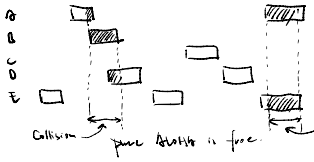
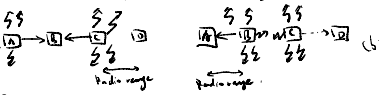
4.2 Multiple access protocols 4.2.1 ALOHA

Pure ALOHA: send the frame when ready, resend if the frame is destroyed later



From the above diagram we can see that whenever two frames try to occupy the channel at the same time, there will be a collision, and both will be garbled. If the first bit of a new frame overlaps with just the last bit of a frame that has almost finished, both frames will be totally destroyed, and both will have to be retransmitted later.

4.2.5 Wireless LAN Protocols



(a) A and C are hidden terminals to B, when transmit to B

(b) B and C are exposed terminals when transmitting to A and D.

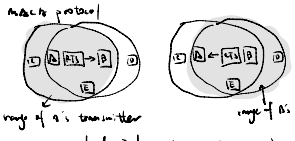
(a)

If A sends and then C immediately senses the medium, it will not hear A because A is out of its range. Thus C will falsely conclude that it can transmit to B. If C does start transmitting, it will interfere at B, wiping out the frame from A. The problem of a station not being able to detect a potential competitor for the medium because the competitor is too far away is called the hidden terminal problem.

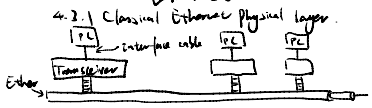
(b)

If C senses the medium, it will hear a transmission and falsely conclude that it may not send to D (shown as a dashed line). In fact, such a transmission would cause bad reception only in the zone between B and C, where neither of the intended receivers is located.

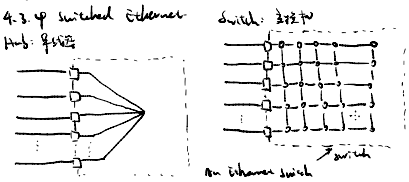
4.3 Ethernet



4.3.1 Classical Ethernet Physical Layer



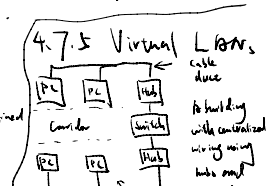
4.3.4 Switched Ethernet



Hub: all stations are in the same collision domain. They must use the CSMA/CD algorithm to schedule their transmissions.

Switch: each port is its own independent collision domain.

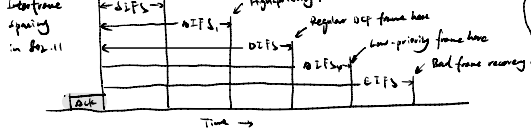
4.3.5 Virtual LANs



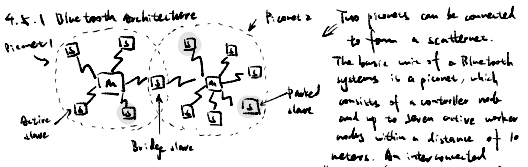
A building with centralized wiring using hubs and a switch

4.3.3 The 802.11 MAC Sublayer Protocol

Two versions: 802.11e. It works by extending CSMA/CA with carefully defined intervals between frames.



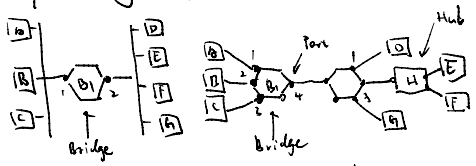
4.5.1 Bluetooth Architecture



Two piconets can be connected to form a scatternet. The bridge unit of a Bluetooth system is a piconet, which consists of a controller node and up to seven active worker nodes within a distance of 10 meters. An interconnected collection of piconets is called a scatternet.

4.7 Data link Layer Switching

4.7.2 Learning Bridge

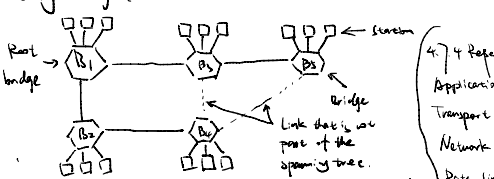


Bridge connecting two multidrop LANs

Bridges (and a hub) connecting seven point-to-point stations

4.7.3 Spanning-Tree Bridges

For the bridges to communicate with each other and overlay the actual topology with a spanning tree that reaches every bridge:



A spanning tree connecting five bridges. The dashed lines are links that are not part of the spanning tree.

Socket programming client-side

The client code starts with some includes and declarations. Execution begins by checking to see if it has been called with the right number of arguments, where argv[0] contains the name of the server (e.g. fits.cs.vu.nl) and is converted to an IP address by gethostbyname. This function uses DNS to look up the name. Next a socket is created and initialized. After that the client attempts to establish a TCP connection to the server, using connect. If the server is up and running on the named machine and attached to SERVER_PORT and is either idle or has room in its listen queue, the connection will (eventually) be established. Using the connection, the client sends name of the file by writing on the socket.

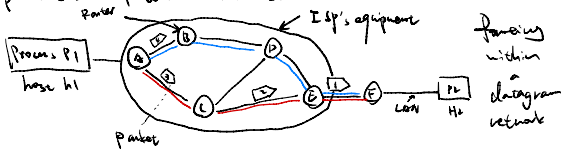
4.7.4 Repeaters, Hubs, Bridges, Switches, Routers, Gateways

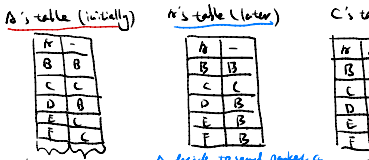
Application layer	Application gateway
Transport layer	Transport gateway
Network layer	Router
Data link layer	Bridge, switch
Physical layer	Repeater, hub

Which device is in which layer.

Chp 5 Network layer

5.1.3 Implementation of Connectionless Service



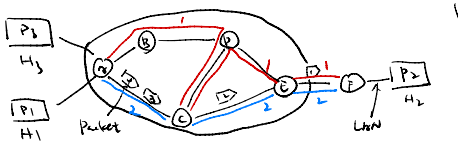


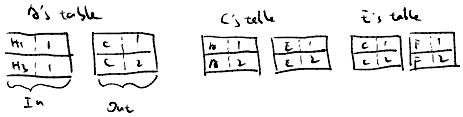
A decides to send packet to C via a different route than that of the first three packets. A has learned of a traffic jam somewhere along the ADB path and updated its routing table.

The algorithm that manages the tables and makes the routing decisions is called the routing algorithm.

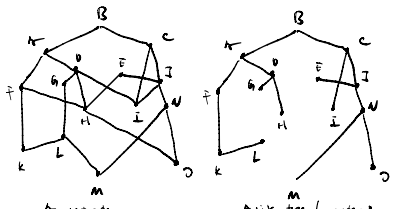
The number of bytes sent is one larger than the name proper since the 0-byte terminating the name must also be sent to tell the server where the name ends. Now the client enters a loop, reading the file block by block from the socket and copying it to standard output. When it is done, it just exits.

5.1.4 Implementation of Connection-Oriented Service





5.2.1 The Optimality Principle



- One can make a general statement about optimal routes without regard to network topology or traffic. This statement is known as the optimality principle.

It states that if router J is on the optimal path from router I to router K, then the optimal path from J to K also falls along the same route. To see this, call the part of the route from I to J r1 and the rest of the route r2. If a better route than r2 existed from J to K, it could be concatenated with r1 to improve the route from I to K, contradicting our statement that r1r2 is optimal.

- As a direct consequence of the optimality, the optimality principle, the set of optimal routes from all sources to a given destination form a tree rooted at the destination. Such a tree is called a sink tree. Note that a sink tree is not necessarily unique. Other trees with the same path lengths may exist. In the above diagram (b) is a sink tree for router B

Distance vector routing: Although it converges to the correct answer, it may do so slowly. Link state routing: Not only is router memory consumed by ever-increasing tables, but more CPU time is needed to scan them, and more bandwidth is needed to send status reports about them.

Hierarchical routing within a network: There is a penalty to be paid: increased path length. For example, the best route from 1A to 5C is via region 2, but with hierarchical routing all traffic to region 5 goes via region 3, because that is better for most destinations in region 5.

Broadcast routing: Each router must have knowledge of some spanning tree.

5.2.8 Multicast Routing

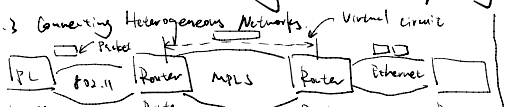
Sending a message to such a group is called multicasting, and the routing algorithm used is called multicast routing

5.2.9 Anycast Routing

- In anycast, a packet is delivered to the nearest member of a group. Schemes that find these paths are called anycast routing

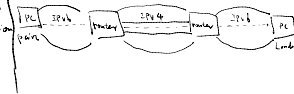
5.4.3 Packet Scheduling FIFO, Fair queueing, weighted fair queueing.

5.5.3 Connecting Heterogeneous Networks



IP packet crossing different networks

5.5.4 Connecting Endpoints Across Heterogeneous Networks



6.2.1 Transport Service Primitives.

Listen. CONNECT. SEND. RECEIVE. DISCONNECT

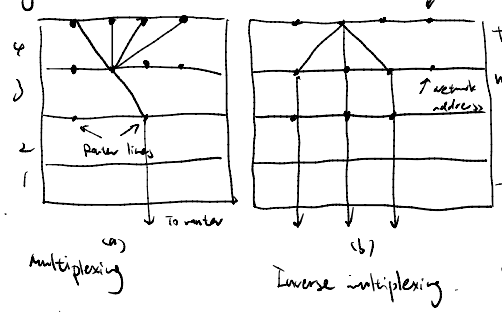
When a frame arrives, the data link layer processes the frame header and, if the destination address matches for local delivery, passes the contents of the frame payload field up to the network entity. The network entity similarly processes the packet header and then passes the contents of the packet payload up to the transport entity.

6.2.2 Addressing

TSAPs, NSAPs, and transport connections

- the transport addresses to which processes can listen for connection requests are called ports.

6.2.5 Multiplexing



Multiplexing

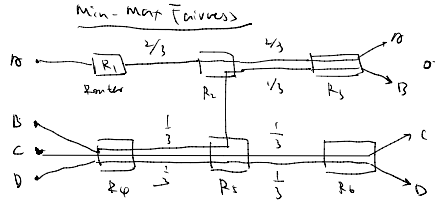
Inverse multiplexing.

(a) If only one network address is available on a host, all transport connections on that machine have to use it. When a segment comes in, some way is needed to tell which process to give it to. This situation called multiplexing.

(b) A host has multiple network ports that it can use. If a user needs more bandwidth or more reliability than one of the network paths can provide, a way out is to have a connection that distributes the traffic among multiple network paths on a round-robin basis. This is called inverse multiplexing.

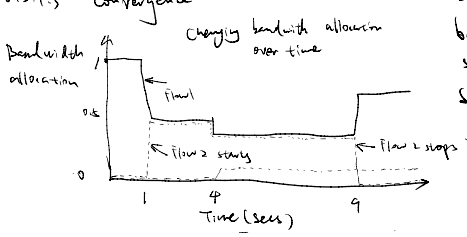
6.3 Congestion Control. The only effective way to control congestion is for the transport protocols to send packets into the network more slowly

6.3.1.2 Desirable Bandwidth Allocation:



The form of fairness that is often desired for network usage is max-min fairness. An allocation is max-min fair if the bandwidth given to one flow cannot be increased without decreasing the bandwidth given to another flow with an allocation that is no larger; In the above diagram, each of the links between routers has the same capacity, taken to be 1 unit, though in the general case the links will have different capacities. If more of the bandwidth on the link between R4 and R5 is given to flow B, there will be less for flow A. This is reasonable as flow A already has more bandwidth. However, the capacity of flow C or D (or both) must be decreased to give more bandwidth B, and these flows will have less bandwidth than B. Thus, the allocation is max-min fair.

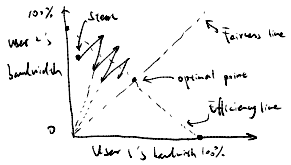
6.3.1.3 Convergence



Initially, flow 1 has all of the bandwidth. One second later, flow 2 starts. It needs bandwidth. At 4 seconds, a third flow joins. However, this flow uses only 20% of the bandwidth, which is less than its fair share (which is a third). Flow 1 and 2 quickly adjust, dividing the available bandwidth to each have 40% of the bandwidth. At 9 seconds, the second flow leaves, and the third flow remains unchanged. The first flow quickly captures 80% of the bandwidth.

6.3.1.4 Regulating the Sending Rate (AIMD)

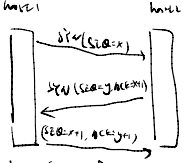
Additive increase multiplicative Decrease (AIMD) control law: The users additively increase their bandwidth allocations (and then multiplicatively decrease them when congestion is signaled) to the AIMD control law to both fair and efficient.



Legend: ↗ = Additive increase (up at 45°)

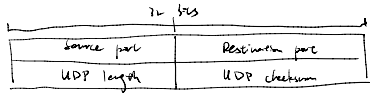
↙ = Multiplicative decrease (line points to origin)

TCP:



6.4.1 Introduction to UDP

The connectionless protocol is UDP (User Datagram Protocol)



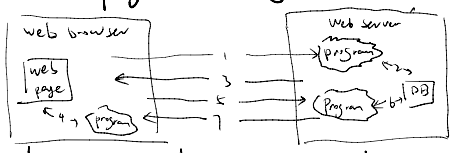
TCP transmission Control Protocol: a reliable end-to-end byte stream over an unreliable network

7.3.4 HTTP and HTTPS | HTTP vs HTTPS:

Both protocols HTTP and HTTPS (Secure HyperText Transfer Protocol) essentially retrieve objects in the same way. The HTTP standard to retrieve Web objects is evolving essentially independently from its secure counterpart, which effectively uses the HTTP protocol over a secure transport protocol called TLS (Transport Layer Security)

Static vs dynamic content or object

Static: The page is a static content if it is a document that is the same every time it is displayed. In contrast, if it was generated on demand by program or contains a program it is dynamic content.



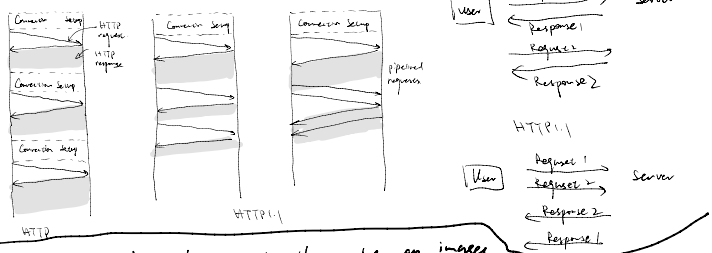
The requests and responses happen in the background; the user may not may not even be aware of them because the page URL and title typically do not change. By including client-side programs the page can present a more responsive interface than with server-side programs alone.

HTTP.1 vs HTTP1.1 HTTP.1: Establishing a separate TCP connection to transport each style icon became a very expensive way to operate.

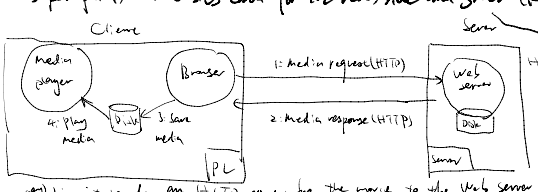
HTTP1.1: which supports persistent connections. With them, it is possible to establish a TCP connection, send a request and get a response, and then send additional requests and get additional responses. This strategy is also called connection reuse.

HTTP1.1 vs HTTP2:

HTTP 1.1: Through a mechanism called server push. HTTP2 allows the server to push out files that it knows will be needed but which the client may not know initially. Besides, in HTTP/2 the server can send smaller files first, so that the browser can start displaying the files before having the larger file available. That is not allowed in HTTP/1.1



The human eye has the property that when an images appears on the retina, the image is retained for some number of milliseconds before decaying; If a sequence of images is drawn at 50 images/sec, the eye does not notice that it is looking at distance images.; all video systems since the Lumiere brothers invented the movie projector in 1895 exploit this principle to produce moving pictures; The simplest digital representation of video is a sequence of frames, each consisting of a rectangular grid of picture elements, or pixels; most systems use 24 bits per pixel, with 8 bits each for the red, blue and green (RGB) components; Red, blue and green are the primary additive colors and every other color can be made from superimposing them in the appropriate intensity.



step 1: it sends an HTTP request for the movie to the Web server to which the movie is linked.

step 2: The server fetches the movie (which is just a file in MP4 or some other format) and sends it back to browser

step 3: The browser then saves the entire movie to a scratch file on disk in steps.

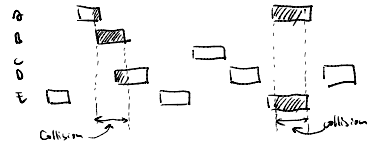
step 4: Finally, in step 4 the media player starts reading the file and play the movie

① JavaScript. Because there are only 14 annual calendars, depending on the day of the week on which 1 January falls and whether the year is a leap year. Thus, a JavaScript program could easily contain all 14 calendars and a small database of which year goes with calendar.

② PHP: This requires a large database. It must be done on the server by using PHP

③ Both web have JavaScript is faster.

Pure ALOHA: send the frame when ready, resend if the frame is destroyed



pure ALOHA is free

Whenever two frames try to occupy the channel at the same time, there will be a collision (as see in the figure) and both will be garbled. If the first bit of a new frame overlaps with just the last bit of a frame that has almost finished, both frames will be totally destroyed (i.e. have incorrect checksum) and both will have to be retransmitted later. The checksum does not (and should not) distinguish between a total loss and and a near miss. Bad is bad.

(a) A and C are hidden terminals to B, when transmit to B.
If A sends and then C immediately senses the medium, it will not hear A because A is out of its range. Thus C will falsely conclude that it can transmit to B. If C does starting transmitting, it will interfere at B, wiping out the frame from A. (We assume here that no CDMA-type scheme is used to provide multiple channels, so collisions garble the signal and destroy both frames.) We want a MAC protocol that will prevent this kind of collision from happening because it wastes bandwidth. The problem of a station not being able to detect a potential competitor for the medium because the competitor is too far away is called the hidden terminal problem.

(b) B and C are exposed terminals when transmitting to A and D.
If C senses the medium, it will hear a transmission and falsely conclude that it may not send to D (shown as a dashed line). In fact, such a transmission would cause bad reception only in the zone between B and C, where neither of the intended receivers is located. We want a MAC protocol that prevents this kind of deferral from happening because it waste bandwidth. The problem is called the exposed terminal problem.

- One can make a general statement about optimal routes without regard to network topology or traffic. This statement is known as the optimality principle.
  e.g. If a router from node A to node B is optimal, then every sub-path of that route must also be optimal. That is, if the path A to B is the best path from A to C, then the path from B to C must also be the best path from B to C.
- As a direct consequence of the optimality, the optimality principle, the set of optimal routes from all sources to a given destination form a tree rooted at the destination. Such a tree is called a sink tree
- Note that a sink tree is not necessarily unique; other trees with the same path lengths may exist.

e.g. (b) represents a sink tree for router B, which means that for every node in the network, the path from B to that node in the sink tree is as short as possible. It's a subset of the network that highlights the optimal paths from the sink (or root) to all other nodes.

Distance vector routing: Although it converges to the correct answer, it may do so slowly.

Link state routing: Not only is router memory consumed by ever-increasing tables, but more CPU time is needed to scan them, and more bandwidth is needed to send status reports about them.

Hierarchical routing within a network: There is a penalty to be paid: increased path length. For example, the best route from 1A to 5C is via region 2, but with hierarchical routing all traffic to region 5 goes via region 3, because that is better for most destinations in region 5.

Broadcast routing: Each router must have knowledge of some spanning tree.

(a) If only one network address is available on a host, all transport connections on that machine have to use it. When a segment comes in, some way is needed to tell which process to give it to. This situation called multiplexing, is shown in Fig (a). In this figure, four distinct transport connections all use the same network connection. (e.g. IP address) to the remote host.

(b) A host has multiple network paths that it can use. If a user needs more bandwidth or more reliability than one of the network paths can provide, a way out is to have a connection that distributes the traffic among multiple network paths on a round-robin basis. This is called inverse multiplexing.

- The form of fairness that is often desired for network usage is max-min fairness. An allocation is max-min fair if the bandwidth given to one flow cannot be increased without decreasing the bandwidth given to another flow with an allocation that is no larger.
- Each of the links between routers has the same capacity, taken to be 1 unit, though in the general case the links will have different capacities

•A max-min fair allocation is shown for a network with four flows, A, B, C, and D. Each of the links between routers has the same capacity, taken to be 1 unit, though in the general case the link will have different capacities, taken to be 1 unit, though in the general case the links will have different capacities. Three flows compete for the bottom-left link between router R2 and R5. Each of these flows therefore gets 1/3 of the link. The remaining flow, A competes with B on the link from R2 to R3. Since B has an allocation of 1/3, A gets the remaining 2/3 of the link. Notice that all of the other links have spare capacity. However, this capacity cannot be given to any of the flows without decreasing the capacity of another, low flow. If more of the bandwidth on the link between R2 and R3 is given to flow B, there will be less for flow A. This is reasonable as flow A already has more bandwidth. However, the capacity of flow C or D (or both) must be decreased to give more bandwidth to B, and these flows will have less bandwidth than B. Thus, the allocation is max-min fair.

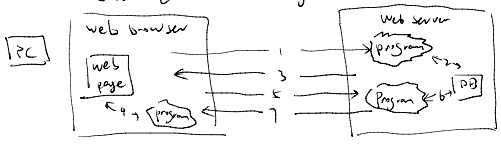
HTTP vs HTTPS: The protocol that is used to transport all the information between Web servers and clients is HTTP. Both protocols HTTP and HTTPS (Secure HyperText Transfer Protocol) essentially retrieve objects in the same way

The HTTP standard to retrieve Web objects is evolving essentially independently from its secure counterpart, which effectively uses the HTTP Protocol over a secure transport protocol called TLS (Transport Layer Security)

Static vs dynamic content or objects:

static objects: Files sitting on a server, presenting themselves in the same way each time they are fetched and viewed
e.g. logo, style sheets, header and footer
Generally amenable to caching

dynamic: This is content that can change based on user interaction, location, permission, etc.



The requests and responses happen in the background, the user may not may not even be aware of them because the page URL and title typically do not change. By including client-side programs, the page can present a more responsive interface than with server-side programs alone

HTTP/1 vs HTTP/1.1

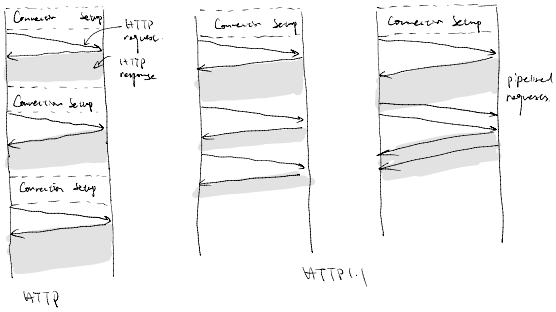
HTTP/1: Supports only one request per connection and does not support persistent connections, leading to more bandwidth waste and less efficient cache management

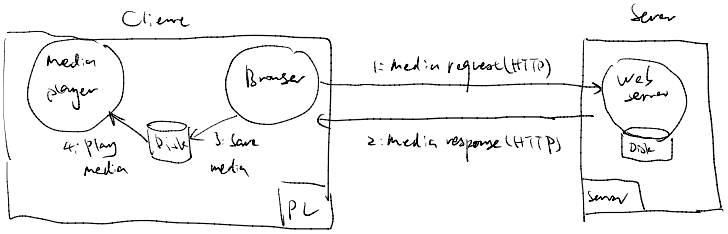
HTTP/1.1 which supports persistent connections. With them, it is possible to establish a TCP connection, send a request and get a response, and then send additional requests and get additional responses. This strategy is also called connection reuse

HTTP/1.1 vs HTTP2:

HTTP 1.1: It is characterized by loading resources one after the other, which can lead to one resource blocking another if there are issues with loading.

HTTP2: It allows a single TCP connection to send multiple streams of data at once, server push, which sends content to clients before they request it, and HPack header compression for faster loading





Step 1: it sends an HTTP request for the movie to the Web server to which the movie is linked.

step 2: The server fetches the movie (which is just a file in MPG or some other format) and sends it back to browser

step 3: The browser then saves the entire movie to a scratch file on disk in steps.

step 4: Finally, in step 4 the media player starts reading the file and play the movie.

① JavaScript. Because there are only 14 annual calendars, depending on the day of the week on which 1 January falls and whether the year is a leap year. Thus, a Javascript program could easily contain all 14 calendars and a small database of which year gets with calendar.

② PHP: This requires a large database. It must be done on the server by using PHP.

③ Both work, but Javascript is faster.