - Addresses are divided into network/host parts:
    - 69.166.48.0 is the network address above
    - 65 is the host address on that network
    - Boundary between network/host is configurable
  - Notice we have said nothing about what kind of network: ethernets, wireless, serial, optical or other link/physical technologies; IP *abstracts* from all of these
- IPv6

IP Routing

- Per-packet router behavior - *forwarding*
  - For each received packet
    - Look up the destination network address in the *forwarding table*
    - Forward the packet on the indicated link
- Long-term router behavior - *routing*
  - Develop a forwarding table that sends packets along short paths toward the destination network while complying with administrative decisions (*I don't want to carry competitor's traffic!)*

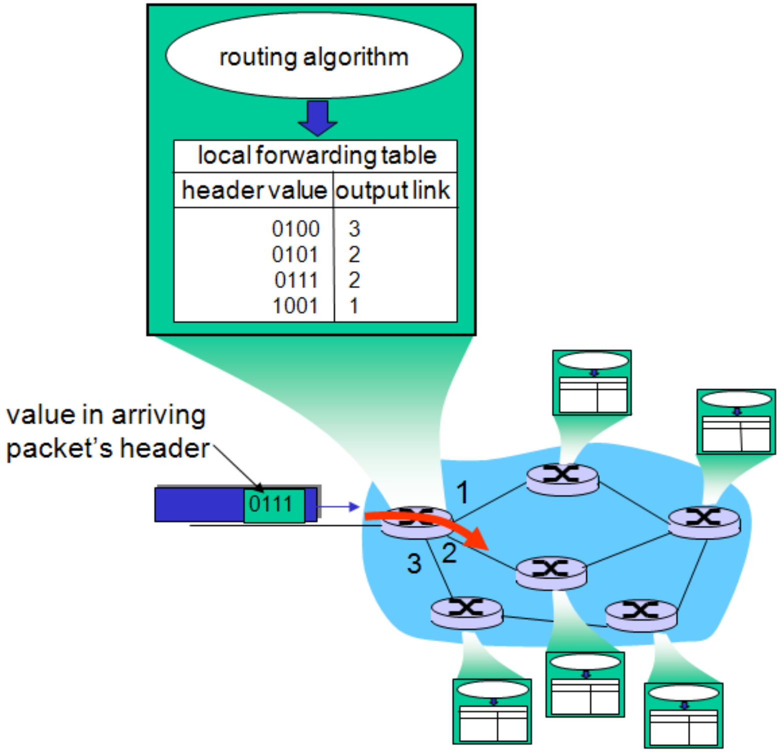


Figure credit: Kurose and Ross

IPv6

- Currently using IP version 4
  - Major problem: not enough 32 bit addresses
  - Minor problems: design decisions made in days when 1Mbyte was a LOT of storage for a computer to have
- IP version 6 has been in the works for 15+ years
  - Not easy to switch
  - Major change: 128 bit addresses
  - Minor changes: fragmentation, checksums, encapsulation technique

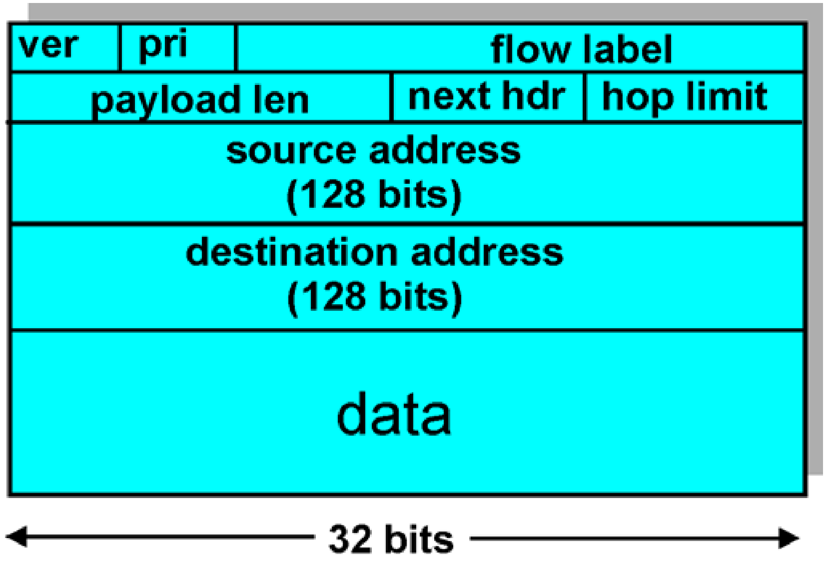


Figure credit: Kurose and Ross

Going down the stack: link layer

- The Internet and its protocols emerged in the late 1970's/early 1980's from
  - ARPAnet
  - Growing need to connect isolated local area networks owned by businesses, universities and research centers
    - Ethernet (and to lesser extent Token Ring) networks were pretty cheap and easy to build so began to appear in greater numbers
    - DEC, Xerox, and IBM commercialized various proprietary internet architectures based on proprietary link layer technologies
    - University and government researchers pursued open standards leading to the Internet
      - One big advantage: agnostic about the link layer
    - ISO was simultaneously developing the OSI standards for same purpose (but with what in retrospect turns out to have been a less good process as measured by the success of the results)

Link Layer

- Ethernet is the quintessential link layer, invented in late 1970's by Robert Metcalfe
  - Today a large family of standards covering
    - Rates from 1Mbit/s to 10,000Mbit/s and more
    - Physical layers: shared coax, twisted pair, optical fiber, wireless of various kinds
  - Predominantly *switched* Ethernet
- Others
  - Token ring
  - SONET ring
  - Serial links of different kinds
  - ATM (itself a network layer as well)
  - Virtual LANs
  - Wireless
  - Tunneling

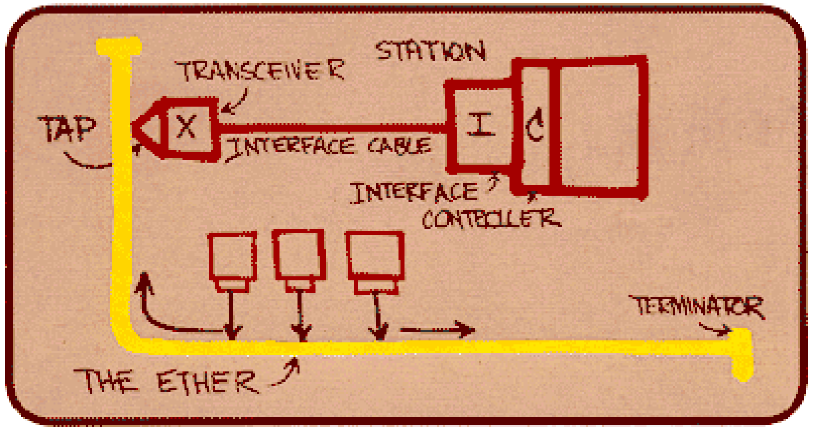


Figure credit: Kurose and Ross

Link Layer Addressing

- Link layers don't support IP addresses directly
  - IP datagrams are encapsulated in link layer *frames*
  - Link layer header (and trailer) – additional data containing link layer addresses, checksums, etc.
- Link layer addresses also called MAC (Medium Access Control) addresses
  - Typically 6 bytes; used by many but not all link layers
  - Manufactured into network interface hardware
  - Globally unique but not structured in a useful way for routing

ARP

- Address Resolution Protocol (ARP) allows determination of link layer address from IP address

```
▷ Frame 18: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
▷ Ethernet II, Src: Netgear_25:a7:b5 (74:44:01:25:a7:b5), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▽ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Netgear_25:a7:b5 (74:44:01:25:a7:b5)
    Sender IP address: 192.168.254.254 (192.168.254.254)
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.254.191 (192.168.254.191)
```

Up the stack from the network layer: the Transport Layer

- IP: deliver packets from source hosts to destination hosts
  - Best-effort delivery model: packet losses are normal events; IP provides no mechanism for reliable delivery
- We really want to move data between programs, not hosts
  - Transport layer protocols provide this functionality
  - Two primary transport layer protocols in the Internet Suite: UDP and TCP
  - TCP provides reliable delivery at the transport layer

UDP

- User Datagram Protocol
- Thin "shim" over IP – additional header contains source and destination *port* addresses
  - Idea of *port* roughly corresponds to running program on a host
  - Service model is still best effort datagram delivery, just like IP
    - Application protocol must provide reliable delivery if needed

TCP

- Transmission Control Protocol
  - Service model: bi-directional reliable byte streams – receiving applications see bytes in the order they were sent, with no gaps
    - Reliability achieved by *timeouts* and *retransmissions*
  - Sending rates controlled to avoid overrunning the receiver's ability to keep up (called *Flow Control)*
  - Sending rates controlled to avoid loss due to *network congestion*
  - Cost of the above: connection setup time; delivery delays when recovering from lost packets

Comparing UDP and TCP

UDP	TCP
Self-contained datagrams (messages)	Datagrams are part of larger byte stream
Unreliable	Reliable
Send immediately	Round-trip setup req'd before first data sent
Send immediately	Data may be delayed while prior data loss is dealt with

Naming: DNS

- Domain Name Service Protocol
  - Convenience
    - www.tcipg.org vs. 130.126.112.3
  - Indirection ("many problems in Computer Science can be solved with another level of indirection")
    - www.tcipg.org is currently an alias for drupal.engineering.illinois.edu, but this can be changed behind the scenes without affecting our web users
  - Another potential point of vulnerability

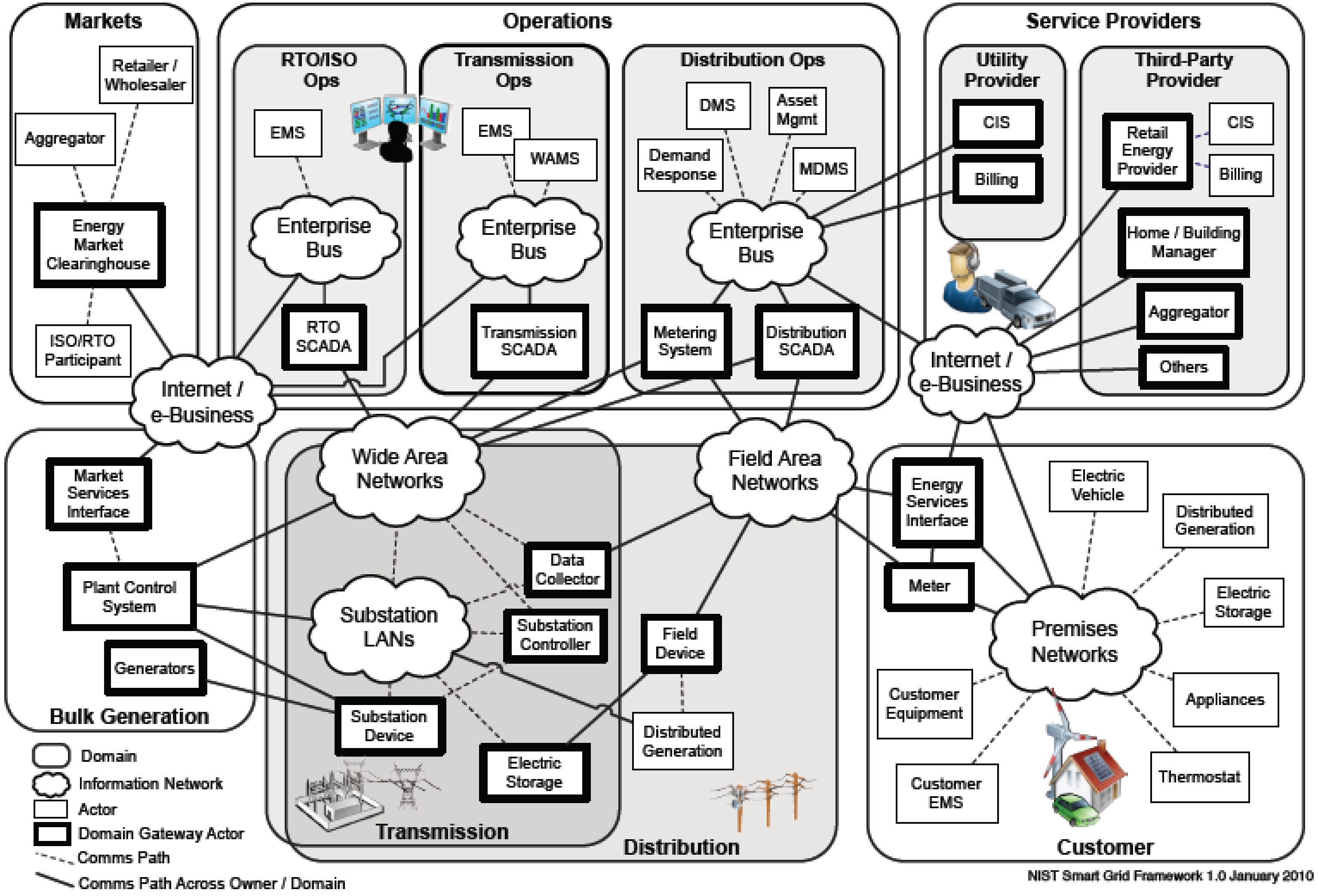
Part III: Networks in Utilities

- Substation
- Wide-area
- Control Center
- Business
- AMI
- Protocols
  - DNP3 -- SCADA
  - C37.118 -- Synchrophasors
  - IEC 61850 – Substations; interesting real-time requirements
  - ICCP – sharing data between control centers
  - Market protocols

Conventional Control Center Communications

- Limited internal and external connectivity
- Within CC: Energy Management System (EMS)
  - Historian
  - HMI stations
  - Control applications (e.g. AGC)
  - Market applications
  - Interface to SCADA system
- Outside of CC:
  - SCADA to control area substations
  - Links to neighboring control centers
  - Links to market systems

Where we're headed



Source: NIST Smart Grid Framework and Roadmap, Conceptual Reference Diagram, January 2010

Firewalls, DMZs, IDSs and all that

- IP protocols invented for friendly, collaborative environment
- Many opportunities for mis-use
- Firewalls – attempt to keep unwanted traffic out of a network
- Intrusion Detection Systems – attempt to find unwanted traffic inside a system
- DeMilitarized Zone networks – boundaries that limit desirable traffic's occurrence on different networks

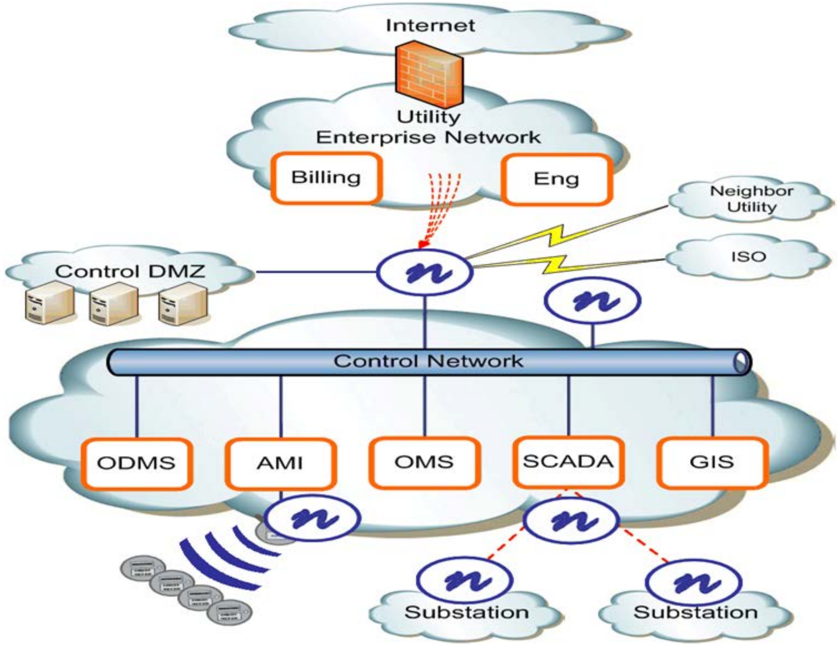


Figure credit: Andrew Wright

Trends in Control Systems Computing Devices

- Ongoing transition to commodity hardware, programming languages and operating systems
  - Started in Control Center systems
  - Now reaching down to *embedded* computers
    - Previously, 4-, 8-, or 16-bit microcomputers running specialized real-time kernel
    - Increasingly, 32- or 64-bit general purpose computer running commodity OS (Windows, Linux), programmed in general purpose language (C, C++, C#, Java)
- Interesting security tradeoffs
  - Knowledge about vulnerabilities of specialized devices not widely known
  - Devices often have severe, undiscovered vulnerabilities (because they have not been exposed to inspections and ongoing attacks like commodity systems have)

Real-time Systems

- Bounded latency – not necessarily "really fast"
- Hard real-time systems
  - Missing a deadline is a system failure
- Soft real-time systems
  - Missed deadlines are tolerated but reduce overall system performance
- Commodity hardware, software, and networking
  - Not typically designed for hard real-time
  - Lots of soft real-time uses now (Internet telephony, video, etc.)
  - "Really fast" makes up for "not very predictable"

Takeaways

- Layered model important for both understanding and implementation
- Different applications require different kinds of network services (no one-size-fits-all)
- Internet protocols and The Internet provide a variety of services in a single framework
- Internet protocols abstract from details of the link and physical layers to provide universal connectivity
- The basic Internet protocols were designed without security in mind – may be both positive and negative
  - Security and universal connectivity are at odds
  - Many opportunities to exploit weaknesses as attacks
- Transition to commodity computing
  - Lowers costs and increases functionality
  - Increases exposure to commodity attacks

Questions?

Credits and Further Reading

- Kurose and Ross, "Computer Networking: A Top-Down Approach," 5th edition, Addison-Wesley, 2010. Copyright figures from lecture notes used with permission. The book is highly recommended for developing an understanding of computer networking concepts.
- Andrew Wright, TCIPG 2011 Summer School Lecture. Figures used with permission

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

http://cred-c.org

@credcresearch

facebook.com/credcresearch/

Funded by the U.S. Department of Energy and the U.S. Department of Homeland Security