

# Data-Link Layer and Management Protocols for IoT

Raj Jain  
Washington University in Saint Louis  
Saint Louis, MO 63130  
Jain@cse.wustl.edu

These slides and audio/video recordings of this class lecture are at:  
<http://www.cse.wustl.edu/~jain/cse570-21/>

**Student Questions**



- ❑ Recent Protocols for IoT
- ❑ Power Line Communication (PLC)
- ❑ HomePlug, HomePlug AV, HomePlug AV2, BPL, Netricity
- ❑ IEEE 1905.1 Management, Security, and Configuration
- ❑ Smart Cards

Note: This is part 2 of a series of class lectures on IoT.

Wireless datalink protocols are covered in CSE 574 Wireless Network Class. More protocols are covered in other parts of this series.

## Student Questions

# Recent Protocols for IoT

Session	MQTT, SMQTT, CoRE, DDS, AMQP, XMPP, CoAP, IEC, IEEE 1888, ...	<b>Security</b>	<b>Management</b>
Network	<b>Encapsulation</b> 6LoWPAN, 6TiSCH, 6Lo, Thread... <b>Routing</b> RPL, CORPL, CARP	IEEE 1888.3, TCG, Oath 2.0, SMACK, SASL, EDSA, ace, DTLS, Dice, ...	IEEE 1905, IEEE 1451, IEEE 1377, IEEE P1828, IEEE P1856
DataLink	WiFi, Bluetooth Low Energy, Z-Wave, ZigBee Smart, DECT/ULE, 3G/LTE, NFC, Weightless, HomePlug GP, 802.11ah, 802.15.4e, G.9959, WirelessHART, DASH7, ANT+, LTE-A, LoRaWAN, ISA100.11a, DigiMesh, WiMAX, ...		

## Student Questions

Ref: Tara Salman, Raj Jain, "A Survey of Protocols and Standards for Internet of Things," Advanced Computing and Communications, Vol. 1, No. 1, March 2017, [http://www.cse.wustl.edu/~jain/papers/iot\\_accs.htm](http://www.cse.wustl.edu/~jain/papers/iot_accs.htm)  
 Washington University in St. Louis <http://www.cse.wustl.edu/~jain/cse570-21/> ©2021 Raj Jain

# L2 Protocols for IoT

Most of the L2 IoT protocols are wireless.

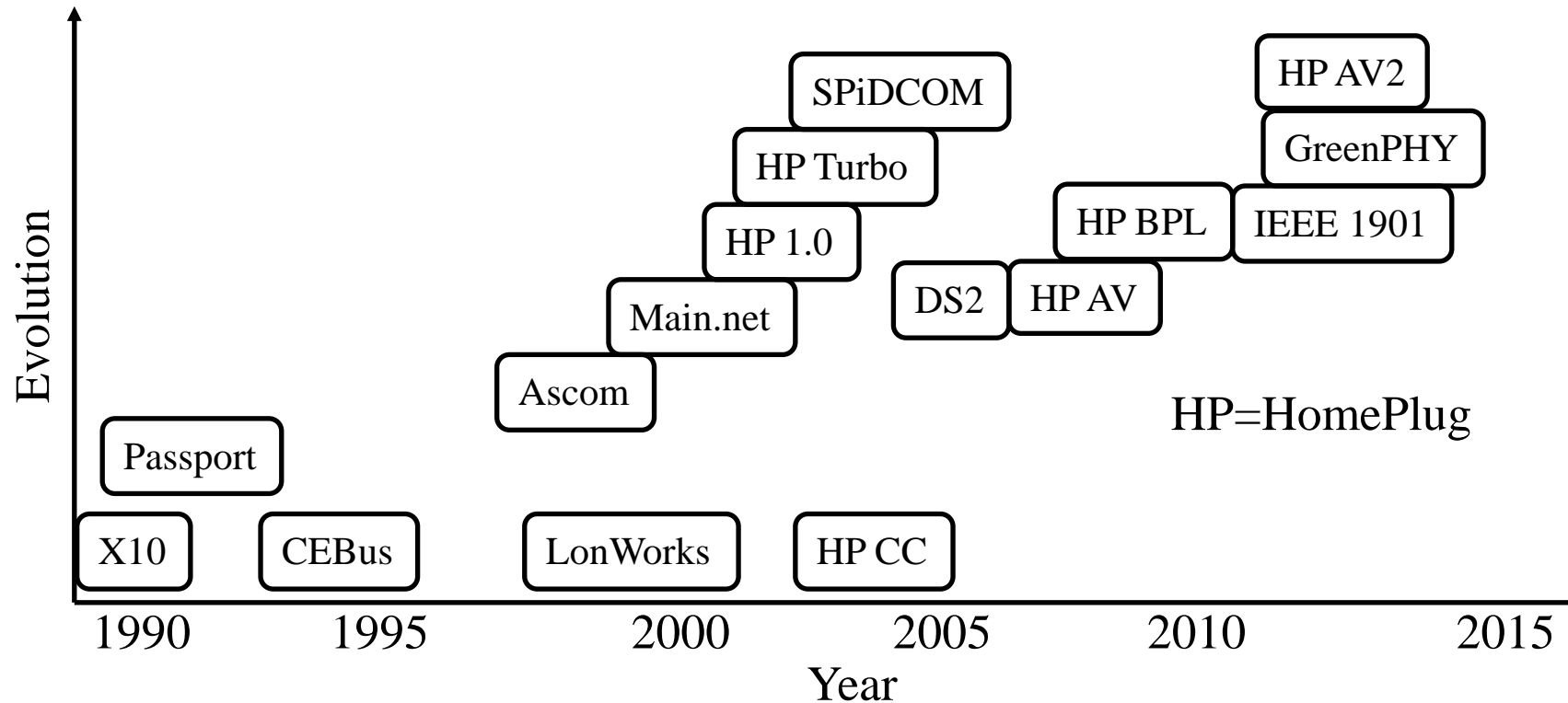
- ❑ **Wireless Protocols:** WiFi, Bluetooth Low Energy, Z-Wave, ZigBee Smart, DECT/ULE, 3G/LTE, NFC, Weightless, IEEE 802.11ah, IEEE 802.15.4, G9959, WirelessHart, DASH7, ANT+, LTE-A, LoraWAN, ISA 100.11a, DigiMesh, etc. These are covered in CSE 574 Wireless and Mobile Networking class.
- ❑ **Wired Protocols:** In this lecture, we cover Powerline Communications (HomePlug GP) and associated management protocols

## Student Questions

Ref: Raj Jain, "CSE574S: Wireless and Mobile Networking (Spring 2016)," <http://www.cse.wustl.edu/~jain/cse574-16/index.html>

# Power Line Communication (PLC)

- ❑ Started in 1950 for remote ignition and lighting of street lights. 100 Hz and 1 kHz signals over electrical wires
- ❑ Two way systems using 3-148.5 kHz for reading electric meters, and home automation, alarms etc.



## Student Questions

Ref: H. Chaouchi, "The Internet of Things: Connecting Objects," Wiley, Jun 2010, 288 pp., ISBN: 9781848211407 (Safari Book)

Washington University in St. Louis

<http://www.cse.wustl.edu/~jain/cse570-21/>

©2021 Raj Jain

# Broadband Over Power Lines (BPL)

- ❑ High-speed internet connection using power lines (like DSL)
- ❑ Also known as HomePlug-BPL.  
Incorporated in IEEE 1901-2010
- ❑ Not cost competitive with optical fiber or DSL  
⇒ Suitable only for remote locations
- ❑ High-frequency signal cannot pass through transformers and so the signal has to be bypassed using a repeater
- ❑ In US, 1 transformer per house ⇒ Very expensive  
In Europe: 1 transformer per 10-100 houses  
⇒ More cost effective
- ❑ Radio frequency interference with existing wireless services is avoided using OFDM

Ref: [http://en.wikipedia.org/wiki/Broadband\\_over\\_power\\_lines](http://en.wikipedia.org/wiki/Broadband_over_power_lines)

Washington University in St. Louis

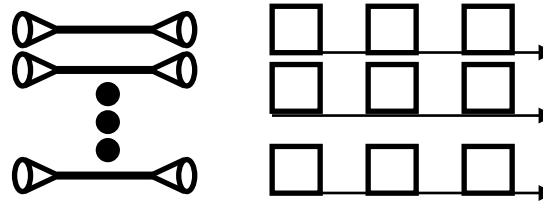
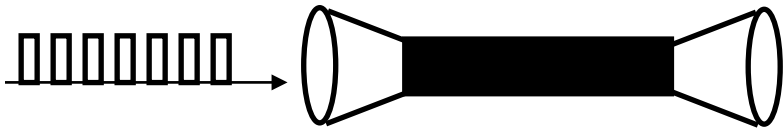
<http://www.cse.wustl.edu/~jain/cse570-21/>

©2021 Raj Jain

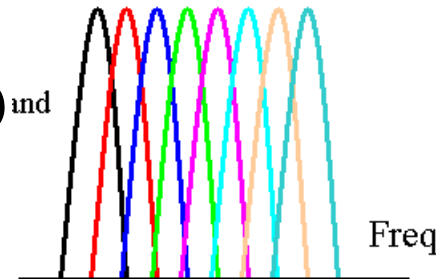
## Student Questions

# OFDM

- ❑ Orthogonal Frequency Division Multiplexing
- ❑ Ten 100 kHz channels are better than one 1 MHz Channel  
⇒ Multi-carrier modulation



- ❑ Frequency band is divided into 256 or more sub-bands.  
Orthogonal ⇒ Peak of one at null of others
- ❑ Each carrier is modulated with a **BPSK** (2bps/Hz), **QPSK** (4 bps/Hz), **16-QAM** (8bps/Hz), **64-QAM** (16 bps/Hz) etc depending on the noise (Frequency selective fading)
- ❑ Used in 802.11a/g, 802.16,  
Digital Video Broadcast handheld (DVB-H)<sub>ind</sub>
- ❑ Easy to implement using FFT/IFFT



## Student Questions

# HomePlug

- ❑ HomePlug 1.0
- ❑ HomePlug AV
- ❑ HomePlug AV2
- ❑ HomePlug GP
- ❑ HomePlug BPL



## Student Questions



# Connected Home



## Student Questions

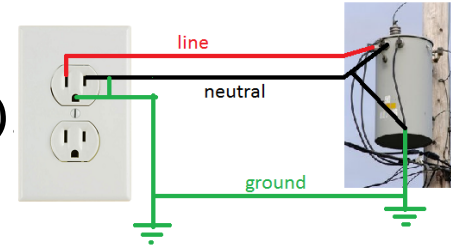
# HomePlug AV

- ❑ HomePlug Alliance: Industry consortium for power line communications Disbanded in October 2016.
- ❑ 90% of PLC devices use HomePlug
- ❑ 1.8 MHz to 30 MHz spectrum = 28 MHz  $\Rightarrow$  20 to 200 Mbps
- ❑ Multipath distortion
- ❑ **Orthogonal Frequency Division Multiplexing (OFDM):**  
Using 1155 carriers at 24.414 kHz spacing of which 917 are used for signal.  
Rest as pilots.
- ❑ **Adaptive bit loading:** Each carrier is modulated based on the noise level and multipath at that frequency.  
2-bits/symbol to 10 bits/symbol.
- ❑ **Tone Maps:** Each receiver keeps a table of signal strengths from each of the other receivers  $\Rightarrow$  n-1 tone maps in a n-device system

## Student Questions

# HomePlug AV (Cont)

- ❑ **Robust OFDM** (ROBO) mode for highly reliable transmission. The same information is transmitted on 2-5 subcarriers using a low-bit rate modulation
- ❑ Use only Line-neutral pair (ground is not used)
- ❑ Four channel access priorities
- ❑ MAC is similar to that of WiFi  
⇒ **Carrier Sense Multiple Access (CSMA)**.
- ❑ All devices part of the same trust domain form a “**AV Logical Network** (AVLN).”
- ❑ All members of the AVLN share a Network Membership Key 128-bit AES.
- ❑ Each AVLN has a **central coordinator (CCo)**



## Student Questions

# HomePlug AV (Cont)

- ❑ CCo transmits beacons containing schedule
- ❑ Long best effort transmissions declare their queues to CCo and use a pre-allocated **persistent shared CSMA** region
- ❑ Short best effort transmissions use **non-persistent CSMA** region.
- ❑ Real-time traffic uses periodic time division multiple access (TDMA) allocation in the **contention-free** period
- ❑ Before video transmission, the transmitter tests the channel for achievable throughput. Helps determine the required transmission interval per beacon period

Beacon Region	Persistent Shared CSMA Region	Non-Persistent Local CSMA	Non-Persistent Local CSMA	Persistent Allocation 1	Persistent Allocation n
---------------	-------------------------------	---------------------------	---------------------------	-------------------------	-------------------------

## Student Questions

# HomePlug AV Security

- ❑ A station can participate in a AVLN if it has the **Network membership key (NMK)**.

A station with multiple keys can participate in multiple AVLNs.

- ❑ All devices have a default NMK and so can form the network. Users should program the devices to use specific NMK.
- ❑ Once a devices has a NMK, it will be given the **network encryption key** which is used to encrypt the data.
- ❑ If there are multiple networks on the same wire, CCoS coordinate their transmission schedules

## Student Questions

# HomePlug AV2

- ❑ Gigabit networking using home powerline wiring. Peak PHY rate of 1.256 Gbps. 600 Mbps net throughput.
- ❑ Can transmit multiple HD video streams
- ❑ Compatible with HomePlug AV devices on the same wires
- 1. **Additional Spectrum:** 2MHz-86MHz (84 MHz)
- 2. **Multiple-input Multiple-output (MIMO):** transmissions using two wires with three-wire configuration (Line-Neutral, Line-Ground, Neutral-Ground)
- 3. **Beam forming:** Bit loading for each transmitter
- 4. **Lower overhead:** Shorter packet delimiter and delay acks.
- 5. **Efficient notching:** Of noisy carriers

## Student Questions

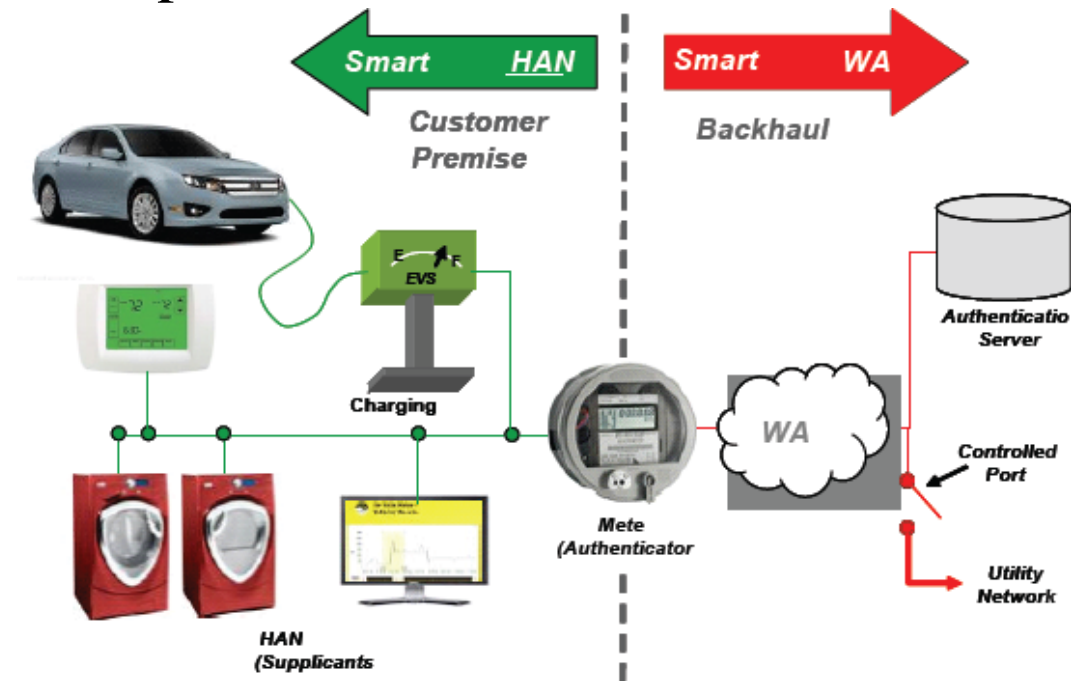
## HomePlug AV2 (Cont)

6. **Repeating**: Signal is demodulated and re-modulated at intermediate devices
7. **Better coding**: 12 bps/Hz and aggressive code rates (8/9)
8. **Power Control**: Manage transmission power to enhance coverage and throughput
9. **Power Save**: Stations can declare sleep periods. Other transmit only when the destination is awake.

### Student Questions

# HomePlug GreenPHY

- ❑ Designed for **home area network (HAN)** for monitoring and control of energy consuming/controlling devices including electric vehicle charging.
- ❑ Low cost. Low power. Low data rate version of HomePlug AV.



## Student Questions



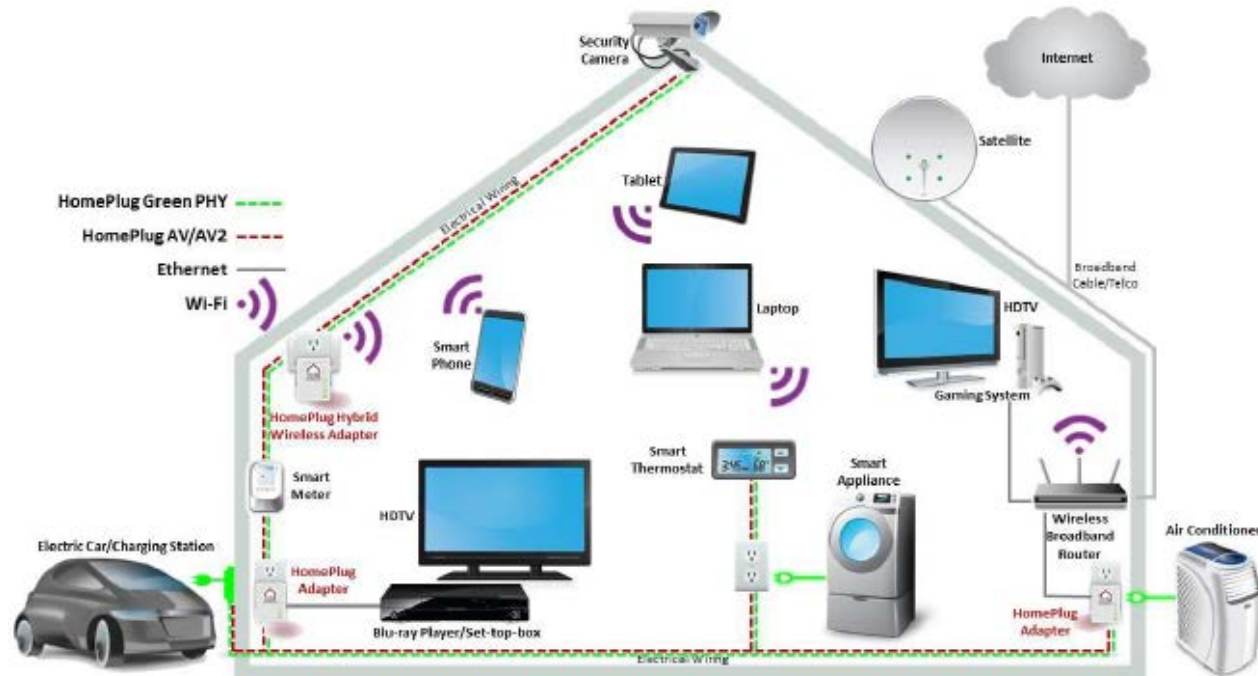
# HomePlug GP (Cont)

- ❑ HomePlug GP is a profile of **IEEE 1901-2010** standard for Powerline Networks and is compatible with HomePlug AV and HomePlug AV2.
- ❑ 28 MHz  $\Rightarrow$  256 kbps to 10 Mbps using only one modulation  
No tone maps.
- ❑ Use 75% less power than HomePlug AV.  
75% less bill of materials
- ❑ Devices coordinate their sleep cycle and may sleep for  $2^n$  beacon intervals,  $n=1,\dots,10$
- ❑ HomePlug GP 1.1 adds new power management and features for electric vehicles. Secure billing is possible at a public charging station.

## Student Questions

# Convergent Digital Home Network

- ❑ IEEE 1905.1-2013 Convergent Digital Home Network for Heterogeneous Technologies
- ❑ Combined use of WiFi, HomePlug, Ethernet, Multimedia over Coax (MoCA) in a home



## Student Questions

Ref: [http://en.wikipedia.org/wiki/IEEE\\_1905](http://en.wikipedia.org/wiki/IEEE_1905)

Washington University in St. Louis

<http://www.cse.wustl.edu/~jain/cse570-21/>

©2021 Raj Jain

# Convergent Digital Home (Cont)

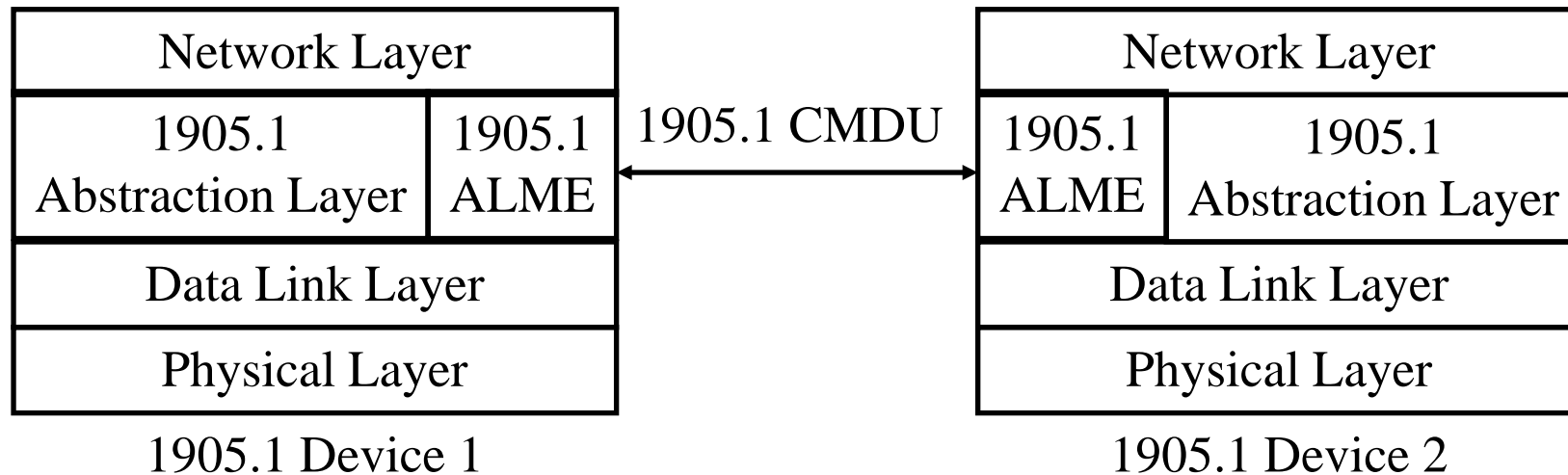
- ❑ Entire home looks like a single network with automated provisioning, management, and operation
- ❑ Allows a device to aggregate throughput from multiple interfaces
- ❑ A link can be used fallback when another link fails
- ❑ An abstraction layer is used to exchange **Control Message Data Unit (CMDU)** among 1905.1 compliant devices
- ❑ No changes to underlying technologies is required.

Network Layer			
1905.1 Abstraction Layer			
802.3	802.11	PLC 1901	MoCA

## Student Questions

# IEEE 1905.1 Management

- 1905.1 compliant devices speak Abstraction Layer Management Entity (ALME) Protocol



## Student Questions

# IEEE 1905.1 Management (Cont)

- ❑ ALME has messages for
  - Neighbor discovery,
  - Topology exchange,
  - Topology change notification,
  - Measured traffic statistics exchange,
  - Flow forwarding rules, and
  - Security associations
- ❑ HomePlug AV2 can be used as a backbone for Wi-Fi
- ❑ Existing IEEE 802.1 bridging protocols are used for loop prevention and forwarding

## Student Questions

# IEEE 1905.1 Security and Configuration

- ❑ Security Setup:
  - **Push Button**: Press buttons on new and existing devices  
The new device gets the keys from the existing device
  - User can configure **passphrase/key** in the new device
  - **NFC**: User touches the new device with a NFC equipped smart phone which is existing member of the network
- ❑ Auto configuration:
  - New Access Points (APs) can get configuration information from existing APs
- ❑ The certification program for IEEE 1905.1 is called “**nVoy**”  
Connects disparate networks = Network Diplomat = Network Envoy ⇒ nVoy
- ❑ Qualcomm Atheros products implementing IEEE 1905.1 are called **Hy-Fi** (for Hybrid Fidelity)

## Student Questions

# Netricity

- ❑ Long-range outside-the-home PLC for smart grid applications
- ❑ Certification for IEEE 1901.2 Low Frequency, Narrowband Powerline Communications Standard is called “Netricity”



## Student Questions

# Industrial Ethernet

- ❑ Same as regular Ethernet but with rugged connectors and designed for extended temperature/humidity environment
- ❑ Full duplex links (no CSMA/CD)
- ❑ Optical fibers (electrical interference)
- ❑ Min frame size of 64 byte may be too big for some applications

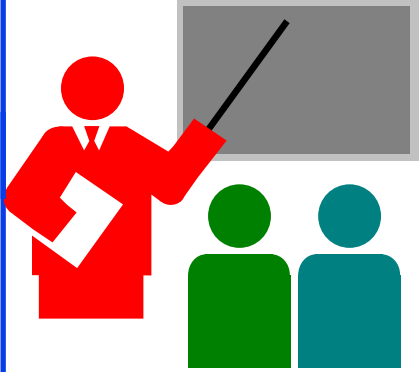
## Student Questions



# IEEE 1451

- ❑ Set of smart transducer interface for sensors and actuators
- ❑ Transducer electronic data sheets (TEDS) is a memory device that stores transducer id, calibration, correction data, and manufacturer information
- ❑ Allows access to transducer data regardless of wired or wireless connection
- ❑ XML based  $\Rightarrow$  Allows manufacturers to change the contents

## Student Questions



# Summary

1. A number of datalink protocols have been proposed for IoT. Among non-wireless protocols, the most common is HomePlug.
2. HomePlug has been extended to provided higher data rate of up to 600 Mbps by HomePlug AV2 standard and to a energy saving HomePlug GP.
3. IEEE 1905.1 provides an abstraction layer to hide the details of various datalink layers, such as, ZigBee, HomePlug, WiFi, ...

## Student Questions

# Reading List

- ❑ Tara Salman, Raj Jain, "A Survey of Protocols and Standards for Internet of Things," Advanced Computing and Communications, Vol. 1, No. 1, March 2017,  
[http://www.cse.wustl.edu/~jain/papers/iot\\_accs.htm](http://www.cse.wustl.edu/~jain/papers/iot_accs.htm)
- ❑ HomePlug Alliance, "HomePlug AV White Paper,"  
[https://www.solwise.co.uk/downloads/files/hpav-white-paper\\_050818.pdf](https://www.solwise.co.uk/downloads/files/hpav-white-paper_050818.pdf)
- ❑ HomePlug Alliance, "HomePlug AV2 Technology,"  
[https://www.codico.com/fxdata/codico/prod/media/Datenblaetter/AKT/HomePlug\\_AV2\\_whitepaper\\_20130909.pdf](https://www.codico.com/fxdata/codico/prod/media/Datenblaetter/AKT/HomePlug_AV2_whitepaper_20130909.pdf)
- ❑ HomePlug Alliance, "HomePlug GreenPHY Overview,"  
[https://www.codico.com/fxdata/codico/prod/media/Datenblaetter/AKT/HomePlug\\_Green\\_PHY\\_whitepaper\\_100614\[1\].pdf](https://www.codico.com/fxdata/codico/prod/media/Datenblaetter/AKT/HomePlug_Green_PHY_whitepaper_100614[1].pdf)

## Student Questions

# References

- ❑ H. Chaouchi, "The Internet of Things: Connecting Objects," Wiley, Jun 2010, 288 pp., ISBN: 9781848211407 (Safari Book)
- ❑ H. Zhou, "The Internet of Things in the Cloud: A middleware Perspective," CRC Press, 2013, 366pp., ISBN:9781439892992 (Safari Book)
- ❑ Dave Evans, "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything," Cisco white paper, April 2011,  
[https://www.cisco.com/c/dam/en\\_us/about/ac79/docs/innov/IoT\\_IBSG\\_0411FINAL.pdf](https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf)

## Student Questions

# Wikipedia Links

- ❑ [http://en.wikipedia.org/wiki/IEEE\\_1905](http://en.wikipedia.org/wiki/IEEE_1905)
- ❑ [http://en.wikipedia.org/wiki/IEEE\\_1901](http://en.wikipedia.org/wiki/IEEE_1901)
- ❑ [http://en.wikipedia.org/wiki/Broadband\\_over\\_power\\_lines](http://en.wikipedia.org/wiki/Broadband_over_power_lines)
- ❑ [http://en.wikipedia.org/wiki/Power\\_line\\_communication](http://en.wikipedia.org/wiki/Power_line_communication)
- ❑ <http://en.wikipedia.org/wiki/HomePlug>
- ❑ [http://en.wikipedia.org/wiki/Cyber-physical\\_system](http://en.wikipedia.org/wiki/Cyber-physical_system)
- ❑ [http://en.wikipedia.org/wiki/HomePlug\\_Powerline\\_Alliance](http://en.wikipedia.org/wiki/HomePlug_Powerline_Alliance)
- ❑ <http://en.wikipedia.org/wiki/MIMO>
- ❑ <http://en.wikipedia.org/wiki/SCADA>
- ❑ [http://en.wikipedia.org/wiki/Smart\\_grid](http://en.wikipedia.org/wiki/Smart_grid)
- ❑ <http://en.wikipedia.org/wiki/G.hn>
- ❑ [http://en.wikipedia.org/wiki/Orthogonal\\_frequency-division\\_multiplexing](http://en.wikipedia.org/wiki/Orthogonal_frequency-division_multiplexing)
- ❑ [http://en.wikipedia.org/wiki/IEEE\\_Smart\\_Grid](http://en.wikipedia.org/wiki/IEEE_Smart_Grid)
- ❑ <http://en.wikipedia.org/wiki/Fieldbus>
- ❑ [http://en.wikipedia.org/wiki/Industrial\\_Ethernet](http://en.wikipedia.org/wiki/Industrial_Ethernet)
- ❑ [http://en.wikipedia.org/wiki/IEEE\\_1451](http://en.wikipedia.org/wiki/IEEE_1451)

## Student Questions

# Wikipedia Links (Cont)

- ❑ [http://en.wikipedia.org/wiki/List\\_of\\_broadband\\_over\\_power\\_line\\_deployments](http://en.wikipedia.org/wiki/List_of_broadband_over_power_line_deployments)
- ❑ [http://en.wikipedia.org/wiki/Qualcomm\\_Atheros](http://en.wikipedia.org/wiki/Qualcomm_Atheros)
- ❑ <http://en.wikipedia.org/wiki/G.9972>
- ❑ [http://en.wikipedia.org/wiki/Home\\_network](http://en.wikipedia.org/wiki/Home_network)
- ❑ <http://en.wikipedia.org/wiki/SPiDCOM>
- ❑ [http://en.wikipedia.org/wiki/Smart\\_meter](http://en.wikipedia.org/wiki/Smart_meter)
- ❑ [http://en.wikipedia.org/wiki/IEC\\_62196](http://en.wikipedia.org/wiki/IEC_62196)

## Student Questions

# Acronyms

- ❑ 6LowPAN IPv6 over Low Power Wireless Personal Area Network
- ❑ AES Advanced Encryption
- ❑ ALME Abstraction Layer Management Entity
- ❑ AMQP Advanced Queueing Message Protocol
- ❑ AP Access Point
- ❑ AV Audio-Visual
- ❑ AVLN Audio-Visual Logical Network
- ❑ BPL Broadband Over Power Lines
- ❑ BPSK Binary Phase-Shift Keying
- ❑ CCo Central Coordinator
- ❑ CD Collision Detection
- ❑ CEBus Consumer Electronic Bus
- ❑ CMDU Control Message Data Unit
- ❑ CoAP Constrained Application Protocol
- ❑ CP Cyber Physical

## Student Questions

# Acronyms (Cont)

- ❑ CPS Cyber Physical Systems
- ❑ CSIA Cyber Security and Information Assurance
- ❑ CSMA Carrier Sense Multiple Access
- ❑ CSMA/CD Carrier Sense Multiple Access with Collision Detection
- ❑ DARPA Defense Advance Research Project Agency
- ❑ DCS DIstributed Control Systems
- ❑ DECT Digital Enchanced Cordless Telephony
- ❑ DOE Department of Energy
- ❑ DS2 Design of Systems on Silicon (name of a company)
- ❑ DSL Digital Subscriber Line
- ❑ DVB-H Digital Video Broadcast handheld
- ❑ ECMA European Computer Manufacturers Association
- ❑ FFT Fast Fourier Transform
- ❑ GE General Electric
- ❑ GP Green PHY
- ❑ GreenPHY Green Physical Layer

## Student Questions



# Acronyms (Cont)

- ❑ HAN Home Area Network
- ❑ HCSS High Confidence Software and Systems
- ❑ HD High Definition
- ❑ HDLC High-Level Datalink Control
- ❑ HEC High-End Computing
- ❑ HP HomePlug
- ❑ HPAV HomePlug Audio-Visual
- ❑ ID Identifier
- ❑ IEC International Electrotelecommunications Commission
- ❑ IEEE Institution of Electrical and Electronic Engineers
- ❑ IFFT Inverse Fast Fourier Transform
- ❑ IM Information Management
- ❑ IoT Internet of Things
- ❑ IP Internet Protocol
- ❑ IPv6 Internet Protocol V6
- ❑ ISO International Standards Organization

## Student Questions

# Acronyms (Cont)

- ❑ IT Information Technology
- ❑ kHz Kilo Hertz
- ❑ LonWorks Local Operating Network
- ❑ LSN Large Scale Networking
- ❑ MAC Media Access Control
- ❑ MHz Mega Hertz
- ❑ MIMO Multiple-input Multiple-output
- ❑ MoCA Multimedia over Coax
- ❑ MQ Multi-Queue
- ❑ MQTT MQ Telemetry Transport
- ❑ NASA National Aeronautical and Space Administration
- ❑ NFC Near Field Communication
- ❑ NIH National Institute of Health
- ❑ NITRD Networking and Info Technology Res and Development
- ❑ NMK Network Membership Key
- ❑ NSF National Science Foundation

## Student Questions

# Acronyms (Cont)

- ❑ OAuth      Open Standard for Authorization
- ❑ OFDM      Orthogonal Frequency Division Multiplexing
- ❑ ONR      Office of Naval Research
- ❑ PHY      Physical Layer
- ❑ PLC      Power Line Communication
- ❑ PROFIBUS      Process Field Bus
- ❑ QAM      Quadrature Amplitude Modulation
- ❑ QPSK      Quadrature Phase Shift Keying
- ❑ RF      Radio Frequency
- ❑ RFID      Radio Frequency Identification
- ❑ RPL      Routing Protocol for Low Power and Lossy Networks
- ❑ SCADA      Supervisory Control and Data Acquisition
- ❑ SDP      Software Design and Productivity
- ❑ SPiDCOM      Name of a company
- ❑ TDMA      Time division multiple access
- ❑ TEDS      Transducer electronic data sheets

## Student Questions

# Acronyms (Cont)

- ❑ US United States
- ❑ WiFi Wireless Fidelity
- ❑ WorldFIP Factory Instrumentation Protocol
- ❑ XML Extensible Markup Language

## Student Questions

**Scan This to Download These Slides**



Raj Jain

<http://rajjain.com>

[http://www.cse.wustl.edu/~jain/cse570-21/m\\_11dpi.htm](http://www.cse.wustl.edu/~jain/cse570-21/m_11dpi.htm)

**Student Questions**

# Related Modules



CSE567M: Computer Systems Analysis (Spring 2013),

[https://www.youtube.com/playlist?list=PLjGG94etKypJEKjNAa1n\\_1X0bWWNyZcof](https://www.youtube.com/playlist?list=PLjGG94etKypJEKjNAa1n_1X0bWWNyZcof)

CSE473S: Introduction to Computer Networks (Fall 2011),

[https://www.youtube.com/playlist?list=PLjGG94etKypJWOSPMh8Azcg5e\\_10TiDw](https://www.youtube.com/playlist?list=PLjGG94etKypJWOSPMh8Azcg5e_10TiDw)



Wireless and Mobile Networking (Spring 2016),

[https://www.youtube.com/playlist?list=PLjGG94etKypKeb0nzyN9tSs\\_HCd5c4wXF](https://www.youtube.com/playlist?list=PLjGG94etKypKeb0nzyN9tSs_HCd5c4wXF)

CSE571S: Network Security (Fall 2011),

<https://www.youtube.com/playlist?list=PLjGG94etKypKvzfVtutHcPFJXumyyg93u>



Video Podcasts of Prof. Raj Jain's Lectures,

<https://www.youtube.com/channel/UCN4-5wzNP9-ruOzQMs-8NUw>

## Student Questions