IB Computer Science Revision Notes

Topic 3 - Networks

3.1 Networks

Network fundamentals

3.1.1 Identify different types of networks

LAN: Local **A**rea **N**etwork. A small group of computers connected, usually over a very small area - a single room or a building. Usually done with copper cables.

MAN: Metropolitan **A**rea **N**etwork. Network over a larger are, usually city-size, connecting computers and LANs. Sometimes done with fiber optics as high speeds are required.

WAN: Wide **A**rea **N**etwork. Network over large geographical areas, often across and beyond entire continents. Most known WAN is the internet. Various transmission media, like phone cables, fiber optics and satellite transmission. Connects many computers, LANs or WANs.

VLAN: Virtual **L**ocal **A**rea **N**etwork. A type of network where computers behave like they were in the same LAN, but in reality they are far apart in different networks, from where they tunnel in into the virtual LAN. An example is Hamachi, often used by gamers to play multiplayer games that only support LAN parties, over the internet.

WLAN: Same as a LAN, just with radio wave connections instead of wires. In general slower than a LAN.

3.1.2 Outline the importance of standards in the construction of networks

Computer need standards to be able to communicate with each other, just as we need clear defined grammatical rules to be able to talk with each other.

3.1.3 Describe how communication over networks is broken down into different layers

The computer communications networks we use today are based on the OSI reference model. Aim of the OSI model is to allow communications across many different technical plattforms and to allow easy development. To reach this, the model defines seven consecutive layers with individual roles. It is easy to switch between the protocols in the same layer, even if they have a central function like the Internet Protocol (IP).

Sketch of the OSI model:

OSI Layer		Category	Protocol example	Units transferred
7	Application	Application oriented	HTTP, FTP, HTTPS	Data
6	Presentation			
5	Session			
4	Transport		TCP, UDP SCTP, SPX	TCP = segments UDP = datagrams

OSI Layer		Category	Protocol example	Units transferred
3	Network	Transport oriented	ICMP, IGMP, IP, IPsec, IPX	packets
2	Data Link		Ethernet, Token Ring FDDI, ARCNET	Frames
1	Physical (bit transmitting)			Bits

Following is a summary of the functions of each layer, but the IB does not require students to understand the functioning of the layers.

Layer 7 - Application layer: Services, applications and network management. This layer provides functions for the applications running on a computer. Data input and output happens over this layer.

Layer 6 - Presentations layer: This layer is the system specific presentations of the data (i. e. ASCII). It enables the correct exchange of data between different systems. Also, data compression and encryption belong to this layer. In general, it ensures that data sent by the application layer can be read by the presentation layer of the receiving system. If necessary, it works as a translation layer between the different data formats used by the two systems.

Layer 5 - Session layer: This layer takes care of the communication between two systems. It provides services to repair broken down sessions and creates the sessions for an organized and synchronised data transfer.

Layer 4 - Transport layer: Functions of this layer include segmenting the data stream and avoiding congestion. It provides a standardised interface for the above layers so that they don't need to be concerned with the features of the communication networks.

Layer 3 - Network Layer: In packet oriented networks, this layer is responsible for the forwarding of data packets. Data forwarding happens over the entire network and includes the routing of packets between the network nodes. The most importand functions of this layer include the provision of addresses across the network, routing and the processes of actualising and creating routing tables and the fragmenting of data packets.

Layer 2 - Data Link layer: Task of this layer is to ensure a faultless transmission of data and to regulate access to the transmission medium, by breaking up the bit stream in frames and providing those with checksums to be able to detect a corrupted data packet.

Layer 1 - Physical layer: This is the lowest layer. It provides mechanic, electric and functional help to activate and deactivate physical connections, keep them active and transmit bits through them. These can be electric, optical, electromagnetic waves or sound signals. This layer involves how a bit is transmitted across a medium.

3.1.4 Identify the technologies required to provide a VPN

One LAN that is connected to the internet.
One computer outside of the LAN that is also connected to the internet.
Some configuration.
VPN client and server.
A gateway.

3.1.5 Evaluate the use of a VPN

Through a VPN, it is possible to connect to a LAN that is protected from outside access through the internet. So, now it is possible for workers to connect to a company's internal network from almost anywhere on the world. This gave rise to home offices, as many office jobs do not require consultation and hence can be completed from home. For example, a mother workin half time as an accountant can bring her children to school in the morning, can then download necessary papers form the company's network through a VPN and complete her work, and by the time she finishes, she can pick her kids up from school. This has saved a significant amount of time in her daily schedule that would otherwise have been spent on travelling to and from work.

Data transmission

3.1.6 Define the terms: protocol, data packet

Protocol: a set of rules that communicating parties use when using a communication network.

Data packet: the compartmentalized pieces of information into which a message is broken down in a packet switching network system.

3.1.7 Explain why protocols are necessary

Protocols are the set of rules computers follow when communicaating across a network. Without them, no information can be transmitted as computers don't know how to interpret the signals coming through the network. Similarly, if you don't know a foreign language, you cannot talk with people who only speak that language.

3.1.8 Explain why the speed of data transmission across a network can vary

- Many users may want to transmit data through the network at the same time
- Interference to the network from the outside can corrupt many data packages, causing them to have been retransmitted

3.1.9 Explain why compression of data is often necessary when transmitting across a network

Earlier, data transmission often happened through the slow phone network, so compressing data for faster transmission was essential. Today, the transmission speeds have greatly increased, but we are transmitting far more data over the networks than earlier (movies, social media, news), so compression is needed to be able to transmit the enormous amounts of data without using up all the bandwidth.

3.1.10 Outline the characteristics of different transmission media

Metal conductor:

- Cheap
- Average to high speed
- High reliability
- Relatively secure

Fibre optics:

- Expensive
- Very high speed
- High reliability
- Relatively secure

Wireless:

- Price varying by size of network (WLAN is usually cheap)
- Middle speed
- Average reliability
- Insecure

3.1.11 Explain how data is transmitted by packet switching

Packet switching is a method of transmitting information over a computer network. The information is broken down into smaller pieces, the packets that are then transmitted across the network.

Every packet contains:

- The source of the packet
- The destination of the packet
- Length of the information part
- A running number of the packet
- Classification of the packet

The packets are transported as individual and independent units through the network, so they can travel on many different ways.

Advantages:

- Because the single packets are small, waiting times are low and because packets can travel through multiple channels independently, the network will be utilized better.
- Resources will be given fairly to participants in the network.
- Because of small packet size transmitting errors can be detected fast.
- High resistance against fallouts. If part of the network falls out packets can route around the broken down transmission lines.

Disadvantages:

- Because transport routes are not fixed, overloadings can occur at transmitting stations.
- Packets don't arrive in order (because they can take separate ways).
- All participants have to use the same network protocols.
- No constant bandwidth can be guaranteed and big fluctuations in bandwidth can happen.

Wireless networking

3.1.12 outline the advantages and disadvantages of wireless networks

Advantages:

- Easy to set up (no cablilng required)
- Can be installed almost anywhere (no need to drill holes etc.)
- Allows mobility (computers don't have to stay in same place)
- Easy to add new participants to network

Disadvantages:

- Traffic through network can be intercepted by unauthorized people
- Slow transmission speeds
- Interference from other wireless stations, cables etc. can happen, reducing speed
- Signal range depends on participating devices' antenna
- Many different standards may not compatible with each other (There are 5 differnt WLAN standards). Making wireless access points compatible with each standard is complicated (differnt antenna) and resource consuming, and can influence transmission speeds for individual participants.

3.1.13 Describe the hardware and software components of a wireless network

Hardware components:

- Antenna
- Networking interface card

Software components:

- Drivers providing the abstraction required by the operating system and inmplenting functions
- Firmware of the network card implementing transport oriented protocols

3.1.14 Describe the characteristics of wireless networks

WiFi:

- Also called Wireless LAN (WLAN)
- Used in laptops to connect wirelessly to home network
- Most preferred netwrok type to implement a home network
- Allows relatively slow to fast data transmissions (depending on the version)
- Backwards compatible with most older WiFi standards
- Small transmitting radius makes it suited for homes

WiMAX:

- Worldwide Interoperability for Microwave Access
- Designed for large distance high speed internet access
- Relatiely cheap method of providing internet over a large area - suited for poorer countries
- Rivaled by Long Term Evolution (LTE) standard
- Can be used as a form of wireless variant of DSL phone transmission lines

3G:

- The primary way mobile phones access the internet today
- Allows the tunneling of phone lines (mibiles don't have to switch back to phone network when receiving a call
- Relatively fast
- Network is heavily overloaded in germany

3.1.15 Describe the different methods of network security

Data encryption: information is scrambled using a set of mathematical rules and passwords so that it is only readable by the communicating parties. Examples are AES and RSA.

userID: a userID and password are used to identify the user. Usually, traffic after identification is handled using some type on encryption method.

3.1.16 Evaluate the advantages and disadvantages of each method of network security

Encryption types:

Advantages:

- A strong encryption is very hard to break
- Computer are fast enough to encrypt data on-the-fly

Disadvantages:

- Often, users are lazy and take a password that is easy to guess
- The password needs to be transmitted over the network to receiver to allow them to read the message
- Some encryptions are designed to haave backdoors built in

userID:

Advantages:

- Access rights to the network can be set for each user
- User groups can be created to manage user rights in batches

Disadvantages:

- A userID can be stolen
- system can be bypassed
- Does not protect against intercepting messages in the network

Created by Matyas Mehn — *Matyas Mehn [mailto:matyas.mehn@gmail.com] 2014/03/28 11:35*

---

topicthree.txt · Last modified: 2018/03/04 00:00 (external edit)