Chapter 10: Glossary

802.11a

802.11b

802.11n

802.11ac

Ali Cloud

AMQP – Advanced Message Queueing Protocol

http://en.wikipedia.org/wiki/Advanced_Message_Queuing_Protocol

http://www.amqp.org

AWS – Amazon Web Services

A secure cloud services platform, offering compute power, database storage, content delivery and other functionality (which makes more money for Amazon than their retail operations). AWS is built from a vast array of both virtual and actual servers and networks as well as a boatload of webserver software and administrative tools.

Azure – see Microsoft Azure

Bluemix – see IBM Bluemix

CA – Certificate Authority or Certification Authority

https://en.wikipedia.org/wiki/Certificate_authority

From Wikipedia:

In cryptography, a certificate authority or certification authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or on assertions made about the private key that corresponds to the certified public key. In this model of trust relationships, a CA is a trusted third party—trusted both by the subject (owner) of the certificate and by the party relying upon the certificate. The most commonly encountered public-key infrastructure (PKI) schemes are those used to implement https on the world-wide web. All these are based upon the X.509 standard and feature CAs.

CoAP – Constrained Application Protocol

http://en.wikipedia.org/wiki/Constrained_Application_Protocol

From Wikipedia:

Constrained Application Protocol (CoAP) is a software protocol intended to be used in very simple electronics devices, allowing them to communicate interactively over the

Internet. It is particularly targeted for small, low-power sensors, switches, valves and similar components that need to be controlled or supervised remotely, through standard Internet networks. CoAP is an application layer protocol that is intended for use in resource-constrained internet devices, such as WSN nodes. CoAP is designed to easily translate to HTTP for simplified integration with the web, while also meeting specialized requirements such as multicast support, very low overhead, and simplicity.[1][2] Multicast, low overhead, and simplicity are extremely important for Internet of Things (IoT) and Machine-to-Machine (M2M) devices, which tend to be deeply embedded and have much less memory and power supply than traditional internet devices have. Therefore, efficiency is very important. CoAP can run on most devices that support UDP or a UDP analogue.

DHCP – Dynamic Host Configuration Protocol

http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

From Wikipedia:

A UDP based protocol (and server) that can provide a device (aka station) the IP information required to connect it to the internet including IP address, Netmask, Domain Name, Domain Name Servers Time Servers and Default IP Gateway. When a client joins a network and is configured to use DHCP it will send out a UDP broadcast request asking for this information. A DHCP server on the network will respond which will then lead to an exchange of information that ends with the required information.

DNS – Domain Name System

http://en.wikipedia.org/wiki/Domain_Name_System

A protocol and hierarchical system of servers that provides the ability to turn IP names (e.g. www.cypress.com) into an IP address (e.g. 23.218.58.225) and vice versa.

ECDH – Elliptic Curve Diffe-Hellman

https://en.wikipedia.org/wiki/Elliptic_curve_Diffie%E2%80%93Hellman

From Wikipedia:

An anonymous key agreement protocol that allows two parties, each having an elliptic curve public–private key pair, to establish a shared secret over an insecure channel. This shared secret may be directly used as a key, or to derive another key. The key, or the derived key, can then be used to encrypt subsequent communications using a symmetric key cipher.

ECDSA – Elliptic Curve Digital Signature Algorithm

https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm

Gedday

HTTP – Hyper Text Transfer Protocol

http://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol

IE

IP – Internet Protocol

IBM Bluemix

JSON – JavaScript Object Notation

http://json.org

From json.org:

JSON is a lightweight data-interchange format. It is easy for humans to read and write. It is easy for machines to parse and generate. It is based on a subset of the JavaScript Programming Language. JSON is a text format that is completely language independent but uses conventions that are familiar to programmers of the C-family of languages, including C, C++, C#, Java, JavaScript, Perl, Python, and many others. These properties make JSON an ideal data-interchange language.

JSON is built on two structures: A collection of name/value pairs. In various languages, this is realized as an object, record, struct, dictionary, hash table, keyed list, or associative array. An ordered list of values. In most languages, this is realized as an array, vector, list, or sequence.

Message Broker

A message broker is a server used in MQTT communication. Devices can publish messages to a specific topic on the broker and can subscribe to a topic to receive any updates.

Microsoft Azure

MIME – Multipurpose Internet Mail Extension

MIMO – Multiple In/Multiple out

In 802.11n/ac you can increase the bandwidth by bonding multiple channel together (e.g. 2x channels will double the bandwith)

MQTT

http://en.wikipedia.org/wiki/MQTT

http://www.mqtt.org

MQTT[1] (formerly Message Queueing Telemetry Transport) is an ISO standard (ISO/IEC PRF 20922)[2] publish-subscribe-based "lightweight" messaging protocol for use on top of the TCP/IP protocol. It is designed for connections with remote locations where a "small code footprint" is required or the network bandwidth is limited. The publish-subscribe messaging pattern requires a message broker. The broker is responsible for distributing messages to interested clients based on the topic of a message.

Mutex

OASIS

OSI Model

OTA – Over the Air

Queue

REST – Representational State Transfer

https://en.wikipedia.org/wiki/Representational_state_transfer

Semaphore

SISO

Sockets

SSDP – Simple Service Discovery Protocol

TCP/IP

Timer

TFTP – Trivial File Transfer Protocol

http://en.wikipedia.org/wiki/Trivial_File_Transfer_Protocol

Thread

UDP - User Datagram Protocol (from Wikipedia)

http://en.wikipedia.org/wiki/User_Datagram_Protocol

The User Datagram Protocol (UDP) is one of the core members of the Internet protocol suite. The protocol was designed by David P. Reed in 1980 and formally defined in RFC 768. With UDP, computer applications can send messages, in this case referred to as datagrams, to other hosts on an Internet Protocol (IP) network. Prior communications are not required to set up transmission channels or data paths.

UDP uses a simple connectionless transmission model with a minimum of protocol mechanism. UDP provides checksums for data integrity, and port numbers for addressing different functions at the source and destination of the datagram. It has no handshaking dialogues, and thus exposes the user's program to any unreliability of the underlying network and so there is no guarantee of delivery, ordering, or duplicate protection. If error correction facilities are needed at the network interface level, an application may use the Transmission Control Protocol (TCP) or Stream Control Transmission Protocol (SCTP) which are designed for this purpose.

UDP is suitable for purposes where error checking and correction is either not necessary or is performed in the application, avoiding the overhead of such processing at the network interface level. Time-sensitive applications often use UDP because dropping packets is preferable to waiting for delayed packets, which may not be an option in a real-time system.[1]

WPS