CS 4453 Computer Networks

Chapter 2 OSI Network Model

2015 Winter

OSI model defines 7 layers

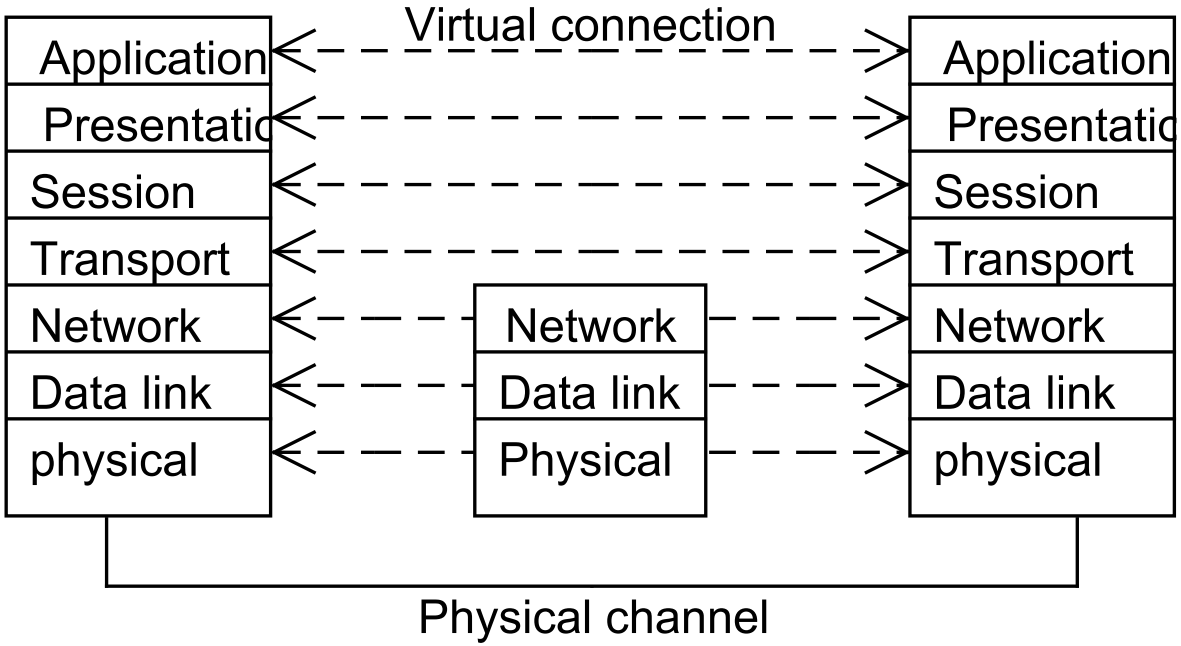

Figure 1: OSI model

The seven layers are as follows:

Application	Detailed application specific data being exchanged
Presentation	Conversions for representing data
Session	Management of connections between programs
Transport	Delivery of sequences of packets
Network	Format of individual data packets
Data link	Access to and control of transmission medium
Physical	Medium and signal format of raw bit transmission

2.1 Physical layer

- The physical layer handles the transmission of raw bits over a communication channel.
- Protocols in this layer specify the medium used for the transmission (electronic, optical or wireless), the signal format (serial or parallel, synchronous or asynchronous), and convert raw bit stream into common codes understandable by all the connected parties.
- CCITT/ITU (International Telecommunication Union) has established X.21 - X.24 to specify the functions at the physical lever for leased circuits. Other standard such as EIA-232 and v.21 - v.24 are widely used for various purpose.

Data encoding

- NRZ-L(non-return-to-zero level): binary data 1s and 0s are simple represented by two different voltages. It is also possible to use different voltage levels to transmit more than one bit at a time.
- NRZ-I (non-return-to-zero, invert-on-ones): similar to NRZ-L, but rather than measuring the absolute value of the signal element, two voltage are compared. If the two voltages are different, a 1 is transmitted, otherwise, a 0.
- Manchester coding (add synchronization), CSMA/CD, etc are also used for encoding.

Multiplexing schemes

Multiplexing schemes are used for more than one communication channels to share one physical link.

- FDM (frequency division multiplexing)
- TDM (time division multiplexing)
- CDMA (code division multiple access)
- WDM (wave division multiplexing)

CDMA uses some code which has orthogonal property:

$$c_i \cdot c_j = \frac{1}{n}\sum_{k=1}^{n} c_{ik}c_{jk} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$$

Where $c_i = (c_{i_1}, c_{i_2}, \cdots, c_{i_n})$ and $c_i \cdot c_j$ is called inner product. One way of implementation can use c_i and $\overline{c_i}$ to represent a bit 1 or bit 0, where c_i is a vector of 1, -1 and $\overline{c_i}$ is obtained by exchange 1 and -1 of c_i. Then

$$c_i \cdot \overline{c_j} = \begin{cases} -1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$$

For example, suppose we have 4 communication channels. Then we can use the following code.

	bit 1	Bit 0
channel 1	(1,1,1,1)	(-1,-1,-1,-1)
channel 2	(-1,-1,1,1)	(1,1,-1,-1)
channel 3	(-1,1,-1,1)	(1,-1,1,-1)
channel 4	(-1,1,1,-1)	(1,-1,-1,1)

It is easy to check that c_1, c_2, c_3, c_4 are mutually orthogonal.

Suppose in a moment, channel 1 is transmitting 0, channel 2 is transmitting 1, channel 3 is not transmitting and channel 4 is transmitting 0. Then

$$\begin{aligned}
S &= (-1,-1,-1,-1)+(-1,-1,1,1)+(0,0,0,0)+(1,-1,-1,1) \\
&= (-1,-3,-1,1) \\
c_1 \cdot S &= \frac{(1,1,1,1)\cdot(-1,-3,-1,1)}{4} = -1 \\
c_2 \cdot S &= 1 \\
c_3 \cdot S &= 0 \\
c_4 \cdot S &= -1
\end{aligned}$$

Data link layer

- Data streams are divided into frames, and the frames are send one by one.
- In data link layer, the addresses are the MAC addresses.
- Address Resolution Protocol (ARP) (RFC 826) is used to resolve the address from IP address to MAC address. But ARP only can resolve address for hosts and router interfaces on the same subnet.
- To connect two subnets, there must be some router with nore than one interface. Each of the interfaces has an IP address but the unique MAC address. Different ARPs use the different interfaces.

- Most popular wired LAN is Ethernet. But the transmission of Ethernet is not reliable (the receiver will not send back acknowledgment).
- In a computer, part of the link layer is implemented in a network adapter, or sometimes called network interface card (NIC). The heart of the network adapter is the link-layer controller, usually a single, special-purpose chip that implement link-layer services (framing, link access, error detection etc.).
- Part of the link layer functionality (link layer addressing, activating the controller hardware, etc) is implemented in software and runs in CPU.

Error detection and correction

Electromagnetic waves traveling over a transmission medium may encounter. Single-bit errors are the most common type in data communication. However, multiple-bit errors or burst errors are possible too. The data link layer must detect any errors in a received message.

- Parity check
- Arithmetic checksum
- Cyclic redundancy checksum (CRC)

The parity bit is obtained based on the count of 1s in the data block. The system can use either odd or even parity. Single-bit parity can detect 1-bit error. (but cannot find out which bit is wrong).

d data bits	parity bit
0111010100010110	0
0110100010001000	1

Figure 2: One-bit even parity

To detect two error bits, a two-dimensional parity mechanism may be used. A two-dimensional parity can correct one bit error or detect two error bits. Some error-correcting code can be used to detect and correct errors. Using error-correcting codes requires more redundancy.

Arithmetic checksum: the sender divides the sending data unit into equal segments. Then ones-complement arithmetic is used to add the segments together to get the result sum. The sum is complemented and appended to the data as the checksum field. As an example, consider four 4-bit data units as 1000, 1101, 0101 and 1110. The sum of these units is 1010 $(1000 + 1101 = 0110, 0110 + 0101 = 1011, 1011 + 1110 = 1010)$.

The check sum will be 0101 which is attached.

The CRC of data is generated at the transmitter end by means of a hardware that involves sequential circuits using shift registers and flip-flops. As as example, a bit sequence 11100110 is represented as $M(x) = X^7 + X^6 + X^5 + X^2 + X$. The CRC implementation using $G(x) = X^4 + X^3 + 1$ (11001), which is of degree 4. We have $X^4 M(x) \equiv X^2 + X \pmod{G(x)}$. So the message gives us 111001100110. Both sender and receiver know $G(x)$. So the receiver can use the last four bits to check if the string is correct. The CRC using $G(x)$ can detect up to 4 error bits. And also can detect more error bits in the probability of $1 - 0.5^4$. We omitted the detailed theory behind the CRC codes.

Framing

The frames help indicate the start and end of packets for the receiver.

Bit-oriented transmission uses a bit pattern 01111110 as a flag to indicate the frame's start and end.

Flag	Address	Control	Data (0 or more bytes)	CRC	Flag

Character-oriented transmission uses an integral number of bytes. The frame start is indicated by a special synchronization character SYN followed by a DLE (data link escape) character and an STX (start-of-text) character. The end of the frame is indicated by DLE and ETX(end-of-text) characters.

SYN	DLE	STX	Header	Data	DLE	ETX	CRC	SYN

Bit stuffing and character stuffing: A flag in the bit-oriented protocol determines the start and end of a frame. However, the data and other fields may also have the same sequence and the receiver may take the wrong sequence as the end of frame flag. A bit stuffing can be used for that purpose. For example, suppose the flag is 01111110. If any sequence of five 1 is found at the sender side after the start flag, a 0 is inserted. For example, if the data is as follows:

$$011110110111111011111011110$$

After bit stuffing, the data becomes:

$$01111011011111o1011111o011110$$

where o denote the 0 bit added.

For character-oriented transmission, similar method can be used. When the pattern DLE is inside the data, another DLE is inserted. This prevents the pattern DEL ETX from appearing anywhere in the frame except at the end.

Flow control

Defines both the way in which many frames are sent and tracked and how the stations do error control. For example, if errors have been found, a request to resend the erroneous frame can be sent to the sender. This type of error control is called automatic repeat request (ARQ). Sometimes the receiver may need the sender to stop sending data (e.g., buffer space not enough) and resume after some time. XON/XOFF characters can be used to do that. This method is more applicable to character-oriented asynchronous transmission.

For Bit-oriented or frame-oriented transmission, the following methods are used.

Stop-and-wait protocol: sender sends out a frame and then wait until receiving a positive acknowledge message from the receiver. The receiver checks the frame when it is received. Then sends a positive acknowledge message to the sender if no errors found, or otherwise sends out a negative acknowledge message. The sender then can send the next frame of resend the previous frame. A timer mechanism must be set for the cases when a frame is lost. When time-out, the sender retransmit the frame. However, the acknowledgment loss will cause duplicated frames. So a sequence bit will be put at each frame, that alternates between 0 and 1.

Sliding window protocol: using this protocol, a sequence of packets may be sent and received simultaneously. A sequence number is used for each packet. For example, if the sequence number uses 3 bits, then the number can be 0 - 7. The sender can send out at most 8 frames at a time. To keep track of sent and received frames, windows are implemented that open and close as frames are being sent or received. In sender's window, the left of the window moves when a frame is being sent and the right side moves when an acknowledged frame is being received. The maximum number of pending frames may not exceed the half of window size (4 if the window size is 8). The receiver's window is designed in a similar fashion.

Broadcast link

In a broadcast link, multiple sending and receiving nodes all connected to the same single shared channel. Ethernet and wireless LAN are examples of broadcast link layer technologies. One important problem for broadcast link is how to solve collisions.

Channel partition protocols: TDM, FDM and CDMA as we mentioned in physical layer. As an example, now we look at the TDM technology to partition a broadcast channel's bandwidth among all nodes sharing that channel. TDM divide time into time frames and each time frame is divided into N slots. Whenever a node has a packet to send, it transmits the packet's bits during its assigned time slot in the revolving TDM frame. One disadvantage of TDM is that some slots may be wasted if some nodes stop sending packets.

Random access protocols: a transmitting node always transmits at the full rate of the channel. When there is a collision, each node involved in the collision repeatedly retransmits its frame.

We use Slotted ALOHA as an example. In that protocol, all the frames are of the same size. The time is divided into slots such that each slot equals the time to transmit one frame. Nodes start to transmit frames only at the beginning of time slots. If two or more frames collide in a slot, then all the nodes detect the collision event before the slot ends. In the case of collision, the nodes retransmits its frame in each subsequent slot with probability p until the frame is transmitted without a collision. There is some method to calculate p to maximum efficiency of the slotted ALOHO. The drawback of this method is that when a collision happens, the slot is wasted.

Taking-turns protocols: let nodes take turns so that no time slot is wasted.

We introduce two important protocols. One is the polling protocol. In this protocol, one of the nodes is designated as a master node. The master node polls each of the nodes in a round-robin fashion. So the master node sends a message to node 1 saying that node 1 can transmit some maximum number of frames, then inform node 2 to transmit certain frames, etc. The procedure continues in this way, so that the nodes are transmitted in a cyclic manner. The drawback of this method is it introduces a poll delay-time needed for master node to notify the nodes. And if the master node fails, then the entire channel become inoperative.

Another protocol is the token-passing protocol. In this protocol, there is no master node. A small frame know as a token is passing though the nodes in some fixed order. For example, node 1 passes the token to node 2, node 2 passes it to node 3 etc. When a node received a token, then it transmits data frames up to some maximum number. Then the node passes the token to the next one. If the node does not have frames to transmit, then it simply pass the token to the next node. One drawback of the protocol is that if some node is failure to pass the token.

Data center networking

Each data center has its own data center network that interconnects its hosts with each other and interconnects the data center with the Internet.

The data center network supports two types of traffic: traffic flowing between external clients and internal hosts and traffic flowing between internal hosts. To handle flows between external clients and internal hosts, the data center network includes one or more border routers. Data center network design has been a research topic in recent years.

A data center usually provides many services. Inside the data center, the external requests are first directed to a load balancer whose job is to distribute requests to the hosts.