How to connect?

Dr. Małgorzata Langer

DHCP – *Dynamic Host Configuration Protocol*

- It is in the application layer
- It was published as the standard in 1993 (RFC 2131); DHCPv6 – described in RFC 3315 is the integral part of the description of IPv6
- **Communication Protocol** – it allows to obtain configuration data from the server (IP host address, network gate, DNS, subnet mask …)

- DHCP protocol describes three technics of granting IP addresses:
- Manual
- Automatic
- Dynamic
- Some DHCP servers grant the specific DNS address to each client, and it is submitted to the ‘names’ server’ by a protocol compatible with RFC 2136 specification

- Manual granting (based on MAC address table and their suitable IP addresses – which is prepared by the administrator of the DHCP server). Only computers that have been registered by the system service office are allowed to work in internet.
- Automatic granting – the administrator determines the range of IP addresses. Unoccupied IP addresses are granted to successive clients that apply – for the whole period of being switched to the network.
- Dynamic granting - the administrator determines the range of IP addresses to be granted but it is rather less than the number of clients. After starting the clients get their addresses automatically, but for a given period, only. Such a configuration allows to obtain addresses by any next successive clients that wait.

Messages for dynamic granting

- **DHCPDISCOVER** – to localise servers
  "To all DHCP servers in the network. I need the IP address”
- The client has no IP address yet, so cannot use TCP /IP – it sends this requirement in UDP
- **DHCPOFFER** – sending parameters
- The DHCP serer send the IP address. It is possible that there are several DHCP servers in the network and the client may obtain several offers – SELECTION CRITERIA ARE NOT DESCRIBED IN THE STANDARD
  The client decides and sends in UDP the requirement to the selected DHCP server: **DHCPREQUEST** – the request to grant applied parameters

DHCP messages – continued

- **DHCPACK** – confirmation of granting parameters

The servers grants the temporary IP number; the client verifies if this number is not used by another computer in the network and records obtained parameters.
The inherent parameter is the valid period for the settings (using the granted IP number) (lease – minutes? hours? days?).

There are two backgrounds clocks - T1 measures the half of the valid period, and T2 – 87.5% of the full period. These values are set and may be changed in optional settings of DHCP server – if such functions are implemented there.

When T1 time passes, the client sends the message **DHCPREQUEST** to the server and asks if this period can be prolonged. This is renewing status. If the possibility exists, the server answers with the message **DHCPACK** and grants a new period. Then T1 and T2 clocks are reset.

DHCP messages – continued

- If the client does not obtain the DHCPACK message and T2 is over, rebinding status begins.
- The client must send the DHCPREQUEST message again to obtain the prolongation.
- The server may answer then with the acknowledgment - DHCPACK. But if there is no answer still, the client must start again, so must send its question to all DHCP servers.

DHCP messages – continued

- DHCPNAK – refusal to grant parameters – the client returns to the start
- DHCPDECLINE – the indication that the IP address that has been sent in DHCPACK is used already
- DHCPRELEASE – releasing the address
- DHCPINFORM – requirement to get the parameters only (without IP address).

Router

- The device that is the communication node
- It works in the third OSI layer
- It operates with the packets exchange between different (various masks) networks
- Basing on the info in TCP/IP packets (but other protocols are also served) – it can send packets from the source network, that is connected to it, to the receiving one
- **Routing – is the process of finding the route.**

- According to various methods to route, the router can estimate all available info and basing on it to undertake the decision – what route will be selected for the packets.
- Router may use info which the administrator has given in the configuration or obtained from processes started on other routers

The table made on the base of known localisations is the base of processing and switching packets. When the table items are credible – the router works properly.

Types of routers

- Access Routers – SOHO *Small Office, Home Office* – Small devices used at home and in small companies (“to distribute internet” to several computers). The most common is that they have one or two WAN links (~ Ethernet), or ADSL (Asymmetric Digital Subscriber Line) modem, wireless access (hotspot), sometimes VoIP socket…

Routers

- Corporation Routers – many additional functions
  - inside the network, to connect different segments
    (routing packet between two end terminals and other routers)
  - edge routers – their key function is SAFETY; there are firewalls installed that allow the remote users to access. These routers should operate with different transmission techniques, and have good telecommunication parameters (high capacity).

Routers

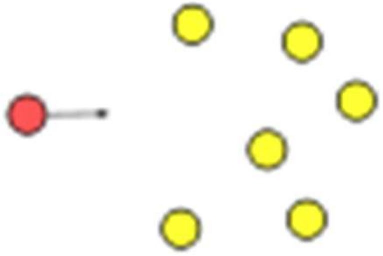
- Core network (Framework) routers – high capacity, many interfaces, many transmission techniques, different standards, high reliability, module structure

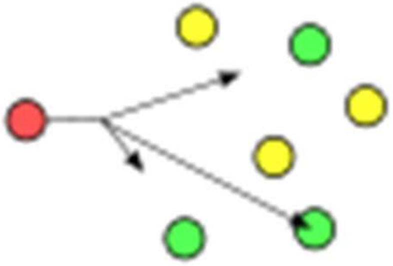
Types of routing depending on the destiny

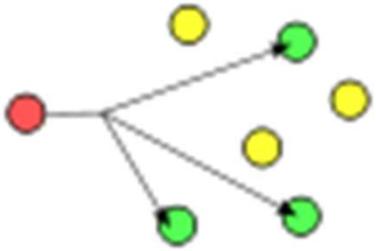
- UNICAST – sending the message to one, single and determined node (it is dominated way in internet)
- BROADCAST – sending the message to all nodes in the network
- MULTICAST – sending the message to the group of nodes which are interested in obtaining such messages
- ANYCAST – to anyone from the group – mostly to the closest neighbour for the source
- GEOCAST – sending the message to a given geographical region

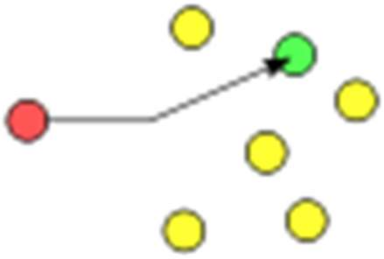
Anycast

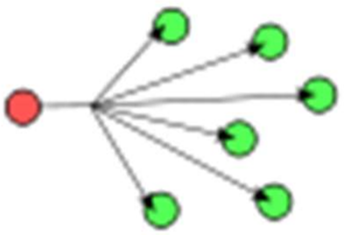
Multicast

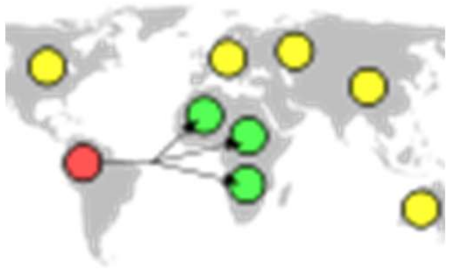












Unicast

Broadcast

Geocast

Routing protocols

- The exchange of information on the routes between networks is possible
- Without such an exchange only the route to the next, closest, known router could be realised
- Thanks to this exchange one may consider loads, fails, configuration changes, etc.

Internal routing protocols – IGP – *Interior Gateway Protocol*

- Designed for the info exchange inside autonomic systems
  - RIP – Routing Information Protocol
  - OSPF (Open Shortest Path First)
  - *Dijkstra algorithm*
  - EIGRP (Enhanced Interior Gateway Routing Protocol) – CISCO

External routing protocols – EGP – *Exterior Gateway Protocol*

- To exchange the info on routes between different autonomic systems, for example:
  - **BGP – Border Gateway Protocol** – v.4 (edge gate protocol) is the base of modern internet.

  BGP protocols work basing on the layer 4 protocol; relations among neighbours are made thanks to TCP protocol

BGP

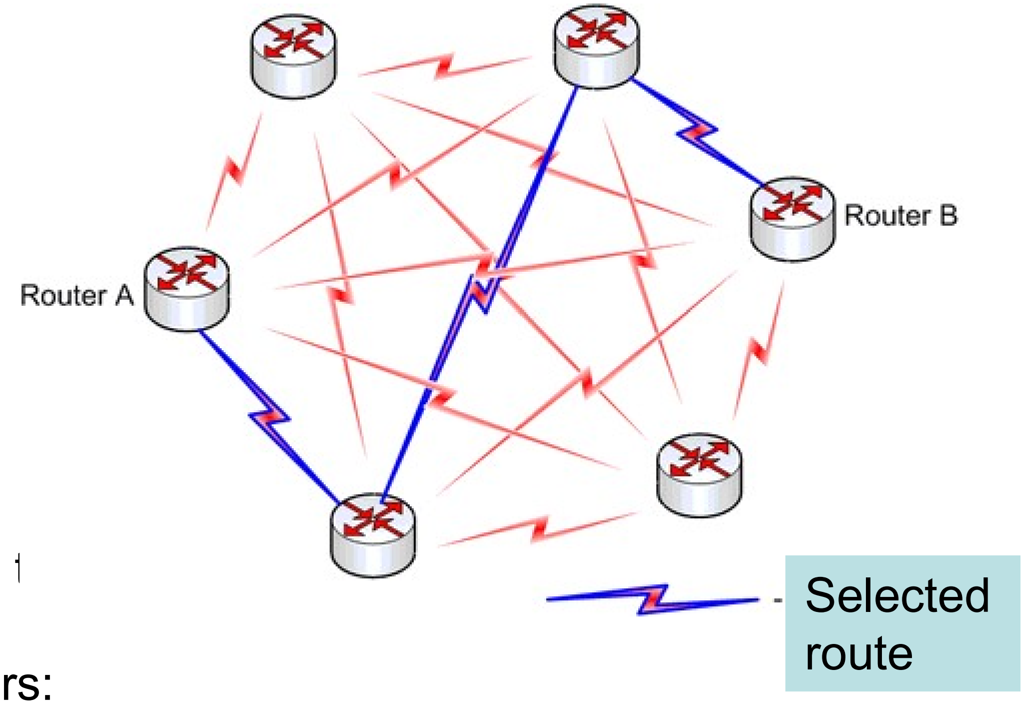
- BGP protocol starts relations between different autonomous systems. *Autonomous System*, AS, is a network or a group of networks with common administration and routing politics.
- Autonomous systems are identified by AS numbers. They cover 4 bytes (2 bytes till 2007).

Routing

- BGP determines the route basing on many parameters (attributes)
- If BGP obtains several routes to a given receiver in a remote network, it chooses one route only. And it will be the best one among equivalent routers
- Attributes are described in details (also in internet) – you are encouraged to study them on your own.

BGP

- Routers set the BGP sessions between each the other, basing on the protocol of the layer 4 (TCP port, No. 179). Thanks to that they may exchange messages on accessible routes (prefixes) and select the best route to destined networks without loops



Routing relies in making possible
choosing the next jump during the t
travel to the receiver.
In the routing process one considers:
- distance
- link capacity,
- overloads in link,
- link cost

and others ……

Networks	Next device	Distance	Timers	Flag
Network No. 1	Router A	4	t1, t2, t3	X, y
No. 2	Router B	5	t1, t2, t3	X, y
No. 3	Router C	7	t1, t2, t3	X, y

Timers

- routing update timer (30 sec)- the frequency of sending out info messages on routing,
- route invalid timer(90 sec)- if the unit does not obtain any renewal of the offer, perhaps the path is not valid
- route flush timer (270 sec)- after 270 sec all routing info pieces on the route are deleted.

RIP – Routing Information Protocol

- Protocol of „distance vector” type; open standard; simple in implementation; often used, mainly inside the network
- Problem – a loop may arrive
- Solution: limit for the maximum number of jumps (15). All networks that are not covered by this number are considered as unreachable.