Communication Protocols and Internet Architectures

Harvard University

Lecture #14

Instructor: Len Evenchik
cs40@evenchik.com or evenchik@fas.harvard.edu

ALIGHLSOD1701

Lecture Agenda

- Course Logistics
- Q&A and Topics from Last Week
- Quality of Service (QoS) for Voice and Video
- Network Issues in the Internet of Things (IoT)
- Course Review
- One Minute Wrap-Up

Course Logistics

Course Logistics

- Final Exam – Please check the weekly course information sheet for detailed information on upcoming final.
- The Homework is being graded and grades will be posted to the course website.
- Please contact me if you would like to schedule office hours.
- Thank you for submitting the Wrap-Up each week!
- This week's section meetings will include a course review. Please check the weekly course information sheet for the details.

Q&A
Topics from Last Week

Voice and Video Over IP

This is Not VoIP

By courtesy of] [The American Telephone and Telegraph Co.

A LONG-DISTANCE TELEPHONE EXCHANGE.

Radio-telephone switchboard circa 1930. From the left the first four stations are to London, the next Ship to Shore, Buenos Aires, and Rio de Janeiro.

AT&T Photo

Audio and Video Codecs

(We'll talk about this more when with discuss QoS.)

- A codec converts an analog signal (either voice or video) to a digital signal (and vice versa)
- Audio Codecs
  - G.711 (8,000 samples per second, 64kbps, 30 msec sample)
  - G.722 (7Khz speech, 48kbps to 64 kbps)
  - G.723.1 (30 msec sample, 6.4kbps)
  - G.728 (16kbps, LD-CELP)
  - G.729 (8kbps, CELP)
  - Plus many proprietary and open source standards
- Video Codecs
  - H.261 (the first packet based video compression standard)
  - H.263, H.263+ and H.263++
  - H.264 (multiple versions and standards)
  - H.265 (most recent standard)
  - Plus many proprietary and open source standards

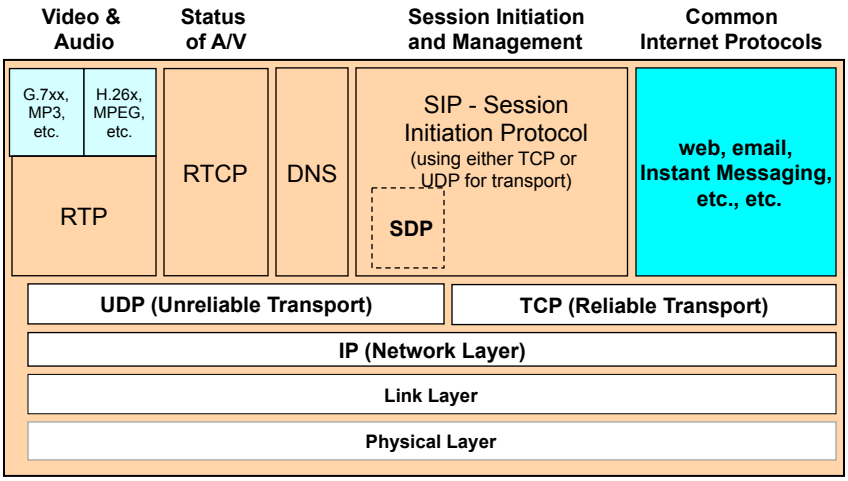
Introduction to RTP (1)

- Video and voice packets cannot be carried directly by UDP without additional functionality.
- The Real-time Transport Protocol is an IETF transport protocol for real time applications such as voice and video. It is standardized in RFCs 3550 and 3551.
- RTP uses UDP transport, with the inherent and limited functionality provided by UDP. This means error detection but not correction.
- RTP provides data sequencing, timing and synchronization
- RTP is augmented by a "control" protocol called RTCP (Real-Time Transport Control Protocol) which loosely monitors the flow

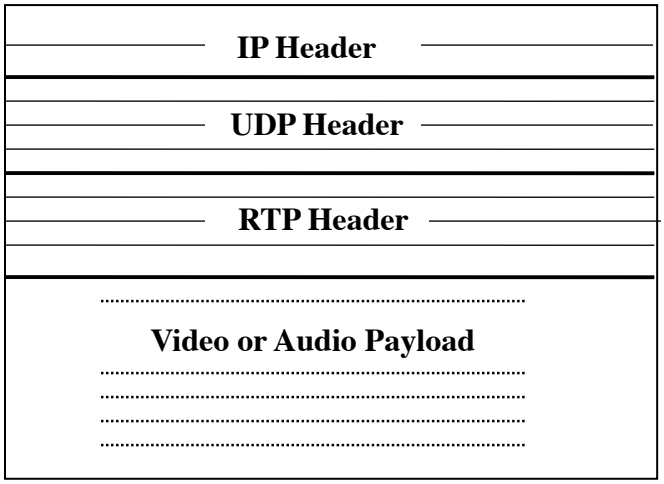
Introduction to RTP (2)

- RTP provides data sequencing, timing and synchronization
- RTCP provides media synchronization, feedback and forward status information
- RTP/RTCP flow uses a pair of UDP channels in each direction
- The Secure Real-time Transport Protocol (SRTP) RTP (RFC 3711) has also been defined and is used. There are other encrypted VoIP protocols such as ZRTP.

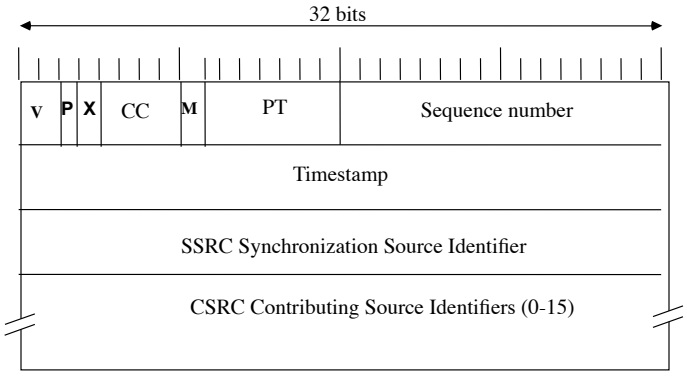
SIP Protocol Architecture



Combined IP/UDP/RTP Packet



RTP Header Format



RTP Header Fields

- V: version number
- P: flag to indicate padding bytes are present
- X: header extension flag
- PT: Payload Type
- CC: CSRC count
- M: marker (media dependent, defined in RTP profile)
- timestamp: sampling instant of the first byte, from media encoding clock
- SSRC: Synchronization source, the source of a single stream
- CSRC: Contributing source, a source that contributes to the combined stream produced by an RTP mixer

RTP Packet Flow for Video Call

© 1998 - 2017 L. Evenchik

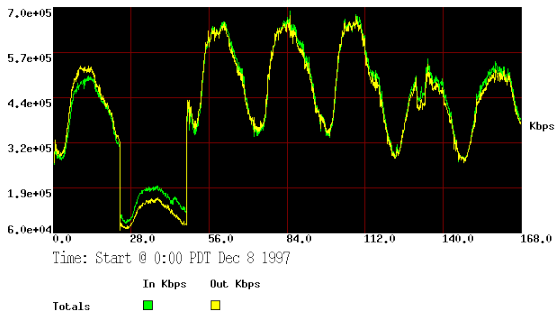
Network Quality of Service QoS

Quality of Service (QoS)

- Every network application has a basic set of requirements that the network must meet in the delivery of the traffic generated by the application. This is not a new problem, it goes back to remote data entry on the first mainframe computers.
- The requirements focus on bandwidth, delay, jitter, and error rate, and are known as Quality of Service (QoS)
- Supporting network QoS enhances the network's ability to provide the characteristics required by a specific application. For example, VoIP has different bandwidth, delay and jitter requirements than email.

QoS is Not a New Issue

7 Day Traffic Query for Sprint New York NAP
Statistics from Dec 15, 1997
Source and copyright (if applicable) to http://www.nlanr.net/NAP/



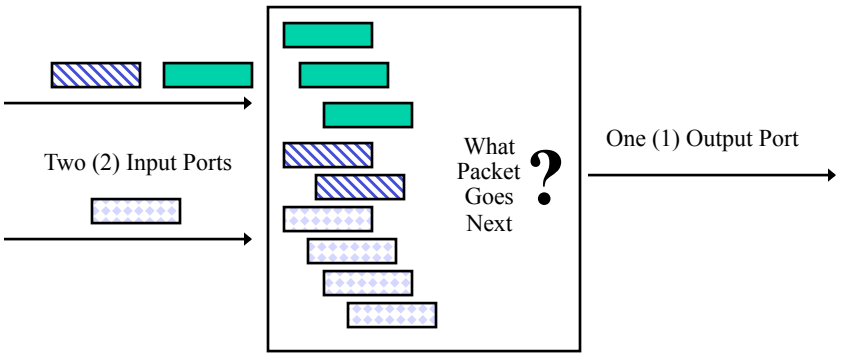
Why QoS?

- The IP network does not guarantee QoS or even delivery
- Resource conflicts with data traffic increase the risk that Audio / Video packets or other "high priority" packets will be delayed or lost
- Real time interactive Audio/Video quality deteriorates quickly when packets are lost or delayed. Is this the case video streaming?
- With QoS, the system could implement priority treatment for some types of user traffic, giving them preferential treatment at each store-and-forward device
- QoS could then improve a packet's chance of successful, timely delivery

QOS - How Do You Define and Specify Quality

- Bandwidth
- Delay
- Jitter
- Error Rate
- Drop Probability Characteristics
- System Reliability
- plus many other choices… but, *we will focus on the first four*

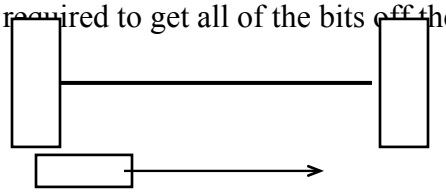
Intuitive Approach to Queueing and Delay



Delay Components

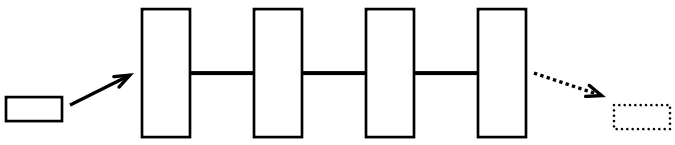
Once a frame is at the front of the queue, delay is determined by:

- Time required to put all of the bits on the wire. This is dependent upon the length of the frame and the clock rate of the wire.
- Plus, the time required for the first bit to reach the far end of the wire. This is dependent upon the distance to the far end, and of course, the speed of light.
- Plus, the time required to get all of the bits off the wire.

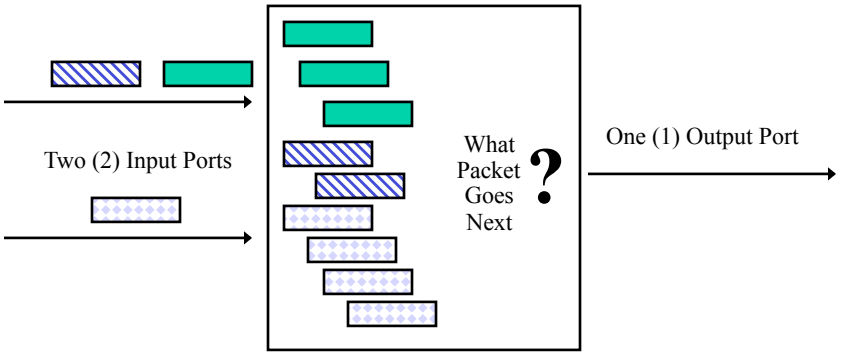


Network Delay in the Real World

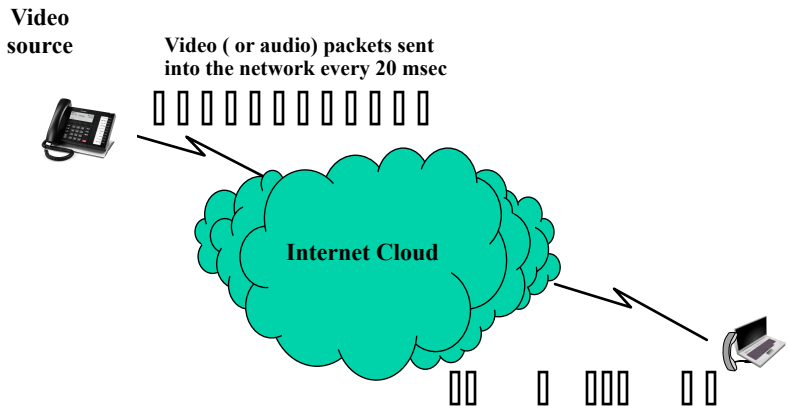
- Packet delay on a link is determined by the three components we have just described.
- **However, the most significant delay component** today is the queueing (or buffering) of a packet in a device while it waits to reach the front of the queue. Only one packet can be sent at a time and all other packets must wait until it is their time to be sent.
- All of these factors are of course present for each and every device along the path. **Delay is cumulative.**



Intuitive Approach to Queueing and Delay



Internet Jitter and Delay



Jitter Queue Tradeoff

- Jitter queues help overcome network jitter
- But a Jitter Queue adds delay to the stream
- Delay and jitter must be managed for interactive audio/video.
- The industry has set standards for delay, jitter and error rate for VoIP and video conferencing.
- Delay can be very long for streaming audio/video and it does not change the perceived quality. Jitter is also not important. Why is this the case?

Approaches to Managing QoS

- Have a lot of bandwidth available !! This is the typical solution for campus networks.
- Allocate bandwidth to particular conversations or users just before it is needed, and then keep track of the reservations and allocations as they change. (This is Int-Serv and RSVP.) This approach is rarely used today.
- Mark the packets using some specific criteria and then treat the packets differently in the network using the marking as a guide (DiffServ)
- Try to ignore that there is a problem
- Or as a friend in the telephone business said to me a few years ago, "Use circuit switching instead of packet switching."

Increase Bandwidth?

- Increasing bandwidth always helps video and audio quality if no QoS is present
- Increasing bandwidth in the LAN is relatively inexpensive
- Increasing bandwidth over the WAN can be prohibitively expensive. Also, user organizations do not control the queueing or traffic management policies of ISPs

Differentiated Service, DiffServ

- Diffserv was defined by the IETF about twenty years ago and it has been a very active area of work.
- Diffserv can be applied both to the Internet and private networks. Almost all implementations are in private networks today (MPLS, private IP, etc.)
- Approach provides for "the overall treatment of a defined subset of a customer's traffic within a DS-domain"
- The approach is to mark high priority packets in some special way, and then for the network to give preferential treatment to these special packets.
- Diffserv is not implemented in the general Internet. Why not?

Differentiated Service, DSCP

- Diffserv re-uses the high order six bits of the original IPv4 TOS (Type of Service) field.
- End systems or some other edge device (router, firewall) mark the DSCP field of each packet with a specific value. These values then specify in some way how the packet is treated within the network.
- Packets can be remarked at a later time by the network
- Once marked each device in the network treats the packets in some specified way depending on the Diffserv marking.
- A DSCP (Diff Serv Code Point) identifies a Per Hop Behavior (PHB.)
  - ***In case you are confused, the above is anything but obvious.***

Differentiated Service, Codepoints

- Codepoint = 000000

  Best effort
- Codepoint = xxx000

  Provides for compatibility with previously defined approach called IP precedence
- Codepoint = 101110

  Expedited Forwarding (EF) – strict low latency queue
- Codepoint = 001010, 001100, plus 10 more

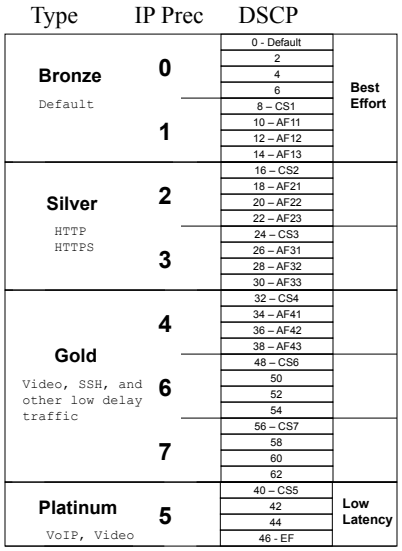
  Assured Forwarding (AF) – 4 queues with 3 levels of drop preferences (probabilities) in each queue

Differentiated Services Field Codepoints

Name	Space	Reference
CS0	000000	[RFC2474]
CS1	001000	[RFC2474]
CS2	010000	[RFC2474]
CS3	011000	[RFC2474]
CS4	100000	[RFC2474]
CS5	101000	[RFC2474]
CS6	110000	[RFC2474]
CS7	111000	[RFC2474]
AF11	001010	[RFC2597]
AF12	001100	[RFC2597]
AF13	001110	[RFC2597]
AF21	010010	[RFC2597]
AF22	010100	[RFC2597]
AF23	010110	[RFC2597]
AF31	011010	[RFC2597]
AF32	011100	[RFC2597]
AF33	011110	[RFC2597]
AF41	100010	[RFC2597]
AF42	100100	[RFC2597]
AF43	100110	[RFC2597]
EF PHB	101110	[RFC3246]

http://www.iana.org/assignments/dscp-registry/

Typical Code Point Assignment



ISPs and Carriers Implement Versions of QoS in Their Networks

Class of Service Data Collection

TOS (first 6 bits)	Standard Per Hop Behavior	AT&T Class
101 110	DSCP Expedite Forwarding (EF)	COS1
101 000*	IP Precedence 5	COS1
011 010	DSCP Assured Forwarding 31 (AF31)	COS2 compliant
011 100	DSCP Assured Forwarding 32 (AF32)	COS2 noncompliant
011 000	IP Precedence 3	COS2 compliant
010 010	DSCP Assured Forwarding 21 (AF21)	COS3 compliant
010 100	DSCP Assured Forwarding 22 (AF22)	COS3 noncompliant
010 000	IP Precedence 2	COS3 compliant
000 000	DSCP Best Effort (DEFAULT)	COS4
011 xxx*	DSCP Assured Forwarding 3x (AF3x)	COS2 noncompliant
110 xxx	Reserved for control and signaling	Highest supported data class
111 xxx	Reserved for control and signaling	Highest supported data class
010 xxx	DSCP Assured Forwarding 2x (AF2x)	COS3 noncompliant
101 xxx		COS4
001 xxx	DSCP Assured Forwarding 1x (AF1x)	COS4
100 xxx	DSCP Assured Forwarding 4x (AF4x)	COS4
000 xxx		COS4

Table 1. AT&T Class Markings

5 What Traffic Profiles are offered by AT&T?

The bandwidth allocation for each class is based on twenty-five (25) pre-defined "Traffic profiles". You will be required to select an egress queuing profile for traffic leaving the backbone network toward the customer premise router. If AT&T manages the customer premise router, the same queuing profile will be used for traffic flowing to-wards the backbone network. Additionally, you will be required to select an ingress classification

114	20% RT, 40/30/30 Data	20	32	24	24	Yes	Yes	N/A	N/A	N/A
115	10% RT, 80/10/10 Data	10	72	9	9	Yes	Yes	N/A	N/A	N/A
116	10% RT, 60/30/10 Data	10	54	27	9	Yes	Yes	N/A	N/A	N/A
117	10% RT, 40/30/30 Data	10	36	27	27	Yes	Yes	N/A	N/A	N/A
118	ONE CoS CoS2	0	100	0	0	Yes	Yes	Yes	N/A	N/A
119	0% RT, 80/10/10 Data	0	80	10	10	Yes	Yes	Yes	N/A	N/A

Source, December 2016
planner.bus.att.com/tab004.pdf

Page 9 of 22 Version 1.0

DiffServ Block Diagram

Fig. 1 shows the block diagram of a classifier and traffic conditioner. Note that a traffic conditioner may not necessarily contain all four elements. For example, in the case where no traffic profile is in effect, packets may only pass through a classifier and a marker.

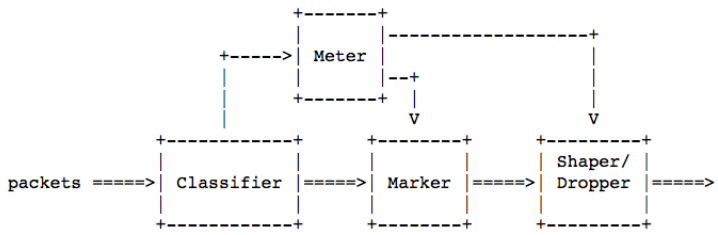


Fig. 1: Logical View of a Packet Classifier and Traffic Conditioner

Source RFC 2475

Current example of Diffserv Work

[Docs] [txt|pdf|xml|html] [Tracker] [WG] [Email] [Diff1] [Diff2] [Nits]

Versions: (draft-szigeti-tsvwg-ieee-802-11)
00 01 02 03 04 05 06 07 08 09

Transport Working Group — T. Szigeti
Internet-Draft — J. Henry
Intended status: Standards Track — Cisco Systems
Expires: March 22, 2018 — F. Baker
September 18, 2017

Diffserv to IEEE 802.11 Mapping
draft-ietf-tsvwg-ieee-802-11-09

Abstract

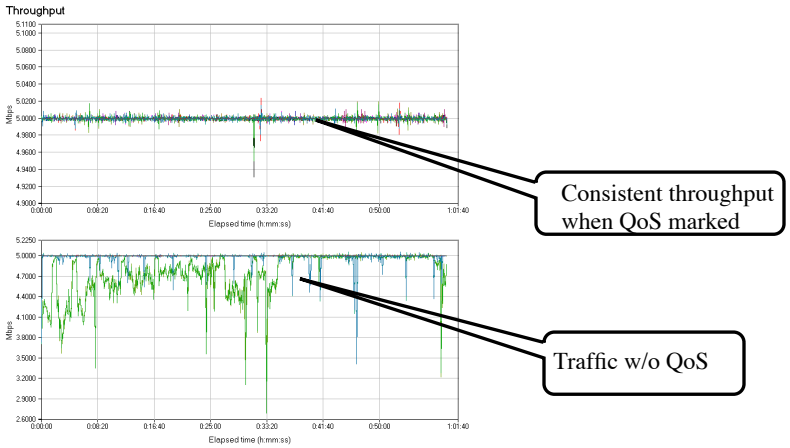
As internet traffic is increasingly sourced-from and destined-to wireless endpoints, it is crucial that Quality of Service be alig between wired and wireless networks; however, this is not always case by default. This document specifies a set of Differentiated Services Code Point (DSCP) to IEEE 802.11 User Priority (UP) mapp to reconcile the marking recommendations offered by the IETF and IEEE so as to maintain consistent QoS treatment between wired and IEEE 802.11 wireless networks.

4.3. DSCP-to-UP Mapping Recommendations Summary

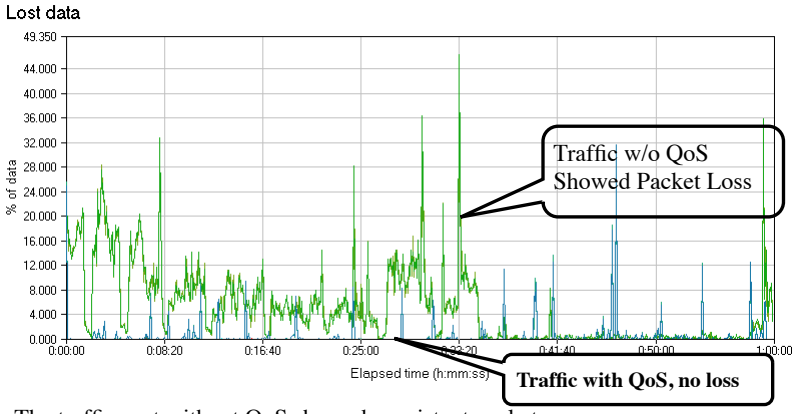
Figure 1 summarizes the [RFC4594] DSCP marking recommendations mapped to [IEEE.802.11-2016] UP and access categories applied in the downstream direction (i.e. f to-wireless networks).

IETF Diffserv Service Class	PHB	Reference RFC	IEEE 802.11 User Priority	IEEE 802.11 Access Category
Network Control (reserved for future use)	CS7	RFC2474	7 OR 0	AC_VO (Voice) OR AC_BE (Best Effort)
			See Security Considerations-Sec.8	
Telephony	EF	RFC3246	6	AC_VO (Voice)
VOICE-ADMIT	VA	RFC5865	6	AC_VO (Voice)
Signaling	CS5	RFC2474	5	AC_VI (Video)
Multimedia Conferencing	AF41 AF42 AF43	RFC2597	4	AC_VI (Video)
Real-Time Interactive	CS4	RFC2474	4	AC_VI (Video)

Real World Network Test Results
Throughput with/without QoS

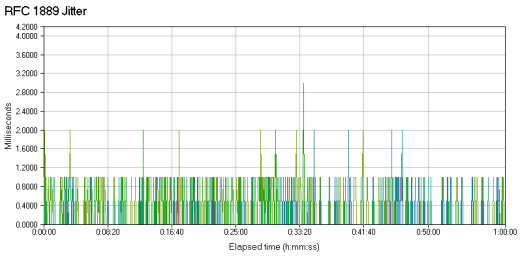


Real World Network Test Results
Packet Loss with/without QoS

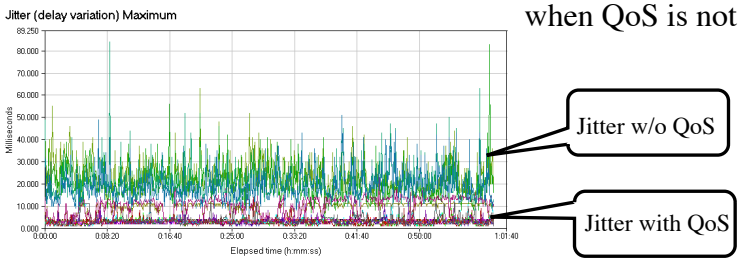


The traffic sent without QoS showed consistent packet loss, while the traffic with QoS marked showed almost no loss.

Real World Network Test Results
Jitter with/without QoS



There is increased jitter when QoS is not marked.



Internet of Things (IoT)

Philosophy of the Internet of Things (IoT)

- The philosophy or motto of the Internet of Things (IoT) is that anything that can be connected to the Internet, should be connected to the Internet. The corollary to this statement extends the reach of this statement even further.

Let's Build an IoT Coffee Maker

The Original IoT Coffee Pot, circa 1991

University of Cambridge Computer Laboratory, UK, 1991

Web enabled device known as The Trojan Room Coffee Machine
Used MSRPC2. It ran over MSNL
See http://www.cl.cam.ac.uk/coffee/coffee.html

Also see RFC 2324, 1998
Hyper Text Coffee Pot Control Protocol (HTCPCP/1.0)
Extension to HTTP to define the new BREW method

CMU Coke Machine (1980s – 1990s)

APNIC

Or, if you prefer Coke over coffee:

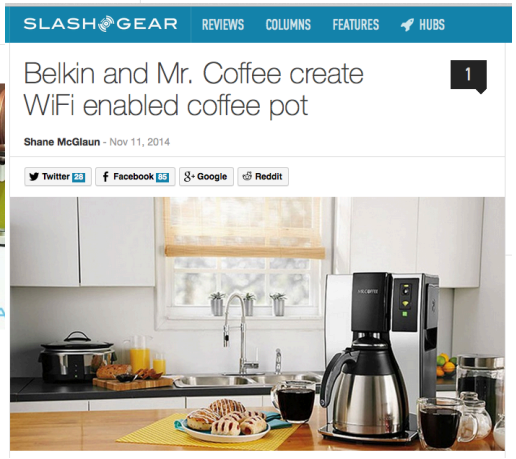
IoT Coke Machine at CMU, mid 1970s
Used ARPANET standard Finger protocol
See https://www.cs.cmu.edu/~coke/history_long.txt

History of IoT *Internet Toaster, 1990, SNMP*

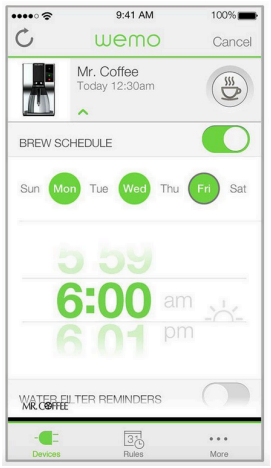
- **1990**: John Romkey created the first Internet 'device', a toaster that could be turned on and off over the Internet
- At the October '89 INTEROP conference, Dan Lynch, President of Interop promised Romkey that, if Romkey was able to "bring up his toaster on the Net," the appliance would be given star placement in the floor-wide exhibitors at the conference. The toaster was connected to a computer with TCP/IP networking. It then used an information base (SNMP MIB) to turn the power on.

Credit: Living Internet

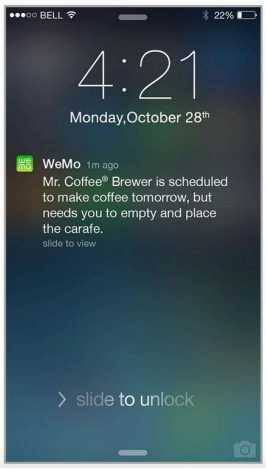
Current IoT Coffee Makers



IoT Coffee Maker Control
Control via both Android and IoS



Set the schedule



Notification to clean the pot

IoT Coffee Maker Security Problem

Characteristics of the Internet of Things (IoT)

- The philosophy or motto of the Internet of Things (IoT) is that anything that can be connected to the Internet, should be connected to the Internet. The corollary to this statement extends the reach even further.
- The vast majority of devices that will be connected within the IoT will not communicate directly with people. It will be M2M, which is Machine to Machine communications. These devices are also called smart objects.
- The projections are that there will be 20 billion IoT devices by 2020. (Lets consider the number of light bulbs that could be connected.)
- The course readings discuss the possible applications and use cases for the IoT in almost every field, including health care, transportation, housing, education, etc., etc.
- The assumption is that IPv6 will be used to support the billions of new devices that make up the emerging IoT. We will focus our discussions on the use of IPv6 within the IoT comprised of smart objects with limited functionality and limited capabilities.

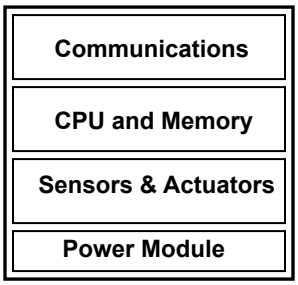
Smart Objects with Limited Functionality (1)

- The majority of the devices that will be part of the IoT will have limited capabilities. This means that they will be limited in one or more of the following ways: processing capability, communications, power, and sensor/actuator functionality. Regardless of these limitations, the intent is that they be able to operate unattended for years.
- One major problem with these types of devices is security and how they will be updated as problems are found in them.
- Today's smart phones, game consoles, household control systems, and building automation systems are part of the IoT, but they have extensive functionality and few limitations.

Smart Objects with Limited Functionality (2)

- An IoT chip connected to a small container used in a factory to track its location and contents might have limited capability. For example, it might not have a battery, and would scavenge power for its processor and communications. It also might only turn on when it is being moved around.
- Lets study 6LoWPAN as a good example of supporting IoT objects with limited capabilities. 6LoWPAN is "IPv6 over Low-Power Wireless Personal Area Networks"

Building Blocks of an IoT Device

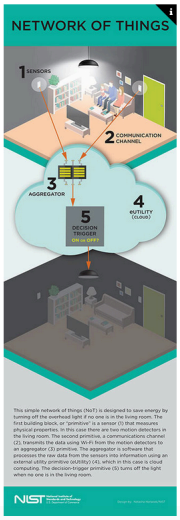


Note: Given that this a networking course, it's no surprise that we place the communication module at the top of the diagram.

NIST has Defined a Good Reference Model

You should review their work if you are working in this area.

See https://www.nist.gov/itl/applied-cybersecurity/nist-initiatives-iot



NIST Special Publication 800-183

Networks of 'Things'

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-183

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

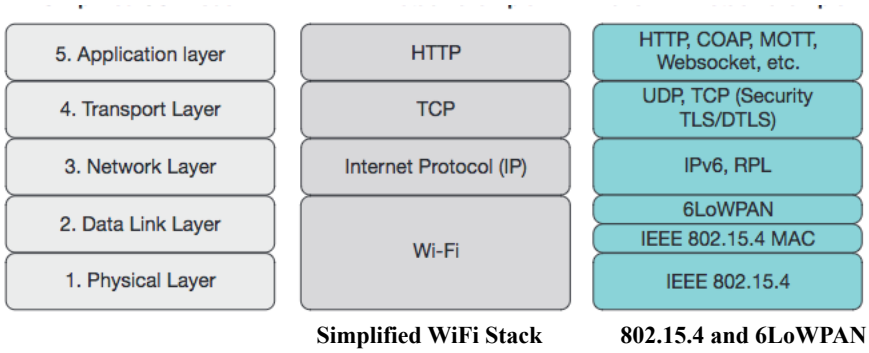
IETF 6LoWPAN and IEEE 802.15.4 (1 of 2)

- 6LoWPAN is described in RFC 4919 (2007), and others. It defines the functionality that is required to support IPv6 on devices that use IEEE 802.15.4 (RF) for communications.
- The characteristics of IEEE 802.15.4 include:
  - Multihop mesh networks
  - Bandwidth of approximately 250 Kbps
  - Range of 10 to 100 meters
  - Frame size of 127 bytes (or less)

IETF 6LoWPAN and IEEE 802.15.4 (2 of 2)

- Given this limited functionality, or constrained capability, 6LoWPAN defines an adaption layer for IPv6 that provides fragmentation, header compression, and IPv6 Neighbor Discovery (ND). Remember that the minimum MTU for IPv6 is 1280 bytes versus 127 bytes for 802.15.4.
- The work that has been done in 6LoWPAN is now being applied to Bluetooth Low Energy (LE) and NFC.

6LoWPAN Protocol Stack



Simplified WiFi Stack **802.15.4 and 6LoWPAN**

Source: www.ti.com/lit/wp/swry013/swry013.pdf

IPv6 Packet Compression and 6LoWPAN Headers

* This will not be on the Final Exam

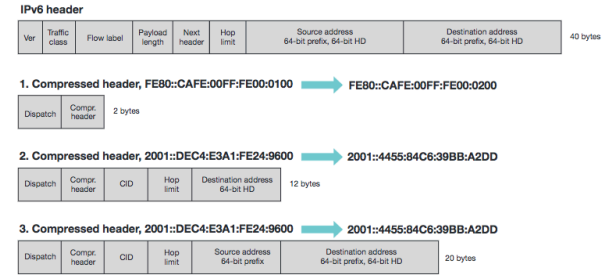


Figure 3. 6LoWPAN IPv6 header compression examples

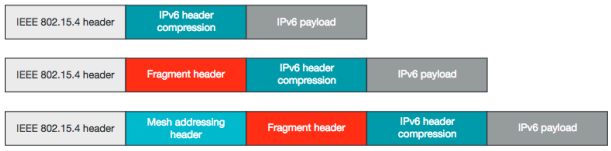
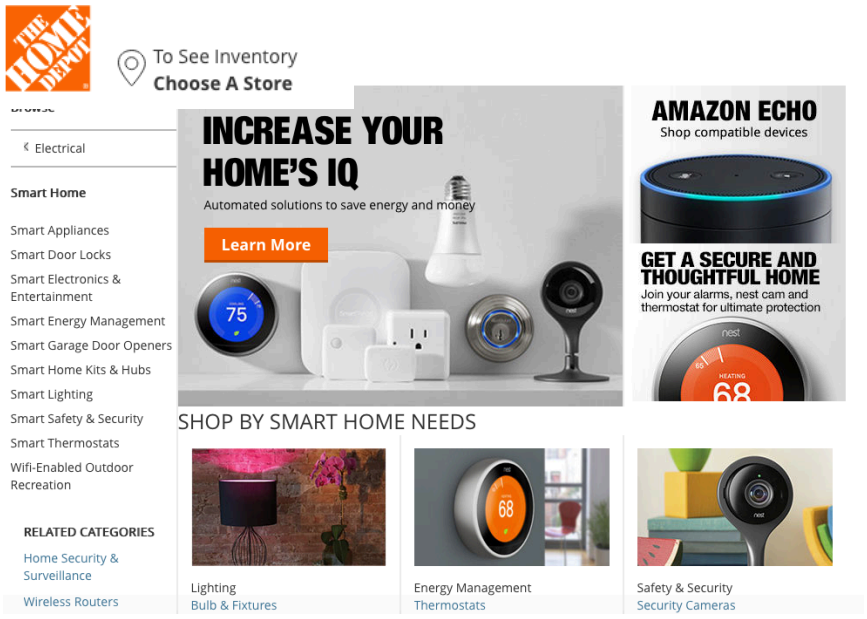


Figure 4. 6LoWPAN stacked headers

Source: www.ti.com/lit/wp/swry013/swry013.pdf

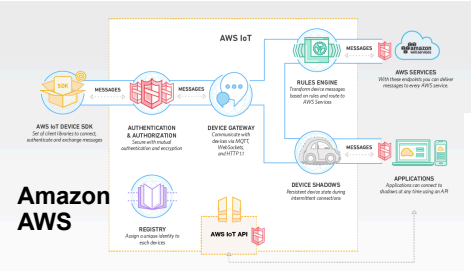
The Smart Home is a Consumer Facing IoT



Evolution of IoT

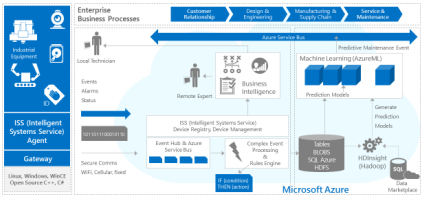
- The initial focus for the IoT was on the hardware, sensors and systems that Moore's Law made possible. Remember the IoT coffee maker is 20 years old. It was a smart but fairly isolated device.
- Communications and the Internet has become the focus of IoT as sensors and communications improved.
- This has morphed even more, and today, discussions about IoT almost always include the Cloud, Big Data and analytics, machine learning and AI, etc., etc.

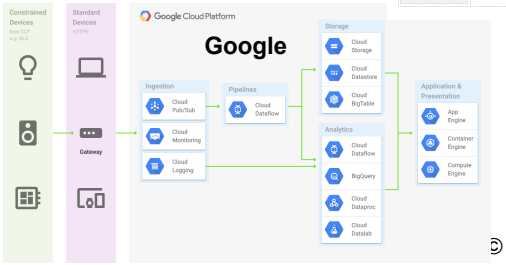
IoT Platforms and the Cloud



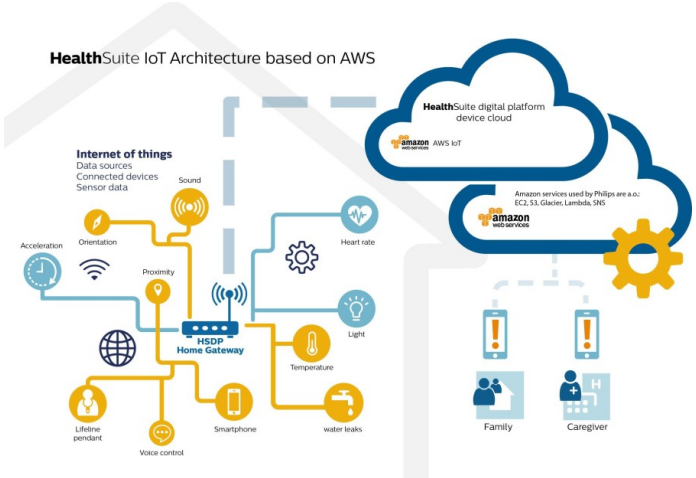
Microsoft Azure

An IoT Services Architecture with the Azure platform





IoT Home Health Suite



http://hitconsultant.net/2015/10/09/aws-philips-strengthens-digital-health-iot/

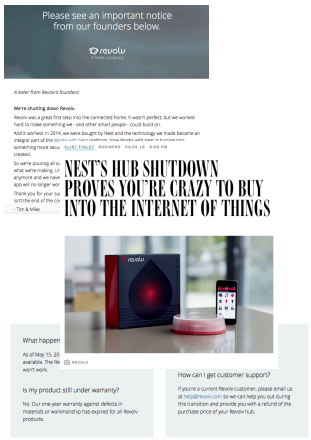
Nest Labs Builds IoT Devices

Real World Problems with the IoT

What happens with a software upgrade you did not ask for fails?

Real World Problems with the IoT

What happens with a company decides they no longer want to support your device?



Real World Problems with the IoT

What happens with a company decides they no longer wants to support your device?

KLINT FINLEY BUSINESS 04.05.16 6:06 PM

NEST'S HUB SHUTDOWN PROVES YOU'RE CRAZY TO BUY INTO THE INTERNET OF THINGS

Source: Wired Magazine

A letter from Revolv's founders:

We're shutting down Revolv.

Revolv was a great first step into the connected home. It wasn't perfect, but we worked hard to make something we - and other smart people - could build on.

And it worked. In 2014, we were bought by Nest and the technology we made became an integral part of the Works with Nest platform. Now Works with Nest is turning into something more secure, more useful and just flat-out better than anything Revolv created.

So we're pouring all our energy into Works with Nest and are incredibly excited about what we're making. Unfortunately, that means we can't allocate resources to Revolv anymore and we have to shut down the service. As of May 15, 2016, your Revolv hub and app will no longer work.

What happens to my Revolv service?

As of May 15, 2016, Revolv service will no longer be available. The Revolv app won't open and the hub won't work.

Is my product still under warranty?

No. Our one-year warranty against defects in materials or workmanship has expired for all Revolv products.

What will happen to Revolv data?

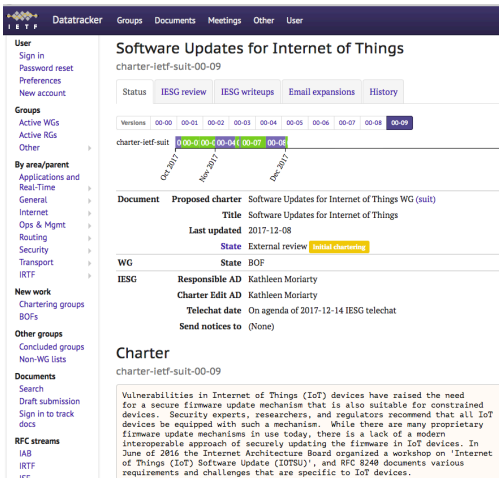
Revolv data will be deleted.

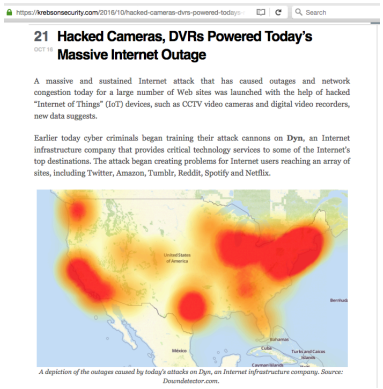
How can I get customer support?

If you're a current Revolv customer, please email us at help@revolv.com so we can help you out during this transition and provide you with a refund of the purchase price of your Revolv hub.

Source: Revolve Website

Current IETF Work on IoT





Source is https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/

Course Summary

What are some of the "Great Ideas" in Networking

Thank You!

Please Keep In Touch!