Introduction to Networking - Notes

Stylianos Gisdakis

November 6, 2014

Contents

1 Introduction to Networking

1.1 Networks

Definition of network, elements, and link. Basic types of links.

1.2 Network Topologies

From a single link to multiple links: network topologies.

1.3 Internet

Several networks with different topologies join together for Internet. Very complex and heterogeneous system.

2 Networking

Knowledge needed for enabling the communication between two entities in a network. Main challenges of transferring information to the next hop and forwarding to the destination.

2.1 Protocols

Definition of protocol and layer. Motivation of protocol adoption: network is heterogeneous and every node needs to agree on common rules. Protocols enable communication at the same layer in two different ends. Introduction to the Open Systems Interconnection (OSI) model through use cases.

2.2 Layers

Brief description of physical and data link layer and their difference: the first standardize the rules for signal propagation, the second manage the access to the medium.

2.3 Layers (cont'd)

Brief description of network and transport layers. Comparison of competences of the data link, network, and transport layers. The first manage the connection between two neighbors, the second provides the forwarding capabilities through the network, while the third enables direct communication end to end.

2.4 Layers (cont'd)

Brief description of session, presentation, and application layers. The session layer could handle the transferring of an audio and video streams tied together, while the presentation also handles for example the transformation between locales. The Application layer represents everything upper, e.g. sending / receiving emails, browsing Internet, etc.

2.5 Addresses

Introduction to addressing, used for identifying the nodes at every layer. Inspired by [1]. Existence of special addresses for "this node", "all nodes",

"some nodes", etc.

2.6 Encapsulation

How the data moves from one layer to the other: an *header* is introduced when the data is pushed to the lower layer, and removed when the data is received by the layer before it is forwarded to the upper layers. The header usually contains protocol information for that and only that layer.

3 Physical Layer

More detailed description of physical layer, characterization and some examples of the medium, signal, and encoding protocols.

3.1 Physical Layer: Cable

Two examples of common cables: twisted pair and optical fiber. In the first the cables are twisted to cancel the effects of electromagnetic interference (E.g. *crosstalk* is when a signal propagates undesirably to near circuits). In the second the light propagates by bouncing on the walls of the glass core.

3.2 Physical Layer: Wireless

The electromagnetic spectrum is divided in bands. Examples of channel subdivision for IEEE 802.11: sub-band inside the Industrial, Scientific and Medical (ISM) band, divided in 13 overlapping channels of 22 MHz each, and their central frequencies are separated by 5 MHz.

3.3 Physical Layer: Wireless (cont'd)

Introduction to wireless problems: the signal propagation is attenuated by the distance and various fading effects (E.g. shadowing, scattering, etc.). There is also the background noise and other sources of interference that make decoding more complex.

3.4 Physical Layer: Wireless (cont'd)

There are ways to overcome the issues on the wireless medium, like introducing redundancy, use robust coding and/or multiple channels. Those solutions also helps to increase the limit of channel capacity imposed by the Shannon-Hartley theorem.

4 Data Link Layer

More detailed description of the data link layer. Mostly inspired by [2].

4.1 Wired

4.1.1 Ethernet: IEEE 802.3

Ethernet frame and addressing description. Using the preamble to synchronize the terminals during the transmission.

4.1.2 Ethernet: IEEE 802.3 (cont'd)

Carrier Sense Multiple Access with Collision Detection (CSMA/CD) in Ethernet. The station jams the channel to ensure the frame is dropped. Protocol constraints: the minimum transmission time needs to be equal or greater than twice the propagation time for enabling the carrier sensing. As a matter of fact, the transmitter should be still active when it will receive the broadcast jamming signal from the station that detects the collision. In the worst case scenario the latter station starts transmission just before the signal arrives. Hence, the first station should wait the jamming signal comes back. Thus, given the minimum packet size and the data rate, there is a constrain for the network size.

4.2 Wireless

4.2.1 WiFi

Introduction to the terminology for WiFi.

4.2.2 WiFi: IEEE 802.11a/b/g/n

Data frame specification of the IEEE 802.11. The address 1 is always the receiver so the other stations can stop listening the medium (e.g. energy saving) after the reception of duration and receiver address fields. The different Phy Layer Convergence Procedures (PLCPs) for a/b/g/n can be found on http://zone.ni.com/devzone/cda/tut/p/id/7131.

4.2.3 WiFi: Medium Access

Simple Distributed Coordination Function (DCF) with Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). The stations compete for channel access by drawing a random r number and waiting r slot before starting transmission (backoff), while listening the channel. If another station starts to transmit during this backoff period, the timer is paused and resumed after the the transmission is completed. Possible issues:

- **Hidden Terminal**: A station, out of sender range, start transmitting. It will interfere at the receiver and none of the transmitters will be able to detect the problem by themselves.
- **Exposed Terminal**: A station could sense the active channel ad it will back-off, even though his communication will not interfere with others.

4.2.4 WiFi: Medium Access (cont'd)

A way to resolve the problem of hidden/exposed terminal is to use an handshaking protocol between sender and receiver. With an Request to Send (RTS) frame the sender will inform the neighbors of the intention to start a transmission (and for how long), while with a Clear to Send (CTS) the receiver will acknowledge that request and it will inform as well his neighbors of the duration. So the stations will allocate the channel into a virtual Network Allocation Vector (NAV).

4.2.5 Bluetooth

How to address coexistence in the same ISM band as the WLAN: utilization of a Frequency-Hopping Spread Spectrum (FHSS) mechanism to avoid local channel interference. The Bluetooth technology is not limited to the Data link layer but provides a complex protocol stack.

4.2.6 IEEE 802.15.4: ZigBee

Protocol tailored for low energy devices. Use duty-cycling for limit power consumption by alternating active and sleep states.

4.2.7 Global System for Mobile Communications

Hybrid network of wired - wireless infrastructure. Frequencies are assigned to the operators and they are employed with Time Division Multiple Access (TDMA) and Frequency Division Multiple Access (FDMA), dividing the assigned band in multiple channels and reserving time slots for each user.

4.3 Interconnections

Differences between hub, switches and bridges. The hub simply propagate the signal without decoding it. The switch interconnects two different network segments and implements a data link layer, while the bridge interconnects two different data link layers.

5 Network Layer

Description of the network layer and its role as forwarder of packets.

5.1 Internet Protocol (v4)

Characteristics and header of the Internet Protocol (IP) version 4 (IPv4). With a 32 bit field, there are *only* 4 294 967 296 choices and the pool of unallocated addresses exhausted on 3rd February 2011[1]. One *escamotage* is to employ the Network Address Translation (NAT), where more private addresses (and hence terminals) refer to only one public IP.

5.2 Internet Protocol (v6)

Enhancements to the IPv4, and the number of addresses in IP version 6 (IPv6) is dramatically increased.

5.3 Address Resolution Protocol

Address Resolution Protocol (ARP) is a cross-layer protocol needed for translating network address to data link address and vice versa. Proxy ARP stands for impersonating another device in the case the true destination is not accessible directly, but it needs to go through another device.

5.4 Routing

The data link layer takes care of transferring data to the neighbors while the network layer provide *routing*, that means transferring information across multiple hops.

5.4.1 Routing: Autonomous System (AS)

Hierarchical description of the networks and relation to the hierarchical routing: different Autonomous System (AS) (AS) may have different internal routing protocols but they must agree on the same intra-domain routing protocol.

5.4.2 Routing: Subnets

The network mask (*netmask* defines a group of IP belonging to the same network. This helps the routing process, since a router needs to know only where the network is and not every single IP address. By increasing the netmask, a network can be split in multiple sub-networks in a hierarchical process.

[1] http://en.wikipedia.org/wiki/IPv4_address_exhaustion

5.4.3 Routing: Table

Definition of a routing table and its fields. Through this table, that can be learned or fixed by the administrator, the router has enough information to forward the messages towards the right path.

5.4.4 Routing: Build the table

Routing protocols: Link state and distance vector routing. The Dijkstra's algorithm is a greedy approach for producing a shortest path tree associated to a graph, by starting with a set containing only the source node and including step by step the closest node to the set[1]. The Bellman-Ford algorithm, instead, produces the shortest path tree by relaxing all the links and iterating the procedure until it stabilizes[2].

5.5 Dynamic Host Configuration Protocol

Simplify the configuration of the terminals in a network, by providing the basic connectivity information to the station of the network. It has been developed for IPv4, it works for IPv6 but there are also alternatives protocol-specific for the latter.

5.6 Ad Hoc Networks

Description of the Ad Hoc Networks and their challenges.

6 Transport Layer

End-to-end layer built on top of a unreliable network. Once we have a way to forward data from a source to a destination, we can think of different protocols that rely on that capability and provide for example a reliable data transfer.

6.1 User Datagram Protocol

Description of the User Datagram Protocol (UDP) protocol and its header. The UDP provides the simplest transport model, by only showing the functionalities provided by the Network layer.

[1] http://en.wikipedia.org/wiki/Dijkstra's_algorithm
[2] http://en.wikipedia.org/wiki/Bellman%E2%80%93Ford_algorithm

6.2 Transmission Control Protocol

Description of the Transmission Control Protocol (TCP) protocol and its header. The TCP, compared to UDP, provides a more complex transport model. It uses the lower layer functionalities for building a stream-oriented connection.

6.2.1 TCP: Handshaking

How to establish and close a connection within the TCP. While during the opening the connection establishment is obviously synchronous, during the closure of the duplex channel the other station could still have some data to transmit and, thus, the process is asynchronous.

6.2.2 TCP: Flow and Congestion Control

Motivation of the Flow and Congestion control techniques in TCP. The sliding window[1] algorithm is used to avoid the receiver overflow, by adding in every response a field indicating how much data the terminal is still willing to buffer for the connection. As for the congestion control, brief descriptions are at:

- http://en.wikipedia.org/wiki/Slow-start
- http://en.wikipedia.org/wiki/TCP_congestion_avoidance_algorithm
- http://en.wikipedia.org/wiki/Fast_retransmit
- http://en.wikipedia.org/wiki/Slow-start#Fast_recovery

7 Application Layer

Introduction to the application layer and some utilizations.

7.1 Hyper-Text Transfer Protocol

Brief description of Hyper-Text Transfer Protocol (HTTP) and how the resource pointed by the Uniform Resource Locator (URL) can be retrieved from the webserver. The RFC can be found at http://tools.ietf.org/html/rfc2616.

7.2 Domain Name System

The URL also contains the host name of the webserver. That is a mnemonic address that needs to be translated into an IP address. The protocols that enables this is the Domain Name System (DNS) and uses a predefined set of IP addresses that run the service that is able to translate the query.

[1] http://en.wikipedia.org/wiki/Sliding_Window_Protocol

7.3 Network Time Protocol

Synchronization between stations sometimes could be crucial. It is done through the Network Time Protocol (NTP). More resurces are at http://www.eecis.udel.edu/~mills/ntp.html

7.4 Peer-to-peer

The advantages of Peer-to-peer (P2P) are many but the main problem is the coordination among all the peers. It is nontrivial knowing which terminal belongs to the P2P network and how the content is distributed.

7.4.1 P2P: Bittorrent

The Bittorrent protocol address the issue of coordinating by employing a dedicated server (*tracker*) that coordinates the activity of the peers. Thus, instead of providing the data to all the peers, the server consumes less bandwidth to only advise the clients on the download status.

8 Summary

From OSI model to the reality: the TCP/IP protocol stack. Application, Presentation, and Session layer converge in a more general application layer.

[1] Philip Levis. *Introduction to Computer Networking. Lecture 1*. CS144. Standford University. 2011. URL: http://cs144.scs.stanford.edu/.

[2] Philip Levis. *Introduction to Computer Networking. Lecture 8*. CS144. Standford University. 2011. URL: http://cs144.scs.stanford.edu/.