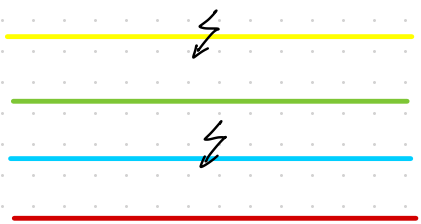
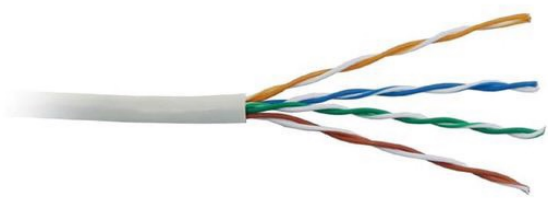
КУРС: КОМПЮТЕРНИ МРЕЖИ.
Networking

Cabling devices

Modern UTP cabels contain four pairs of wires where each pair forms a circuit electrical signals over copper cabels can be disrupted = нарушено
disrupted by interference
Electricity flowing through a copper cable creates a magnetic field. A magnetic field and a copper cable can create electricity. The problem is that a pair of wires running parallel creates a small electromagnetic field.



The field from one pair of wires can affect the signal on another pair of wires. this is called crosstalk. UTP eliminates most crosstalk by twisting the pairs of wires together



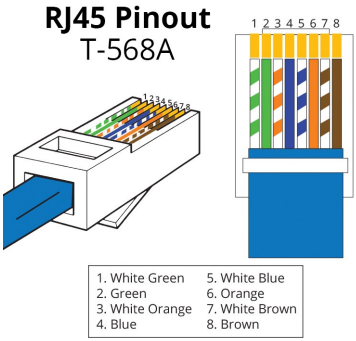
Интернет кабел

Each pair is no longer running in parallel so they don't generate the field. Each pair has a solid color and striped color

CATEGORY defines things like the number of pairs in the cable the thickness of the wire and how tightly they are twisted

RJ45 connector

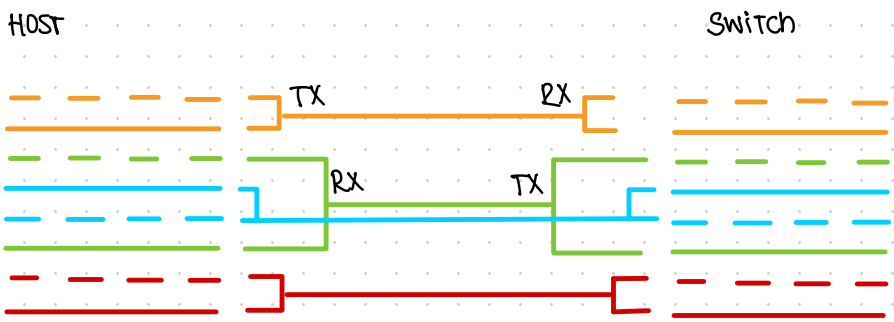
RJ45 is the part that you connect to your network card or switch port. This connector has eight pins. These pins line up with the 8 wires inside the cable.



The wires need to line up with the correct pins. That's why the wires are color-coded. There are different color-schemes you could use. like 568b

A STANDART UTP cable will MATCH the wires ON BOTH ends. This is called a STRAIGHT THROUGH cable

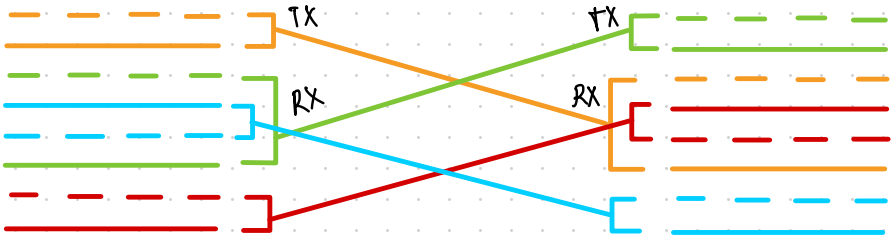
some pairs are used for transmitting data and others are used for receiving data.



A STANDART UTP is used to connect HOST to switch. if it is used to connect HOST to HOST OR OTHER, the wires wont line up correctly

CROSSOVER CABLE

CROSSOVER CABLE swaps the pairs at one end so transmitted lines up.

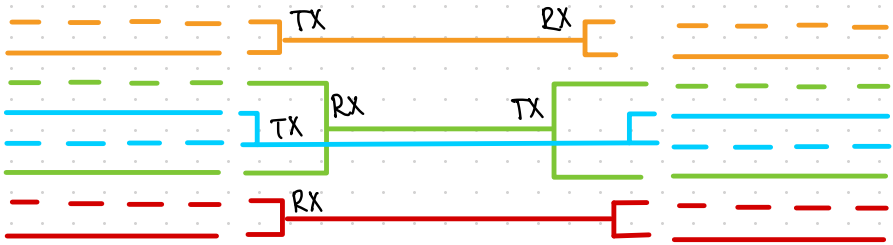


connecting one switch to another switch

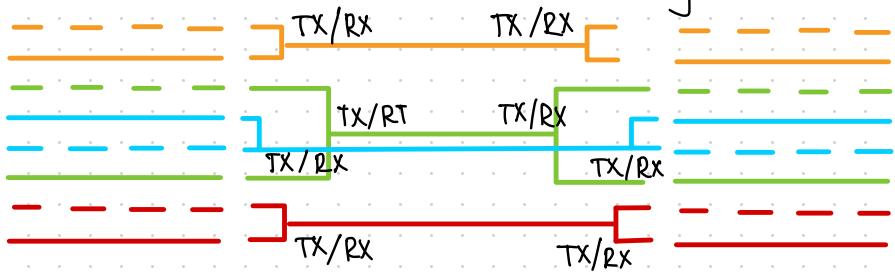
AUTO MDI-X - can detect if the wrong cable is used. it can then logically switch the functions of the pins so they match the cable. **100 Base TX**

1000Base TX

There are 2 ways this can work, which are called 1000 Base T and 1000 Base TX. The TX standart uses two pairs for sending and 2 paths for receiving. you will need cat 6 cabling or heigher if you want to use



The T standart uses all ports for sending and receiving



CAT5E

Fiber cabling

the alternative to copper cables are fiber cabels.

Fiber cables use strands of glass, which are sometimes called a pipe. A light pulses down the fiber strand. Light is another way to encode information.

Fiber is often used between networking devices like routers and switches.
it may also be used in servers

Duplex

Duplex devices need to both send and receive data.
UTP cables can send & receive at the same time. if both ends of the link support this — Full Duplex

Half Duplex - send -> stop -> receive -> stop ....

There are two different ways that fiber can be used.

single core → operates in half duplex mode

dual core → operates in full duplex

TX ——— RX
RX ——— TX

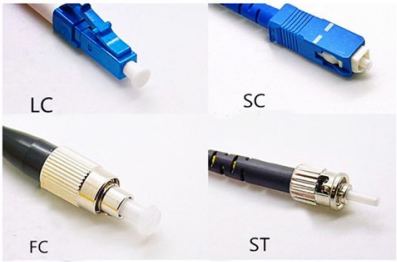
Types of Fiber

diff

Single mode fibre (SMF)	multi mode fibre (MMF)
laser light	LED Ligths - not powerful light
long distances (>2km)	short distances 500m
more expensive	cheaper

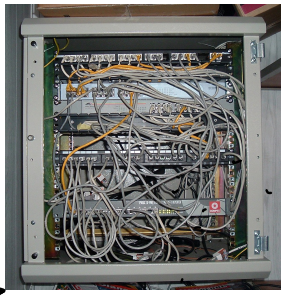
attenuation = degrading signal or signal loss

connectors



The main ones we see in data networking are called LC & SC. LC smaller connection types are used on switches and routers. LC -> dual core configuration

SC cables are older and larger. They are usually used in wiring closet



Wi-Fi

wireless connecting → Wi-Fi uses access points.

802.3 (Ethernet cabels) - ethernet

802.11 (Wi-Fi) = wireless

summary

- cables may be copper or fibre (LAN = local area network)
- The enthernet protocol describes physical links, and how data is formatted
- UTP uses pairs of wires, twisted together. some are for sending, others are for receiving
- straight-through UTP connects a host to switch. crossover UTP connects hosts to each other
- Auto MDI-X detects the cable type, and adapts if needed

- FULL DUPLEX devices send and receive at the same time.

HALF DUPLEX takes turns sending and receiving

- dual core = full duplex, single core = half duplex

Quiz

1) What speed does 1000Base-T run at? What type of cable does it use?

1000 GIGABITS CAT5E

2) What type of cable would you use to connect a host to a switch? What cable connects a switch to another switch?

straight-through UTP

3) When do you need to use MDI-X?

4) When might you want to use fibre instead of UTP? When would you need single-mode instead of multi-mode?

single mode - longer distances

5) What is bend radius? With which type of cable do you have to be especially careful of the bend radius?

6) What is required to support full duplex?

MAC addresses are used within the local LAN segment

IP addresses may be used to get to other segments

OSI MODEL

upper	Application	away
	Presentation	pizza
	Session	sausage
lower	Transport	throw
	Network	not
	Data Link	DO
	Physical	Please

Data as the application sees it starts at the application layer. This is where Network API's and apps that access the network live. For example, this includes FTP and web browsing. The data needs to be in format that can be easily understood. thats what the presentation layer is for. Anything related to data formats lives here such as image and video files. Session layer tracks application process. this include remote procedure calls and requests → building a session between local application and a remote one.

Upper layers → Application, Presentation, Session work with big amount of data, which don't work well for lower levels.

When the data reaches the transport layer it is broken into manageable chunks.

More information → destination address

Any information we add to the front of our data is called the header. Any information we add to the back in called trailor.

Each piece of data gets bigger as it moves through the network stack.

Application (Applications access network)

Applications access the network : web browsing, email, tranferring files, management sessions (SSH), Appication may contain a lot of data. this data may not always make sense to the rest of the network

Presentation encryption, compretion

so the presentation layer heeps by converting it if needed (encryption, compretion)

An application may need to talk to several other endpoints. So it is important to track

Session creates session between applications

where these conversations are occuring. Each of these conversations is called a session requests to remote services

Session control protocol - SCP

Transport : transports data between endpoints

Transport layer is used to transport traffic between processes on to endpoints. breaks data into segments.

We have many blocks of data probably going to different hosts for different applications. How do we track what goes where?

Uses port numbers Each flow of data has port number associated with the source and destination host. these values are added as part of a header to each block of data.

Network : adds network address ; add routing - маршрутизиране

To send information from one host to another we need some form of addressing. In addition to that we need a way to route through the network . Enthernet protocol. Adds another header

In the case of IP this includes the source and destination addresses. Once this is done the block of data is called packet

Header	→ IP source and sink address
Header	→ port number
data	→ some info

Now we have to think getting data from one device to another

Data link : creates logical link between devices on the same network segment

we need to have logical link as devices probably aren't directly connected. They are usually connected with a shared medium. → another heather with the MAC address is added (local address is added)

A trailor can also be added with error correction info

Once the header and the trailor are added. this block is now called frame.

The data link layer is special as it contains two sub layers.

the logical link control sub layer is responsible for

translating between the network layer and the data link layer. the media access control sub layer is the part that's responsible for adding headers and trailors to the packet + error correction

As data moves accross the network it will likely pass through one or more routers as each of these roures are a seperate device. the destination layer 2 addresses will change with each hop. But the destination layer 3 address will remain the same.

Physical layer: encodes data into physical signals

Concerns itself with the physical components of the network. This includes radio frequences & channels, pulsing light, pins... and standarts of copper cabeling.

IP addresses

192.168.0.100 - ipv4

FD3B:F15C:C672:34B8::100 - ipv6

192. 168. 0. 100

octet

1100 0000 1010 1000 0000 0000 0110 0100

$2^7+2^6 = 128+64 = 192$ $2^8+2^5+2^3 = 128+32+8 = 168$

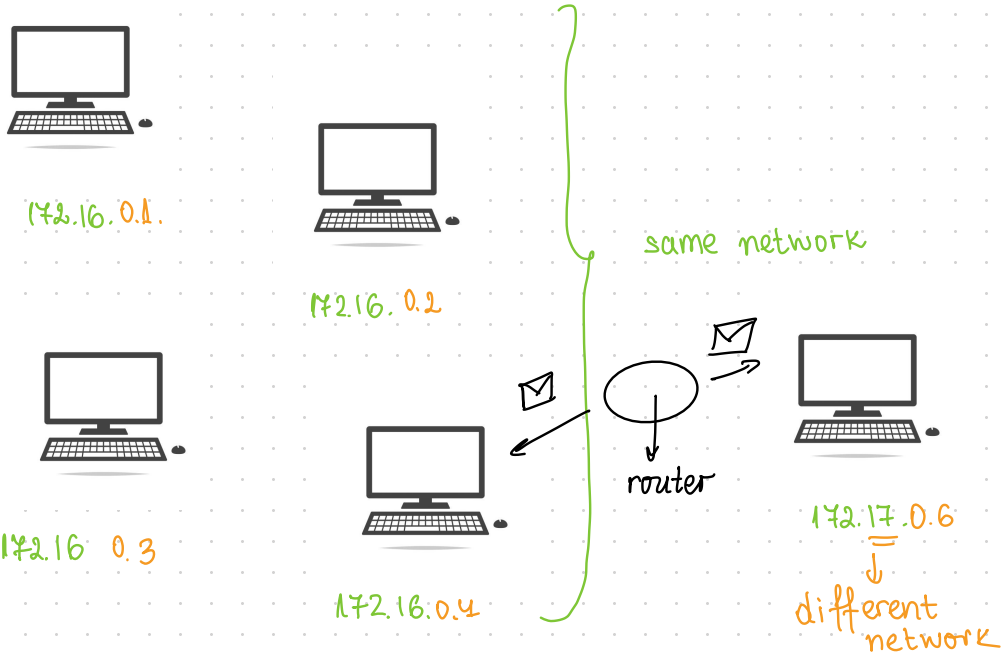
We call a range of addresses the IP space

IP addresses are two addresses in one

1. Host address 2. Network address

172.16.0.1

Network Host address



class A - large networks

1.2.3.4

network — host → 16 million hosts

0 000 0000 — reserved

128.0.0.0 → reserved

127 networks

IP space:

1.0.0.0 - 126.0.0.0

class B - medium networks

129.2.3.4 → Each network can have 65 thousand hosts

network — host

IP space:

128.0.0.0 - 191.255.0.0

The first bits of the network are always 10

1 000 0001 → 16 384 networks

2^7

Class C - small networks

IP space:
192.0.0.0 - 223.255.255.0

130.2.3.4 → 255 hosts
network host

1100 0001 0000 0010 0000 0010
fixed bits

- Summary:

Class A: one octet minus 1 bit

Class B: two octets minus 2 bits

Class C: three octets minus 3 bits

Ex. which class are they in?

9.4.3.147 - class A 1.0.0.0 - 126.0.0.0

203.42.62.1 - class C 192.0.0.0 - 223.255.255.0

103.88.77.22 - class B 128.0.0.0 - 191.255.0.0

151.10.13.55 - class B 128.0.0.0 - 191.255.0.0

222.127.16.4 - class C 192.0.0.0 - 223.255.255
hosts

Classes Networks and subnets

classless inter-domain routing or cidr

subnet mask

The subnet mask is also made up of four octets. This lines up with the IP address bit for bit. The bits set to one tell us which part of the IP address is the network. The zero bits are used for hosts. It's important to notice that all the ones go on the left and all the zeroes go on to the right

172.16.3.4

1010	1100	0001	0000	0000	0011	0000	0100
network				host			
1111	1111	1111	1111	0000	0000	0000	0000

Subnet mask tells us which part of the IP is for the network and which part is for the host

We haven't seen anything on how to save IP addresses

The real power of cider is to break a large network into small ones. We call this subnetting.

172.16.0.0 Now we can allocate 256 host

mask: 255 255 255 0 IPs per network

Devices in the same network must be in the same IP network

Ex. How many subnets do we have? How many host IP's per subnet?

172.16.0.0 class B

255.255.0.0 → subnets: 256^2 host IPs: 256^2 per subnet

mask → 255.255.240.0

1111 1111 1111 1111 1111 0000 0000 0000

subnets: $256^2 \cdot 240$ host

host IP's per subnet: $16 * 256$

Cidr notation

172.16.1.0 /24 /24 = 255.255.255.0

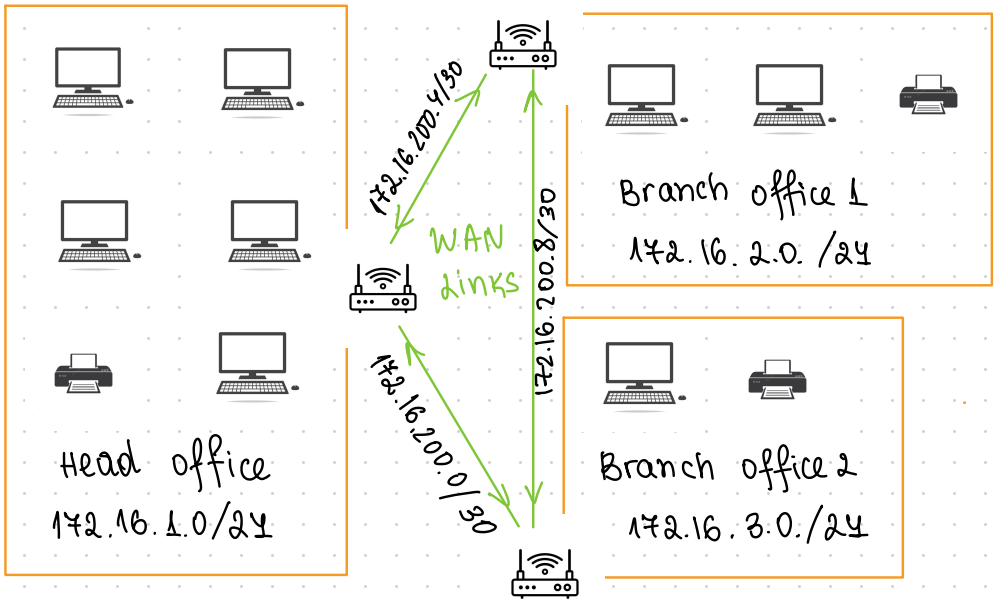
the first 24 bits are turned on

Joining networks is called supernetting

192.168.0.0/24 + 192.168.1.0/24 = 192.168.0.0/23

IP addresses in depth

VLSM = Variable Length subnet mask



172.16.0.0/16

we are wasting over 200 IP addresses

Break the /24 network further -> /30 thats 4 IP addresses in each network

The original network has been broken into subnets of different sizes

VLMS - creating subnets of different sizes

Address types

All the IP addresses that we have spoken about so far are addresses that are assigned to devices → host addresses

Often our devices only want to send traffic to one other device at a time. This is called unicast traffic

sometimes the device will want to send a message to every other device in the local network. This may happen if it wants a particular resource but it doesn't know where it is. it may broadcast a message asking who owns this resource or "where can I find this". This is called broadcast traffic.

to Broadcast to every other device we have a special IP address - broadcast IP. - the very last IP in the in the local network. (all host bits are turned on)

172.16.2.255 /24

=> 32 - 24 = 8 bits for the host

Broadcast = 172.16.2.255

Network address - the very first address all the host bits are zero 172.16.2.0

Network : 172.16.200.0

First IP : 172.16.200.1

Last IP : 172.16.200.2

} usable

Broadcast : 172.16.200.3

Let's have a device with IP 172.16.0.10/24

From the /24 we can see that the first three octets are the network and the last octet are the host bits.

Network 172.16.0.0 Broadcast : (255) 172.16.2.255.

8 bits = 256 addresses 256 - 2 = 254 usable ips

Example 2:

10.42.37.12 /22

1111 1111 1111 1111 1111 11 00 0000 0000

host

the magic number method

$$\underbrace{1111\ 1111}_{255}\quad \underbrace{1111\ 1111}_{255}\quad \underbrace{1111\ 1100}_{252}\quad \underbrace{0000\ 0000}_{0}$$

- Find the octet in the subnet mask that we need to work with - the one that's got a mixture of ones and zeroes

$$1111\ 1111\quad 1111\ 1111\quad \underbrace{1111\ 1100}_{252}\quad 0000\ 0000$$

- subtract its value from 256

$$256 - 252 = 4$$

- now we need to know the value of the third octet in our IP 10.42.37.12
- we count by four until we find the numbers that are next to the value of the third octet

4 8 12 16 20 24 28 32 36 40

we want the numbers immediatly smaller than and larger than 37. If we count by 4 that's 36 and 40. 36 is the start of the network that gives us the network address. 40 is the start of the next network. So we go back one IP and that gives us the broadcast. We know there are 10 host bits. that gives us 1024 IP adresses. Substract our two special addresses and we have 1022 usable IPs on this network.

network: 10.42.36.0

Broadcast: 10.42.39.255

Ex. ① 192. 168. 24. 210/24

1111 1111 1111 1111 1111 1111 0000 0000

Network: 192. 168. 24. 0

Broadcast: 192. 168. 24. 255

usable: 254.

② 172. 16. 111. 1 /30

1111 1111 1111 1111 1111 1111 $\underbrace{1111\ 1100}_{252}$

256 - 252 = 4 0 4

Broadcast: 172. 16. 111. 3

network: 172. 16. 111. 0

usable: 4 - 2 = 2

③ 10. 222. 76. 14/26

1111 1111 1111 1111 1111 1111 1100 0000 192

128 + 64 = 192

256 - 192 = 64

Network: 10. 222. 76. 0

Broadcast: 10. 222. 76. 63

usable: $2^6 - 2 = 64 - 2 = 62$

④ 203. 77 56. 89/22

1111 1111 1111 1111 1111 1100 0000 0000

256 - 252 = 4

Broadcast: 203. 77. 52. 0

network: 203. 77. 59. 255

usable: $2^{10} - 2 = 1022$

⑤ 88. 43. 59. 123/20

1111 1111 1111 1111 1111 0000 0000 0000

256-240 = 16 64-16 = 48

network: 88.43.48.0

broadcast: 88.43.63.255

usable: $2^{12} - 2$

we configure an IP address on e.g. windows machine we will also configure a default gateway. this is the local routers IP address. So when a host has no way of sending traffic to this destination on its own. It will forward it to the default gateway. Some device is called the default gateway the Gateway of last resort.

There's another special IP used for broadcasts. It's

255.255.255.255 Broadcast : send this traffic everywhere

routers are made to forward traffic between networks

routers never forward Broadcast messages

Multicast traffic : opt-in to receiving certain traffic

unicast, Broadcast, multicast traffic

Public and private

10.0.0.0/8 172.16.0.0/12 192.168.0.0/16 → no Internet

NAT - network address translation

The TCP/IP Model

TCP (reliable)	UDP (unreliable)
additional features	lightweight
connection oriented	connectionless
error recovery + flow control	doesn't care about errors

SOCKET = local IP + local port number + protocol

socket can identify which application the network data belongs to

TCP -> windowing : both sides of the conversation agree on how much data can be sent at once

ordered data delivery TCP

UDP -> good for real time applications