One view of the Internet architecture

AfriSIG

October 2018
Zanzibar

Avri Doria

[ ] Some initial questions

- What does this have to do with Internet governance?
  - do those creating the protocols, standards and codes think they are doing Internet governance?
  - Should they be aware?
- Are principles involved in protocols & architecture?
  - Internet principles? What sort of principles?
    - What about each “in their respective roles”, is that relevant to protocol principles?
  - does it have an effect on what is produced?
- Should protocols be related to Rights and other Policies?

GOVERNANCE

Back to the internet governance working definition

A working definition of Internet governance is the development and application *by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet. (WGIG and Tunis Agenda § 34)*

- *Creative ambiguity*
  - *at its best or at its worse?*
- *What do all these words mean?*
  - *especially when juxtaposed in this way?*
  - *How many ways can they be used?*

An example of creative ambiguity

- A political scientist's understanding of *Principles, norms, rules and decision-making procedures and programs* *may be* based international regime theory - "(*free-standing injunctions or coherent international regimes)*"

Or

- *Principles, norms, rules and decision-making procedures and programs* – *includes the code, protocols and standards used to allow an emergent internet to function properly. And this notion includes the most critical Internet policies*
  - *those embedded in code.*

some more very basic definitions

In English	In network engineering
a protocol is a code of correct conduct, forms of ceremony and etiquette observed by diplomats and heads of state, sometimes a basis for comparison;	a protocol is the set of rules determining the format and transmission of data
a standard is any distinctive flag, a reference point against which other things can be evaluated	a standard is a formalization of a protocol or a practice
a code is a set of rules or principles or laws (especially written ones), a coding system used for transmitting messages requiring brevity or secrecy	code is the symbolic arrangement of data or instructions in a computer program or the set of such instructions, the implementation of that protocol, what makes the Internet a unique thing in itself

Two views on Internet Governance

- the Internet can be understood by reference to other institutions in society, e.g
  - telecommunications,
  - media
  - trade
- and thus is subject to the same rules
- and warrants the same form of analysis

it is
a new sort of thing
that requires new rules
and new analysis

Is it a thing in itself?

- Is the Internet sui generis?
- While at a high enough level of abstraction we can use pre-existing knowledge structures to try and understand it by analogy, those explanations will always fall short, though they may provide a clue.
- What makes it is a unique thing in itself?
  - The Internet is a self healing system composed of a boundless complexity of code created in a novel political environment, a thing that continually captures and recombines human intent and know how, and a system that can behave dynamically to produce an unlimited number of unexpected new possibilities.

PRINCIPLES

Internet principles?

- Engineering constructs
  - guide system designers
  - give a basis for making choices between equally acceptable engineering solutions.
    i.e. to balance between
    - Cost
    - Ease of deployment
    - Human rights
      - Of Expression, Association, Privacy, Access to Culture and Knowledge
      - Property rights, et al.
  - enable distributed community of designers and architects to build a single consistent system
  - Two types
    - Design
    - Operational

Some Internet principles

- Design Principles
  - Packet based nature of the network
  - The End to End Principle
  - Postel Robustness Principle
  - Layered architecture
  - Hourglass Model
  - Shared Fate
  - Creative Anarchy
  - Variation in outcome
  - Principles for protocol design
- Operational Principles
  - Naming – "there only can be one"
  - Routing & Addressing
    - Routing on addresses not names
    - Overloading/Separation of Location ID and Endpoint ID
    - Scope of address/name
    - Early vs. Late Binding
    - Types of routing protocol
      - Metric Vector
      - Shortest Path

Packet based network

- First discussed by Leonard Klienrock and Paul Baram and Donald Davies in 1960.
- Moved away from the centralized switching network paradigm of the telecommunications era
  - create connections, control and manage connections, billing
- Allows for a confederated network of networks where each network handles the datagram (aka packet) using the best paths that exist at that point in time according to its own policies. (hop by hop)
- Allows for development of a network with emerging properties.

end to end principle

The function in question can completely and correctly be implemented only with the knowledge and help of the application standing at the end points of the communication system.

Corollary: the only elements that belong in the lowest layers of the network are those elements that are useful to all of the other parts of the network

Difficulty: identifying the ends or edges
Question: to what extent does this remain true in the age of the cloud.

e2e too

- First defined in 1980 (Saltzer et al.)
- Often used in political discourse
  - occasionally abused, often misunderstood
- Principle focuses on putting the information at the appropriate place in the network.
  - so for applications, yes, it is at the user interface
  - but, e.g., for routing it might be at the edge of a network
- Does not speak to putting all intelligence at the edges
- Does not speak of a dumb network
  - whatever that may mean.

Postel robustness principle

"Be conservative in what you send and liberal in what you accept"

- Documented in RFC 793 - Transmission Control Protocol (i.e TCP)
- Important in building networks
  - Being strict means following the protocols specifications as carefully as possible to avoid ambiguity
  - Being liberal means that if there is enough information to support a request then don't throw it out because of a difference in coding or interpretation (sometimes called an error, but it might not be)

Layered architecture

- A layered architecture is one where data moves from one layer to another and is subject to a different form of processing at each layer
- A layered architecture encapsulates or transforms the data packet received from the next higher layer, or
- A layered architecture de-encapsulates or transforms the data packet received from the next lower layer
- e.g.

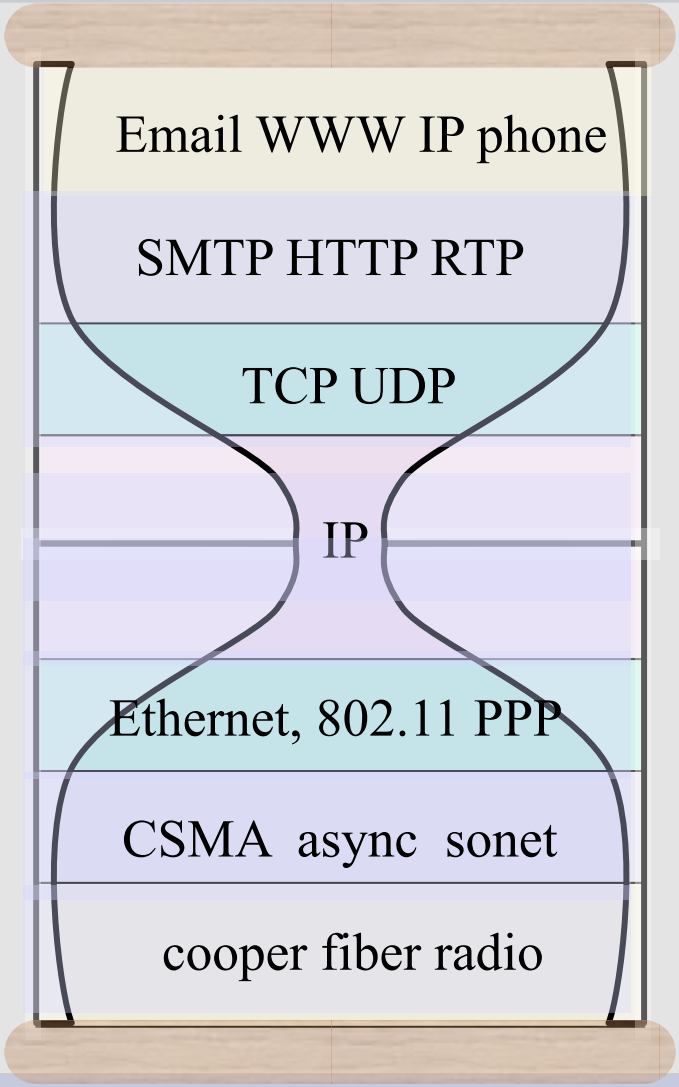
{link layer {ip layer {transport layer {application layer { data} } } } }

hourglass model

All application (upper) layers converge on IP at the network layer
All (infrastructure) lower layers converge on IP at the network layer
IP is the traditional waist of the hourglass

- A de facto principle.
- A common point in the architecture that allows for multiple applications to sit over multiple forms of link technology
- A key factor in allowing for innovation.
  - An application layer developer does not need to worry about the infrastructure details
  - Infrastructure developers don't need to worry about applications.

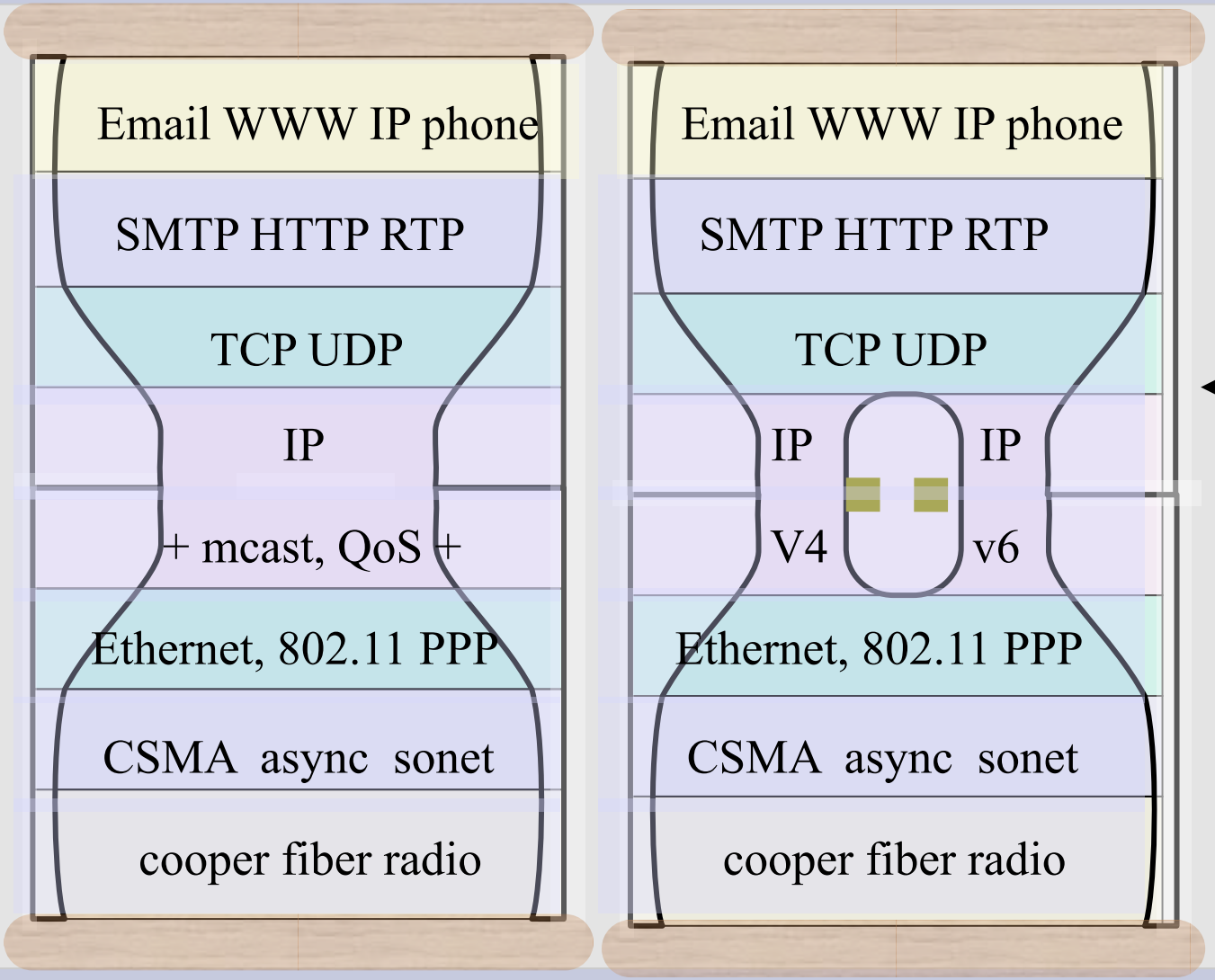
The proverbial IP hourglass



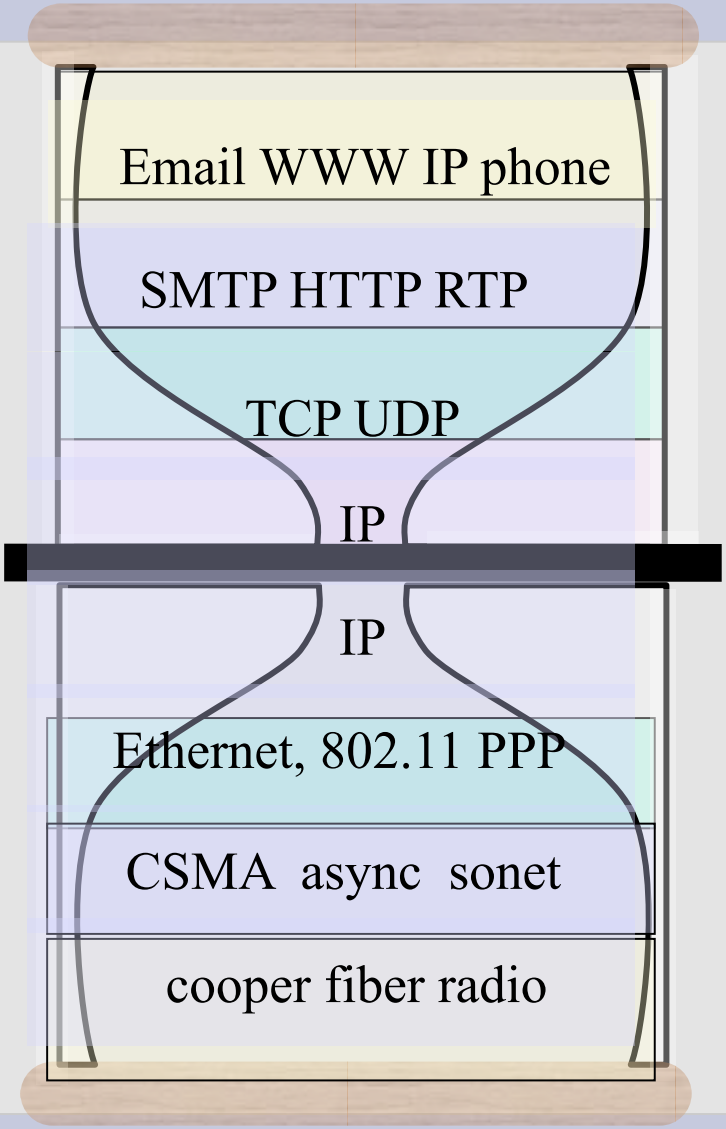
Please do not worry about
the acronym salad.
They can all be found
In wikipedia
And elsewhere.

Original picture taken
from Terena presentation
by Steve Deering in 2001

Fattening and Splitting

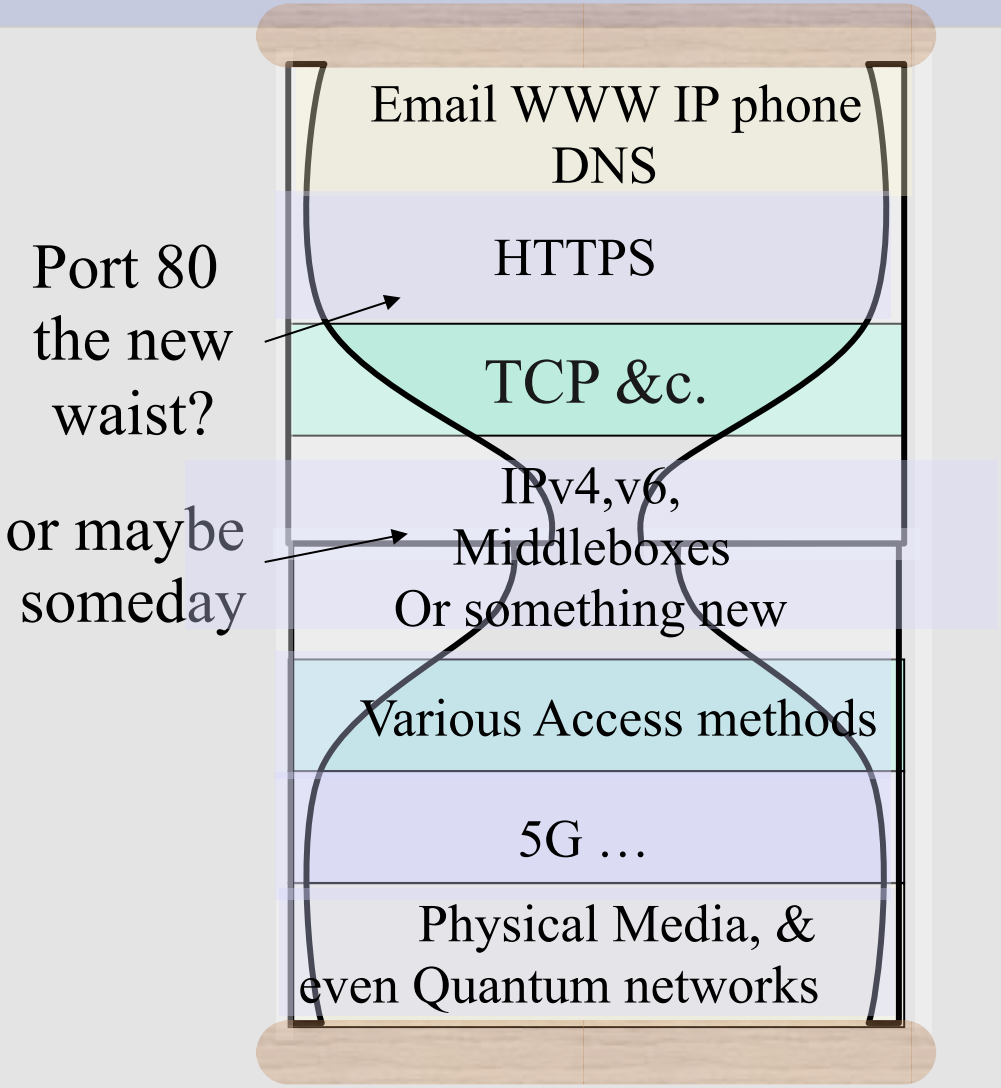


Middleboxes



e.g. NAT,
firewall,
VoIP server,
VoD server,
3G service box
DSLAM, ...

Ultimately?



Port 80 the new waist?

or maybe someday

Under construction

Shared fate

- Means that control information travels the network along the same transport as the data.
- Fundamental to the management of the network
- Without an assumption of shared fate, there needs to be an entire separate network management structure
- Fundamental in Routing design
- 'Broken' by Multipath Label Swapping (MPLS) tunnel based routing techniques and the cloud.
  - Creates new difficulties in managing today's networks

Creative Anarchy

- Also known as Generative nature
- No top down design
- Principles and creativity instead of a design committee
- Anyone, anywhere, can still contribute the next innovation.
  - Just need to be creative and know how to code.
- Credited for invention of new application models such as wikis and social networks
- Seen as a fundamental problem by some e.g. Jonathan Zitrain, ITU…
  - Responsible for span and viruses?

Variation in Outcome

- Just because something is built for one purpose, does not mean it will be used for that purpose.

"so that the outcome can be different in different places, and the tussle takes place within the design, not by distorting or violating it. Do not design so as to dictate the outcome. Rigid designs will be broken; designs that permit variation will flex under pressure and survive."
Clark et al.

Principles for protocol design

- In order for two network entities to talk to each other, they need messages that:
  - are part of an ordered set
    - (does not need to be strict ordering)
  - include request & response mechanisms
  - strictly defined syntax
  - strictly defined semantics

Human Rights Protocol Considerations

Example of intermingling of internet architecture and human rights

Purpose of HRPC Research Group

- The Human Rights Protocol Considerations Research Group chartered to research whether standards and protocols can enable, strengthen or threaten human rights, as defined in the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR).

- The research group takes as its starting point the problem statement that human-rights-enabling characteristics of the Internet might be degraded if they are not properly defined, described and sufficiently taken into account in protocol development. Not protecting these characteristics could result in (partial) loss of functionality and connectivity.

Output of HRPC Research Group

- RFC 8280
  - Attempts to bridge language of rights and protocol technologists
  - Did ethnographic analysis of the IETF RFC repository
  - Developed hypothesis on the relationship between protocol elements and rights.
  - Suggested considerations that protocol designers can use when developing or evaluating protocols.
  - Now using, and testing, those considerations for usefulness.
- Created Human Right Review team that reviews current IETF draft according to the consideration extracted into: draft-irtf-hrpc-guidelines/

Guidelines for Human Rights Considerations

- From https://datatracker.ietf.org/doc/draft-irtf-hrpc-guidelines

  - *Connectivity*: Do you add function at edges on in middle
  - *Privacy*: Did you take consideration for privacy into account [RFC6973]
  - *Content agnosticism*: Do you use info from packet not in header
  - *Security*: Did you have a look at Guidelines for Writing RFC Text on Security Considerations [BCP72]?
  - *Internationalization*: Does your protocol have text strings that have to be understood or entered by humans?
  - *Censorship resistance*: Does this protocol introduce new identifiers or reuse existing identifiers (e.g. MAC addresses) that might be associated with persons or content?
  - *Open Standards*: Is your protocol fully documented in a way that it could be easily implemented, improved, built upon and/or further developed
  - *Heterogeneity Support*: Does your protocol support heterogeneity by design? Does your protocol allow for multiple types of hardware?
  - *Pseudonymity*: Have you considered the Privacy Considerations for Internet Protocols [RFC6973], especially section 6.1.2 ? Does the protocol collect personally derived data? Does the protocol generate or process anything that can be, or be tightly correlated with, personally identifiable information?

Guidelines for Human Rights Considerations, cont'd

- *Accessibility*: Is your protocol designed to provide an enabling environment for people who are not able-bodied? Have you looked at the W3C Web Accessibility Initiative for examples and guidance?
- *Localization*: Does your protocol uphold the standards of internationalization?
- Decentralization: Can your protocol be implemented without one single point of control?
- *Reliability*: Is your protocol fault tolerant? Does it degrade gracefully? Can your protocol resist malicious degradation attempts?
- *Confidentiality*: Does this protocol expose information related to identifiers or data?
- Integrity: Does your protocol maintain, assure and/or verify the accuracy of payload data?
- *Authenticity*: Do you have sufficient measures to confirm the truth of an attribute of a single piece of data or entity?
- *Adaptability*: Is your protocol written in such a way that is would be easy for other protocols to be developed on top of it, or to interact with it?
- *Outcome Transparency*: Are the effects of your protocol fully and easily comprehensible, including with respect to unintended consequences of protocol choices?
- *Anonymity*: Often protocols expose personal data, it is important to consider ways to mitigate the obvious privacy impacts.

An example of a candidate for review

- DNS Queries over HTTPS (DoH)) to Proposed Standard]
  - draft-ietf-doh-dns-over-https-12.txt
  - This document describes how to make DNS queries over HTTPS which uses TLS.
  - Considered by some to be more secure
  - Privacy concerns documented in draft
  - Other concerns include (From email to HRPC from Stephane Bortzmeyer)
    - HTTP sends much more metadata than the DNS
    - Some vendors believed to have alreeady abused DoH
      - E.g. redirecting users by default to a big cloud provider
    - < https://blog.nightly.mozilla.org/2018/06/01/improving-dns-privacy-in-firefox/>)
  - Possible questions for HR Considerations analysis:
    - Is censorship resistance as strong as current DNS
    - Pseudonymity – Web browsers have ability to correlate additional information
    - Outcome transparency – Can the outcomes be seen or are they hidden within the browsers

questions?

thanks

avri@acm.org