Network forwarding and routing.

1. IP-forwarding and IP-routing.

- **IP forwarding**- this is the process of forwardingIP packets from a source node to a destination node in an IP network with an arbitrary topology based on the solution of a routing problem.
- **IP routing**- is a process that solves the problem of choice the best route.
- **Node**(network node) - any device that has a network interface with configured TCP/IP protocol;
- **Host**(host) - a node that does not have the ability to route packets;
- **Router**(router) - a node that has routing capabilities (redirecting datagrams from one network to another), usually such a node has several network interfaces (with their own MAC and IP addresses) connected to different IP networks.

The fundamental difference between a host and a router is that a host never forwards datagrams from one of its interfaces to another, but the IP layer on a host can be configured to perform routing functions (ip-forwarding), in addition to acting as a network interface, otherwise datagrams not destined for the host will be silently dropped.

The figure shows a simplified model of the forwarding and routing processes at the IP level.

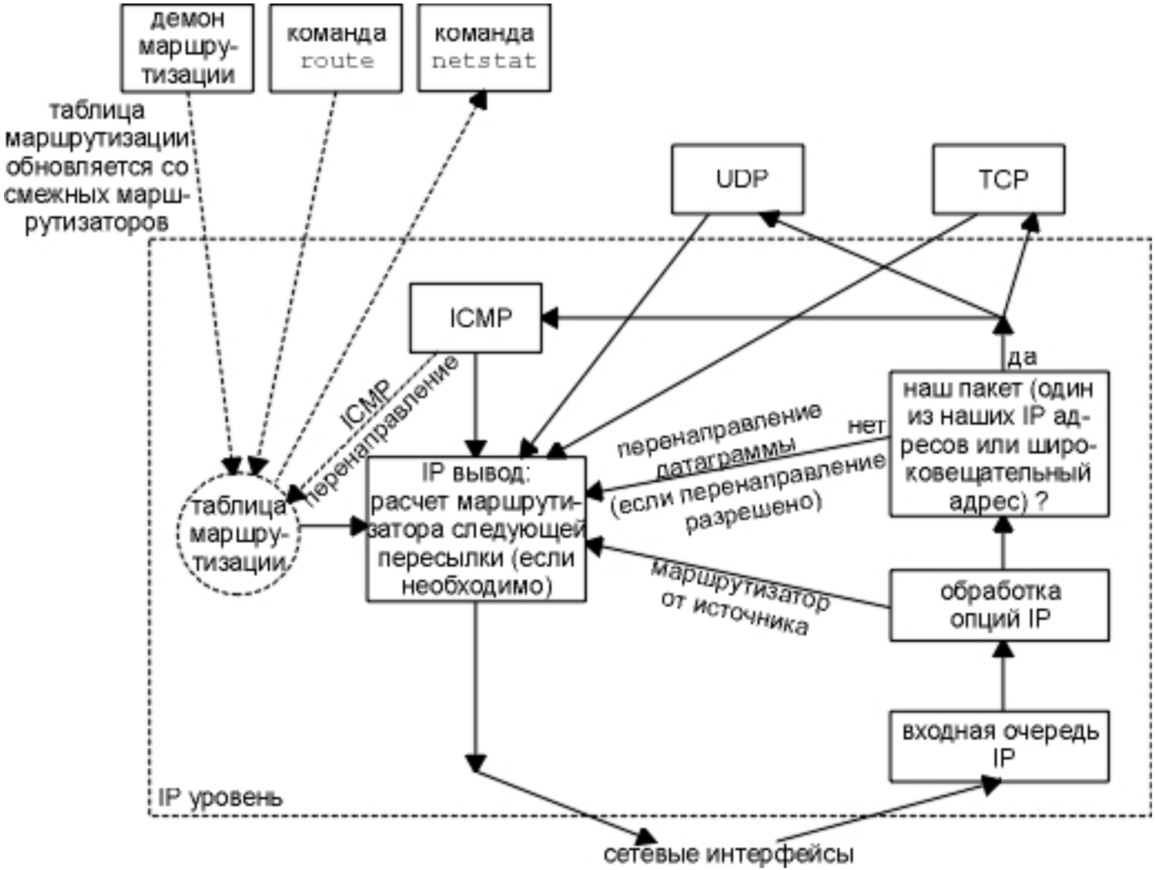

демон маршру-тизации
команда route
команда netstat
таблица маршрутизации обновляется со смежных марш-рутизаторов
UDP
TCP
ICMP
ICMP перенаправление
да
нет
наш пакет (один из наших IP ад-ресов или широ-ковещательный адрес) ?
перенаправление датаграммы (если перенаправление разрешено)
таблица маршру-тизации
IP вывод: расчет маршрути-затора следующей пересылки (если необходимо)
маршрутизатор от источника
обработка опций IP
входная очередь IP
IP уровень
сетевые интерфейсы

Fig. Actions performed by the IP interface layer.

To forward a packet, the IP layer must have the following information:

- Destination address.
- The address of a neighboring router from which it can learn about remote networks.
- Accessible paths to all remote networks.
- The best path to each remote network.
- Methods for maintaining and verifying routing information.

In general, the IP forwarding process is the same in networks of any size and consists of a series of individual direct or indirect packet routing operations.

If the target network is directly connected to the router, then the following is used to send packets: **direct forwarding**, otherwise -**indirect forwarding**through an intermediary.

The router learns the access paths to the remote network using routing **static**(information is entered manually by the administrator) or**dynamic**
(the location of networks is determined from information from neighboring routers).

If online**a change will occur**, then the dynamic routing protocol informs all routers about the change**automatically**. If static routing is used, the system will have to update the routing tables on all devices. **Administrator manually**.

2. The process of direct IP forwarding.

When one IP network node sends a packet to another node, the IP header specifies the sender's IP address and the recipient's IP address. The packet is sent as follows:

1) The sender determines whether the recipient is on the same IP network as the sender (local) or on a different IP network (remote). To do this, the sender performs a bitwise multiplication of the sender and recipient IPs by the sender's subnet mask. If the results match, then both nodes are on the same subnet.

2) If the nodes are in the same IP network, the sender checks the ARP cache for the recipient's MAC address. If the required entry is present, then the packets are sent directly to the recipient node at the data link level. If the required entry is not present, the sender sends an ARP request with the recipient's IP address, places the response in the ARP cache, and the packet is also sent at the data link level (between the computers' network adapters).

3) If the sender and receiver are located in different IP networks, the sender sends this packet to the network node that is specified in the routing table as the best or that is specified in the sender's configuration as the DefaultGateway. The default gateway is always located in the same IP network as the sender node, so interaction occurs at the data link level (after executing the ARP request).

In general, the process of IP forwarding a series of individual operations, direct or
is indirect packet forwarding

3. Indirect forwarding and routing tables.

Each network node makes a decision about forwarding a packet based on the routing table, which is stored in the RAM of the node. The interface to which the packet will be sent is determined in the following sequence:

- Search for a matching host address.
- Search for a matching network address.
- Search for a default item (usually specified as a network with an identifier0.0.0.0).

On the other hand, the routing policy sets the rules by which it is decided which route will be entered into the routing table.

The IP module implements**forwarding mechanism**, whereas the routing daemon typically determines**routing policy**.

Routing tables exist not only in routers with multiple interfaces, but also in workstations connected to the network via a network adapter.

The routing table in Windows can be viewed using the route print command, and in Linux using the netstat -r command.

Each routing table contains a set of entries that can be formed in different ways:

- **automatic entries**, created automatically by the system based on the TCP/IP protocol configuration on each of the network adapters, see ifconfig/ipconfig;
- **automatic entries**, created automatically by the system for special routes, for example, loopback 127.0.0.0/8.
- **static records**, created by the administrator, for example, by the route add command (Linux, Windows) or in the Routing and Remote Access Service console (Windows);
- **dynamic records**, created by the ICMP redirect message, see the ICMP lecture;

- **dynamic records**, created by ICMP Router Discovery and ICMP Router Advertisement messages, see the ICMP lecture;

- **dynamic records**, created by various routing protocols (RIP v1/v2, RIPng (IPv6) OSPF, BGP v1/v2, BGP v3/v4 (IPv6), etc.). These protocols will be discussed below.

Let's look at examples of typical routing tables: for workstations in a local network and for a server with several network interfaces.

3.1. Routing table (TM) of Windows workstation.

An example of a TM that a Windows XP host builds based on the configuration of its interfaces.

```
C:\>route print
IPv4 route table
===========================================================================
Interface List
0x1 .......................................... MS TCP Loopback interface.
0x10002 ...00 26 a1 6f 05 ......
                                        Realtek RTL8139 Family PCI Fast Ethernet NIC
===========================================================================
Active Routes:

       Network address          Network mask     Gateway address     Interface       Metrics
 (Network Destination)             (Netmask)           (Gateway)    (Interface)      (Metric)
               0.0.0.0               0.0.0.0         192.168.1.1   192.168.1.10             1
             127.0.0.0             255.0.0.0           127.0.0.1      127.0.0.1             1
           192.168.1.0         255.255.255.0        192.168.1.10   192.168.1.10            20
          192.168.1.10       255.255.255.255           127.0.0.1      127.0.0.1            20
         192.168.1.255       255.255.255.255        192.168.1.10   192.168.1.10            20
             224.0.0.0             240.0.0.0        192.168.1.10   192.168.1.10            20
       255.255.255.255       255.255.255.255        192.168.1.10   192.168.1.10             1
Default Gateway: == ...                    192.168.1.1



  None
```

Example, for Windows XP, with settings: IP/mask - 192.168.1.10/24, gateway - 192.168.1.1.

Interface List(Interface List) - List of network adapters installed in computer. The Loopback interface is always present. Ethernet NIC is a network card.

Active Routes. Next comes the route table itself. Each row of the table is a route for any IP network.

Default Gateway(Main Gateway) - corresponds to the valueThe IP address of the default gateway in the TCP/IP configuration of this station. This is the address of the router to which traffic is sent for which a route cannot be determined based on the routing tables.

What happens if no match is found for the specified destination and there is no default route?

If the datagram was generated directly by this host, the error (host unreachable) or (network unreachable) is returned to the application that sent the datagram. If the datagram must be forwarded, an ICMP host unreachable message is returned to the sending host.

Persistent Routes(Permanent Routes) - a list of static routes for the workstation, which are created by the administrator using the route command. There are none of them in this example.

To read any entry in the routing table, you need to do the following: *"To deliver a packet to the network with an address from the field**Network address** and a mask from the field**Network mask**,*
it is necessary through the interface with the IP address from the field
***Interface** send packet to IP address from field**Gateway address**,*
*and the "cost" of such delivery will be equal to the number from the field**Metrics**.»*

The table defines multiple entries (routes) with different parameters.

- 0.0.0.0/0 - "undefined" route (compared last) for sending packets to the default gateway.
- 127.0.0.1/8 — route for sending unicast packets in the internal network of the node (to itself).
- 192.168.1.0/24 is a route for sending unicast packets in a local IP network (your own network).
- 192.168.1.10/32 — route for sending unicast packets for the IP of this node (to itself).
- 192.168.1.255/32 is a route for sending packets to the broadcast address for all network nodes.
- 224.0.0.0/6 — route for sending multicast packets in the internal network of the node (to itself).
- 255.255.255.255/32 is a route for sending unicast packets to a given node in a given network.

Windows uses a cost metric that is based on the connection speed.

Connection speed	Metrics
Greater than or equal to 2 GB	5
More than 200 MB	10
Greater than 80 MB and less than or equal to 200 MB	20
Greater than 20 MB and less than or equal to 80 MB	25
Greater than 4 MB and less than or equal to 20 MB	30
More than 500 KB and less than or equal to 4 MB	40
Less than or equal to 500 KB	50

3.2. Linux routing table.

The route -n, netstat –nr commands. Without the -n option, the netstat command looks at the /etc/networks file and takes the network names from there, which can cause some confusion with host names.

```
$ netstat -nr
Kernel IP routing table
Destination      Gateway          Genmask          Flags      Metric Ref   Use   Iface
0.0.0.0          192.168.111.1    0.0.0.0          UG         0 0          0     eth0
192.168.111.0    0.0.0.0          255.255.255.0    U          0 0          0     eth0
127.0.0.1        127.0.0.1                         UH         0 0          0     lo0
224.0.0.0        140.252.1.32                      U          1 0          0     eth0
140.252.13.35    140.252.1.183                     UGHD       1 0          0     eth0
```

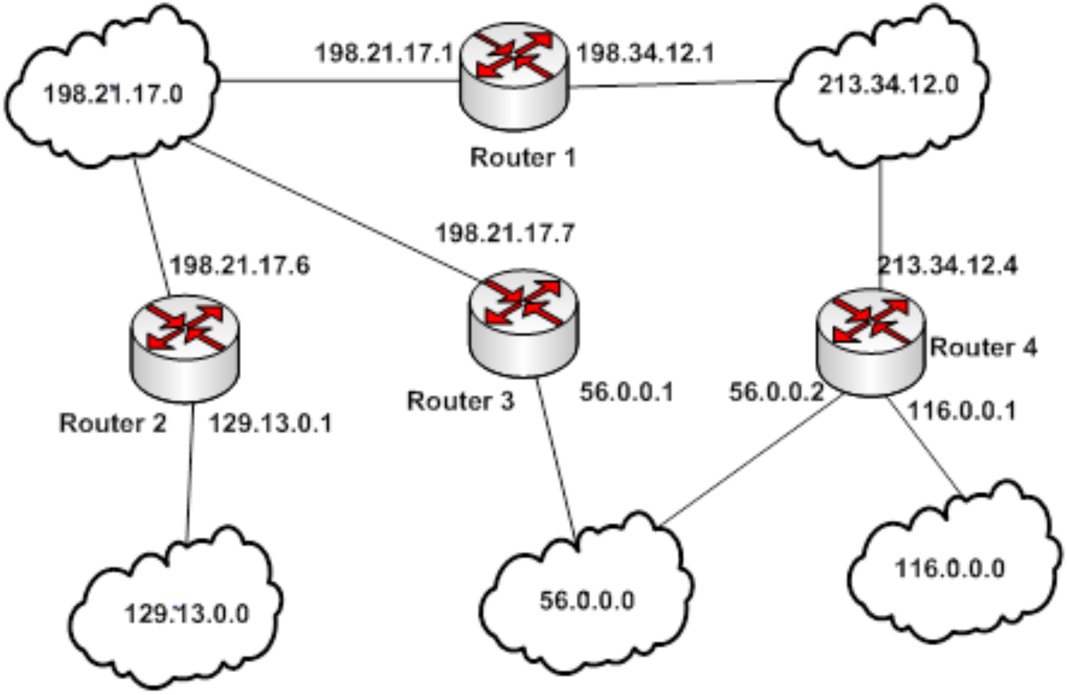
On Linux/UNIX, several flags may be shown for a particular route, for example:

- U - route is active.
- G - the route is connected to a gateway (router). If this flag is not set, the destination is considered to be directly connected.
- H - The route points to a host, which means that the full host address is used as the destination. If this flag is not set, the route points to a network.
- D - The route was created via an ICMP redirect.
- M - the route was modified by an ICMP redirect.

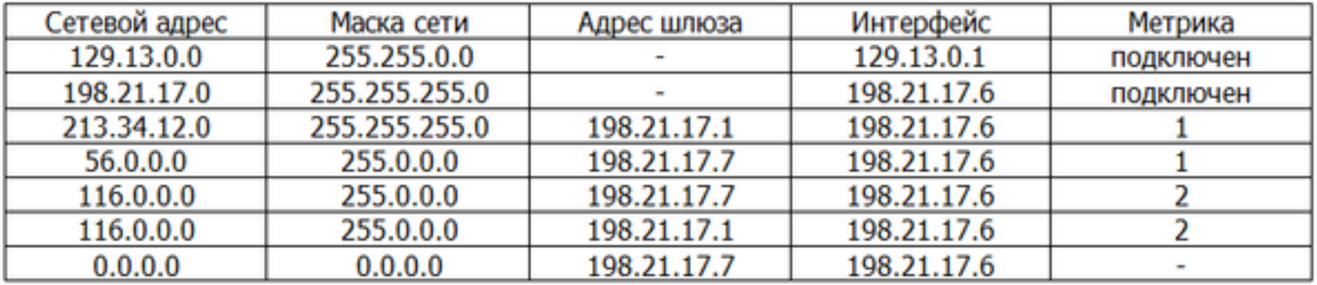
Ref is the connection counter, Use is the counter of the number of transmitted packets.

3.3. Router routing table (TM).

Let's consider a typical network with multiple routers.



Routing table for Router 2is a typical example of a table routes using network IP addresses for the network shown in the figure above.



Сетевой адрес	Маска сети	Адрес шлюза	Интерфейс	Метрика
129.13.0.0	255.255.0.0	-	129.13.0.1	подключен
198.21.17.0	255.255.255.0	-	198.21.17.6	подключен
213.34.12.0	255.255.255.0	198.21.17.1	198.21.17.6	1
56.0.0.0	255.0.0.0	198.21.17.7	198.21.17.6	1
116.0.0.0	255.0.0.0	198.21.17.7	198.21.17.6	2
116.0.0.0	255.0.0.0	198.21.17.1	198.21.17.6	2
0.0.0.0	0.0.0.0	198.21.17.7	198.21.17.6	-

Multi-route tables. Here presented multi-route table routing, since it contains two routes to the 116.0.0.0 network. In the case of building a single-route routing table, only one path to the 116.0.0.0 network is specified based on the lowest metric value or for other reasons. Multi-route tables allow for more flexible and faster response to changes in networks.

Next hop routing. In this table, the "Network Address" column contains the addresses of all networks, which this router can forward packets. The TCP/IP stack uses the so-called one-step approach to optimizing the packet forwarding route (**next-hop routing**) – each router and end node takes part in choosing only one step of packet transmission. Therefore, each line of the routing table does not indicate the entire route as a sequence of IP addresses of routers through which the packet must pass, but only one IP address -**next router address**, which needs pass the packet. Along with the packet, the next router is given responsibility for choosing the next routing hop. The one-hop approach to routing means **distributed solution of the route selection problem**This removes the limitation on the maximum number of transit routers along a packet's path.

Default gateway. One-hop routing has another advantage - it allows to reduce the volume of routing tables in end nodes and routers by using the so-called default route (0.0.0.0) as the destination network number, which usually occupies (is processed) the last line in the routing table. If the routing table contains such an entry, then all packets with network numbers that are not in the routing table are transmitted to the router specified in the default line. Therefore, routers often store limited information about the networks of the Internet in their tables, forwarding packets for other networks to the port and router used by default. It is assumed that the router used by default will forward the packet to the backbone network, and the routers connected to the backbone have full information about the composition of the Internet.

Specific route entries to a node.A node-specific route contains instead network numbers, a full IP address, i.e. an address that has non-zero information not only in the network number field, but also in the node number field. It is assumed that for such an end node, the route should be selected differently than for all other nodes of the network to which it belongs. In the case where the table contains different records on packet forwarding for the entire network N and its individual node D, which has the address ND, when a packet addressed to node ND arrives, the router will give preference to the record for ND.

3.4 Routing table support.

There are two ways to keep routing tables up to date: manual and automatic.

Manual methodsuitable for small networks. In this case, the routing tables static entries for routes are manually entered. Entries are created either with the route add command (Linux) or in the Routing and Remote Access console (Windows).

In large networks, the manual method becomes too labor-intensive, error-prone, and not fast enough.**Automatic construction**and modification of tables
Routing is performed by so-called "dynamic routers".

Dynamic routing algorithms monitor changes in network topology, make necessary changes to route tables, and exchange this information with other routers.

4. Routing algorithms.

Basic requirements for routing algorithms:

- accuracy;
- simplicity;
- reliability;
- stability;
- justice;
- optimality.

There are various algorithms for constructing tables for one-step (**Next hop routing**) routing. They can be divided into three classes:

- fixed routing algorithms;
- simple routing algorithms;
- adaptive routing algorithms.

Regardless of the algorithm used to build the routing table, the result of their work has a single format. Due to this, in the same network, different nodes can build routing tables using their own algorithms, and then exchange missing data with each other. Therefore, a router operating on an adaptive routing algorithm can provide an end node using a fixed routing algorithm with information about the path to a network about which the end node knows nothing.

4.1 Fixed Routing.

This method is used in networks with a simple connection topology and is based on manual compilation of the routing table by the network administrator.

Often used for large network backbones, since the backbone itself may have a simple structure with obvious best paths for packets to follow to the subnets attached to the backbone.

The following algorithms are distinguished:

- **Single-path fixed routing**- this is when between two subscribers a single path is established. A network with such routing is unstable to failures and overloads.

- **Multipath Fixed Routing**– several can be installed possible paths and a path selection rule is introduced. The efficiency of such routing decreases with increasing load. If any communication line fails, it is necessary to change the routing table; for efficiency, several tables are usually stored in each communication node.

4.2 Simple Routing.

These are routing methods that do not require changes to routing tables when the topology and state of the data transmission network change, and are provided by various algorithms:

- **Random routing**– is the transmission of a message from a node to any random the selected direction, with the exception of the directions in which the message arrived at the node.
- **Cyclic maintenance (RR - Round Robin)**– is the transmission of a message from a node to one direction selected sequentially around the circle, with the exception of the directions in which the message arrived at the node.
- **Flood routing**- is the transmission of a message from a node in all directions, except for the direction in which the message arrived at the node. Such routing guarantees short packet delivery time, at the expense of reduced throughput.
- **Routing by previous experience**- each packet has a number counter nodes passed, in each communication node the counter is analyzed and the route that corresponds to the minimum value of the counter is remembered. Such an algorithm allows adapting to changes in the network topology, but the adaptation process is slow and inefficient.

In general, simple routing does not provide directional packet transmission and has low efficiency. The main advantages are simplicity and ensuring stable network operation when various parts of the network fail, and can be used by a router during heavy overload.

4.3 Adaptive Routing.

This is the main type of routing algorithms used by routers in modern networks with complex topology. Adaptive routing is based on the fact that routers periodically exchange special topological information about the networks in the Internet, as well as about the connections between routers. Usually, not only the topology of the connections is taken into account, but also their throughput and state.

Adaptive protocols are distributed in nature, the work is distributed between all routers, the following algorithms are distinguished:

- **Local adaptive routing**– each node independently forms and maintains information about the status of communication lines, queue length and routes.
- **Global Adaptive Routing**- based on the use of information received from neighboring nodes. For this purpose, each node contains a routing table, which specifies the message passing metric. Based on the information received from neighboring nodes, the table value is recalculated taking into account the queue length in the node itself.

- **Centralized adaptive routing**- there is some central a node that collects information about the state of the network. This center generates control packets containing routing tables and sends them to communication nodes.

- **Hybrid Adaptive Routing**- based on the use of a table periodically sent by the center and on the analysis of the queue length at the node itself.

4.4 Routing algorithm indicators (metrics).

How is the preference of a route determined over others? Routing algorithms use various metrics to do this. Complex routing algorithms can be based on multiple metrics, combining them into a single hybrid metric. Commonly used metrics include:

4.4.1. Route length.

Route length is the most common routing metric. Routing protocols specify a "hop count," a measure of the number of passes a packet must make on its way from source to destination through internetwork elements (such as routers).

4.4.2. Cost.

Some routing protocols allow network administrators to assign arbitrary costs to each link in the network. In this case, the path metric is the sum of the costs associated with each link that is traversed.

4.4.3. Reliability.

Reliability, in the context of routing algorithms, refers to the reliability of each network link (usually described in terms of bit-to-error ratio). Some network links may fail more frequently than others. Failures of some network links may be more easily recovered from.

or faster than failures of other links. Any reliability factors may be taken into account when assigning reliability ratings. Reliability ratings are usually assigned to network links by network administrators. They are usually arbitrary numerical values.

4.4.4. Delay.

Routing delay is generally defined as the length of time it takes for a packet to travel from its source to its destination across an internetwork. Latency depends on many factors, including the bandwidth of the intermediate links in the network, the queues at the port of each router along the packet's path, the congestion on all intermediate links in the network, and the physical distance the packet must travel. Because it is a conglomeration of several important variables, latency is the most general and useful metric.

4.4.5. Bandwidth.

Bandwidth refers to the available traffic capacity of a link. All other things being equal, a 10 Mbps Ethernet link is preferable to any leased line with 64 KB/s of bandwidth. Although bandwidth is an estimate of the maximum achievable throughput of a link, routes through higher bandwidth links are not necessarily better than routes through slower links. Used as a metric on Windows hosts.

5. Routing protocols.

Routing protocol— is a network protocol used by routers (routers) for the purpose of determining data transmission routes in a composite computer network (intranet).

Routing protocols are classified according to the routing algorithms described above in the previous section.

Routing protocols are divided into two types depending on the area of   application:

- **Interior Gateway Protocol**(IGP) - intra-domain routing (**RIP**,**OSPF**);
- **External Gateway Protocol**(EGP) - interdomain routing (EGP,**BGP**).

Also, routing protocols are divided into three types depending on the types of algorithms that build routes in the network:

- **Source or Policy Based Algorithm**– source routing algorithms (**IP**And**ACL**).
- **Distance Vector Algorithm**(DVA) - distance vector protocols (**RIP**, GGP, EGP, IGRP,**BGP**);

- **Link State Algorithm**(LSA) - link state protocols (IS-IS,**OSPF**).

The list of the most frequently used routing protocols includes the following protocols: RIP v1/v2, RIPng (IPv6), OSPF, BGP v4 (IPv6).

5.1 Internal and external routing protocols.

5.1.1. Autonomous systems.

The Internet was initially built as a network that united a large number of existing systems. From the very beginning, its structure included a core backbone network, and networks that joined the backbone were considered autonomous systems (AS).

The backbone network and each of the autonomous systems had its own administrative control and its own routing protocols.

It must be emphasized that an autonomous system and an Internet name domain are different concepts that serve different purposes.

An AS unites networks in which routing is performed under the general administrative control of a single organization, and a domain unites computers (possibly belonging to different networks) in which assignment of unique symbolic names is performed under the general administrative control of a single organization. Naturally, the scopes of an autonomous system and a name domain may coincide in a particular case if a single organization performs both of these functions.

All**AS have a unique 16-bit ASN (32-bit ASNs were depleted in 2008)**. InterNIC allocates a number to the organization that establishes a new autonomous system.

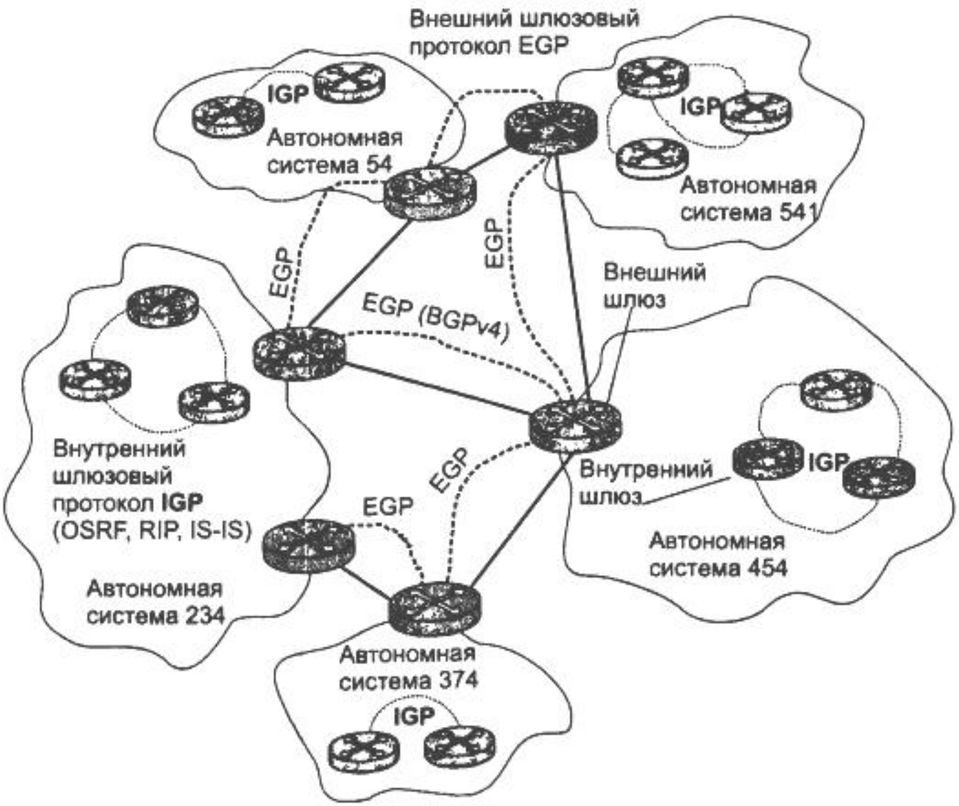


Fig. 1 Autonomous Systems (AS) of the Internet.

Routing protocols within autonomous systems are called interior gateway protocols (**interior gateway protocol, IGP**), and the protocols that determine the exchange of routing information between external gateways and backbone network gateways are external gateway protocols (**exterior gateway protocol, EGP**).

The network backbone is also an autonomous system. Any internal IGP protocol is also allowed within the backbone network.

The purpose of dividing the entire Internet into AS is in its multi-level**modular representation**, which is necessary for any large system capable of scaling on a large scale. Changing the routing protocols within any AS should not affect the operation of other ASes. In addition, dividing the Internet into ASes should facilitate **aggregation**information in trunk and external gateways.

Before the introduction of autonomous systems, a two-tier approach was used, whereby a route is first defined as a sequence of networks, and then leads directly to a given node in the final network (this is the approach we have used so far).

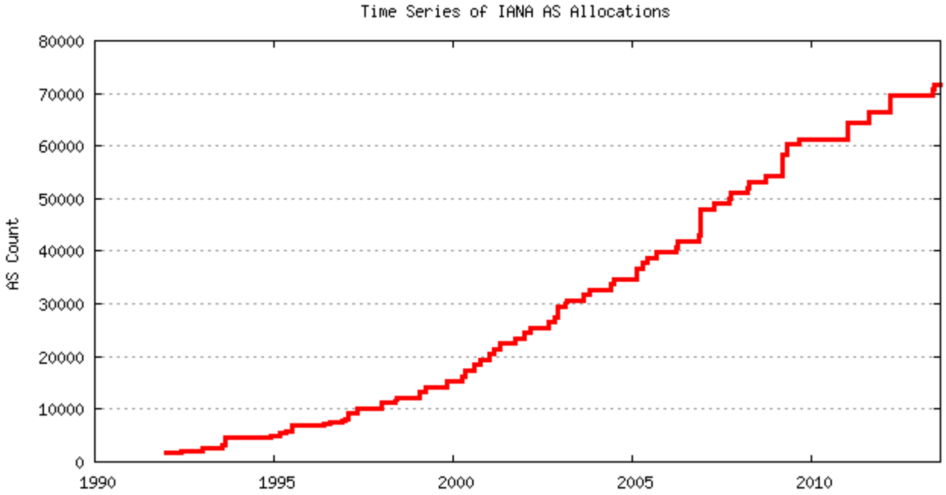
With the advent of autonomous systems, a third, upper, level of routing appears
— first the route is defined as a sequence of autonomous systems, then as a sequence of networks, and only then leads to the final node.

The choice of route between autonomous systems is carried out by external gateways using a special type of routing protocol, the so-called external gateway protocol (**Exterior Gateway Protocol, EGP**). Currently, to work in such a role

The Internet community has approved the standard Border Gateway Protocol version 4 (**Border Gateway Protocol, BGPv4**). The next router address in BGPv4 is specified as the address**entry points to the neighboringAS**.

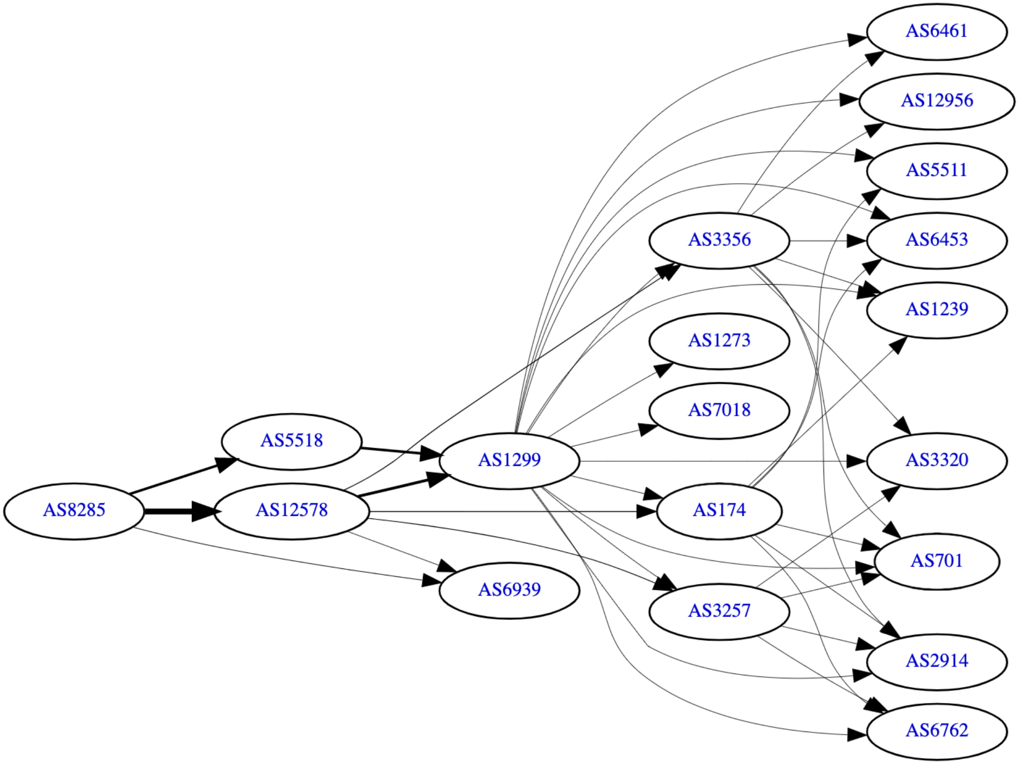
Internal gateway protocols are responsible for the route within an autonomous system (**Interior Gateway Protocol, IGP**). IGPs include the familiar RIP, OSPF, and IS-IS protocols. In the case of a transit autonomous system, these protocols specify the exact sequence of routers from the entry point to the exit point of the autonomous system.

At the end of 2016, 64,495 ASNs were allocated, see http://thyme.rand.apnic.net/current/data-used-autnums



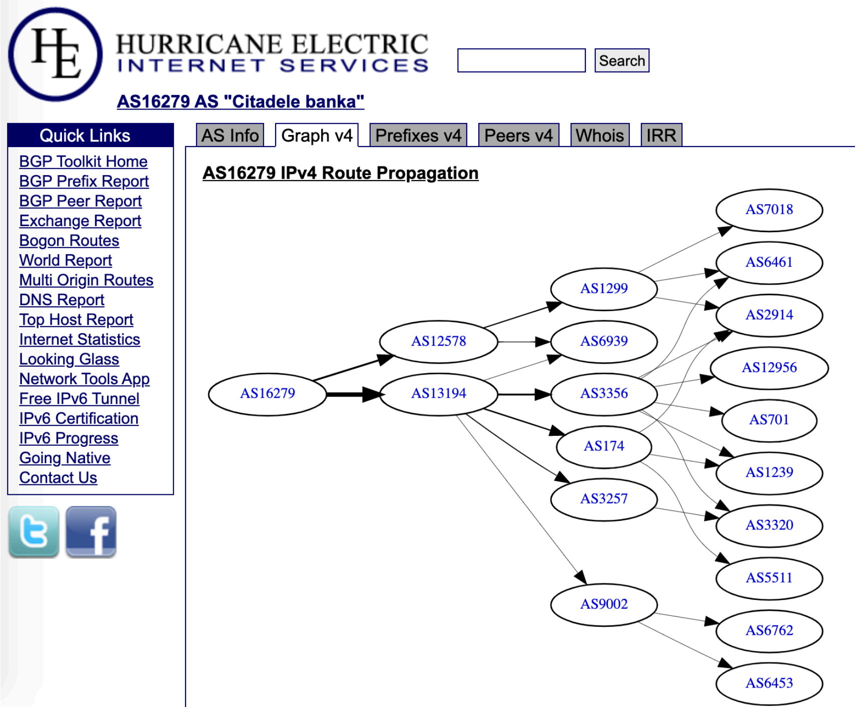
For a demonstration of ASN interoperability, seehttp://bgp.he.net/AS8285#_graph4 for Versia Ltd.

AS8285 IPv4 Route Propagation



AS BGP propagation graph example for Citadele Banka Ltd.

1. Find Latvian ASNs Reporthttps://bgp.he.net/report/world
2. Find Citadele Banka Ltd AS16279https://bgp.he.net/AS16279
3. Look BGP Peers on Graph v4 (“Path to Internet”):
   - AS16279->AS12578->AS6939 (Hurricane Electric)
   - AS16279->AS13194->AS174 (Cogent Communication)
4. Read AS Info about all Ass
   - Company Name & Origin Country
   - Company Website & Network Map
   - Internet Exchanges Nrs
   - Prefixes Originated Nrs
   - Prefixes Announced Nrs
   - AS Paths Observed Nrs
5. Find CAIDA AS Rank on site https://asrank.caida.org/



AS16279 AS "Citadele banka"

AS16279 IPv4 Route Propagation

5.2. Distance Vector Algorithm DVA.

IN**DVA**(Distance Vector Algorithm) routers send each other a vector containing the "distance" from the transmitting router to all networks known to it. "Distance" means any of the metrics, in particular, it can be the number of routers passed (by hops) or the time spent transmitting packets.

The router modifies the vectors received from neighboring routers (increases the metric values), supplements them with its own data (about its directly connected networks), selects the best one from several alternative paths according to the selected metric, builds its own vector, and broadcasts the vector further along the network on its behalf.

As a result, all routers receive information about all networks connected to the interior network and the distance (metrics) to them through neighboring routers.

Disadvantages of DVA.DVAs only work well in relatively small networks because:

- routers constantly exchange distance vectors, which leads to clogging communication lines with broadcast traffic in large networks;
- the algorithm does not always respond correctly to changes in the network configuration, since Routers transmit generalized information received indirectly from other routers and do not contain a specific idea of the topology of connections.

The most common representatives of DVA are protocols**RIP**And**BGP**.

5.3. Link State Algorithm - LSA.

LSA(Line State Algorithm) provides all routers with the information needed to construct the graph of connections of a composite computer network. All routers are based on identical graphs, as a result of which:

- routers respond faster to network configuration changes;
- the optimal route is calculated faster, based on the selected metrics.

Routers obtain additional information about other networks by exchanging short packets.**HELLO**, with its neighbors. Unlike DVA, which constantly exchanges large broadcast packets, the LSA algorithm uses small packets with information only about the states of communication lines. The LSA algorithm transmits more detailed information about networks in the case when, based on HELLO packets, a change in the state of communication lines was recorded (for example, a router failed or a new router was added). Based on the LSA network graph, an SP Tree is built to determine the route.

As a result, LSA is more suitable for large composite computing networks because it contains fewer broadcast packets, which increases the throughput and resilience of the composite network.

Link State Algorithm (LSA) based protocols are**OSPF**(Open Shortest

Path First (the shortest path algorithm) of the TCP/IP stack and**IS-IS**(Intermediate System to Intermediate System) OSI stack.

6. Additional router features.

In addition to the routing function, many devices have the following important additional functionalities, which significantly expand the scope of application of these devices.

6.1 Support for multiple routing protocols simultaneously.

Routing protocols usually assume that a router builds its table based on the operation of only this one protocol. The division of the Internet into autonomous systems is also aimed at eliminating the use of several routing protocols in one autonomous system. However, sometimes in a large corporate network it is necessary to support several such protocols simultaneously, most often this is a historical occurrence. In this case, the routing table may be inconsistent - different routing protocols may select different next routers for some destination network. Most routers solve this problem by prioritizing the decisions of different routing protocols. The highest priority is given to static routes (the administrator is always right), the next priority is given to routes selected by link-state protocols such as OSPF, and the lowest priority is given to routes of distance-vector protocols, as the most imperfect.

6.2. Network protocol priorities.

It is possible to set the priority of one network layer protocol over others. These priorities do not affect the choice of routes, they only affect the order in which the multiprotocol router services packets of different network protocols. This feature is useful in cases where the bandwidth of the cable system is insufficient and there is traffic that is sensitive to time delays, such as voice traffic carried by one of the network protocols.

6.3. Protection against broadcast storms.

One from characteristic malfunctions network software provision - spontaneous generation of high-intensity broadcast packets. A broadcast storm is a situation in which the percentage of broadcast packets exceeds 20% of the total number of packets in the network. A normal switch or bridge blindly transmits such packets to all its ports, as required by its operating logic, thus clogging the network. Fighting a broadcast storm in a network connected by switches requires the administrator to disable the ports generating broadcast packets. The router does not distribute such packets to all the networks it connects.

6.4 Support for route announcement policies.

In most routing information exchange protocols (e.g. RIP, OSPF), it is assumed that a router announces all networks that it knows in its messages. Similarly, it is assumed that when constructing its table, a router takes into account all network addresses that it receives from other routers in the network. However, there are situations when an administrator would like to hide the existence of some networks in a certain part of his network from other administrators, for example, for security reasons. Or an administrator would like to prohibit some routes that could exist in the network. When constructing routing tables statically, solving such problems is not difficult. Dynamic routing protocols do not allow implementing such restrictions in a standard way.

There is only one widely used dynamic routing protocol that specifies the possibility of rules restricting the distribution of some addresses in advertisements: BGP. The need for such rules in BGP is understandable, since it is a protocol for exchanging routing information between autonomous systems, where there is a strong need for administrative regulation of routes (for example, one Internet service provider may not want another service provider's traffic to transit through it). Router vendors correct this deficiency in protocol standards by implementing rules for the transmission and use of routing information similar to those recommended by BGP.

6.5 Support for non-routable protocols.

Such as NetBIOS, NetBEUI or DEC LAT, which do not operate with such a concept as a network. Routers can handle packets of such protocols in two ways.

Brouter. In the first case, they can work with packets of these protocols as bridges, that is, transmit them based on the study of MAC addresses.

The router must be configured in a special way so that it acts as a bridge for some non-routable protocols on some ports, and as a router for routable protocols.

Such a bridge/router is sometimes called a brouter (bridge plus router).

Encapsulation in protocol. Another way to transmit non-routable packets protocols is the encapsulation of these packets into packets of some network protocol.

Some manufacturers routers developed own protocols, specifically designed to encapsulate non-routable packets. In addition, there are standards for encapsulating some protocols within others, most notably IP.

An example of such a standard is the DLSw protocol, which defines methods for encapsulating SDLC and NetBIOS packets in IP packets, as well as the PPTP and L2TP protocols, which encapsulate PPP protocol frames in IP packets.

6.6. Separation of functions of construction and use of TM.

The main computational work is done by the router when compiling a routing table with routes to all the networks it knows. This work consists of exchanging routing protocol packets, such as RIP or OSPF, and calculating the optimal path to each target network based on some criterion.

Computing the optimal path through a graph, as required by link state protocols, requires significant computing power.

Once the routing table is compiled, the packet forwarding function is quite simple - the table is looked at and a match is found between the received address and the target network address. If there is a match, the packet is forwarded to the appropriate router port.

Some routers only support the functions of forwarding packets according to a ready-made routing table. Such routers are truncated routers, since their full-fledged operation requires the presence of a full-featured router, from which you can take a ready-made routing table. This router is often called a route server.

Refusal to independently perform the functions of constructing a routing table significantly reduces the cost of the router and increases its performance.

7. Exercises.

1. Should the loopback interface address always be 127.0.0.1?
2. Can the IP packet path be different for different UDP ports?
3. Can the IP packet path differ for different protocols (TCP, UDP, ICMP)?
4. Review your system's routing table and describe each entry.
5. Find and view AS information for well-known Latvian banks: Swedbank, DNB Nord, Citadele.

Use

- http://www.bgplookingglass.com/list-of-autonomous-system-numbers to search for an organization's ASN number;
- http://viewdns.info/asnlookup/ to analyze information about where and who controls the AS;
- https://mxtoolbox.com for further information.