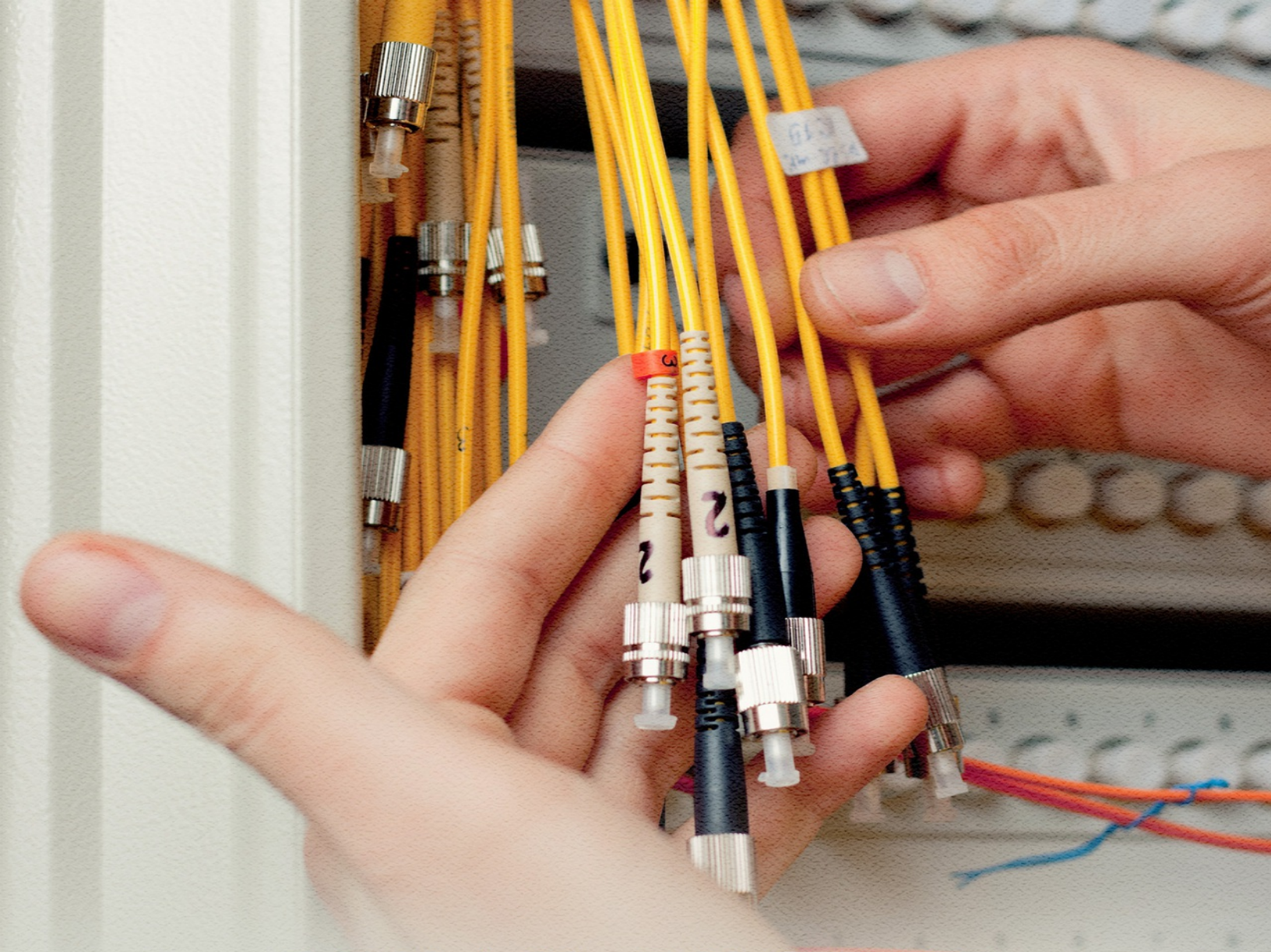


ETHAN THORPE

CCNA

ADVANCED METHODS AND STRATEGIES TO LEARN ROUTING AND SWITCHING ESSENTIALS

CCNA

Advanced Methods and Strategies To Learn Routing And Switching Essentials

Table of Contents

鸿鹄论坛 bbs.hh010.com

Introduction

Switching is the process of connecting subscribers to a communication network through transit nodes.

Communication networks should ensure that their subscribers connect with each other. Subscribers can be computers, LAN segments, fax machines, or telephone conversations. As a rule, public access networks can't provide each pair of subscribers with their physical link, which they could monopolize and use at any time. Therefore, any method of subscriber switching is always used in the network, which ensures the separation of existing physical channels between several communication sessions and between subscribers of the network.

Switches connect each subscriber to an individual communication line assigned to that subscriber. Communication lines established between switches are divided into several subscribers; that is, they are shared.

There are three fundamentally different subscriber switching schemes in networks:

1. Circuit switching.
2. Packet switching.
3. Message switching.

Kalpana proposed ethernet segment switching technology in 1990 in response to the growing need to increase the throughput of high-performance servers with workstation segments. The block diagram of the EtherSwitch switch offered by Kalpana is described below.

The Structure Of The Kalran Etherswitch Switch

Each of the eight 10Base-T ports is serviced by a single Ethernet Packet Processor (ERP). In addition, the switch has a system module that coordinates the operation of all ERP processors. The system module maintains a common switch table and controls the switch via SNMP. For

transferring frames between ports, a switching matrix is used, similar to those used in telephone switches or multiprocessor computers, connecting multiple processors with multiple memory modules.

The switching matrix operates on the principle of switching channels. For eight ports, the matrix can provide eight simultaneous internal channels in the half-duplex mode of operation of ports and 16 - in full-duplex mode when the transmitter and receiver of each port operate independently of each other.

When a frame enters a port, the ERP processor buffers the first few bytes of the frame to read the destination address. Upon receiving the destination address, the processor immediately decides to send the packet without waiting for the last byte of the frame to arrive. To do this, it scans its own address table cache, and if it does not find the address it needs, accesses a system module that works in multitasking, simultaneously serving the requests of all ERP processors.

The system module scans the common address table and returns to the processor, a found string, which it buffers in its cache for later use. After finding the destination address, the ERP processor knows what to do next with the incoming frame (while viewing the address table, the processor continued buffering frame bytes coming into the port).

If the frame needs to be filtered, the processor simply stops buffering bytes of the frame, clears the buffer, and waits for a new frame to arrive.

If the frame is to be transferred to another port, the processor accesses the switching matrix and tries to install a port in it, which connects it to the port through which the route to the destination address goes. The switching matrix can only do this if the destination address port is currently vacant, i.e., not connected to another port. If the port is busy, then like in any channel switched device, the matrix refuses to connect.

In this case, the frame is completely buffered by the input port processor, after which the processor waits for the output port to be released, and the switching matrix forms the desired path.

Once the desired path is established, it is sent buffered frame bytes received by the output port processor. As soon as the output port processor accesses the CSMA / CD algorithm connected to its Ethernet segment, the frame bytes immediately begins to transmit to the network. The input port processor constantly stores several bytes of the received frame in its buffer, allowing it to independently and asynchronously receive and transmit frame bytes.

Routing is the process of determining the routing of information in communication networks. In Russian, the word "routing" is often used. It should be noted that the correct pronunciation of this word is "routing." (In the US, "routing" is pronounced, respectively the router is "router").

Routes can be set administratively (static routes), or calculated using routing algorithms based on topology and network status information obtained through routing protocols (dynamic routes).

Static routes can be:

- Routes that do not change over time
- Routes that are scheduled
- Changing routes according to the situation - administratively when the standard situation arises.

Special software and hardware - routers perform the process of routing in computer networks. The name comes from the process (the main function) - routing.

In addition to routing, routers also switch channels/messages/packets/cells, just as a computer network switch performs routing (determining which port to send a packet from based on the MAC address table), and is named after the main function - switching.

Chapter One: Addressing in IP Networks

Type Address Stack TCP / IP

There are three types of address stack TCP / IP: local, IP addresses, and domain names.

Local (hardware, physical) address refers to the type of address used by basic technology to deliver data within a subnet, which is an element of a composite intranet. Different network technologies and different protocol stacks are acceptable to different subnets, so when creating a TCP / IP stack, different types of local addresses are assumed.

Ethernet networking requires local address delivery, which requires a computer addressing system and an interface. Each node has a unique way of self-identification. No two physical addresses on the network should match. Physical addresses, also referred to as Ethernet Media Access Control (MAC) addresses in Ethernet, recorded in a PC network adapter or network device interfaces (routers, switches, etc.).

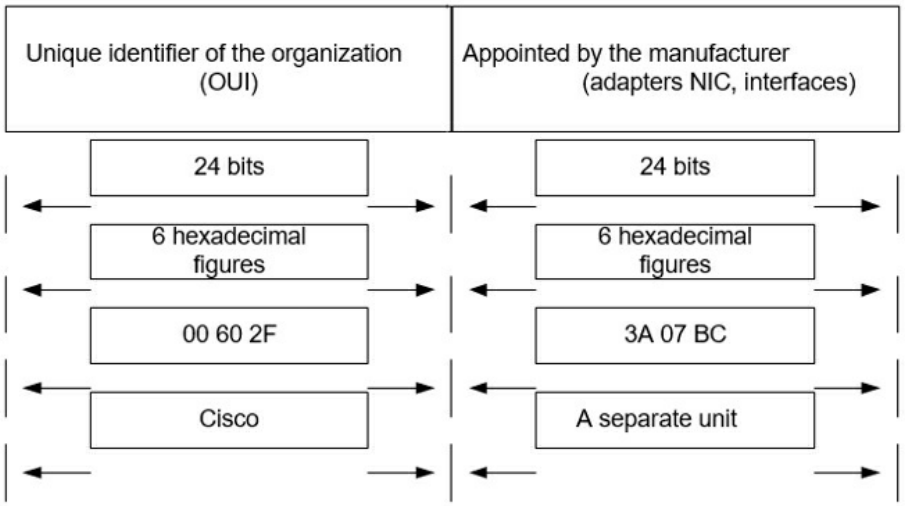
The MAC address is 48 bits long and is written in twelve hexadecimal digits (for example, 00-60-2F-3A-07-BC). The first six digits assigned to the IEEE identify the manufacturer or seller of the device and contain a unique Organizationally Unique Identifier (OUI). The second six digits contain the serial number of the interface or other value specified by the manufacturer. The MAC address is sometimes referred to as a Burned-In Address (BIA) because it is stored in a read-only memory (ROM) of the interface or device. The Fig. below shows the MAC address format.

Without MAC addresses, the LAN would be only a group of isolated computers, and Ethernet frames would not be able to be delivered. As a result, a header containing the MAC address of the device and the destination is appended to the upper layer data. The header and the destination contain the service information intended for the channel level of the device to which the frame is sent. The upper-level data is encapsulated in the header and the

end of the link layer.

IPs are the primary type of address by which the network layer transmits packets between networks. These addresses are 4 bytes long and are written in decimal notation (for example, 195.1.7.26). Each of the parts of an address separated by dots is called an octet (since it comprises 8 bits). The administrator assigns the IP address when configuring computers and routers.

IPs form the network number and node number. The network number can be chosen arbitrarily by the administrator or assigned as recommended given by a special unit of the Internet (Internet Network Information Center, InterNIC) if the network is to operate as part of the Internet. Typically, ISPs receive ranges of addresses from InterNIC units and then distribute them to their subscribers. The node number in the IP protocol is assigned regardless of the local node address. By default, a router enters several networks at once. Therefore, each router port has its own IP address. The end node can also be part of multiple IP networks. In this case, the computer must have multiple IPs, based on the number of network connections. Thus, the IP address is not a single computer or router, but a single network connection.



Characteristic Domain Names

The entire Internet is built on a hierarchical addressing system. This approach allows routing based on address classes rather than individual addresses.

However, using IPs is not very user-friendly. Thus, the difference between addresses 194.6.197.26 and 194.6.197.62 is practically unnoticeable, although both addresses belong to different network resources. The likelihood that a user might make a mistake and enter the wrong IP address is quite high since the numeric IP address is not related to the subject matter of the resource.

A dedicated Domain Name System (DNS) was developed to bind the content of the webpage and its address. DNS is intended to translate IP addresses into names and vice versa. A domain is a group of nodes located in the same geographical area or nodes used for a common purpose. A domain name is called a string of characters and/or numbers, and usually, the name corresponds to the digital IP address of the Web site on the Internet. Today, there are more than 200 top-level domains on the Internet (or first) level. The first level domains can be created geographically: .uk - United Kingdom; .us - United States; .de - Germany. In addition, there are many common domain names: .edu - Web pages dedicated to educational institutions.

.com - commercial Web sites; .gov - government nodes; .org - non-commercial sites; .net - network services.

A domain name server is a network device that, at the request of a user, converts domain names into appropriate IPs and returns the result to the client. The domain system is strictly hierarchical, so there are several levels of names and corresponding DNS servers.

If the name cannot be translated to the IP address on the spot, then the request is passed to a higher-level DNS server, which in turn also tries to determine the IP address of the node. If at this level, the DNS server can convert the name to an IP address, the result of the request is returned to the client. If this server cannot detect the required record, the request is transmitted above. The process is repeated until the IP address of the requested node is determined, or the top-level DNS server is reached. If the domain name is not found at this level, the client is sent an error message. All applications that use domain names to provide IP addresses go to the DNS servers that perform the corresponding broadcast.

Classes of IP Addresses

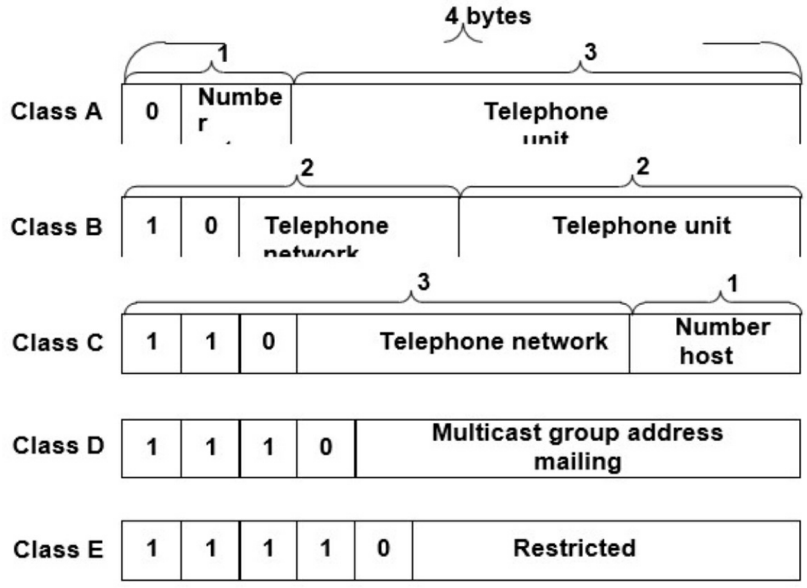
To enable the description of networks of different sizes and to facilitate their classification, IPs were divided into groups called classes. Such an addressing

scheme is called class. Each full 32-bit IP is divided into two parts, describing the network and the node. The bit or sequence of bits at the beginning of each address defines its class (Fig below). There are five classes of IP addresses.

Class A addresses are for a very large network, using only the first octet as the network identifier. The three remaining octets identify the node address. The first bit in the class A address is always zero. With this in mind, the minimum number will be 00000000 (decimal 0), and the highest will be 01111111 (decimal 127).

It should be noted that both numbers 0 and 127 are reserved and cannot be used as network addresses. Any addresses that start with a number in the range from 1 to 126 in the first octet are Class A network addresses are few, but the number of nodes in them can reach 2^{24} - 2 = 16,777 214 nodes (two numbers identify network numbers and broadcast address).

127.0.0.0 cannot be assigned to a network because it is reserved for loopback testing (routers or local nodes can use it to transmit packets to themselves).



Structure of IP-addresses various classes

Class B addresses are used for medium to large networks. In Class B IP, the first two octets are used for the network address, and the second two are the node address.

The first two bits of the first octet always take the values "1" and "0," and the

remaining six bits can contain any combination of zeros and ones. Thus, the smallest number that can be used for addresses in this class is 10000000 (decimal 128), and the largest number is 10111111 (decimal is 191). Any addresses containing numbers from 128 to 191 in the first octet are Class B addresses. A Class B network may contain a maximum of 2^{16} -2 = 65 534 nodes.

Class C addresses are the most commonly used addresses for use on small networks. The address of this class begins with a binary combination of 110. Therefore, the lowest number available is 11,000,000 (decimal 192) and the largest 1101111 (decimal 223). If the address in the first octet contains numbers from 192 to 223, then it belongs to class C. The maximum number of nodes in the network is 2^8 - 2 = 254.

Class D addresses were created to implement the IP address of a multicast mechanism. A multicast address is a unique network address used to send packets to certain groups of network devices. Thus, a single network station may transmit a single data stream to multiple recipients.

The range of Class D addresses, called multicast IPs, is also somewhat limited. The first four bits of this address is 1110, so the first octet of addresses in this class can be in the range 11100000 to 11101111 or in decimal notation 224 to 239.

Class E addresses have also been described in the standards and highlighted in a separate block. However, they were reserved by the Internet Engineering Task Force (IETF) for their own research purposes and were not used on the Internet. The first four bits of Class E addresses are always single. The value of the first octet is in the range from 11110000 to 11111111 or from 240 to 255 - in decimal.

We show the ranges of values of the first octet in the IPs for each class in the Table below.

Table 1.1 - Classes of IP-addresses a range of the first octet

Class	The first bits	The minimum number of network	The maximum number of network	The maximum number of networks	The maximum number of quantities to units in a

					network
A	0	1.0.0.0	126.0.0.0	27 - 2 = 126	224 - 2
B	10	128.0.0.0	191.255.0.0	214 = 16384	216 - 2
C	110	192.0.0.0	223.255.255.0	221 = 2097152	28 - 2
D	1110	224.0.0.0	239,255,255,255	-	Multicast
E	1111	240.0.0.0	255.255.255.255	-	Reserved

Special IP Addresses

Some addresses are special and may not belong to network devices. These include the following:

- IP addresses consisting of binary zeros only indicate the address of the node that generated the packet. We only use this mode in some ICMP messages.
- IP addresses with binary zeros in the network number field. By default, the destination node is considered belonging to the same network as the node that sent the packet.
- IPs in which all bits are single. A packet with the same destination address must be sent to all addresses in the same network as the source of the packet. Such a broadcast is called a limited broadcast.
- IPs that contain only zeros in the destination node field. These addresses indicate network numbers. For example, 198.150.11.0.
- IPs that contain only units in the destination node field. A packet that has this address is sent to all network nodes with the specified network number. For example, a packet with address 198.150.11.255 is delivered to all nodes in the 198.150.11.0 network. Such a broadcast is called a broadcast message.
- Thus, the actual number of addresses that can be assigned to network devices is two times less, since a network or broadcast address cannot be assigned to the device.
- IPs, whose first octet is 127. 127.0.0.1 (loopback) is used to test programs and interact processes within a single machine. Data sent to this address forms a "loop." The data is not transmitted over the network but returned to the top-level modules as just received.

- IP addresses for multicast packets (class D). For example, to exchange messages, routers that use the OSPF routing protocol send messages to 224.0.0.5. The routers will receive any message sent to this address in this group.

Application of Masks During IP Addressing

We base the traditional scheme of dividing an IP address into a network number and a node number on the class concept; the values determine which of the first few bits of the address. Just because the first byte of address 129.54.65.3 falls in the range of 128 - 191, we can say that this address belongs to class B, and therefore the network number is the first two octets, supplemented by two null bytes - 129.54.0.0. and the node number is 0.0.65.3.

An alternative to this traditional scheme is to use another feature that allows you to more flexibly define the boundary between the network number and the node number. Such a feature is a mask, a 32-bit number that is used in conjunction with an IP address. The binary mask record contains units in the digits that are to be interpreted in the IP address as the network number. Since the network number is an integral part of the address, the units in the mask must be a continuous sequence.

For standard classes, IP masks have the following values: Class A - 11111111. 00000000. 00000000. 00000000 (255.0.0.0).

Class B - 11111111. 11111111. 00000000. 00000000 (255.255.0.0).

Class C - 11111111.11111111.11111111.00000000 (255.255.255.0).

It is quite common to designate a mask as a number recorded after a slash, for example, 129.54.65.3/16. This entry means that the mask for address 129.54.65.3 contains 16 units, i.e., 16 bits (the first 2 bytes) are assigned to the network number.

It bases the mechanism of masks on the principle of getting the network number by bit multiplication of the node and mask address. For example, for IP address 180.34.23.134 with mask 255.255.0.0, we have.

10110100.00100010.00010111.10000110

11111111.11111111.00000000.00000000

00001010.00100010.00000000.00000000 = 180.34.0.0

By accompanying each IP address with a mask, one can abandon the concepts of address classes and make the addressing system more flexible. For example, if you associate address 129.54.170.164 with a mask 255.255.255.0 - number, the network (or, more precisely, the subnet) will be 129.54.170.0 (not 129.54.0.0, as defined by the class system) if with the mask 255.255.248.0 - then 129.54.168.0 and if with the mask 255.255.255.224 - then 129.54.170.160.

In general, to allocate a subnet, the portion of the bits responsible for the node numbering must be defined as a network. This mechanism is often referred to as bit borrowing. The fission process always begins with the leftmost bit of the node whose position depends on the class of the IP address.

It should also be noted that, in addition to increasing manageability, subnetting allows network administrators to restrict broadcasting and implement a low-level security mechanism on the LAN.

As you know, broadcast packets are sent to all nodes in the network or subnet. When broadcast traffic begins to consume a large portion of the available bandwidth, the network administrator may decide to reduce the size of the broadcast domain.

Security, when using subnets in the LMC, is realized because access to other subnets is organized through routers that can be configured to allow or deny access to subnets based on different criteria. In addition, the outside world “sees” the LAN as a single network knowing nothing about its internal structure. In addition to improving security, this approach also helps reduce TM and use them effectively. After receiving the local node address 192.168.10.14, the outside world outside the LMC uses only the declared primary network address 192.168.10.0, since the local address 192.168.10.14 is valid only within its limits.

Some organizations have also found that using a subnet allocation mechanism can generate additional revenue through the sale or lease of an address that has not been used before.

Selecting the number of bits required to create a subnet depends on the maximum number of nodes it needs. The following expressions can be used to determine the subnet mask based on the number of subnets and nodes available: 2^n - the number of subnets used, where n is the number of bits

borrowed from the node portion; 2^m - 2 - is the number of nodes available, where m is the number of bits of the remaining node (the number of bits of the node v = n + m).

For example, when borrowing three bits from a node of a class C network, 5 bits will be used to address nodes, so the number of nodes in each subnet is equal to 2^5 - 2 = 30, and the maximum number of subnets is $2^{(v-5)}$ = 3 (here v = 8).

Mask mechanism is widely used in IP routing, and masks can be used for various purposes. With their help, the administrator can structure their network without requiring the service provider to provide additional network numbers. Based on the same mechanism, service providers can merge the address spaces of several networks by introducing so-called “prefixes” to reduce routing tables and increase the performance of routers.

The Use Of Permanent Length Masks

Consider, for a specific example, the process of network segmentation by applying fixed-length subnet masking (FLSM - Fixed-Length Subnet Masking).

For example, a network administrator needs to set up four networks, and the service provider is allocated only one network class B number 129.144.0.0. This problem can be solved by using constant length masks. The mask chosen in this case would be 255.255.192.0 (since to address four of our networks; we need to borrow from the bits of the node number two senior bits of the third octet). After applying such a mask to the issued address, the number of digits corresponding to the network number increased from 16 to 18. Two additional bits (Nos. 17 and 18) in the network number are often interpreted as subnet numbers.

As a result of the use of masks, the distribution scheme of the address space took the form, as shown in the table below.

Table 1.2 - Separation of network address space class technology with FLSM

1 octet	2 octets	3 octets		4 octets	
Field Class B network number		Number of subnets	Field	host address	Description of network

129	44					
10000001	00101100	0	0	000000	00000000	Network 129.44.0.0
...	...	...	...	...	...	mask 255.255.192.0
10000001	00101100	0	0	111111	11111111	Node 214 - 2
10000001	00101100	0	1	000000	00000000	The network 129.44.64.0
...	...	...	...	...	...	mask 255.255.192.0
10000001	00101100	0	1	111111	11111111	Node 214 - 2
10000001	00101100	1	0	000000	00000000	Network 129.44.128.0
... 10000001	... 00101100	... 1	... 0	... 111111	... 11111111	mask 255.255.192.0 Node 214 - 2
10000001	00101100	1	1	000000	00000000	Network 129.44.192.0
10000001	00101100	1	1	000000	00000001	mask 255.255.192.0
10000001	00101100	1	1	000000	00000010	Node 214 - 2
...	...	...	...	...	...	
Unused addresses (214 - 4)						
10000001	00101100	1	1	111111	11111111	

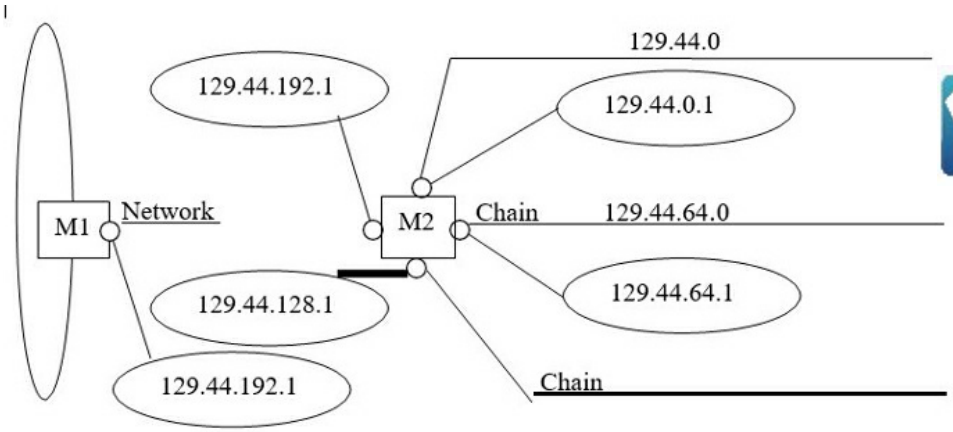
The network is resulting from such structuring shown in Fig. below. All traffic from the outside world gets in our internal no network through the router M1. To continue current structuring information on the internal network, the router installed an additional M2.

Each of the four subnets can be up to 214 - 2 knots. If this is not the number of nodes - , the address space is unused.

Outside, this network looks like an ordinary class B network and locally on

the framework of development - it is composed of a network that has a subnet. It also has another advantage because it allows you to hide from the surveillance of the network structure.

This approach allows the class compared to the effective addressing, importantly, allocate address space.



Understandably, in the case of IP address deficits, such inefficient use of IP addresses is also inadmissible. The Variable Length Subnet Masking (VLSM) technology can be used to solve this problem.

Use Of Variable Length Masks

The use of variable length masks provides more economical use of address space. An example of the distribution of address space with variable length masks for the previous example is given in the table below. The main idea behind using VLSM is that, unlike FLSM technology, the mask is calculated separately for each subnet.

Note that the use of VLSM technology not only saves the space of IP addresses but also, in some cases, solves the problem of network segmentation, which would be impossible if FLSM technology is used.

Consider the following example. Let the provider allocate a class C network number: 210.100.45.0, and the administrator needs to set up four subnets with the number of nodes 120, 58, 28, and 4. Note that this task cannot be solved in principle using constant length masks.

This is because the subnet mask must be selected for the largest number of nodes (for each node in each subnet to have a unique address). So in our case, the subnet mask would be 255.255.255.128. This indicates that of the eight

bits of IP addresses responsible for node numbering, one bit is allocated for subnet numbering. So, we can only get two subnets instead of the desired four.

Calculating the mask separately for each subnet allows for solving the task (in the next table).

Division of address space of a class B network using VLSM technology

1 octet	2 octet	3 octet	4 octet	Description of the network
Class B network field number		Subnet number	Node address field	
129	44			
10000001	00101100	0 0000000	00000000	Network 129.44.0.0
... 10000001	... 00101100	... 0 1111111	... 11111111	Mask 255.255.128.0 Nodes $2^{15} - 2$
10000001	00101100	1 0 000000	00000000	Network 129.44.128.0
... 10000001	... 00101100	... 1 0 111111	... 11111111	Mask 255.255.192.0 Nodes $2^{14} - 2$
10000001	00101100	1 1 0 0 0 0 0 0	0 0 0 0 0 0 00	Network 129.44.192.0
... 10000001	... 00101100	... 1 1 0 0 0 0 0 0	... 0 0 0 0 0 0 ... 11	Mask 255.255.255.248 Nodes $2^{4} - 2$
The address range ($2^{13} - 4$) is free to form new networks				
10000001	00101100	1 1 1 00000	00000000	Network 129.44.224.0
... 10000001	... 00101100	... 1 1 1 ... 11111	... 11111111	Mask 255.255.224.0 Nodes $2^{13} - 2$

Separation of network address space of class technology with VLSM

1 octet	2 octets	3 octets	4 octets		Description network
Field Class C network numbers			Field node address		
210	100	45			
			0	0000000	Network 210.100.45.0
210	100	45	.. 0	... 1111111	mask 255,255,255,128 Node 27 - 2 = 126
			1 0	000000	Network 210.100.45.128
210	100	45	... 1 0	... 111111	mask 255,255,255,192 Node 26 - 2 = 62
			1 1 0	00000	Network 210.100.45.192
210	100	45	... 1 1 0	... 11111	mask 255,255,255,224 Node 25 - 2 = 30
			1 1 1 0 0	000	Network 210.100.45.224
210	100	45	... 1 1 1 0 0	... 111	mask 255,255,255,224 Node 23 - 2 = 6

IP Address Resolution Protocols

For device interaction, the transmitter device must have the recipient's IP and MAC address. When one device attempts to communicate with another that has a known IP address, it must determine the recipient's MAC address (if the recipient is not in the local network segment, there is a need to determine the physical addresses of the intermediate devices to your destination). This is

required for the frames encapsulated in the frames to reach their destination.

A set of TCP / IP protocols has a special protocol called ARP (Address Resolution Protocol), which automatically obtains a MAC address. The Fig below illustrates a process to determine the MAC address associated with a known IP address.

Some devices store special ARP tables that contain information about the MAC and IP addresses of other devices connected to the same LAN. ARP tables allow you to establish a unique relationship between IP and MAC addresses. Such tables are stored in specific areas of memory and are automatically served on each of the network devices (Tables below.

Record in ARP-table

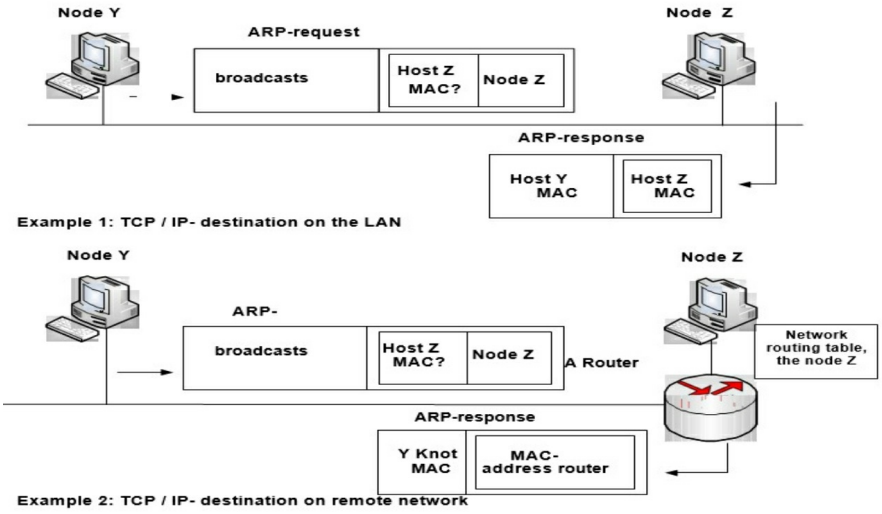
IP-address	Physical address	Type
68.2.168.1	00-50-57-00-76-84	Dynamic

Sometimes you have to create ARP tables manually. Note that each computer on the network supports its own ARP spreadsheet.

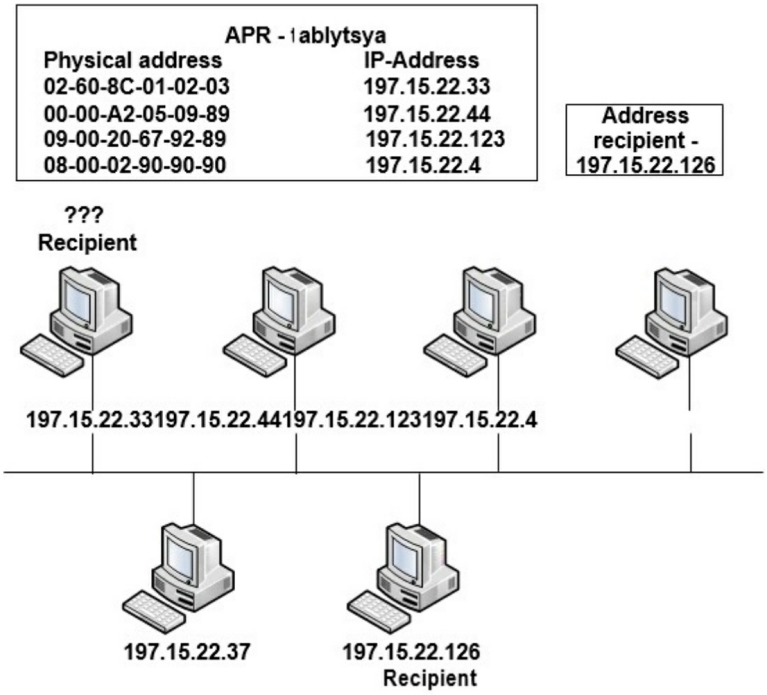
Wherever data is transmitted to network devices, they always use the information stored in the ARP table for forwarding them (Fig below). In case the sender cannot obtain the requested physical address from his own ARP table, a process called an ARP request is initiated.

ARP-table for address 198.150.11.36

MAC-address	IP-address
FE: ED: F9: 44: 45: 66	198.150.11.34
DD: EC: BC: AB: 04: AC	198.150.11.33
DD: EC: BC: 00: 94: D4	198.150.11.35
FE: ED: F9: 23: 44: EF	198.150.11.36



Getting the MAC-address-based IP-address



ARP-table for small networks

An ARP request allows a node to determine the recipient's MAC address. The node creates an ARP request frame and sends it to all network devices. The frame of an ARP request comprises two parts:

- frame header
- ARP request message

For all devices to receive an ARP request, we use a broadcast MAC address

(this address contains single values in all bits: FF-FF-FF-FF-FF-FF). Because it transmits ARP request frames in broadcast mode, all network devices connected to the LMC can receive such frames and transmit the encapsulated information in them to higher-level protocols for further processing. If the IP address of the device is the same as the IP address of the recipient, in a broadcast ARP request, then the device responds to the sender by reporting its MAC address. This message is called an ARP response.

When an ARP response is received, the sending ARP request sender removes the MAC address from the sender's hardware address field and updates its ARP table. This device can now properly address packets using both MAC and IP addresses. The information obtained is used to encapsulate data at the second and third levels before sending them to the network.

When the data reaches the destination, a link-level check is performed at the link layer, and a channel header containing MAC addresses is discarded, and it transmits the data to the network layer. At the network level, the correspondence of the recipient's own IP address and the IP address of the third-level header is checked. At the network level, the IP header is dropped, and it transfers the encapsulated data to the next layer of the OSI transport model (layer 4). This process is repeated until the remaining data is partially unpacked to reach an application (level 7) in which it will read some user data.

It is worth knowing that there is also a protocol that solves the inverse problem—Find your IP address at a known local address. It is called Reverse Address Resolution Protocol (RARP) and is used, for example, when starting diskless stations that do not know their IP address initially but know the address of their network adapter.

Chapter Two: Network Hardware

Equipment directly connected to the network is a network device. All network devices can be classified into the following groups:

- End-user devices (endpoints stations) - are devices that connect users to a network by linking to it through a network adapter or network interface card (Network Interface Card, NIC). This group includes computers, printers, scanners, and other devices that perform functions directly intended for the user of the network;
- Network devices - These are devices that are connected to end-user devices and allow them to communicate. They provide data transfer between end-user devices, extend and connect cable connections, convert data from one format to another, and control data transmission. Examples of such devices are repeaters, hubs, bridges, switches, and routers.

Network Adapter Boards

Ethernet network adapter used to connect a PC to the network. It communicates with the network through cable (or radio waves in wireless communication technology) and with a computer through an expansion socket. When choosing a network adapter, the following factors should be taken into account:

- Network type. Different types of networks require different network adapters (for example, Gigabit-Ethernet adapters are designed for use on Ethernet LANs);
- Type of data medium - the type of port or network connector used to connect to different data media (for example, twisted pair, WOK, or wireless network);
- System bus type (there are different types of the system bus, such as PCI).

Repeaters

LMCs combine many devices of different types. As mentioned above, there are many different media environments, each with its own advantages and disadvantages. For example, one of the drawbacks of a Category 5 UTP cable

(which is by far the most commonly used one) is its length limitation. Yes, the maximum length of a UTP cable for one network segment is 100 m. If it requires a longer distance, we should use repeaters. In most modern Ethernet networks, switches are used instead of repeaters, and sometimes hubs (multi-port repeaters) can also be encountered.

The purpose of the repeaters is to regenerate and re-synchronize the network signals at the bit level so that they can travel a greater distance over the medium in which the transmission is performed.

Repeaters are usually used when there are too many nodes in the network, or the length of the available cable is insufficient to reach remote workstations.

Functions, Designation, And Classification Of Hubs

Hubs are multi-port repeaters. The use of a hub transforms the network topology from a bus to a star-shaped one. Concentrators belong to one of the following types :

- the active hub must be connected to an external power source as it needs the energy to amplify the input signal before transmitting it to external ports;
- Smart hubs - function as a normal hub; however, it has a built-in microprocessor and has diagnostic capabilities. It is more expensive than a regular hub, however, useful in emergencies;
- the passive hub acts solely as a point of the physical connection of the devices. Such a hub does not check the traffic flowing through it and does not perform any action on the data streams; it does not amplify or clear the signal, but only gives access to the common bus.

Bridges and Switches

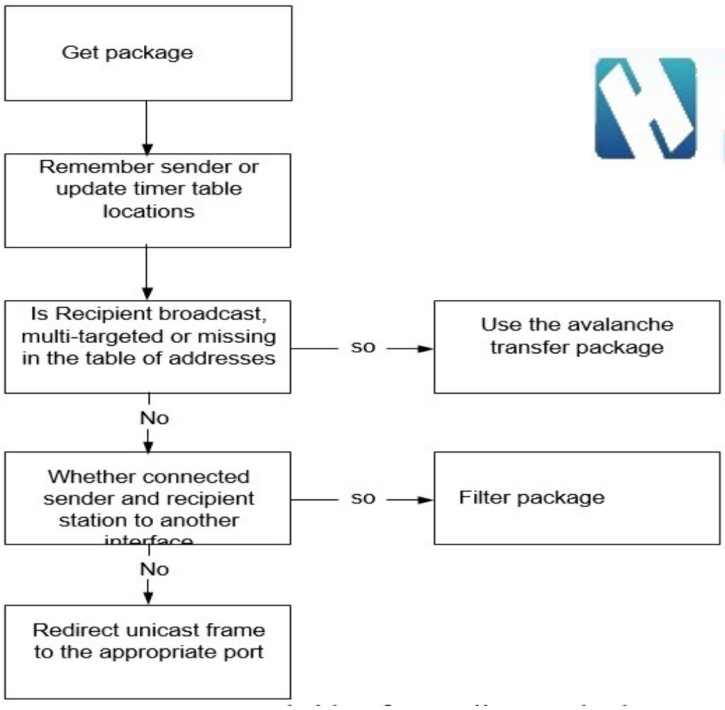
Fundamentals of Bridge Functioning

As mentioned in the previous section, large LMCs often need to be subdivided into smaller, easily managed segments. The devices used to connect the network segments may be bridges, switches, routers, and gateways. Bridges and Switches operate at the link layer of the OSI model. The function of the bridge is to determine whether signals sent to one of its ports should be sent to another segment of the network. Bridges can also be

used to connect networks using different protocols or different transmission media.

While operating, cities use the transparent redirect method. This method is described in the IEEE 802.1d specification, which defines five frame processing processes when passing through a switch (Fig below).

1. Forwarding frames.
2. Avalanche frames (flooding).
3. Frame filtering.
4. Switching with topology or learning.
5. Aging of the MAC address table (aging).



Steps transparent bridge forwarding method

When a bridge receives a frame, it compares the MAC address of the sender with the address table. It has to determine whether it should be filtered (discarded), sent in an avalanche fashion, or to a designated network segment.

This decision is made as follows:

- If the receiving device is in the same segment from which the frame was obtained, then the bridge prevents it from being

transmitted to other segments. This process is called filtering;

- If the receiving device is in another segment and its address is present in the address table, the bridge sends the frame to the corresponding segment;
- If the receiving device is not in the address table (i.e., "unknown" bridge) or the frame is broadcast or multicast - then the bridge sends the frame to all segments except where the frame was received from. This behavior is called avalanche mailing.

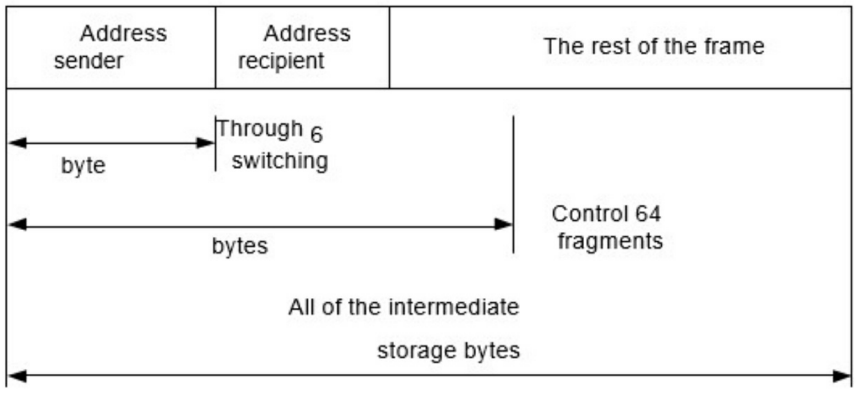
A strategically installed bridge can significantly increase network performance.

Switching Modes

There are several switching modes during the operation of the bridges. They differ at the moment when the frame should be switched. Three switching modes are most commonly used:

- Store-and-Forward;
- Cut-through;
- Fragment free.

The switching times for these modes are shown in the Fig.2.2. Each of these modes has its advantages and disadvantages. For example, commutation is characterized by maximum speed, but the inability to analyze the facts of frame distortions. Switching with intermediate storage.



Switching Modes

On the contrary, it is characterized by a lower speed, but the possibility of analyzing the frames. In this case, if the frame is skewed, it is discarded by the switch, and therefore the channel bandwidth is used more economically.

The fragment control switch takes an intermediate place in the control level and speed and allows only frames smaller than 64 bytes for collisions to be discarded. Several bridges support all of these modes and allow them to be selected automatically, depending on network features.

Even switching can be symmetric and asymmetric. The first one provides switched connections between ports with the same bandwidth (for example, all 100 Mbps ports). Asymmetric switching provides switched connections between ports with different bandwidth values (for example, 100 Mbps and 1000 Mbps).

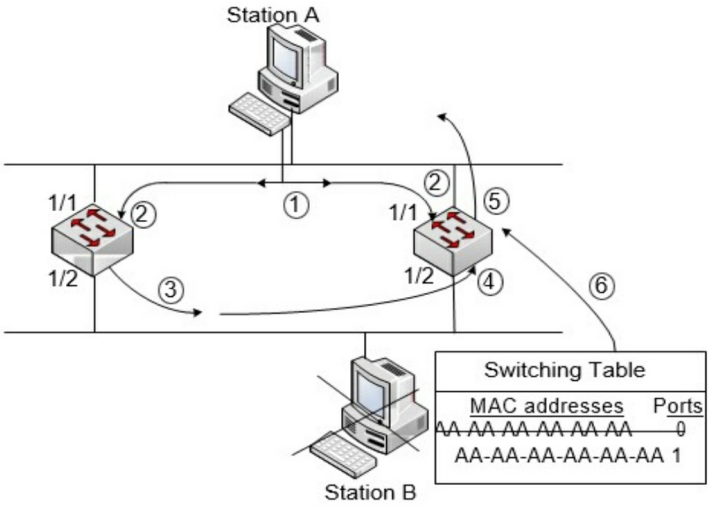
Asymmetric switching is used in the case of large client-server network streams when many users are simultaneously communicating with the server. This obviously requires a larger bandwidth for the switch port to which the server is connected to redirect the data stream from the 1000 Mbps port to the 100 Mbps port without overflowing on the latter, and the asymmetric switch must have a buffer memory. An asymmetric switch is also required to provide a larger bandwidth for channels between switches that make vertical cross-connections or channels between trunk segments.

Problems with Bridge-Based Networking

Bridges with redundant element bridges that are used to improve network reliability (without STP) may experience several issues, such as

- Broadcast storms;
- Information distortion in switch MAC address tables. Let's look at these issues in more detail.

A broadcast storm is a process of endlessly circulating broadcast messages in network switches based on switches. Such storms are caused by bridges sending broadcast messages to all ports. Except the one from which this message was received. Thus, when station A sends a broadcast frame to the network, it enters the ports 1/1 of both bridges (Fig2.3). These bridges are then sent to each other through ports 1/2. And so on. Therefore, broadcast frames in both directions (clockwise and counterclockwise) will endlessly circulate on the network. Broadcasting frames significantly reduce network bandwidth, and in some cases, make it generally inoperable.



A simple network-based bridge with elements of redundancy

The distortion of information in the MAC address tables of bridges is the process of infinitely circulating unicast messages in network loops based on bridges.

Suppose, for example, that station A has a record of station B in the ARP table and sends a unicast ping packet to station B. Station B is temporarily disconnected from the network, and the corresponding entry in the switch table is deleted. Suppose that both switches do not use STP.

Then, the frame arrives at ports 1/1 of both switches (step 2). Let's take a look at the Cat1 bridge situation. Because station B is in a malfunctioning condition, there is no record of the MAC address BB-BB-BB-BB-BB-BB in the Cat1 bridge table, and therefore Cat1 passes the received frame further into the network (step 3). In Step 4, Cat2 receives a frame-corrected Cat-1 via port 1/2. This leads to two such situations.

1. The Cat-2 switch table does not have an entry with a BB-BB-BB-BB-BB-BB MAC address (step 5), and the frame is then sent to port 1/1, which creates a loopback and renders the network unusable.
2. The Cat2 switch receives frames with the MAC address of the AA-AA-AA-AA-AA-AA-AA sender via port 1/2 and then changes the entry in its table of station A's MAC address from port 1/1 to the port 1/2.

Since the frames circulate in the opposite direction (as shown above, the

frame circulation loops exist in both directions), there is a cyclic change in the MAC address of station A from port 1/1 of the Cat2 switch to port 1/2.

Thus, unicast messages not only saturate the network but also distort information in the MAC tables of the switches, which leads to a disruption of such a network. The bridge tree protocol is used to avoid the above problems on bridge-based networks.

The STP Binding Tree Protocol and its Modification

The Spanning Tree Protocol (STP) is a link-layer protocol that is used to maintain a loop-free state of the network. Digital Equipment Corporation developed STP in 1983. The IEEE 802 Committee then upgraded it and published it in the form of the IEEE 802.1d specification (this specification describes the transparent bridge algorithm itself).

For the network to be free from loops, the bridge automatically blocks one or more redundant ports when loops are detected.

Basic Terms Of The STP Protocol

- Bridge ID (BID) is an eight-byte number whose six bytes are the MAC address of the bridge control unit, and the two highest bytes are the priority of the bridge.
- The Port ID of a bridge is a two-byte number whose lower byte contains the serial number of the given port in the switch, and the older byte is manually set.
- Root Bridge - A bridge that performs the function of a tree root.
- Root Port Bridge is a port that has a minimum distance to the root bridge.
- Designated Port Designated Bridge is a port that has a minimum distance to the root bridge among all ports of all bridges in a given segment.
- Designated Bridge is the bridge that owns the designated port of a given segment.
- Bridge Protocol Data Unit (BPDU)
- Special packages that periodically exchange bridges to determine the configuration of the spanning tree automatically. Such packages carry information such as bridge and port identifiers, distance to the root bridge, and the like.

Operation of STP

It should be noted that after the convergence of the network, that is, after completion of STP operation, each network has one connecting tree, i.e., the following conditions are fulfilled :

- there is one root bridge in each network;
- each root bridge has one root port;
- there is one designated port in each segment;
- All other ports (unassigned and unrooted) are not used. Only the root and destination are used to transmit data.

The STP algorithm has three steps.

1. Choosing a root switch

Immediately after loading, each bridge considers its root. All bridges start exchanging BPDUs (default every 2 seconds). During this exchange, the city with the lowest value of the switch ID is assigned a root. Note that all bridges, by default, have 32768.MAS identifiers, so the smallest identifier will have a bridge with a minimum MAC address. In this case, any bridge that may not be the "center" of the network can be selected as the root. For a rational selection of the root bridge, it is necessary to change (reduce) the priority (the value of the highest two bytes of VID) to the one that, at the request of the administrator, should become root.

2. Root port selection

Each non-root bridge must have a root port. The root port is the port with the lowest root value. Root cost - is the total cost of a route from a given port to the root switch and is calculated as the sum of the conditional times of the segments through which the path from the given port to the root switch passes.

Segment channel cost - is the value inverted to the bandwidth of the channel. The values of the channel values, depending on their bandwidth, are shown in the table below.

Routing Value of the path for some channel bandwidths

Throughput channel (Mbit / s)	Cost way	Throughput channel (Mbit / s)	Cost way
10	100	155	14

16	62	622	6
45	39	1000	4
100	19	10000	2

If multiple ports have the same root value, then the port with the lowest identifier value is selected.

3. Selection of designated ports

STP selects one assigned port for each segment. The designated port is the one that has the lowest route estimate to the root switch. A switch that has a designated port for a given segment is called a designated switch.

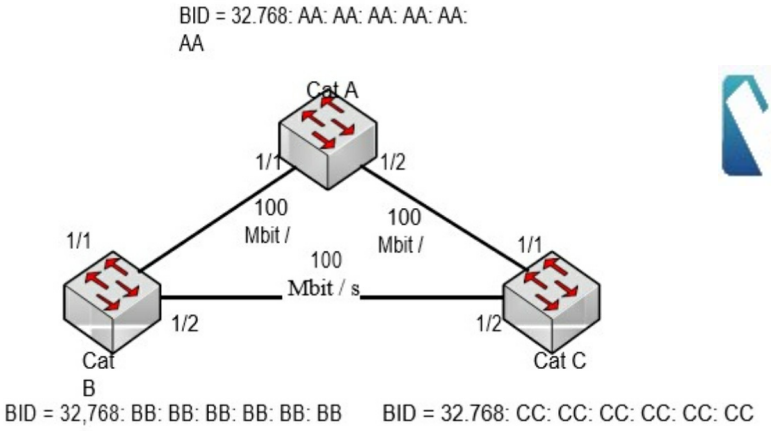
In the root switch, all ports are assigned (the only exception is when some ports of the root switch form physical loops).

Ports that have not become rooted and designated - are blocked and cause logical loop breaks in the network.

It is mathematically proved that as a result of the operation of this algorithm for the network, we obtain a covering tree.

An Example of the STP Protocol

Let's take a step-by-step look at how STP works of the network shown in Figure 2.4.



Example of STP protocol

1. ***Choosing a root switch.*** Since the priorities of the three bridges are the same (32768), the bridge with the smallest MAC address, i.e., the Cat A bridge, becomes the root.

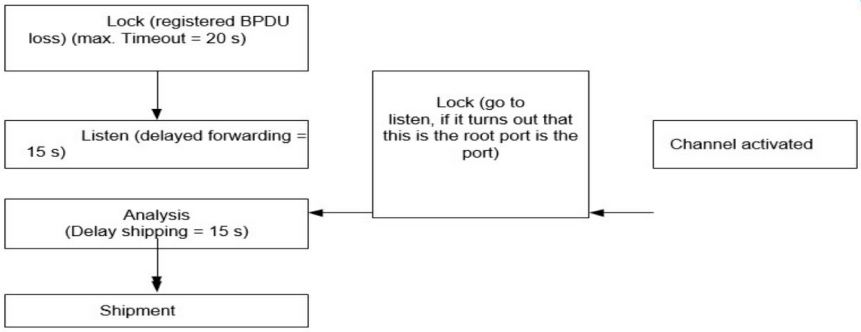
2. ***Root port selection.*** Since each non-root bridge must select at least one root port with the lowest root value, such root ports will be ports 1/1 of Cat B and Cat C bridges, since the root value of each is 19 (root value of ports 1 / 2 Cat B and Cat C bridges are 19 + 19 = 38).
3. ***Selection of designated ports.*** Since each segment in the network must have one designated port, the ports for the left and right segments of the network are respectively the ports 1/1 and 1/2 of the Cat A bridge (since they have the lowest root cost). For the lower segment, port 1/2 of Cat B bridge was designated. This is because the root value of ports 1/2 of Cat B and Cat C bridges have the same value 19. In this case, the value of the sender ID is decisive. And the Cat B bridge identifier is smaller than Cat C. Bridge The remaining port (Cat 1/2 bridge port C) becomes unassigned and enters the lock state. So now the loop is logically broken.

The sequence of port states for STP

There are five basic states of ports.

1. In the lock state, custom frames are not forwarded, BPDU modules are listened to.
2. In the listening state, the user frames are not forwarded but are being listened to. In this state, the root switch, root, and destination ports are selected.
3. In the state of topology study, user frames are not forwarded, but the addresses of other devices are studied, and the MAC address table is populated.
4. In the forwarding state, user frames are forwarded as well as addresses of other devices are examined, and a MAC address table is populated.
5. In the disconnected state, the user frames and BPDUs are not overridden.

The Fig. below shows the sequence ports are running STP protocol.



Initially, all switch ports are locked. It takes between 30 and 50 seconds to switch to forwarding status.

If the port is connected to the end nodes (not connected to other switches), the portfast feature must be enabled to speed it up to the port forwarding state. Then, when the port is activated, it automatically switches from blocking to forwarding. This is possible because such ports can not cause loops.

STP Extension

STP has several limitations and disadvantages, such as slow network convergence times, the need to list a tree every time a network topology is changed, and so on. Many other protocols have been developed to address these shortcomings. In this section, we will not discuss the basics of these protocols but only list the main ones.

Rapid Spanning Tree Protocol (RSTP)

Rapid STP (RSTP) is a significantly improved STP. Described in IEEE 802.1w (from now on referred to as 802.1D-2004). Its advantages include a decrease in convergence time and greater durability.

Per-VLAN Spanning Tree (PVST)

Per-VLAN STP (PVSTP) extends STP functionality in networks with VLANs. A separate STP instance runs here in each VLAN. At first, this protocol worked only through ISL trunks, then PVST + extension was developed, which allowed working through 802.1Q trunks, which are used much more often than ISL.

There are rapid-pvst implementations. They combine PVST + and RSTP properties.

Multiple Spanning Tree Protocol (MSTP)

Multiple STP (MSTP) is a state-of-the-art standard STP implementation that takes into account all the advantages and disadvantages of previous solutions. MSTP is described in IEEE 802.1s (from now on included in IEEE 802.1Q-2003).

Unlike PVST + (in which the number of instances of the connecting tree equals the number of VLANs), MSTP provides the configuration of the required number of instances regardless of the number of VLANs) on the switch. Multiple VLANs can be included in one MST instance. However, all switches participating in the MST must have equally configured VLANs that limit the flexibility of changing the network configuration.

Application of Switches

The switch is sometimes called a multi-port bridge. While a typical bridge has only two ports, the switch has several dozen - hundreds of ports depending on the model. Like bridges, switches receive some packet information from different computers on the network. In the future, this information is used to construct data switching tables, which are then used to determine the direction of data flows sent from one computer to another.

Although there is much in common with bridges and switches, a switch is more complex than a bridge. The bridge determines whether the frame is forwarded to another network segment based on the recipient's MAC address. The switch has several ports to which network segments are connected. The switch selects the port to which the receiving device or workstation is attached.

Switching is a technology that reduces the likelihood of congestion in the Ethernet LAN network by reducing the amount of data transmitted over the network and increasing the bandwidth. Switches are often used to replace hubs because they do not require modification of the existing cable infrastructure, which improves network performance with a minimum of changes to the existing network. Nowadays, in the field of data transmission, all switching equipment performs two main operations :

- Switching of data frames. This term refers to the process of transferring a frame received from one network environment to another (source) environment;

- Support for switching. To perform this function, switches build and maintain switching tables and monitor the possible formation of route loops.

Switches operate at higher speeds than bridges and can support additional and important enough features, such as VLANs (Virtual LANs).

The Ethernet switch has many advantages, in particular, allowing many users to communicate in parallel by using virtual channels and creating collision-free network segments, as shown in above Figure. This approach maximizes the available bandwidth of the general environment. The second advantage is the ability to reuse already existing hardware and cable infrastructure, which makes the transition to switching cost-effective.

Routers

Routers are designed to communicate between a large number of networks. This connection allows computers from different networks to exchange information with each other. Connected networks may belong to one company or be geographically dispersed and belong to anyone. Typically, long-distance networks are connected through distribution networks. Distribution networks are based on a large number of different technologies, including routers, transmissions, and different types of lines. Routers were created only to integrate distribution networks into a single global network.

The router is an intelligent device that operates predominantly on the first three levels of the OSI reference model. However, like any other node in the network, the router is capable of interacting on any of the seven levels of the OSI model. The need to use the first three levels is almost always there. To connect to the local network, the router uses the first two levels of the reference model (channel-level design). The most important feature is the ability of routers to identify network routes based on layer three addresses. This mechanism allows routers to communicate with multiple networks using network layer addressing regardless of location and network technology.

To understand the principles of routing and to understand the work of routers, it is necessary to understand two aspects of their work: physical and logical. From a physical point of view, the router consists of a huge number of components, each of which performs a strictly specified function. From a logical point of view, the router performs certain actions, including identifying other routers, obtaining information on potentially achievable

networks and nodes, identifying and tracking potential routes, and transmitting datagrams to recipients. This allows the formation and use of international networks, including distribution networks.

Basic Features And Classification Of Routers

The logical functions of the router are as important as providing the physical interconnection of multiple networks. For example, for a consolidated network, there must be at least one physical data channel between the sender and the recipient. However, the existence and use of a physical channel are two different things. Naturally, for normal operation, the sender and the recipient must "speak" in the same language (use a single routing protocol). In addition, such language (routing protocol) makes it possible to find the shortest route for data transmission by communicating with intermediate routers.

Thus, the router should provide the following functions :

- Physical interaction;
- Logical interaction;
- Security;
- Determining the route of data transmission.

The router has at least two (usually many more) physical I/o ports. I/o ports, or as they are often called interfaces, are used to attach the event of transmission to the router physically. Each port is connected to an extension card, which in turn connects to the router's system board. In this way, the router's motherboard enables the interaction of several networks.

The system administrator must configure each router interface using the appropriate interface (console). The configuration involves determining the port numbers in the router by specifying the data technology and available bandwidth for the networks connected to the interface, specifying the types of protocols to be used with this interface. The parameters of a particular port must depend on the type of network interface.

It should be noted that on top-level platforms, interfaces (VIP2 or PCB) are capable of transmitting packets without interrupting the main processor.

By scope, routers are divided into several classes.

Backbone routers are designed to build the corporation's central network. A central network can consist of a large number of LANs scattered across

different buildings and using a variety of network technologies of types of computers and operating systems. Backbone routers are the most powerful devices capable of handling hundreds of thousands or even millions of packets per second, with a large number of LAN and WAN interfaces. Not only medium-speed WANs such as T1 / E1 are supported, but also high-speed, such as ATM or SDH with 155 Mbps or 622 Mbps or more. Most often, the backbone router is structurally designed on a chassis-based modular circuit with a large number of slots - up to 12 - 14. Much attention is paid to backbone models of reliability, and fault-tolerant router, which is achieved through thermoregulation systems, redundant power supplies, replacement hot-swap modules, as well as symmetric multiprocessing.

Regional Branch Routers connect regional branches to each other and a central network. A regional branch network, as well as a central network, can consist of several local networks. Such a router is usually some simplified version of a backbone router. If it is made on the base chassis, the number of slots on its chassis is smaller: 4 - 5. A constructive with a fixed number of ports is also possible. Supported LAN and WAN interfaces are slower.

As a rule, ***remote office routers*** connect a single remote office network to a central or regional network with a global connection. As much as possible, such routers can also support two LAN interfaces. The remote office router can support dial-up as a backup for a dedicated channel. There are many types of remote office routers. This is explained by both the mass of potential consumers and the specialization of this type of device, which is manifested in support of one specific type of global communication.

LAN routers (Layer 3 switches) are designed to separate large LANs into subnets. The main requirement for them is the high speed of routing since, in this configuration, there are no low-speed ports. All ports have a speed of at least 10 Mbps, and many operate at 100 Mbps or more.

The Main Components Of Routers

Routers are extremely sophisticated devices. The complexity of their structure lies in a certain logic of the routing mechanism that enables the physical device to perform routing functions.

In the general case, the router is a normal specialized computer and accordingly consists of similar components :

- Central processing unit (cpu);
- Random-access memory (ram);
- Basic input / output system (bios);
- Operating system;
- Motherboard;
- I / o ports;
- Power sources, frame, metal casing.

The functions of some internal components of the router are shown in the table below.

Much of the router's components are enclosed and inaccessible to system administrators. These components are extremely reliable and should not fail under normal conditions. An exception to this rule is the installation of additional modules in the router. Additional resources can be added to the router at any time, but the outer casing will need to be removed. Most often, the specialist has to install additional I/o ports or additional memory.

When working with routers, the system administrator will most often deal with his operating system - software that enables hardware components to work together (in the case of Cisco routers, it will undoubtedly be the Internetwork Operation System, abbreviated IOS), and ports input-output. To modify and create a router configuration, the system administrators usually use the command line interface. The system configuration determines the number, location of I/o port types, addressing parameters, and bandwidth formation of interfaces and devices. In addition, the router configuration may include information about user access rights and types of individual I/o ports.

The router's I/o ports are the only physical component that an administrator can see. Ports provide a unique opportunity to create, perhaps, an infinite number of local and distribution network combinations implemented based on different data transmission technologies. Each port on the LAN or LAN must have its own I/o port on the router. These ports perform functions similar to those of Network Interface Cards (NICs) on a computer connected to a network; they are related to the frameworks of the framework and provide support for the respective interfaces. Many physical interfaces appear to be the same. However, at a higher level, they are completely different. Therefore, it is useful to study the relevant transmission technologies before using these or other interfaces.

Functions of some router components

Component	Function
1	2
Operational Memory (RAM / DRAM)	Used to store routing tables Saves ARP Cache Contains high-speed cache Responsible for packet buffering (shared memory) Provides storage of packages Provides temporary and working memory for router configuration files with power on RAM content is lost after the power is turned off or the device is restarted
Non-volatile memory (NVRAM	Contains a backup or startup copy of the configuration file when you restart or after shutdown, the data in this memory is not erased
Flash Memory (Reprogrammable Memory that Usually Uses Read Only (EPROM)) Contains data that, when restarted or shut down, teasers are not destroyed	Contains operating system image and microcode (Flash-in memory can store multiple versions of the operating system Cisco IOS) Allows you to update the software without replacing the chip
Permanent Memory (ROM)	Contains Power-On Self Test (POST) command code Contains bootstrap programs and basic operating system software To upgrade the software in the ROM requires a chip

	replacement on the system board of the device
Interface (Located on the motherboard or a separate modulator Lee interface)	Form a network connection through which packets are transmitted from The given router and enter the device

Comparison Of Switching And Routing

Routing is often confused with second-level switching. The fundamental difference between them is that the switching is implemented on the second level of the OSI model and routing on the third, and therefore they use different information for the organization of data transmission.

Routing is intended for data transmission between broadcast domains and requires a hierarchical addressing scheme, which is implemented in Layer 3 protocols (e.g., IP). The switch knows nothing about IP addresses and works only with MAC addresses of nodes. When a node sends information to a non-local recipient, it sends the frame to its standard gateway using its MAC address.

The switch combines segment that belongs to one logical network or subnetwork (subnetwork). The router also supports a routing table that allows you to select a route for data delivery outside the broadcast domain. Each ARP table contains pairs of IP and MAC addresses. The routing table contains information about routes. MAC addresses are not organized according to a certain principle, but this disadvantage does not cause problems with network management since individual network segments do not contain a large number of nodes.

If the IP address complying with the same rules, the Internet simply would not be able to function because there would be no way to determine the route to reach specific destinations. The hierarchical organization of IP addresses allows you to treat groups of addresses as a single entity until you need to determine the address of an individual node.

Another difference is that Tier 2 switches do not block Tier 3 broadcasts. As a result, they may be prone to broadcast storms. Routers typically block broadcast packets, thus limiting the coverage of broadcast storms to the local broadcast domain and providing a higher level of protection and bandwidth control than switches.

Comparison of the functions of routers and switches

Function	Router	Switchboard
Speed	Slower	Rather
OSI level	level 3	level 2
Used addressing	IP	MAC
Broadcasting	blocked	Skip
Security	Above	Lower
Segmenting networks	Segments the network into broadcast and conflict domains	Segments the network into collision domains

Chapter Three: Introduction to CISCO IOS

To date, Cisco is the leader in network equipment manufacturing. This equipment is mostly powered by Cisco IOS (Internetworking Operating System). So, let's take a closer look at some of the features and features of this operating system for both the router and the switch. Note that some IOS commands are common to both the router and the switch; other commands only make sense for one of these devices.

Cisco IOS provides basic routing and switching services, reliable and secure access to network resources, providing network scaling tools.

Cisco IOS Function Modes

There are three modes of operation in the Cisco IOS.

1. ***ROM monitor.*** This mode is used mainly for router faults or for password recovery. An invitation in this mode is> or ROMMON>.
2. ***Download from ROM.*** This mode is used for a replacement image of the OS; the ROM monitor software performs the bootstrap process and provides lower-level hardware operation and diagnostics. This mode is only accessible through a console session. When the router (or switch) boots from ROM, there are limited features available: you can burn an iOS image to Flash to replace the OS. The invitation in this mode is Router (boot)>.
3. ***Full-featured Cisco IOS mode.*** In the process of launching into the norm in standby mode, the router (or switch) loads the IOS into RAM. A configuration register is used to determine or set the boot parameters. An invitation in this mode looks like Router> (or Switch>).

User Interface

The Cisco Command Line Interface (CLI) is used as a traditional interactive environment in Cisco IOS. There are several ways to access the CLI.

1. You are using a session through the console port of the router (switch). In this case, a low-speed serial connection to a computer emulating the terminal is used. This connection uses a rollover cable. The computer must support VT100 mode emulation. To set

up a session, for example, you can use HyperTerminal from the Windows operating system by selecting the following settings: select the com port you want; set the baud rate to 9600 baud; set 8 bits of data; specify no parity check; select one stop bit (1 stop bit); specify no flow control mechanism.

2. You are using a dial-up modem connection or a null-modem connection to the AUX port of the router (or switch).
3. You are using SSH- (Secure Shell) or Telnet session.

The first two methods do not require any configuration of the router (or switch), and the third one requires it.

Console access and SSH access were the most widely used (SSH is a much more secure way of communication than Telnet) since it involves transmitting information, not in plaintext (like Telnet), but encrypted using the MD5 algorithm (Message Digest 5). access is more secure than access through a virtual terminal.

Modern networking equipment also supports configuration via Graphical User Interface (GUI), Web interfaces.

Command-Line Modes

The Cisco Command Line Interface has a hierarchical structure. To accomplish different tasks, this structure requires a transition to different modes. Each command line has different invocation labels, which allows the administrator not to confuse modes and to use only those commands that are supported by this mode.

Cisco IOS provides a command interpreter (EXEC) that checks and executes all commands that are entered. For security purposes, EXEC sessions are divided into two levels of access: User Executive Mode and Privileged Executive Mode.

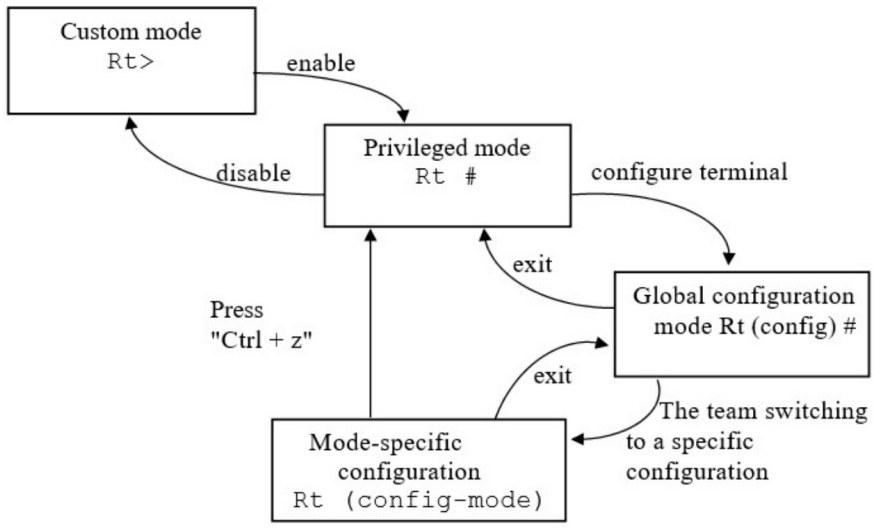
In user mode, only a limited set of basic commands are available to track the router's modes. It is often referred to as the view mode because it does not allow the configuration file to be modified. The word "user" does not mean that any ordinary user of the network can access the device. This mode is for employees who need access to the device for monitoring purposes only, but do not need permissions to change the device configuration. At the command line, this mode is identified by the symbol ">."

Privileged access mode allows everyone to use OS commands. It is authorized and may be restricted by a password and user ID. You must enter privileged mode to execute the configuration and management commands of the system administrator since access to the global configuration mode and other special modes is accessible only from the system administrator.

At the command line, this mode is identified by the symbol "#." It is necessary to switch from custom to privileged mode, enter the enable command and disable for the reverse transition (Fig below). If the privilege mode password has been set, the router will prompt it to continue. If the password you entered is correct, then the command prompt is changed to "#," and the IOS switches to privileged EXEC mode.

You can access the global configuration mode from privileged mode. On the command line, it is identified as "(config) #." It allows you to configure global parameters and ratings in a specific configuration mode, which is identified at the command line as "(config-mode) #," where mode indicates what that mode is. For example, you can switch from global configuration mode, in particular to configuration mode: interface (command prompt in this mode looks like:

> (config-if) #); subinterface: (config-subif) #; lines: (config-line) #; routing: (config-router) #.



Modes UI Router

Help with Cisco IOS Commands

While working in the CLI, there is often a need for help with commands,

arguments, command formats. To get this kind of help, you should remember the following.

To display the list of commands, type the question mark "?". If the listing does not fit on the screen, “- More--” will be displayed at the bottom of the screen. You can view one row below by pressing Enter, and the screen below is a space. Pressing any other key will return to the command line mode.

Any command and its format can be specified using the "?" Sign. If the question mark is placed directly in the command word (without space), then a list of commands starting with the corresponding initial letters is displayed, if after the command, the format of the corresponding argument. An example illustrating the above is given below.

Note that while working in the CLI, you can receive three different types of error messages.

- ***Ambiguous command*** - means that the command entered (or rather part of it) is ambiguous and does not allow you to determine which command the administrator wanted to enter since several commands begin with these letters (see the second line of Example 3.1).
- ***Incomplete command*** - means that the command is not fully entered, for example, all its arguments are not entered, etc. (see the eighth line of Example below).
- ***Incorrect command*** - a command entered incorrectly, i.e., you incorrectly typed this command or its arguments, etc. (for example, in the fifth line of Example below I typed the wrong command "clock" instead of "clock" and line 20 instead of the word "July" the number of this month is incorrectly entered - 7, and this is indicated by the "^" symbol of the 21st line).

Router#cl

% Ambiguous command: “cl.”

Router#cl?

clear clock

Router#clock

%Unknown command or computer name or unable to find computer

address

Router#clock

%Incomplete command. Router#clock?

set Set the time and date

Router#clock set

%Incomplete command.

Router#clock set ?

hh:mm:ss Current Time

Router#clock set 15:37:00

%Incomplete command.

Router#clock set 15:37:00 ?

<1-31> Day of the month

MONTH Month of the year

Router#clock set 15:37:00 14 7

^

% Invalid input detected at "^" marker.

Router#clock set 15:37:00 14 July

% Incomplete command.

Router#clock set 15:37:00 14 July ?

<1993-2035> Year

Router#clock set 15:37:00 14 July 2009

Router#

Routing Sequence of the Router and Switch

Consider the features of the router boot. When the router is turned on, a POST (Power-On Self-Test) self-test is stored and stored in the ROM. After that, the software initialization process begins, which consists of two steps.

1. System startup programs initialize the router software.
2. Backup software recovery programs perform alternative software

startup as needed.

Starting programs should ensure that the hardware is functioning properly; find and download iOS; find and apply the configuration startup file (if not, enter the initial configuration mode).

So, after the POST test, the following events occur.

1. The Bootstrap program is running.
2. IOS image is loaded (Fig above). As a standard, when booting the router (switch), the location of the IOS is determined by the hardware platform. However, most often the router first searches for boot system commands stored in NVRAM:

    - Router(config)# boot system flash ios_filename,
    - Router(config)# boot system tftp ios_filename tftp_addr,
    - Router(config)# boot system ROM.

In general, IOS software provides the user with several possible alternatives; for example, the user may specify other sources of IOS download. You can also use your own fallback backup as needed. Setting the appropriate values for the Configuration Register download field allows you to use several alternatives. The user can also enter several boot systems commands (in global configuration mode) that will determine the backup sources that the router will consistently use. If NVRAM does not have boot system commands, then by default, the router uses IOS with Flash memory, if there is no IOS there, - the router tries to use TFTP. If it is not available, a reduced version of IOS from the ROM will be downloaded.

NVRAM memory is loaded into the RAM, and the startup configuration file is executed. If the configuration file is missing or incorrect in the NVRAM - , IOS searches for it on the TFTP server; otherwise, it invokes the Setup program, which asks the system administrator a series of questions. Its purpose is to create a minimum configuration. You can interrupt the configuration process at any time by pressing Ctrl-C. Note that this mode is not recommended as the primary configuration tool.

Now let's briefly describe the process of downloading the switch (which has a lot to do with the process of loading the router). After switching on (or rebooting), the switch loads a boot loader stored in NVRAM. This program:

- Low-level processor initialization. Processor registers are initialized to control physical memory mapping, memory capacity, and speed.
- Performs POST self-testing for processor subsystems. The memory and part of the flash device containing the file system are checked.
- Initialize the flash file system on the motherboard.
- Downloads the default image of the operating system into memory and downloads the switch. The bootloader finds a Cisco IOS image on a switch by browsing a directory that has the same name as the Cisco IOS image file (excluding the .bin extension). If no image is found there, the bootloader scans each subdirectory before continuing the search in the current directory.

The OS then initializes the interfaces using the commands of the config.text configuration file stored in the flash memory of the switch.

Router and Switch Configuration Files

Recall that the configuration file contains commands for configuring the router (switch) and its services. In most cases, the size of this file ranges from a few hundred to tens of thousands of bytes. In general, there are two configuration files: Running config - stored in RAM (also known as current or active). After the restart, the working configuration file is lost because RAM is memory dependent power supply (Fig below); Startup config starter is stored in NVRAM, independent of power, and copied to RAM at system startup.

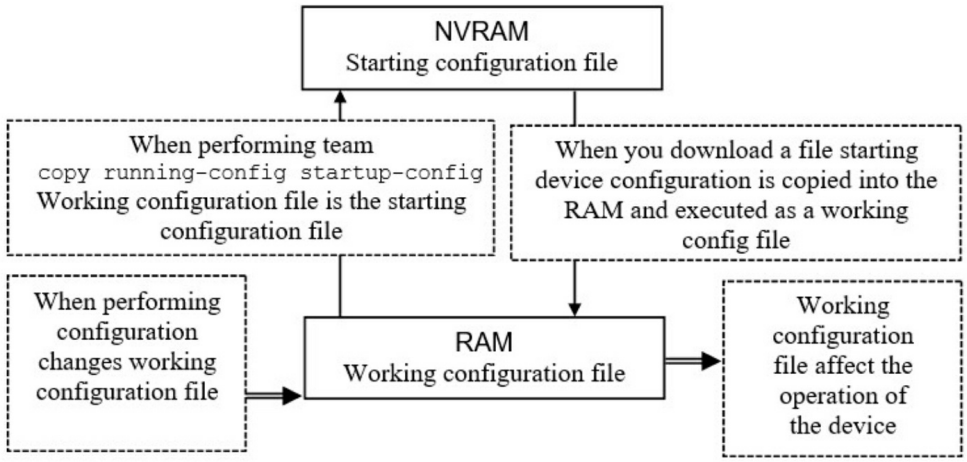
After any changes to the router (switch) configuration, these changes can be checked using the show running-config command, which displays the current configuration. If the values of the variables are wrong - , you can do one of the following:

- use configuration commands with the prefix no.
- Restart the system and restart the original configuration file from NVRAM.
- Copy a backup file of the configuration file from the TFTP server.
- Delete the initial configuration file using the erase startup-config command, restart the router, and enter the Setup mode.

You must enter the command to save the configuration changes to NVRAM

Router # copy running-config startup-config

It is important to note that it is very important within each organization (especially if it is large) to develop a single standard for configuration files. This will avoid the chaos, unnecessary complexity of network setup, reduce unplanned downtime, and more.



Files and start working configurations

Initial Configuration Of The Switch

It is worth noting that the new switch, unlike the router, has a standard initial configuration set by the manufacturer. The configuration of the switch can be changed via the command-line interface as well as the web interface using a browser.

The first time the switch is powered on, the configuration file contains the default settings. The switch has the standard name Switch. There are no passwords set on the console and virtual terminal (VTY) lines.

By default, switch ports are set to automatic mode, which means that they automatically determine the mode of operation (duplex or half-duplex) and port speed.

By default, all switch ports are in the first virtual LAN (virtual LAN, VLAN). It is considered the standard management VLAN. The show VLAN command is used to display information about the VLANs defined on the switch.

Because the new switch has not yet been configured, it's in its flash directory;

there is no VLAN database file (vlan.dat) and a saved configuration file (config.text). The vlan.dat file is used to store local VLAN information for a given switch, and the switch uses it to share VLAN information with other switches. By default, the flash directory contains an IOS image (.bin file extension), an environment variable file named env_vars, and a subdirectory named html. The dir flash command is used to display the contents of the flash directory.

In the standard configuration, the switch has one broadcast domain and can be managed and configured through a console port using the CLI. This configuration also sets the binding tree protocol. In the standard configuration, the highest level of security is guaranteed, since the switch has not yet been assigned an IP address.

Finally, for smaller networks, the standard configuration may be sufficient, and the user can immediately benefit from the micro-segmentation and high network performance provided by the switch. However, if necessary, the user can completely change the existing configuration. To do this: delete the existing VLAN information by deleting the vlan.dat file of the VLAN database from the flash directory, remove the backup configuration file and restart the switch.

The example below shows how to remove the current configuration in the Catalyst 2950 series switches.

Switch # delete flash: vlan.dat Delete filename .?

Delete flash: vlan.dat? . Switch # erase startup-config

<output part omitted> Switch # reload

Commands for Initially Configuring and Monitoring the Router and Switch

First of all, it should be noted that some IOSs issue certain messages when executing commands. Such messages can be inserted inside the commands that the network administrator types. Although this does not necessitate new recruitment of these appropriate commands and the operating system understands them correctly, it may cause some discomfort to the administrator. To correct this situation, it is advisable to use the synchronous logging command:

Router(config)#line console 0

Router(config-line)#logging synchronous

Router(config-line)#line vty 0 4

Router(config-line)#logging synchronous

Now, during the console or VTY session, the admin commands will not be broken by system messages.

Name customization is one of the first commands to be executed on a router or switch. The name should tell the administrator about the location and features of this device. As an administrator, as a rule, deals with many routers, switches, etc. and to configure them (especially with the help of SSH sessions), the administrator needs to navigate on what device he is on. The name assignment is performed globally:

Router(config)#hostname

Rt1_VNTU Rt1_VNTU(config)#

Setting Passwords

Passwords are used to protect against unauthorized access. Password can protect access to:

- ***Console.*** The password for the console is set using commands:

  Router (config) #line console 0

  Router (config-line) #password <password>

  Router (config-line) #login

- ***Virtual terminal line (VTY).*** Telnet access. Multiple Telnet sessions can be set up at a time. You can set a password for each line individually, and you can set a password for all lines. The password is set using commands:

  Router (config) # line vty 0 4

  Router (config-line) # password <password>

  Router (config-line) # login

- ***Preferred mode of operation.*** To restrict access to privileged mode, a command like below one must be entered:

Router (config) # enable secret <password>.

One-sided MD5 encryption is used here to save the password, which makes it impossible to recover the password. If this command is not supported, you can use the command

Router (config) # enable password <password>,

but in this case, the password will be stored in the configuration files in unencrypted form. You can use the command to prevent the password from being displayed in the open

Router (config) # service password-encryption.

In this case, all passwords will be encrypted (except for the password set by the enable secret command), but the level of information protection is low here.

The command is used to cancel encryption of all passwords

Router (config) #no service password-encryption.

Configuring serial interfaces (performed for the router) involves the following steps:

- enter global configuration mode.
- Enter the configuration mode of the desired interface.

The format of the command can be

Router (config) # interface type port,

Router (config) # interface type slot / port,

Router (config) # interface type slot / subslot / port,

where the interface is the type of interface (e.g., Serial, FastEthernet, GigabitEthernet, Loopback, etc.); port, subslot, slot мери port, slot, and floor numbers, respectively.

- Set the IP address of the interface and the mask on the network.
- Specify channel bandwidth (optional).
- Set the clock frequency for DCE (by default, routers function as DTE but can also be configured as DCE).
- Describe the interface - so that the administrator can recall any important information about that interface. It is advisable to create

the description in a special format (for example, the purpose and location of the interface, a description of the devices connected to it, etc.).

- Enable the interface.

The commands that follow these steps are:

Router # configure terminal

Router (config) # interface serial 0/0/1

Router (config-if) # ip address <ip address> <netmask>

Router (config-if) # bandwidth 56

Router (config-if) # clockrate 56000

Router (config-if) # description interface from others

Router (config-if) # no shutdown

By default, all router interfaces are disabled. Use the no shutdown command to enable the router or switch interface, and shutdown to disable the interface.

Configure Ethernet Interfaces

For a router, this setup is similar to configuring its serial interfaces, except that the router, the fourth and fifth steps are not required.

There is something different about configuring Ethernet interfaces. The switch's FastEthernet ports are set to automatic baud rate and duplex mode by default. This allows the interface of the participating devices to modify these settings. If the administrator needs to be sure that this interface has a specific bit rate and duplex or half-duplex mode, then these values should be manually set, as shown in the below Example.

Switch(config)# interface FastEthernet0/2

Switch(config-if)# duplex full

Switch(config-if)# speed 100

Another useful feature that can be installed on a port is the portfast option. If the switch port is only connected to end-user stations (i.e., not connected to another switch), then the portfast function should be installed on it using the command

Switch # set spantree portfast 4/1 enable.

In this case, the first time the port is used, it automatically switches from the blocked state to the forwarding state.

Configure Loopback Interfaces

Sometimes there are times when you need to emulate a connection that does not currently physically exist (for example, in the future, it is planned to connect to a provider, another organization, etc.). To do this, you can configure the router's Loopback interface by specifying the desired IP address and mask:

Router (config) # interface loopback number

Router (config-if) # ip address <ip address> <netmask>

Router (config-if) # description My virtual interface

Router (config-if) # no shutdown

Customize Banners

The banner is the message that appears when you log in. Such a message (also called the Message of the Day MOTD) can be used to transmit some information to all network users. For example, often, this message warns users that logging in is forbidden for unauthorized users. Use the command to set the message of the day banner motd followed by the text you want, highlighted with the characters "#," as shown in the below Example.

Router(config)# banner motd #

Enter TEXT message. End with the character '#'.

********** WARNING!!

Unauthorized Access Prohibited!!

**********#

Set up Telnet and SSH access

First of all, specify the required access method: either telnet, or SSH, or telnet and SSH can be as follows:

Router (config) # line vty 0 4

Router (config-line) # transport input <mode>,

and to choose one of the above three alternatives, the value of the argument mode will be telnet, ssh, and all, respectively.

Telnet Access

For the router, as mentioned above, to obtain Telnet access, it is sufficient to set a password for VTY access and set the IP address and subnet mask to the appropriate interface.

For a switch, Telnet access involves assigning it an IP address and setting a default gateway. The below example shows how to do this for Catalyst 2950 switches. By default, VLAN 1 is a virtual management network. On a network built on switches, all devices on the core network must be on a VLAN. This allows you to access, configure, and manage all devices on the integrated network from one workstation.

```
Switch(config)# interface VLAN1
Switch(config-if)# ip address 192.168.1.2 255.255.255.0
Switch(config)# ip default gateway 192.168.1.1
```

SSH Access

SSH access also requires an SSH client and SSH server. RSA (Rivest, Shamir, Adleman encryption) keys must be generated to implement such access. RSA involves the use of a public key stored on a public RSA server and a private key known only by the sender and receiver. The public key can be known to anyone and used to encrypt messages. Such encrypted messages can only be decrypted using a private key.

You need to generate RSA keys using the command

```
crypto key generate rsa
```

This procedure is required if you are configuring a device (such as a router) as an SSH server. You should enter privileged mode, assign a device a name, select a domain name, and generate a pair of RSA keys:

```
Router# configure terminal
Router(config)# hostname
Rt(config)# ip domain-name my_domain
Rt(config)# crypto key generate rsa
```

In the fourth command (crypto key generate rsa), you allow the SSH server to perform local and remote authentication and generate a pair of RSA keys. When generating these keys, you must choose their length (Cisco, for

example, recommends choosing a length of 1024 bits). Although longer, it would be safer, it also takes longer to generate and use.

You can see the status of the SSH server by using the show ip ssh or command show ssh. To remove an RSA key pair, enter the command

Rt(config)# crypto key zeroize rsa,

after which the SSH server automatically shuts off.

When configuring SSH access, you can also specify:

- the used version of SSH (first or second) using the command Rt (config) # ip ssh version <v_num>, where v_num is the version number.

If you do not enter this command, the SSH server will select the oldest ver-

client-supported session (for example, if the client supports SSHv1 and SSHv2, the server selects SSHv2).

- SSH control parameters: time-out time in seconds from 0 to 120 (standard 120 seconds) can be specified using the command Rt (config) # ip ssh timeout <seconds>. This time is taken to establish a connection; the maximum number of client authentication attempts from the range 0 to 5 (default 3) can be specified using the Rt (config) #ip ssh authentication-retries <number> command.

Working with MAC Address Table (for Switches)

Switches learn about the MAC addresses of computers or other end devices connected to their ports by analyzing source addresses in frames that arrive at a given port. These addresses are then entered into the MAC address table of the switch. To view known switch addresses, you must enter privileged mode, as shown in the following example.

Switch#show mac-address-table

Dynamic Address Count: 2

Secure Address Count: 0

Static Address (User-defined) Count: 0

System Self Address Count: 13

Total MAC addresses: 15

Maximum MAC addresses: 8192

Non-static Address Table:

Destination Address	Address Type	VLAN	Destination Port
0010.7a60.ad7e	Dynamic	1	FastEthernet0/2
00e0.2917.1884	Dynamic	1	FastEthernet0/5

The addresses are dynamically studied, and the switch can support as many as a thousand MAC addresses, with several tens of addresses on each port. To conserve memory and optimize the switch, it may sometimes be necessary to remove some items from the MAC address table. For this purpose, all table items have timestamps that reflect the time of arrival at the packet port with the given address. Workstations can be disconnected from the port, switched off or switched to another port on the same or another switch, possibly replacing the network interface card. This can all be confusing when sending frames. To avoid this, the switch is configured to automatically remove the corresponding MAC address from the table in the absence of frames with a previously recorded address within a certain time (typically 300 seconds).

Instead of waiting for the natural aging of the dynamic address position, the administrator can use the clear mac-address-table command to remove it (see the example below).

MAC addresses configured by the administrator can be deleted similarly, which instantly removes the table entries with the addresses that have become invalid.

Switch#clear mac-address-table

Switch#show mac-address-table

Dynamic Address Count: 0

Secure Address Count: 0

Static Address (User-defined) Count: 0

System Self Address Count: 13

Total MAC addresses: 14

Maximum MAC addresses: 8192

Non-static Address Table:

Destination Address Address Type VLAN Destination Port

---------- ---------- ---- --------------

Configuring Static MAC Addresses

There may be situations where it is advisable to bind a MAC address to a specific switch interface permanently. In this case, the automatic deletion of the MAC address will not occur after the normal storage period has expired.

The permanent address may be linked to the interface, if necessary, to connect the user's server or workstation to the port provided that the MAC address is known. This can also increase the level of security. The following command syntax is used to set a static MAC address on the switch interface:

Switch (config) # mac-address-table static mac-address-of-host interface FastEthernet ethernet-number vlan vlan-name

Example,

Switch (config) # mac-address-table static 0a40.4v00.2341 interface FastEthernet0 / 5 vlan VLAN1

To remove an address position from a table, use the same command- yes, with the keyword no.

Configuring Switch Port Security

Securing a unified network is an important task for the administrator. Due to the wiring diagram, switch ports related to the access level are available in wall connectors of offices and other premises and can be connected to any of them using a PC. They are also potential entry points for unauthorized users. Switches have a port security feature. In particular, you can limit the number of addresses that can be found on a specific interface. During configuration, certain actions can be specified if this number is exceeded, such as commands.

Switch (config) # interface FastEthernet0 / 1

Switch (config) # port security action shutdown

This leads to disabling the corresponding port if the number of MAC

addresses exceeded). Secure MAC addresses can be set statically, but this way may be quite complex, besides large probable errors.

An alternative approach is to implement security measures for ports on the switch interface. The first address, which learns dynamically switch, is safe to change the security on the interface being used in the form of this command with the keyword no to test the Status of safety at the port use the command show port security.

Teams Show

There are several show commands in the operating system that provides static information about the operation of the device. For example, they provide information about the configuration, operation, and status of parts of a router or switch.

You can view a list of all show command settings show

Some command options are listed below:

- show arp - displays the ARP table of the device.
- Show startup-config - displays the configuration contained in NVRAM (configuration startup file).
- Show running-config - Displays the configuration available in RAM (working configuration file).
- Show interfaces - displays statistics about all device interfaces. If you want to see statistics for a specific interface, enter show interfaces FastEthernet 0/1.
- Show ip interface brief - provides brief information on all device interfaces and their status.
- Show controllers serial - displays information about the router's hardware.
- Show clock - displays the set time.
- Show hosts - displays a list of managed hostnames and addresses.
- Show users - displays a list of users connected to the device.
- Show history - displays a list of entered commands.
- Show flash - displays information about the flash memory and the files in it.
- A very useful command that provides a lot of information is the show version command. It outputs information, for example, to

the router about: the IOS version and its concise description; Bootstrap ROM version; version of shortened IOS in ROM (Boot ROM); device uptime (Router uptime); the last method of restarting the device (restart method); the name of the system file image and its location; the hardware platform number of the device; settings of the configuration register;

- show protocol - displays the global status and status of the interfaces of any third-level router.
- Show mac-address-table - Displays the MAC address table of the switch.

Note that there are a lot of show commands, and it is inappropriate to list them in this guide. These commands and their functions can be seen in more detail, for example, in.

General Information about Debug Group Commands

Debug commands (or debugging commands) allow you to locate problems with protocols and incorrect settings. While show commands only provide a static picture of the device, the data generated by the debug commands are dynamic and provide a deeper understanding of current events as the device works. The dynamic style of debug commands is due to system resources, which can overload the processor and disrupt the normal operation of the device. Therefore, they should be used only when necessary.

It is also recommended to narrow the search box to several options. In other words, the debug group command should use to locate specific problems and not to monitor the normal operation of the CM. It is especially important to keep in mind that the debug all command should be used as rarely as possible, as it may disrupt the network.

An additional useful Cisco IOS service that enhances the value of debug commands is the timestamp command, which notices debug commands with timestamps that tell you the time when an event occurred and the time interval between them.

The no debug all and undebug all commands disable all diagnostic messages. To disable a specific debug command, use the same command with the addition of the keyword no. You can view everything currently being explored with the debug command using the show debugging command.

Chapter Four: The Basic of Routing Protocols

Assignment and Classification of Routing Protocols

Routing protocols are designed to automatically build routing tables (TMs) based on which packets are moved. The following tables contain enough data to make a decision to forward any packet received to the router. Table content depends on the technology of the stacked network. As a rule, the shortest route is chosen (the length of a route means its metric, which is a numerical value that affects the choice of route: the smaller the metric the better.

The metric can be determined, for example, by the number of intermediate nodes, the bandwidth, the delay time, the reliability of the channels between the routers).

All routing methods can be divided into two large groups: without tables and with TM.

Routing without tables is divided into an avalanche event driven from the source.

Avalanche routing is the simplest way of transmitting, which implies that each router sends a packet to all its neighbors, in addition, from whom it received its packet. In this case, the network bandwidth is used very inefficiently.

Event-driven routing implies that a packet to a specific destination network is sent along a route that has already been successful. In this case, the sending router must be able to capture the success of the packet delivery.

Source routing implies that the sender places information in the packet on which intermediate routers should participate in packet transmission. This information is either provided manually by the administrator or automatically generated by the sender node.

Table-based routing is, in turn, divided into static and dynamic (adaptive). Static routing requires manual routing by an administrator. Such routing requires a manual change of routes when changing the network structure.

In the case of dynamic routing, networks can update their TMs and adapt quickly to changes in topology and connection status. The successful operation of this type of routing depends on the router's performance of two of its main functions: maintaining the TM in an up-to-date state and timely

dissemination of information in the form of announcements and updates of routes among other routers.

When distributing network information, the dynamic routing mechanism uses one of the routing protocols. Such a protocol defines a set of rules that a router uses when communicating with neighboring routers. Route Protocol-

The definition defines how updates of routes are sent, what information is contained in the updates, how often updates are sent on how to search for update recipients.

Each of the routing algorithms uses its own way of choosing the best route. To do this, it generates a value called a metric for each route in the network. Usually, the smaller the metric value, the better is the route.

Metrics are calculated based on one or more parameters:

- Bandwidth - describes the bandwidth of the channel.
- Delay - the time it takes a packet to pass through the channel from the sender to a recipient.
- Load - the degree of utilization of network resources on a router or channel.
- Reliability characterizes the level of errors in a network channel.
- The number of conversions - the number of routers through which a packet must pass before reaching its destination.
- Cost - an arbitrary value, calculated based on bandwidth, financial costs, or other characteristics selected by the network administrator.

Therefore, the routing protocol is a means of communication between routers that allows devices to share network information and to determine distances to different nodes and networks. The information that one router receives from another (via routing protocol) is used to build and maintain an up-to-date TM status.

Most routing algorithms can be classified into one of two categories:

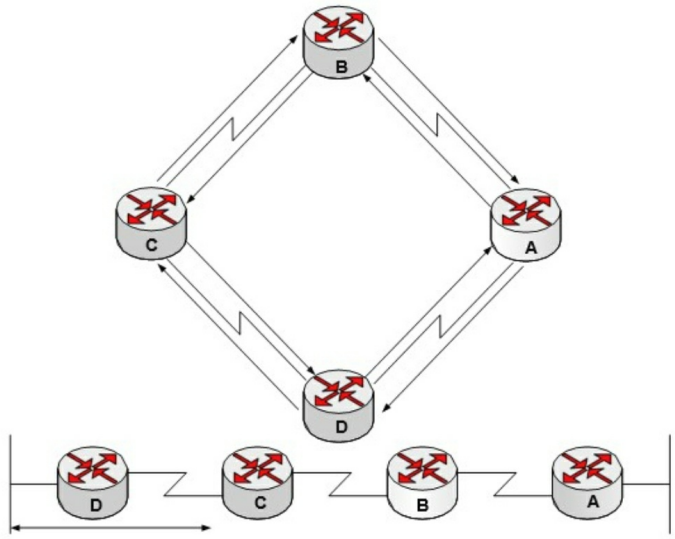
- Remote vector protocol (DVP).
- Channel-based protocol (PSTC).

The remote vector protocol determines the direction or vector and the distance to the desired node of the integrated network. Examples of such

protocols are RIP, IGRP, EIGRP, BGP. For a while, EIGRP was considered a hybrid protocol because it combines the features of both remote-vector and channel-based algorithms, but today Cisco is referring to it as DVP, although it is worth noting that it has much better characteristics than classic fiberboard.

The channel-state protocol, also called the shortest path first (SPF), reproduces the topology of the entire network. Examples: OSPF, IS-IS, NLSP.

When using distance vector algorithms, copies of routing tables are periodically sent between routers. In such regular updates, routers notify each other of changes in the network topology. Remote-vector routing algorithms also called Bellman-Ford algorithms. In Fig. below Each router receives a TM from neighboring routers.



The concept of remote vector routing

Router B receives a table from router A. The router adds the value of the distance-vector, the number of transitions, which increases the resulting distance vector. Subsequently, router B transmits its new routing table to its neighbor, router B. Such a step-by-step process occurs on all adjacent routers.

The distance vector algorithm accumulates distances on the network, which allows maintaining a database (DB) that contains information about the network topology. However, remote vector algorithms do not provide routers with an accurate topology of the entire network, since each router is known only to neighbor (adjacent) routers.

Each router that uses remote vector routing begins its work by identifying adjacent routers. In Fig. above illustrates the formation of a distance vector. For each interface directly connected to the network, the distance vector is set to zero. In the process of calculating the distance vector, the routers find the best route to the receiving neighbors based on information received from the neighbors. For example, router A learns about other networks based on the information it receives from router B. Each of the TM positions has a total distance vector that shows what distance the corresponding remote network is located.

TM updates occur when the network topology changes. As the vectors form, distances of topology change are recorded in the TM of the following routers. Remote-vector algorithms require that each router sends the entire TM to each of its neighbors.

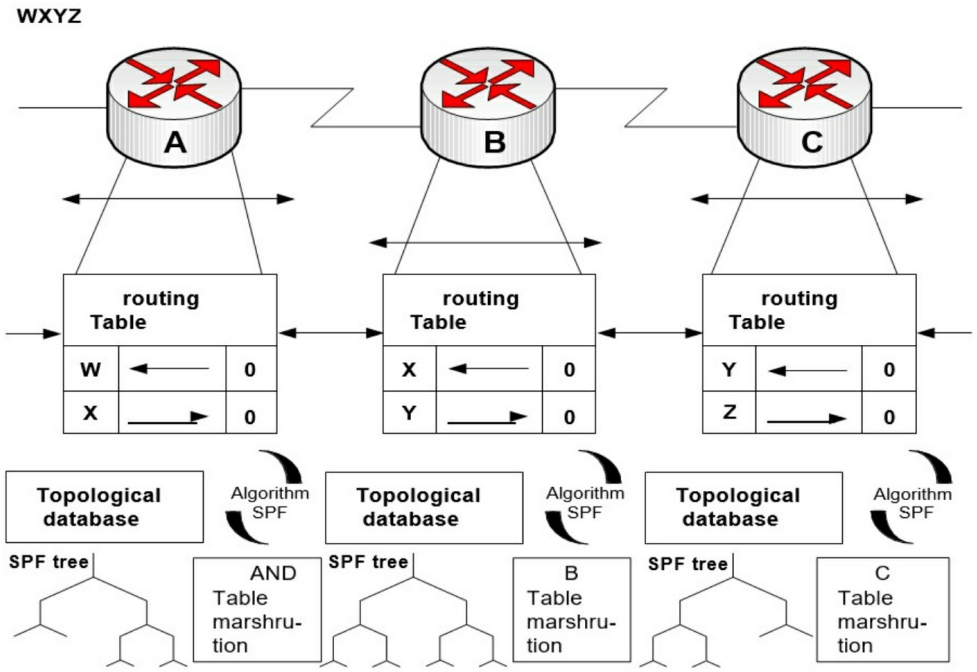
The distance vector is comparable to the highway road signs. These signs point to the destination and the distance to it. Further, along the same highway signs may be indicated, indicating the same direction. However, they will be shorter to indicate — a decrease in this distance when driving indicates the correct direction of travel.

The second basic routing algorithm is the channel mapping algorithm. Such algorithms are known as Dijkstra algorithms or Shortest Path First. They maintain a complex base of topological information. Since remote vector algorithms do not contain specific information about remote networks and routers, algorithms using channel state support complete information about remote routers and their connections are used for channel state routing:

- Channel status announcements (Link-State Advertisement - LSA). These are small packages containing information about routes sent between routers.
- Topological Database. This database contains information obtained from LSA messages.
- Shortest Path First algorithm. The corresponding algorithm performs calculations over a database, which results in the construction of an SPF link tree.
- Routing Table. This table contains known routes and related interfaces.

Routers communicate with LSAs starting from directly connected networks.

Each router, in parallel with the other, creates a topological database, which consists of the information received from these messages (Fig below). If a router becomes aware of a channel status change, it sends this information to all other routers on the network so that they can use it for routing. To complete convergence, each router maintains information about neighboring routers, their names, interface states, and the cost of channels to neighboring devices. The router creates an LSA package that lists information about new neighbors, changes in channel costs, and discontinued channels. This LSA packet is then sent to all other routers.



Calculating the shortest path

By default, each routing protocol on a particular router distributes only the information that the router received through the same routing protocol. Since not every router always supports all protocols for a given network, they use a special internal mode of operation called a redistribute.

It should be noted that with the growth of networks, the problem of router interaction is increasing, and to solve it, a different approach was found, namely the division of the network into autonomous systems.

Internal and External Internet Protocols

The Internet is a worldwide system of voluntarily integrated KMs, built on the use of IP and packet routing. From the beginning, the Internet was built as

a network that brought together a large number of existing systems. Its structure defines the core backbone network, and networks connected to the backbone are considered as autonomous systems (AS).

An Autonomous System (AS) is a set of networks that are under single administrative management and that use a single routing strategy and rules. External speakers are the only object.

Each AS must have its own unique Autonomous System Number (ASN). The numbers are allocated by the Internet Assigned Numbers Authority (IANA), which also allocates IPs to the Regional Internet Registry (RIR) blocks. Local RIRs then assign the organizations an AS number from the block obtained from IANA. Organizations wishing to obtain an ASN must complete the registration process at their local RIR and receive approval.

Previously, 16-bit AS numbers were used, allowing a maximum of 65,536 assignments. Today, 32-bit ASNs are already in use, allowing a maximum of 232 standalone systems to be addressed.

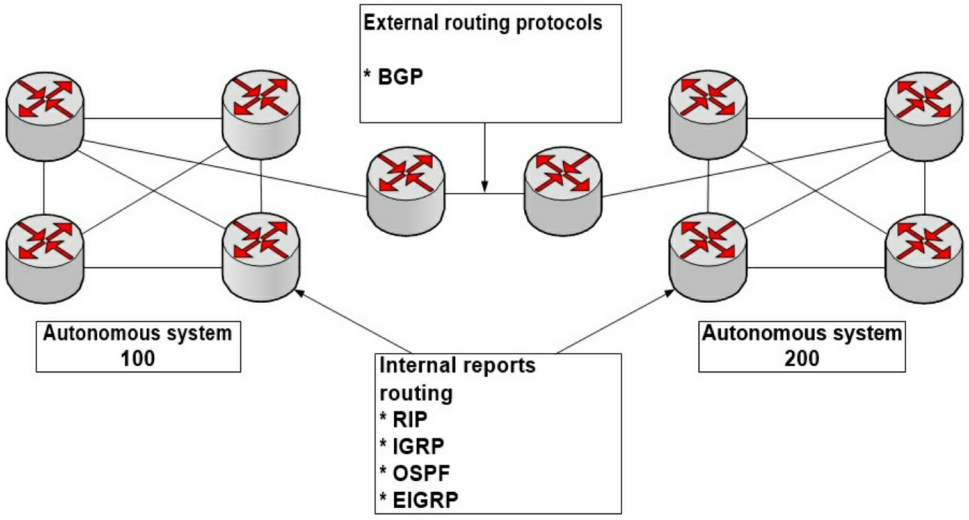
AUs divide a merged KM into several smaller and more easily managed networks. Each AU has its own set of rules and policies, and its number is globally unique, that is, distinguishes it from all other autonomous systems of the world.

The gateways used to form networks and subnets inside the autonomous system are called interior gateways, and the gateways used to connect autonomous systems to the backbone are referred to as exterior gateways. The highway itself is also an AU. According to these definitions, routing protocols are also divided into two types: the internal protocol and the external gateway protocol (Fig below).

An interior gateway protocol (IGP) is intended for use on a network managed or administered by an individual organization. Such a protocol is used to find the best route on a single network. In other words, metrics and the nature of their use are the most important elements of the IGP protocol.

The Exterior Gateway Protocol (EGP) is designed to route routing between networks managed by different organizations. Typically, these protocols are used when routing between Internet Service Providers (ISPs) or between an individual company and an ISP. The EGP protocol must isolate the AU. Because in every speaker they use.

For these rules to be in place, there should be a common protocol on the integrated network that will allow them to communicate.



Types of routing protocols

Comparison Of Static And Dynamic Routing

Static routing has the following features:

- Provides TM support for small networks that are not expected to expand substantially.
- Provides routing for the end (deadlock) network.
- Specifies a single default route to any network if the TM does not contain a more specific route.

Therefore, analyzing the above, you can identify the advantages and disadvantages of static and dynamic routing.

Static routing benefits: The common benefits of static routing are minimal CPU usage, easier for the administrator to understand, and easier to configure.

Disadvantages of static M: configuration and maintenance take a long time; errors may occur during configuration (especially on large networks); administrator intervention is required to support the replacement of route information; network growth is poorly scaled; proper implementation requires complete knowledge of the entire network.

Advantages of dynamic routing: requires less admin intervention when adding or removing networks; protocols automatically respond to topology

changes; configuration is less error-prone; more scalable, building a network usually does not cause problems.

Disadvantages of dynamic routing: router resources are used; need more admin knowledge to configure, validate, and troubleshoot.

Comparison of static and dynamic routing

Criterion comparison	Static routing	Dynamic routing
Difficulty of configuration	Complicated with growth network complexity	In general terms, not depending on the complexity of the network
Requirements Knowledge administrator	Need a low level knowledge	Need more knowledge
Change Topologies	Required administrative intervene Channa	Automatically adapts change
Scaling	Suitable only simple topologies	Suitable for complex and simple topologies
The degree of security	More secure than dynamic routing	Do not guarantee the safety
degree application resources	Does not require an additional resource of villages	Applies processor, memory, bandwidth
predictable ness	Marshut is constant	The route depends the current topology

Comparison of Some Dynamic Routing Protocols

As noted above, dynamic routing algorithms are divided into Remote Vector (DVA) and Link State (LSA). The distance vector protocols use the Bellman-Ford algorithm to find the best path. Some DVAs periodically send neighbors full TMs, which can generate significant traffic. DVAs have no idea of the topology of the entire network. They know about remote networks only the distance to them and the output port (or next-hop address).

DVA protocols work best in situations where the network is simple and does not require a special hierarchical structure; administrators do not have sufficient knowledge of LSA configuration selection and support; specific types of networks are used, for example, hub-and-spoke networks; worst-case convergence time is unprincipled for the network.

The LSA uses the Dijkstra algorithm to find the best path. Routers are aware of the entire KM by collecting information from all routers. Each router has a complete topological map of KM, and all KM routers use the same topological map. LSAs do not make periodic updates. After the convergence of the KM, updates are sent only if its topology changes.

LSA protocols work best in situations where: KM is large and hierarchical; the administrator has sufficient knowledge; rapid convergence in KM is very important.

A comparison of traditional distance vector protocols with the EIGRP protocol is given in the below Table and some dynamic mapping protocols in the following table of the next one.

Comparison of conventional DVA EIGRP

Traditional DVA	EIGRP
Using the algorithm Bellman-Ford or Ford-Fulkerson	Uses diffusion algorithm updates Routing (Diffusion Update Algorithm)
Used periodic innovation and lifetime records TM	Not used periodically updated to help attitude, no items lifetime TM
Saves only the best route to the destination	Supports topological table (other than TM), which contains both the best and reserve way to a destination
When the route becomes invalid router must wait until the next renewal	When the route becomes invalid, DUAL performed reserved backup path with topological Table
Slow convergence by using hold-down timers	Fast convergence due to lack of hold-down timer and system coordination route calculation

Comparison of some dynamic routing protocols

Criterion	DVA				LSA	
	RIPv1	RIPv2	IGRP	EIGRP	OSPF	IS-IS
Speed convergence	Slow	Slow	Slow	High	High	High
Scalability (The size of the network)	Small	Small	Small	Great	Great	Great
Support VLSM	-	+	-	+	+	+
degree we used last one resource	Low	Low	Low	The average	High	High
Introduction and support	Easy	Easy	Easy	Difficult	Difficult	Difficult

Comparison of OSPF with RIP

A comparison of OSPF and RIP protocols is not entirely legitimate since the two protocols are designed for a completely different network environment. OSPF is designed to be used in large, complex networks designed with a thoughtful approach. The RIP protocol is intended for small networks where the use of a simple protocol makes it easy to design and shorten the configuration time. In fact, if the network is small enough to use the RIP protocol, it is best to stay on the RIP protocol and then switch to EIGRP.

The benefits of OSPF over RIP: much more scalable; supports VLSM and CIDR (unlike RIPv1); overall, it consumes fewer network resources on sufficiently resilient networks; provides the choice of the best routes; allows correct prevention of route cycles; characterized by a more useful metric; facilitates the creation of hierarchical projects of networks; provides a quick transition to a steady-state.

Disadvantages of OSPF compared to RIP: does not allow the use of hierarchical projects in conjunction with poorly designed IP structures; is much more complicated than RIP; requires more CPU and RAM resources;

requires more time spent on design and implementation.

Comparison of OSPF with EIGRP

The OSPF and EIGRP protocols are, in many ways, similar. The EIGRP protocol, like OSPF, provides for the formation of a topology table and the search for routes to recipients based on it. In addition, under normal circumstances, the EIGRP protocol, like OSPF, eliminates the possibility of creating route cycles. However, in some conditions, OSPF is more appropriate than EIGRP, and in others, it is more appropriate.

OSPF advantages over EIGRP: facilitates the creation of hierarchical network projects; has a less sophisticated metric than the composite EIGRP metric; not prone to problems associated with the permanent stay of the route in an active state; does not depend on the manufacturer of the specific product.

The disadvantages of OSPF compared to EIGRP: the metric is not as flexible as the composite EIGRP metric; does not provide load distribution along uneven cost routes; does not allow hierarchical projects to be used in conjunction with poorly designed IP structures; requires more CPU and RAM resources; requires more time spent on design and implementation.

Essentials of Static Routing

When assigned a static route by the administrator, the router remembers it in its TM and uses it to forward packets. The static route job command has the following syntax: Rt (config) #ip route prefix mask {ip | int-type int-num} [dist], where prefix, mask P IP address and destination mask, respectively; ip, int-type, int-num P The IP address of the next-hop (hop) port, the type and number of the local interface to which the packet should be sent, which should reach the above destination; dist - administrative distance. Administrative Distance (AB) is an optional parameter that characterizes route reliability. The smaller the AB, the more valid the route. A route with less administrative distance will be where it is listed in the TM.

Configuring static routes

The following steps are required to configure static routes.

1. Identify all recipient networks, their masks, and gateways (the gateway address can be either the local interface of the router or the next-hop address on the way to the desired destination).

2. Enter the global configuration mode.
3. Enter the ip route command with the appropriate parameters, as shown above.
4. Repeat step three for all recipient networks to which the static route should be specified.
5. Exit Global configuration mode.
6. Run the copy running-config startup-config command.

For example, for the network shown in Fig. below static route commands, for example, R2 will be:

R2(config)#ip route 192.168.1.0 255.255.255.0 192.168.4.1,

R2(config)#ip route 192.168.3.0 255.255.255.0 192.168.4.6,

(the R2 router knows static routes to all other networks 192.168.2.0/24, 192.168.4.0/30, 192.168.4.4/30 because they are directly connected to it). The commands above indicate the IP addresses of the next hop on the path to the recipients. If you specify the source interfaces, the static path command commands will look like this:

R2(config)#ip route 192.168.1.0 255.255.255.0 s0/1,

R2(config)#ip route 192.168.3.0 255.255.255.0 s0/0.

Note that the data and the two previous commands, in this case, are equivalent. The only difference between them is that there will be different values of AB. By default, when using the next junction address, AB = 1, and the source interface - AB = 0.

Generally, AB values are integers ranging from 0 to 255. If you need to enter a non-standard administrative distance (for example, which is 140), then the command should be given

R3 (config) #ip route 192.168.1.0 255.255.255.0

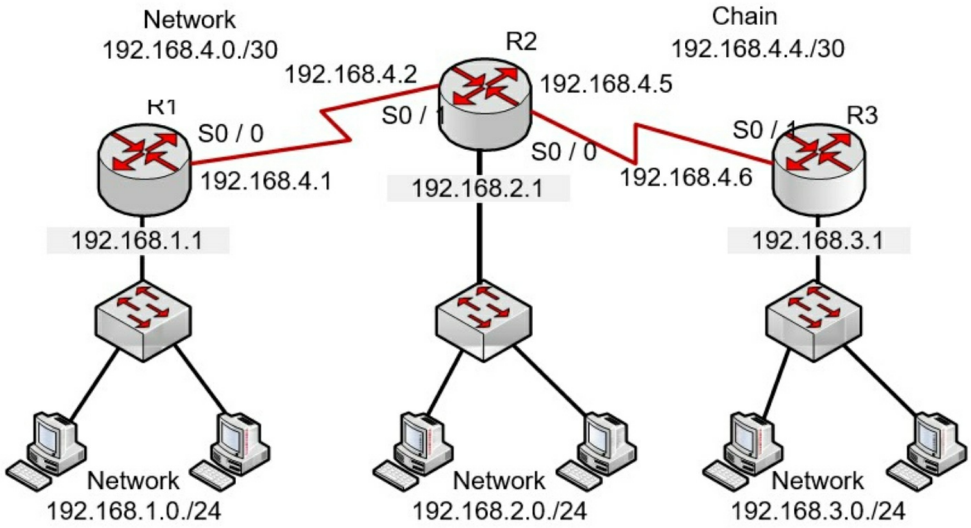
192.168.4.5 140

If for some reason, the router cannot use the source interface specified in the route, this route will not be used, i.e., it will not be stored in the TM.

Sometimes static routes are used as backup routes, which will only be used if dynamic route data cannot be sent. In this case, the AB should be greater than that of the route obtained by the dynamic routing protocol.

Note that on router R1, the paths to 192.168.2.0/24, 192.168.3.0/24 and

192.168.4.4/30 networks should be similarly specified, and R3 to 192.168.1.0/24, 192.168.2.0/24 and 192.168.4.0/30. However, instead of prescribing these three paths, only one default route can be specified on R1 and R3 routers.



A simple computer network

Set a Default Route

The default routes (or standard routes) are used by routers when the packet destination network address does not match any TM route. Standard routes are, as a rule, configured to transmit data streams over the Internet since it is not rational, and there is no need to support all routes to all Internet networks. Thus, standard routes allow to reduce the number of records in the TM and to reduce the time of their processing.

You can specify a standard route using the command ip route 0.0.0.0 0.0.0.0 {ip | int-type int-num}.

An operation of logical "AND" over the 0.0.0.0 mask and packet IP address always results in a 0.0.0.0 network. If the packet in TM does not match the receiving network - it is sent to the network 0.0.0.0.

So, going back to the previous example (see Figure 9.5), the default route command for R1 will be

R1 (config) # ip route 0.0.0.0 0.0.0.0 s0 / 0,

and for R3: R3 (config) # ip route 0.0.0.0 0.0.0.0 s0 / 1.

Checking and Fixing Static Route Configuration Errors

Once the static routes are configured, you should make sure that they are in the TM, and the packet forwarding is done correctly. You can use the show running-config and show ip route commands to do this. The first command allows you to view static routes in the router's work configuration file and the second one in its router. However, if a route is entered incorrectly, it should be deleted, and the correct route entered instead.

The following steps are suggested to find and eliminate static route configuration errors.

1. Ensure that the channel to be used as the gateway is accessible.
2. Execute the show interfaces command and verify the interface and channel protocol activity.
3. Check that the IP address is correct on the interface.
4. Run the ping command for the IP address of the remote router directly connected to the routing gateway. If the result of this command is negative, then the problem is not related to routing.
5. If the command does not work on the remote router, - you must execute the traceroute - command to determine the node where the packet is lost.
6. Connect to a router that did not work on the route and perform the steps described in step one.
7. If the ping command worked at the far end of the route, - the test could be considered successful and completed.

Chapter Five: RIP Remote Vector Protocol

Building a Routing Table

The Routing Information Protocol (RIP) was originally identified in RFC 1058 in 1988. The most important are its characteristics:

- RIP is a remote vector routing protocol.
- The number of conversions (or hop) is used as a metric when choosing a route.
- if the number of conversions is more than 15, the package is discarded
- The standard routing updates are broadcast every 30 seconds.

The RIP protocol has evolved significantly: from a class-based protocol of the first version (RIPv1) to a classless protocol of the second version (RIPv2). Improvements to the latter are as follows:

- The ability to carry additional routing information packages.
- An authentication mechanism for secure TM updates.
- Support for variable-length masks.

RIP prevents routing loops from occurring through which packets can circulate indefinitely, setting the maximum number of route crossings between the sender and receiver. The standard maximum number of conversions is 15. When a router receives a route update that contains a new or changed entry, it increases the metric value by one. If the metric value exceeds 15, then the receiving network is considered unreachable. RIP has several features common to it and other routing protocols. For example, it allows the use of horizon splitting mechanisms and retention timers to prevent the dissemination of incorrect route knowledge.

Consider the process of building a routing table using the RIPv1 protocol on the example of the network shown in Fig. below.

Step 1 - Create minimum routing tables

This network contains eight IP networks connected by four routers with IDs: M1, M2, M3, and M4. RIP routers may have IDs, but they are not required for the protocol to work. These identifiers are not transmitted in RIP messages.

In the initial state, each router automatically creates a minimum routing table with TCP / IP stack software, which takes into account only directly connected networks.

The table below allows us to estimate the approximate appearance of the minimum TM of the M1 router.

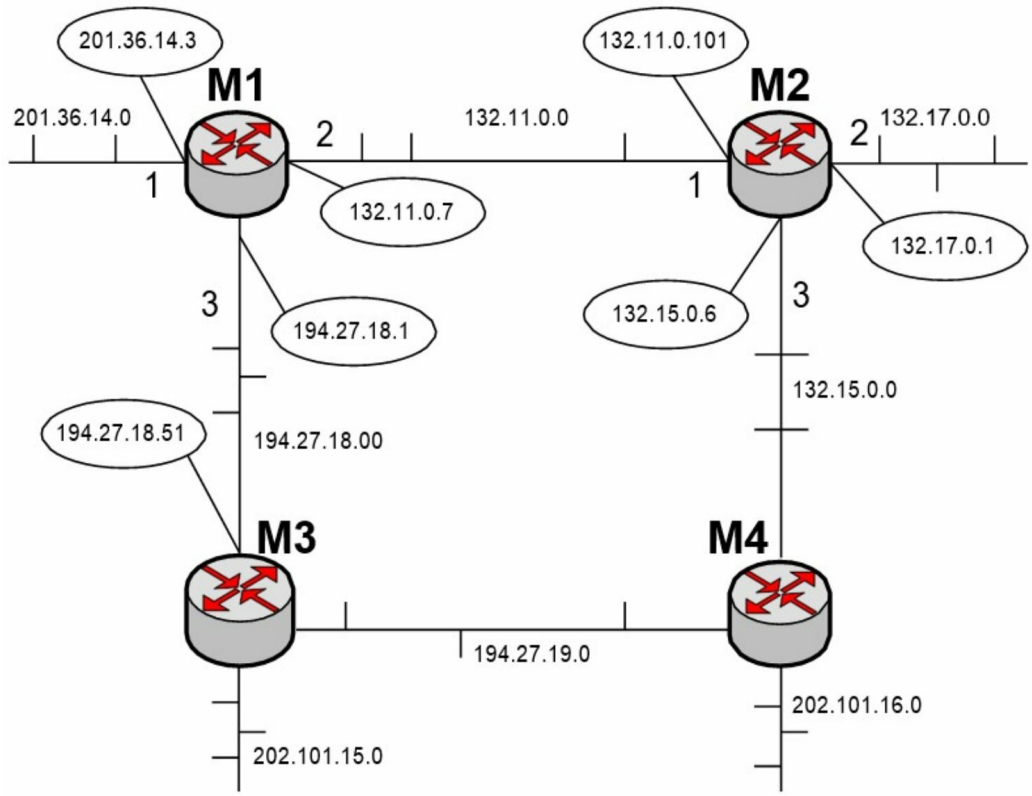
Minimum router's routing table M1

Telephone network	Address of the next router	Port	Distance
201.36.14.0	201.36.14.3	1	1
132.11.0.0	132.11.0.7	2	1
194.27.18.0	194.27.18.1	3	1

Minimum TMs of other routers will look accordingly.

Step 2 - Distribution of minimum tables to neighbors

After the initialization of each router, it starts sending to its neighbors RIP messages containing its minimum TM. RIP messages are sent in UDP packets and content for each network: its IP address and the distance to it from the router that sends the message. Neighbors are routers to which this router can send an IP packet without using the services of intermediate routers. The M1 router sends messages to M2 and M3: network 201.36.14.0, distance 1; network 132.11.0.0, distance 1; network 194.27.18.0, distance 1.



Network combined RIP-routers

Step 3 - Receive RIP messages from neighbors and process the received information

After receiving similar messages from the M2 and M3 routes, the M1 router extends each metric field received per unit and remembers through which port and from which router this information is received (the address of this router will be the next-hop address if this entry is entered into the TM). Then the router starts comparing the new information with the one stored in its TM (Table below).

Routing table router M1

Telephone network	Address of the next router	Port	Distance
201.36.14.0	201.36.14.3	1	1
132.11.0.0	132.11.0.7	2	1
194.27.18.0	194.27.18.1	3	1
132.17.0.0	132.11.0.101	2	2
132.15.0.0	132.11.0.101	2	2

194.27.19.0	194.27.18.51	3	2
202.101.15.0	194.27.18.51	3	2
~~132.11.0.0~~	~~132.11.0.101~~	~~2~~	~~2~~
~~194.27.10.0~~	~~194.27.10.51~~	~~3~~	~~2~~

Records 4 - 9 are from neighboring routers and claim to be logged into the TM. However, only records from 4 - 7 fall into it, since the last two - contain data on existing M1 tables in the grid, and the distance to them is greater than in existing records.

RIP replaces a record on any network only if the new information has a better metric than the existing one. As a result, TM has only one entry for each network. If there are several equivalents by metric of paths to the same network, then TM remains one entry, which came first. There is an exception to this rule - if the worst information about any network came from the same router based on which the record was created, it replaces the better one.

Other routers perform similar operations with new information.

Step 4 - Mailing a new table to neighbors

Each router sends a new RIP message to all its neighbors. In this message, he posts information about all the networks he knows, both directly and remotely.

Step 5 - Receive RIP messages from neighbors and process received information

Step 5 actually repeats Step 3. Consider how the M1 router does (Table below).

Routing table router M1

Telephone network	Address of the next router	Port	Distance
201.36.14.0	201.36.14.3	1	1
132.11.0.0	132.11.0.7	2	1
194.27.18.0	194.27.18.1	3	1
132.17.0.0	132.11.0.101	2	2
132.15.0.0	132.11.0.101	2	2

~~132.15.0.0~~	~~194.27.10.51~~	~~3~~	~~3~~
194.27.19.0	194.27.18.51	3	2
~~194.27.19.0~~	~~132.11.0.101~~	~~2~~	~~3~~
~~202.101.15.0~~	~~194.27.18.51~~	~~3~~	~~2~~
202.101.16.0	132.11.0.101	2	3
~~202.101.16.0~~	~~194.27.10.51~~	~~3~~	~~3~~

At this stage, the M1 router received information from the M3 network about 132.15.0.0, which is, in turn, received from the M4 in the previous work cycle. The router already knows about the 132.15.0.0 network, and the old information has a better metric than the new one, so this new information is dropped.

For the first time, the M1 router learns about network 202.101.16.0, with data from two neighbors - M3 and M4. Since the metrics in these messages are the same, the data that came first comes in the TM. In our example, the routing is torus M2 was ahead of M3 and was the first to send RIP messages to M1.

If the routers periodically repeat the steps of sending and processing RIP messages, then the correct routing mode is set in the network for a certain period when all the networks will be accessible from any network by some rational route. Packages will reach recipients and not loop in loops.

RIP Counterfeit Methods

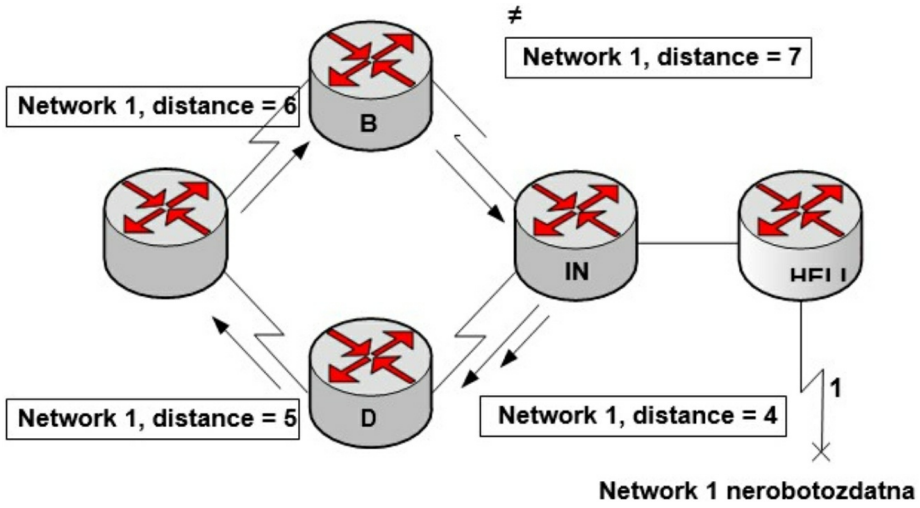
The main methods of counterfeit RIP are the splitting of the horizon, deleting the route in the opposite direction, instant updates, timers of information retention .. Routing loops can occur if the routing protocol is characterized by slow convergence after changes in the network or the network topology in the routers has a mismatch between the TM records. In the next Fig showing routing notches. Their occurrence is as follows.

1. Before network failure 1, all routers have a consistent and correct TM. In this case, they say that the network has converged. By the end of this example, it is assumed that for router B, the best route to network 1 passes through router B, and the distance (metric) from router B to network 1 is 3.
2. If network 1 fails, router D sends a message when router A is upgraded. Upon receiving the router, A stops sending packets to

network 1. However, routers B, C, and D continue because they are not yet aware of network failure 1. When router A sends an update message, m routers B and D stop sending packets to network 1. However, at this time, router B has not yet received an update message. For him, the network, as before, is considered accessible through router B.

3. Suppose that router B sends periodic updates to routers D, pointing the route to network 1 through router B. Router D changes its TM to account for such incorrect information and sends this information to the router. A, which sends it to routers B and D, etc. Now any packet destined for network 1 moves in a circular route (loop) from router B to router B, then to A and D, and again to Mar. - the screwdriver B.

Incorrect information about network 1 continues to circulate around the ring route until any other process stops. In this state of the network, called count to infinity, packets continue to move continuously over the network, despite the failure of the recipient network. And as long as the router increases the number of transitions (potentially to infinity), incorrect information allows the loop to exist (Next Fig.).

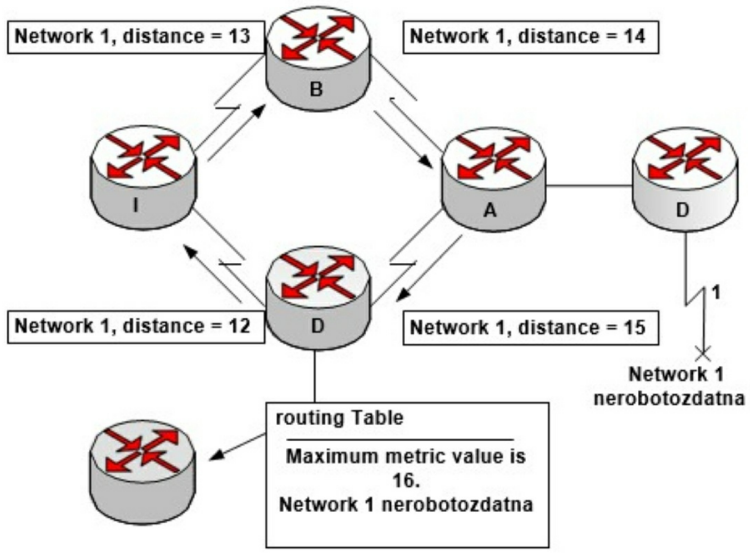


Loop

Unless certain steps are taken to stop this process, the distance vector or the metric displaying the number of conversions will increase each time the packet passes through the next router. Thus, packets move in a circle because the TM contains incorrect information.

Remotely vector routing algorithms can self-correct; however, special steps

are required to eliminate routing loops and looping problems. To avoid the problem of a cyclical metric, infinity is defined as some finite number. For RIP, the number is 16. Now, the routing protocol allows loops to exist only until the metric exceeds 16. The Fig below shows that the metric reached sixteen; since the distance vector has exceeded the standard maximum of 15 transit transitions, the packet is discarded by the router. In any case, when the metric value exceeds the maximum allowable, network 1 is considered unreachable.



Setting a maximum metric

Now let's see what happens to other IP packets that are not routing protocol messages when a loop occurs. It is clear that packets will be transmitted from one router to the other. The IP protocol has its own mechanism for preventing the endless circulation of packets in a circle - the TTL (Time-to-Live - packet lifetime) field. Before a node transmits the IP packet in this field, a value between 1 and 255 can be written according to the standard. When such a packet arrives at the router, the device reduces the value in the TTL field by one. When the TTL value reaches zero, the routers are obliged to reject the IP packet and send the corresponding ICMP informational message to the sender. This mechanism eliminates the possibility of endless circulation of IP packets on the network and helps to solve the problem of ring routes.

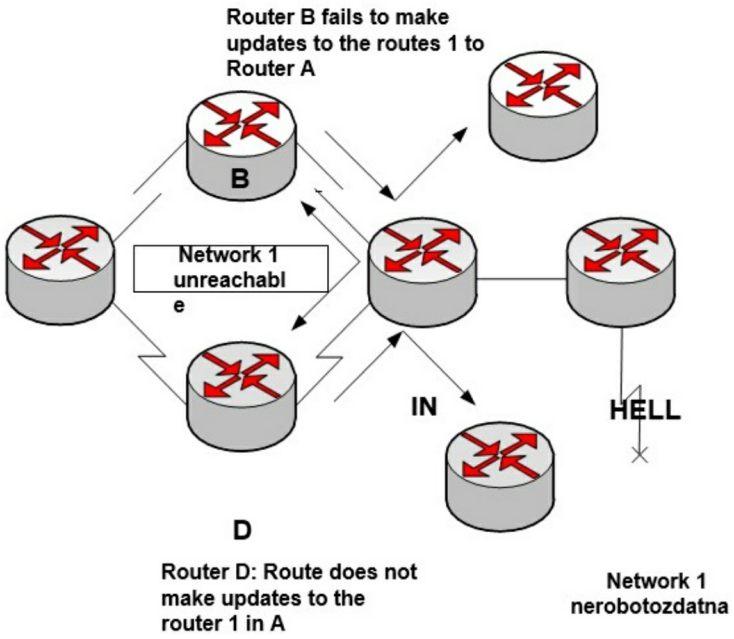
The second possible source of a loop in routing arises when information is sent to the router that contradicts the correct one it initially disseminated. As

shown in Fig. below, the following process occurs, which creates the problem of the routing loop.

1. Router A sends routers B and D with an update indicating that network 1 is down.
2. However, router B transmits to router B another message indicating that network 1 is accessible through the router at a distance of four junctions. This action does not violate the rules of splitting the horizon.
3. After receiving the last message, router B incorrectly concludes that router B still has a valid route to network 1. Router B sends an update message to router A, notifying it of a new route to network 1.
4. Upon receiving it, device A concludes that it can send information to network 1 via router B. Router B decides that it can send information to network 1 via router D. In this situation, any the packet will move in a circular route between these routers.

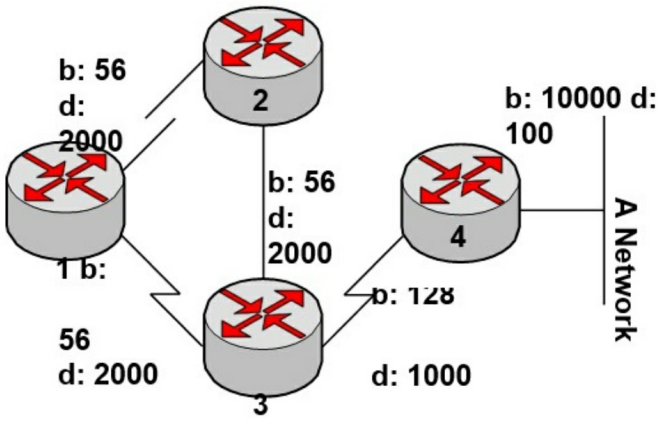
The split horizon tries to prevent this from happening. According to this method, when a route update message for network 1 is received from router A, routers B and D cannot send information about network 1 in the opposite direction, that is, router A, as shown in the next Fig. In this way, splitting the horizon prevents the dissemination of incorrect routing information and reduces the volume of service messages transmitted.

Route poisoning is utilized by various DVPs to prevent large routing loops from occurring and providing explicit route information when the network is unreachable. Such route deletion is usually done by setting the number of conversions per unit greater than the maximum value. This mechanism is an alternative way of preventing routing loops. This approach can be formulated as follows: after receiving information about a route through any interface, it is necessary to declare it inaccessible through the same interface. It is better to tell the router explicitly that the route should be ignored rather than left uncontrolled.



Splitting horizon

Suppose that on all the routers In Fig. below, the route ejection mechanism is activated. After receiving information about router 1 about the network and from router 2, device 1 declares network A inaccessible through its channels to routers 2 and 3. If router 3 has any route to network A through router 1, it deletes that route because it has received an unavailable network message.

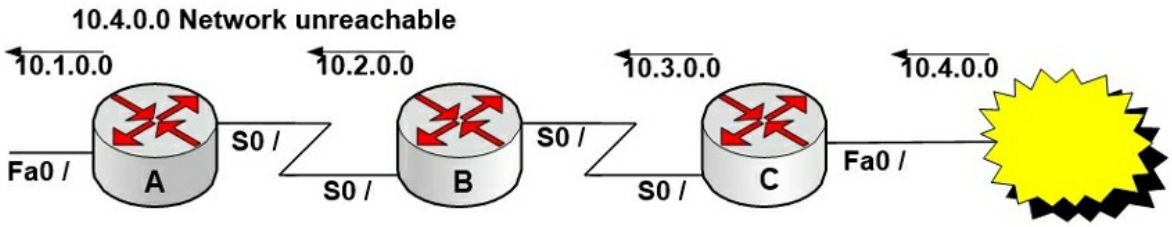


Removal of the route in the opposite direction

New copies of the TM are usually sent regularly to neighboring routers. The protocol sends an update every 30 seconds. However, triggered updates are sent immediately in response to any change in the TM. A router that has detected a change in the topology immediately sends updates to adjacent routers. Those routers, in turn, also generate instant updates, notifying their

neighbors of changes. When any route fails, a message is sent without waiting for the update timer to expire. The use of instant updates in combination with route deletion mechanisms ensures that all routers will be notified of route failure before the end of any storage timer.

An instant update is thus an announcement that is sent before the update timer expires. The router also immediately sends an update message to all its other interfaces without waiting for the timer to expire. This principle of operation leads to the distribution of updated information on the status of the route and resets the timers on neighboring routers. This wave of updates is transmitted throughout the network. The principle of the described mailing is illustrated in the following Fig.



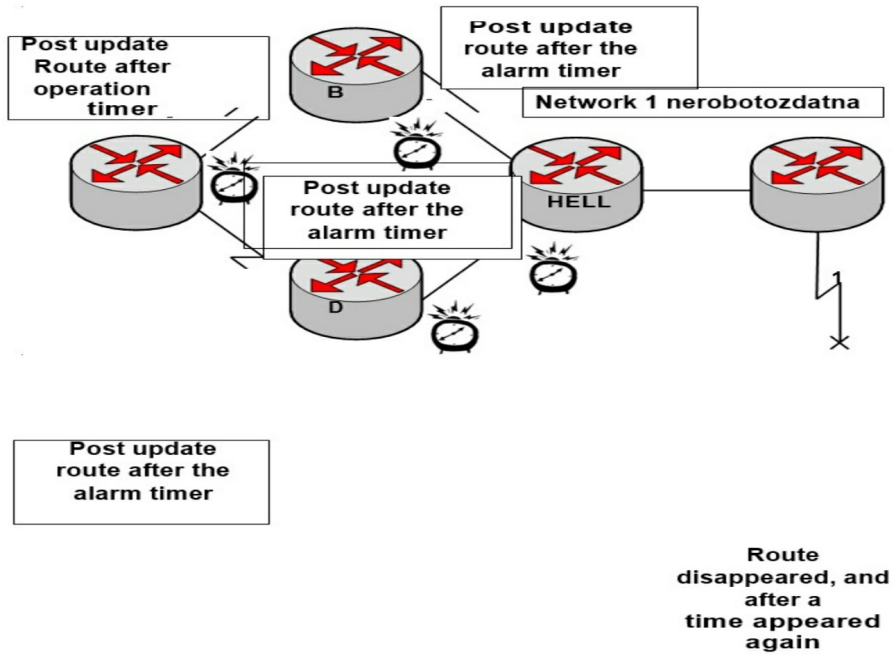
Instant update

Router B generates an instant update, reporting that the 10.4.0.0 network is unreachable. Upon receipt of this information, Router B notifies other routers about the failure of the 10.4.0.0 network through the S0 / 1 interface. In turn, Router A sends this update message via the Fa0 / 0 interface.

The looping can be avoided by using hold-down timers. The sequence of actions is thus:

1. When a router receives a route update from a nearby device that indicates that a previously available network is not working, it routes that route as unavailable and starts a timer.
2. If, by the end of the timer, a new message is received from the same adjacent device that the failed network is again available, the router notices the network as accessible and disables the information hold timer.
3. If the new update comes from another neighboring router, and the metric specified in it is better than the one previously registered for the network, the router notices the network as accessible and disables the timer.

If, by the end of the timer, the hold of information from another neighboring router receives a new update and the metric specified for it, the network is worse than the registered one, and the update message is ignored. In such a situation, ignoring update messages gives more time to disseminate information about network topology changes across the network, as shown in Fig. below.



Timers maintenance information

Configuring RIP

You must first enter the RIP configuration mode using the router rip command (you can stop the RIP protocol by deleting its configuration using the no router rip command). Next, use the Rt (config-router) #network ip-directly- connected-classful-net command to specify the class of networks that are directly connected to this router and should be announced. It allows you to send and receive RIP updates for interfaces belonging to these networks, as well as network data in RIP messages.

Note that when multiple subnets of the same class are directly connected to the router, it is sufficient to specify only one of these class networks. If you specify a subnet, the IOS automatically converts it to a full address (for example, if you specify the network 192.168.1.64 command - the router will accept it as network 192.168.1.0)

Examples of such settings for the R1 - R3 routers shown below.

R1(config)# router rip

R1(config-router)# network 192.168.1.0

R1(config-router)# network 192.168.4.0

R2(config)# router rip

R2(config-router)# network 192.168.2.0

R2(config-router)# network 192.168.4.0

R3(config)# router rip

R3(config-router)# network 192.168.3.0

R3(config-router)# network 192.168.4.0

Note that router rip and network commands are required to configure the protocol.

By default, the software receives RIPv1 and RIPv2 packets and sends only RIPv1 packets. As is known, the RIPv1 protocol does not support VLSM technology, and if the network uses variable-length masks, this protocol will not work properly, so in this case, RIPv2 should be used.

To configure the router to send and receive packets of only one version of RIP, use the following commands: Router (config-router) # version {1 | 2} - specifies IOS to send only packets of RIPv1 or RIPv2.

Router (config-router) # ip rip send version XX - configures the interface to send RIP packets of a particular version (XX can be set to "1" or "2" or "1 2", in the latter case packets are accepted 1 or 2). Configuring the interface to receive RIP packets of a particular version is similar. The corresponding configuration command has the syntax R1 (config-router) # ip rip receive version XX. The use of RIPv2 should be indicated.

After executing these commands, you can view the TM on the routers using the show ip route command. For router R1, TM looks like:

C 192.168.1.0/24 is directly connected, FastEthernet0 / 0

R 192.168.2.0/24 . via 192.168.4.2, 00:00:21, Serial0 / 0

R 192.168.3.0/24 . via 192.168.4.2, 00:00:21, Serial0 / 0 192.168.4.0/30 is subnetted, 2 subnets

C 192.168.4.0 is directly connected, Serial0 / 0

R 192.168.4.4 . via 192.168.4.2, 00:00:21, Serial0 / 0

For the R2 Router, TM is:

R 192.168.1.0/24 . via 192.168.4.1, 00:00:05, Serial0 / 1

C 192.168.2.0/24 is directly connected, FastEthernet0 / 0

R 192.168.3.0/24 . via 192.168.4.6, 00:00:00, Serial0 / 0 192.168.4.0/30 is subnetted, 2 subnets

C 192.168.4.0 is directly connected, Serial0 / 1

C 192.168.4.4 is directly connected, Serial0 / 0

For the R3 TM Router is as follows:

R 192.168.1.0/24 . via 192.168.4.5, 00:00:27, Serial0 / 1

R 192.168.2.0/24 . via 192.168.4.5, 00:00:27, Serial0 / 1

C 192.168.3.0/24 is directly connected, FastEthernet0 / 0 192.168.4.0/30 is subnetted, 2 subnets

R 192.168.4.0 . via 192.168.4.5, 00:00:27, Serial0 / 1

C 192.168.4.4 is directly connected, Serial0 / 1

The first column of the TM contains characters that indicate the source of the route. C - indicates that it is directly connected to this router (this entry appears in the TM as a result of configuring a specific router port) and R - that this route is derived from RIP.

Consider the components of routes in TM, for example, the third row of the routing table of router R1 R 192.168.3.0/24. via 192.168.4.2, 00:00:21, Serial0 / 0

Here 192.168.3.0/24 is the destination network address with its mask; - Administrative distance and after slash of route metric; 192.168.4.2 P IP address of the port of the adjacent device through which the given string is received; 00:00:21 - elapsed time of receipt of this route (21 seconds elapsed, next update should occur in 9 seconds); Serial0 / 0 is the type and local port number of the router to which the packet should be sent to reach the destination specified above.

Auto Summarization of Routes

Consider the case where the above RIP configuration commands will not cause the network to work properly. Yes, if there are subnets in a composite network that belong to the same class network but are connected to different routers, the routing tables to those subnets will be incorrect. For example, if the network shown In Fig.1 to split 192.168.1.0/24 into two subnets 192.168.1.0/25 and 192.168.1.128/25, the first of which will be connected to the Fa0 / 0 port of router R1, and the second - Fa0 / 0 of router R3 will occur problem.

R1 and R3 routers will automatically summarize subnets into a class network that contains subnet data (summarization is performed on a router boundary for these subnets, that is, a router that has one or more subnets in the network of a particular class, and connects to another part of the network via a network not belonging to the class above) and informs the router R2 that they have a direct connection to the network 192.168.1.0/24. The R2 router will then consider that there are two optimal paths to 192.168.1.0/24. The TM router R2 will look like:

R 192.168.1.0/24 . via 192.168.4.1, 00:00:11, Serial0 / 1 . via 192.168.4.6, 00:00:23, Serial0 / 0

C 192.168.2.0/24 is directly connected, FastEthernet0 / 0 192.168.4.0/30 is subnetted, 2 subnets

C 192.168.4.0 is directly connected, Serial0 / 1

C 192.168.4.4 is directly connected, Serial0 / 0

The TM for R1 will be this

192.168.1.0/25 is subnetted, 1 subnets

C 192.168.1.0 is directly connected, FastEthernet0 / 0

R 192.168.2.0/24 . via 192.168.4.2, 00:00:25, Serial0 / 0 192.168.4.0/30 is subnetted, 2 subnets

C 192.168.4.0 is directly connected, Serial0 / 0

R 192.168.4.4 . via 192.168.4.2, 00:00:25, Serial0 / 0

The TM for R3 will be this

192.168.1.0/25 is subnetted, 1 subnets

C 192.168.1.128 is directly connected, FastEthernet0 / 0

R 192.168.2.0/24 . via 192.168.4.5, 00:00:24, Serial0 / 1 192.168.4.0/30 is subnetted, 2 subnets

R 192.168.4.0 . via 192.168.4.5, 00:00:24, Serial0 / 1

C 192.168.4.4 is directly connected, Serial0 / 1

As a result, routing on such a network will be incorrect. For example, if any node of the 192.168.1.0/25 or 192.168.1.128/25 packets is being routed from the router R2, the load balancing will be transmitted in a cyclic (alternate) way via the S0 / 0 and S0 / 1 interfaces. In addition, router R1 does not host a route to network 192.168.1.128/25, and R3 does not route to network 192.168.1.0/25. Obviously, this situation is unacceptable.

To resolve this situation, automatic routing of routes should be canceled on each router using the no auto-summary command in RIP configuration mode. After that, the TM routers take the form for R1:

192.168.1.0/25 is subnetted, 2 subnets

C 192.168.1.0 is directly connected, FastEthernet0 / 0

R 192.168.1.128. via 192.168.4.2, 00:00:02, Serial0 / 0

R 192.168.2.0/24. via 192.168.4.2, 00:00:02, Serial0 / 0 192.168.4.0/30 is subnetted, 2 subnets

C 192.168.4.0 is directly connected, Serial0 / 0

R 192.168.4.4 . via 192.168.4.2, 00:00:02, Serial0 / 0.

for R2:

192.168.1.0/25 is subnetted, 2 subnets

R 192.168.1.0. via 192.168.4.1, 00:00:06, Serial0 / 1

R 192.168.1.128. via 192.168.4.6, 00:00:01, Serial0 / 0

C 192.168.2.0/24 is directly connected, FastEthernet0/0 192.168.4.0/30 is subnetted, 2 subnets

C 192.168.4.0 is directly connected, Serial0 / 1

C 192.168.4.4 is directly connected, Serial0 / 0.

for R3:

192.168.1.0/25 is subnetted, 2 subnets

R 192.168.1.0. via 192.168.4.1, 00:00:06, Serial0 / 1

R 192.168.1.128. via 192.168.4.6, 00:00:01, Serial0 / 0

C 192.168.2.0/24 is directly connected, FastEthernet0/0 192.168.4.0/30 is subnetted, 2 subnets

C 192.168.4.0 is directly connected, Serial0 / 1

C 192.168.4.4 is directly connected, Serial0 / 0.

Disable Route Updates

Another problem is the unwanted sending of updates from some interfaces. The fact is that when using the network command, RIP sends route information to the network specified in this command from all interfaces in the address range of that network. You can use the passive-interface command to disable sending (but not receiving) such updates from individual interfaces. Yes, coming back to our network (see Figure 1), we see that sending RIP updates is inappropriate in the fa0 / 0 ports of R1 - R3 routers since no other routers but only workstations are connected to the respective networks. In addition to the inappropriateness of such updates, they will also generate unnecessary service traffic, which reduces network bandwidth and allows attackers to analyze these updates. So on the R1 - R3 routers, you should type # passive-interface fa0 / 0 Router (config-router).

Application of the ip classless command

Sometimes the router receives packets intended for an unknown subnet of some network that is connected to the device's directly connected networks. For best forwarding, these packets use the ip classless global configuration command. When this feature is off, and the packet is sent to a subnet of a network that does not have a standard route, the packet is dropped by the router.

The ip classless command does not affect the TM, only the packet forwarding operation. If the router receives a packet with an unknown destination address that is on an unknown subnet of the connected network, then it is assumed that such a subnet does not exist. Therefore, the router rejects the packet even if there is a standard route. Running the ip classless - command

solves this problem by specifying a class-based network boundary router in its TM and simply selecting the standard route.

Recall that when receiving information about a network, RIPs rely on neighboring routers. RIP protocols, like any DVP, have problems that cause slow convergence. To avoid routing loops and packet looping, RIP uses: Split horizon; exclusion of routes in the reverse direction (Poison reverse); hold down counters; Triggered updates. Some of these methods require additional configuration, and some do not. In some cases, it is necessary to disable the splitting mechanism of the horizon. This shutdown is done using the Router (config-if) #no ip split-horizon tool.

Setting Timer Values

Another mechanism that may need to be modified is the use of the retention timer. Such a timer prevents packet loops but increases network convergence time. Holddown counters are standard for 180 seconds. During this time, internal routes will not be updated; however, no valid alternative routes will be installed. Holddown counters can be shortened to speed up convergence. Ideally, setting this retention period is a little longer than the maximum route refresh time on this integrated network.

To change the retention timer, use the Rt (config-router) #timers basic update invalid holddown flush. command, where the update innovations update timer (standard 30 seconds) - specifies the route of updates; invalid route validity timer (standard 180 seconds) - specifies the length of time the router waits before announcing this route in the absence of announcements to update a route. The route will be stored in the TM until the flush route reset timer has expired; holddown - hold-down timer (standard 180 seconds) specifies the time during which new routing update messages are ignored; flush ski route reset timer - specifies the time that elapses before the route is removed from the TM (240 seconds default).

An additional parameter that affects the time of convergence and is configurable is the interval of sending updates of routes (the default every 30 seconds). This time can be increased (to save bandwidth) or reduced (to reduce convergence time) with the command

Router (config-router) # update-timer seconds.

Set the number of parallel routes

When configuring RIP, you can set the number of parallel routes. For most dynamic routing protocols, up to four such routes are set as standard (there can be six static routes). You can use the command to change the standard number of parallel routes

Router (config-router) # maximum-paths ..

Announcement of static and standard routes

RIP does not announce the static routes specified on some default interface. If a static route is assigned to an interface not specified in the network command, no routing protocol announces such a route. Announcements can be made using the redistribute static command.

Standard routes (default routes), RIP protocol default, is also not announced. If such routes are to be included in RIP announcements, the default-information originate command should be executed on the router where the default route is specified.

Testing and Debugging RIP

There are many commands for testing the RIP protocol. Let's look at some of them. The show ip protocols command displays information about all the IP routing protocols that are configured on the router. First of all, check that: RIP is enabled on the required interfaces; whether or not RIP routing updates are received and transmitted by the appropriate interfaces; whether the correct version of the RIP routing updates is used, whether the router announces the required networks.

The show ip route - command shows TM and allows you to see if routes received by the RIP protocol are indicated there (indicated by "R"). Such TM entries are delayed by convergence.

The show interface - command displays information about a specific interface (including its activity and protocol type). The show ip interface command displays information about the IP protocol that is specific to the interface. The show running-config - command allows you to check your RIP settings by analyzing a working configuration file. The show ip rip database - command displays a private RIP database.

Note that most errors in RIP are due to executing incorrect network commands, network breaks, or splitting the horizon. An important tool for finding errors related to RIP updates is the debug ip rip command, as it

executes RIP routing updates.

Chapter Six: Advanced EIGRP Routing Protocol

EIGRP Protocol Overview

The Enhanced Interior Gateway Routing Protocol (EIGRPP) was developed and implemented by Cisco in 1992. It is a significant improvement on its predecessor, the IGRP routing protocol, which is not actually used today. Therefore, the IGRP protocol is not considered in this guide, and the focus is on the EGRP protocol.

Advantages of Using EIGRPP

The advantages of the EIGRPP relatively simple remote vector protocols are :

- fast convergence. Convergence is much faster on EIGRPP routers because it is based on a modern DUAL routing diffusion algorithm (Diffusing Update Algorithm). This algorithm guarantees the absence of loops at all times throughout the route and allows all routers belonging to this topology to perform simultaneous synchronization. In addition, if in traditional remote vector protocols, a particular route becomes inaccessible, routers should wait for the next periodic update, and EIGRP will use the backup path (if any).
- Effective use of the bandwidth. First, the EIGRPP uses partial, bounded updates routing, and as a consequence, minimizes the use of such bandwidth updates in a stable network environment. As a rule, EIGRP routers send partial, incremental routing updates, rather than complete routing tables. This process is similar to OSPF, but in contrast, EIGRP routers send these partial updates to not all routers in the area, but only to those who really need them. That is why such updates are called limited. Secondly, in the EIGRPP protocol, instead of sending regular routing updates, routers keep in touch with each other by sending small greetings. Although greetings are sent regularly, due to their small size, they make little use of the bandwidth (unlike the RIP and IGP protocols that send their complete routing table to neighboring devices every 30 or 90 seconds, respectively).
- Support for variable-length VLSM (Variable-Length Subnet Mask) subnet masks and classless interdomain routing of CIRDR

(Glassless Interdomain Routing). Unlike the IGRP protocol, EIGRP provides full class IP support by exchanging subnet masks in route update messages. This allows network designers to make the most of the address space.

- support for multiple network-layer protocols. EIGRP supports IP, IPX, and AppleTalk by using protocol-dependent modules (PDMs).
- Use of complex and flexible route metrics. The EIGP metric, unlike many other routing protocols (except the IGRP protocol), can take into account four indicators at once (bandwidth, delay time, bandwidth, and channel reliability). In doing so, the administrator can set the significance of each of these metrics.

It is worth noting that in some sources, EIGRPP is called a hybrid routing protocol, which combines the best features of remote vector algorithms and channel routing algorithms. For example, EIGRP uses OSPF features such as partial updates of routes and detection of neighboring devices. However, it should be remembered that in technical terms, the EIGRP protocol is purely Fiberboard.

Calculating the EIGRP Metric

The EIGRP protocol uses a 32-bit metric calculated by the formula :

$$M_{EIGRP} = \left(K_1 \cdot \left\lfloor \frac{10^7}{B_w} \right\rfloor \cdot 256 + \frac{K_2 \cdot \left\lfloor \frac{10^7}{B_w} \right\rfloor \cdot 256}{256 - L_d} + K_3 \cdot \frac{D_l}{10} \cdot 256 \right) \cdot \frac{K_5}{R_l + K_4},$$

where Bw is the smallest bandwidth of the channel on the path between the sender and the recipient in Kbps; Dl is the total delay of data channels between the sender and the receiver in us. The delay is determined by the type of connection line (delay values for different types of communication lines are given in Table below); Ld is the maximum channel load between the sender and the recipient; Rl is the lowest reliability of the channel of the route between the sender and the recipient (characterizing how often data transmission errors occur in the channel); K1 - K5 - weighting factors. Know the term ☐ X ☐ , in this case, means ла an integer part of the number X.

Delay value depending on the transmission medium

Environment transfer	Value Delay (ms)	Environment transfer	Value Delay (ms)
Fast Ethernet	100	1544 K	20000
FDDI	100	1024 K	20000
100M ATM	100	512 K	20000
Ethernet	10000	64 K	20000

The values of Bw and Dl are static values, and Ld and Rl - are measured dynamically over 5 minutes (to determine the corresponding averages and avoid the effects of, for example, instantaneous congestion and channel errors).

Reliability values can range from 1 to 255, where 1 - corresponds to the minimum reliability and 255 - to the maximum. Reliability is expressed as a fraction Rl / 255. Yes, 255/255 - means 100% reliability and 250/255 - 98%.

The load value may also be in the range of 1 to 255, where 1 - corresponds to the minimum load and 255 - maximum. Like reality, congestion is also expressed as a fraction of Ld / 255. For example, 51/255 - means a 20% load and 255/255 - that this line is fully loaded.

Note that the default values of the coefficients are: K1 = K3 = 1, K2 = K4 = K5 = 0 and the formula for calculating the metric is:

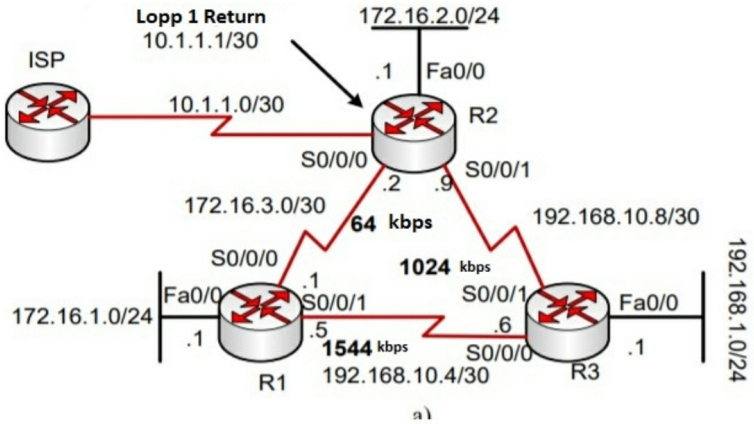
$$M_{EIGRP}^{def} = \left(K_1 \cdot \left\lfloor \frac{10^7}{B_w} \right\rfloor + K_3 \cdot \frac{D_l}{10} \right) \cdot 256.$$

Since the metric in this case only includes static values, frequent top-table table data will not be recalculated.

It should be noted that the maximum number of transitions for the EIGRPP protocol is 224 (for example, for the RIP protocol, the number of transitions is only 16), which is sufficient to support even the largest modern networks.

Consider an example of metric calculation. Let's look at the example of a

small KM and the content of the TM of the router R2 (Fig below). TM contains routes to all known destinations for R2. The letters "C" and "D" in the left positions of the table rows indicate the source of the row. Yes, the letter "C" means directly connected networks and the letter



R2 # show ip route R1 192.168.10.4/30 R3

and)

<Of output omitted>

192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks

D 192.168.10.0/24 is a summary, 00: 00: 9, Null0

D 192.168.10.4/30 via 192.168.10.10, 00: 00: 9, Serial0 / 0/1

C 192.168.10.8/30 is directly connected, Serial0 / 0/1 172.16.0.0/16 is variably subnetted, 4 subnets, masks 3

D 172.16.0.0/16 is a summary, 00: 00: 9, Null0

D 172.16.1.0/24 via 172.16.3.1, 00: 00: 9, Serial0 / 0/0

C 172.16.2.0/24 is directly connected, Fastethernet0 /

0 C 172.16.3.0/30 is directly connected, Serial0 / 0/010.0.0.0/30 is subnetted, 1 subnets

C 10.1.1.0/30 is directly connected, loopback1

D 192.168.1.0/24 via 192.168.10.10, 00: 00: 9, Serial0 / 0/1

"D" - that this string obtained by the protocol EIGRP. Rozhlya- Nemo last

line TM:

D192.168.1.0 / 24 via192.168.10.1000: 00: 09

Serial0 / 0/1.

Here, after the letter "D" is IP address of the destination; cover them in brackets administrative distance (90) and a slash metric route (3014400) IP address of the interface the next node towards point off value (192.168.10.10); how much time there is this line (9 sec.) and a local source interface through which you can reach your destination (Serial0 / 0/1). Calculate the value metric.

To determine the metrics according to (4.2) should determine the lowest bandwidth channel along the route from source to destination and find the total delay. The smallest bandwidth of 1024 kb/s (as the optimal route from R2 to network 192.168.1.0 passes through R3, and channel bandwidth from R2 to R1 is only 64 kb/s). The total path delay is 20000 + 100 = 20100 microseconds (see the above Table). So, given the above, the final desired value will be:

$$M_{EIGRP}^{def} = \left(1 \cdot \left\lfloor \frac{10^7}{1024} \right\rfloor + 1 \cdot \frac{20100}{10}\right) \cdot 256 = (9765 + 2010) \cdot 256 = 3014400.$$

In the following, let us elaborate on the essence of the EIGRP protocol, but first of all, we should familiarize ourselves with its basic terminology.

The Terminology of the EGRP Protocol

The EIGRP protocol uses data from three tables: routing, adjacent devices, and topology. These tables are also called protocol databases. We already know the purpose of TM. Therefore, consider the purpose of the other two tables .

Table of adjacent devices

Each EIGRP router supports a neighbor table listing adjacent routers. For each protocol (for example, IP, IPX) supported by EIGRP, there is a table of adjacent devices (TCP). When new adjacent devices are found, their addresses and interfaces are entered into these tables. You can view the contents of the TSP using the show ip eigrp neighbors command)

When sending a greeting packet, the neighboring device reports a retention

time, indicating how long the router views its neighboring device as reachable and operational. If no greetings have been received from the router during the retention period, the retention time is considered to be exhausted. In this case, the DUAL algorithm (we will discuss this algorithm later) informs of the change in topology and must again calculate the parameters of the new topology.

The TSP has, in particular, the following fields:

- The serial number (H) of the record as the unit is trained with respect to adjacent devices.
- Neighbor Device Address (Neighbor Address) is the network layer address of the adjacent device.
- Interface - The local interface through which a Hello packet was received from a neighboring device.
- Hold Time (Time Hold) is the time interval after which, in the absence of any messages from a neighboring device, the channel is considered inoperable. When any EIGRP packet is received, the timer assumes the initial value.
- Time Available (Uptime) is the time elapsed since the adjoining device was added to the TSP.
- Smooth Round-Trip Timer (SRTT) - The average time it takes to send a packet to a neighboring device and receive the corresponding packet from it. This timer determines the Retransmit Interval (RTI).
- Retransmission Timeout (RTO) is the time in milliseconds during which the software waits for the packet to be retransmitted from the retransmission queue.
- Queue Count - Q Cnt - The number of packets waiting in the queue for transmission. If this value is constantly greater than zero, - the router is likely to overflow. A zero value indicates that there are no EIGRPP packets in the queue.
- Sequence Number - Seq No - is the number of the last packet received from this neighboring device. The EIGRP protocol uses this field to confirm receipt of a packet transmitted to a neighboring device and to identify packets transmitted in violation. TSP ensures reliable and orderly delivery of packages.

For example, the TSP for router R2 (last Figure above) has the form

H Address	Interface	Hold	Uptime	SRTT	RTO	Q	Seq
		(sec)		(ms)		Cnt	Num
1 192.168.10.10	Ser0/0/1	10	00:01:44	20	200	0	7
0 172.16.3.1	Ser0/0/0	10	00:03:27	25	200	0	12

Topological Table

The topology table contains all the EIGRP TMs available on the devices of this standalone system (you can view the contents of the topology table using the show ip eigrp topology command). The DUAL algorithm retrieves information from the TSP and the topological table (TT) and calculates the least-estimated routes to each destination. This allows EIGRP routers to identify alternative routes and use them as needed quickly. The primary successor is recorded in the TM, and its copy is recorded in the TT. All EIGRP routers support TT for each configured network protocol. This table lists routes to all destinations known to the router.

TT has the following fields:

Feasible Distance (FD) is the lowest calculated metric for each destination. The below Example shows the TT for the R2 router from the example shown in the last Fig above. The intended distance, for example, to network 192.168.1.0, is 3014400, as indicated by the entry "FD is 3014400".

R2# show ip eigrp topology

IP-EIGRP Topology Table AS(1)/ID 10.1.1.1

Codes: P - Passive, A - Active, U - Update,

Q - Query, R - Reply, r - Reply Status s - sia Status P 192.168.10.4/30, 1 successors, FD is 3523840 via 192.168.10.10 (3523840/2169856), Serial0/0/1 via 172.16.3.1 (410240000/2169856), Serial0/0/0

P 192.168.1.0/24, 1 successors, FD is 3014400

via 192.168.10.10 (3014400/28160), Serial0/0/1

via 172.16.3.1 (410240000/2172416), Serial0/0/0

P 192.168.10.8/30, 1 successors, FD is 3011840

via connected Serial0/0/1

P 172.16.1.0/24, 1 successors, FD is 3526400

via 192.168.10.10 (3526400/2172416), Serial0/0/1

via 172.16.3.1 (40514560/28160), Serial0/0/0

P 172.16.2.0/24, 1 successors, FD is 28160

via connected FastEthernet 0/0

P 172.16.3.0/30, 1 successors, FD is 40512000

Route Source is the identification number of the router that announced the route. This field is only filled in for routes that are known externally from other EIGRPP networks. In Example 4.1, the sources of the route to the network 192.168.1.0 are 192.168.10.10 and 172.16.3.1, as evidenced by the entries "Via 192.168.10.10" and "Via 172.16.3.1", respectively.

Reported Distance (RD) or Advertised Distance (AD) is the distance that a neighboring router reports to a specific recipient. In Example 4.1, the reported distance to the network 192.168.1.0 is 28160, as indicated by the value of the RD field (3014400/28160).

Interface Information (Interface Information) is an interface number through which you can reach your destination. The example above shows that the 192.168.10.10 network can be reached through the Serial0 / 0/1 interface (via 192.168.10.10 (3014400/28160), Serial0 / 0/1), and can be backed up via Serial0 / 0/0 (via 172.16.3.1 (410240000/2172416), Serial0 / 0/0)

Route Status - can be passive or active. Passive (PASSIVE) are steady and ready-to-use routes; Active (Active) are those for which the DUAL algorithm continues the process of re-calculating the route. EIGRP sorts TT records so that the primary routes are at the top and followed by backup ones. At the bottom of this table are the routes that DUAL considers possible routing loops.

Primary Routes

The primary is called the route selected as the primary one to reach a particular destination. This route is determined by the DUAL algorithm based on the TSP and TT information and is entered into the TM. There may be up to four primary routes per route. They can have both the same and different estimates and are considered the best loop-free routes to this destination.

Backup Routes

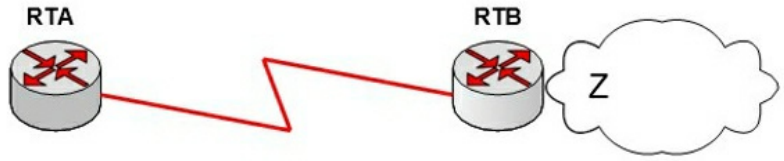
The potential primary (Feasible Successor - FS) is a fallback route. Such routes are established simultaneously with the primary routes; however, they are stored only in the TT. Several backup routes can be stored at a time. The availability of a backup route to reach the recipient is optional.

The router views the devices on the backup route as adjacent to the downstream destination (it considers them to be closer to the destination than it is to itself). They express an estimate of the route to the destination announced by the neighboring router. If the primary route becomes invalid, the router looks for a backup and raises its status to the primary one. The backup route to the destination must have a lower FD value than the RD value of the primary route.

If the backup route has not been established based on available information, the router gives it the status of active (Active) and sends packets of requests to all neighboring devices for topology listing. Once these requests have been answered, the router can set new primary or backup routes based on them. The router then gives the route passive status.

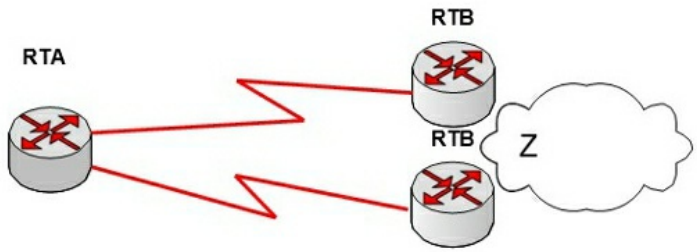
Select Primary and Backup Routes

Consider the issue of determining the router's primary and backup routes. Let the TM of the RTA router have a route to Network Z via the RTB router (Fig below). In terms of the RTA router, the RTB router is on the current primary march RTA sends packets destined for Network Z in the RTB direction. The RTA router must have at least one primary route to Network Z for the DUAL algorithm to enter it into the TM.



Primary route

If some RTC router that is connected to the RTA is similar to the RTB and reports to the RTA that it has a route to Network Z with the same metric as the RTB, then the RTA also considers the RTC as the primary route and DUAL sets the second route to Network Z via RTC (Fig below).



Primary routes EIGRP protocol

Each neighboring RTA device that announces a loop-free route to Network Z (but with an FD greater than the best route metric and smaller than its RD) is identified in the TT as the one on the backup route. The router views its devices on backup routes as adjacent devices in a downward direction, i.e., closer to the recipient than to the recipient. If for any reason, the primary route cannot perform its functions, then the DUAL algorithm can quickly find a backup based on the TT data and set a new route to the destination.

If there is no such backup route, then the DUAL algorithm puts the route into an active state and asks neighbors for help in finding a new loop-free route. Neighboring routers are required to respond to this request. If a nearby router has such a route (s), information about it (s) is sent. Otherwise, the neighboring router reports the absence of a route to this destination.

Excessive route re-routing indicates poor network performance and lower network performance. To prevent convergence problems, the DUAL algorithm always tries to find a fallback route before performing the conversion. If so, the DUAL algorithm can set a new route without listing.

Jams of Active Routes

If one or more of the routers to which the request was sent does not respond within the active time (180 seconds), the route (or multiple routes) is put into a stuck and inactive state. In this case, EIGRP eliminates unresponsive routers from its TSP and logs a "stuck in active" error message for the routes that were active in the system log.

Tagging for Routes

TT may contain additional information about each route. EIGRP classifies routes into internal and external routes. The internal ones are routes inside this autonomous EIGRP system, and external ones are those that originate outside this autonomous system. Routes received or redistributed from other

routing protocols are considered external.

As a tag, the route can be assigned a value from 0 to 255. All external routes are recorded in the TT and assigned a tag containing the following information: the EIGRPP router ID that extended the route to the EIGRP network; Receiver's AC number; the protocol used on the external network; an estimate or metric derived from an external protocol; configured admin tag.

To set a strict and accurate routing policy, it is recommended that you use the route tagging function, and especially the admin tags. The latter can be any number from 0 to 255. In essence, it is a common tag that can be used to implement a special routing strategy. External routes can be accepted, rejected, or distributed based on each of the route tags, including the admin tag. Because the user can set the admin tag in any convenient way, the route tagging feature gives more flexibility when managing the network. This is particularly useful in cases where the EIGRPP network interacts with a policy-based boundary gateway network.

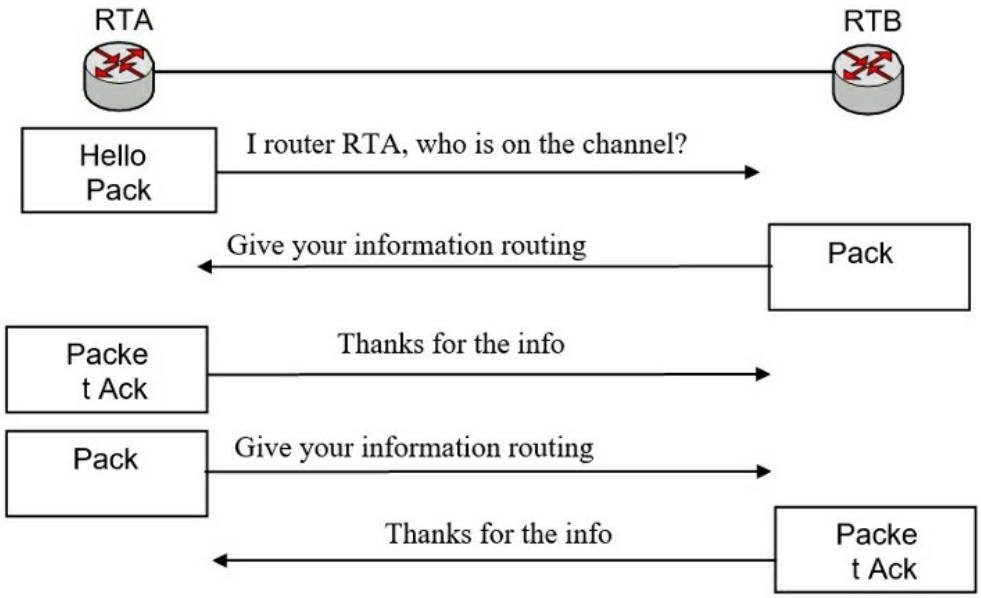
Features and Technologies of the EIGRP Protocol

EIGRPP uses many new technologies, each of which improves operational efficiency, increases convergence speed, and expands the functionality of the IGGRP protocol and other routing protocols. These technologies can be divided into the following four categories.

1. Detect nearby devices and restore lost connectivity.
2. Reliable Transport Protocol. DUAL algorithm of the final states of the machine.
3. Modules of specific protocols.
4. Let's take a closer look at each of these technologies.

Detect nearby devices and restore lost communication

Conventional simple vector remote routers do not communicate with their neighbors. In contrast, EIGRP routers communicate with their neighboring devices. Below Fig illustrates the process of establishing connections between adjacent EIGRPP devices.



Exchange of information neighboring EIGRP routers

EIGRP routers establish contiguity with neighboring routers by sending small greetings. These packets are sent by default every 5 seconds on high bandwidth channels and every 60 seconds on low-speed multipoint channels. The EIGRP router assumes that as long as the packets that are known to it from the neighboring devices are greetings, those devices and the corresponding routes remain valid.

By forming an adjacency relationship, EIGRP routers can: dynamically learn about new routes that appear on the network; identify routers that have become inaccessible or unusable; identify routers that were previously unreachable.

Reliable Transport Protocol

Reliable Transport Protocol (RTP) is a transport layer protocol that can guarantee the orderly delivery of EIGRPP packets to all neighbors. IP protocol networks use the protocol to arrange and deliver packages on time

TCP However, EIGRP is independent of the network protocol used and does not use TCP / IP to exchange routing information (as RIR, IGP, OSPF do). To achieve this independence from IP, EIGRP uses its proprietary transport protocol to guarantee the delivery of information.

EIGRP may activate the RTP protocol to provide a genuine or non-guaranteed delivery service depending on the situation. For example, greetings packages do not require extra load on the network due to

guaranteed delivery, as they are sent frequently, and their size should be small. However, guaranteed delivery of route information can accelerate convergence, since the EIGRP routers do not expect the timer to expire before retransmission. The use of a reliable transport protocol allows the EIGRPP to send multicast and unicast broadcasts for maximum efficiency simultaneously.

The DUAL End State Machine

The main component of the EIGRP protocol is the route calculation algorithm. The full name of this technology is the finite state machine (FSM) of the DUAL algorithm. It defines a set of possible states through which to go, what events cause these states, and what results from those states. The FSM contains all the logical operations required to calculate and compare routes in the EIGRPP network.

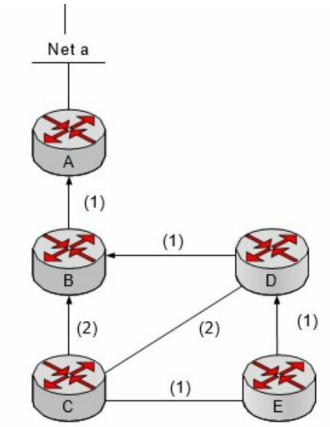
The DUAL algorithm monitors all routes announced by neighboring devices and uses a composite (composite) metric for each route. It ensures that each route does not have loops. After the corresponding calculations, the DUAL algorithm records the routes with the lowest estimates in the TM (that is, the primary routes) and copies them in the TT.

The protocol stores important routing and topological information in TSPs and TTs that provide the DUAL algorithm with routing information in the event of a network disruption using the information in these tables, DUAL can quickly find alternative routes if needed: if any channel becomes inoperative, it looks for an alternative (potentially primary or backup) route to the TT.

Packets sent to the receiving network are immediately sent on the backup route, which at this point, receives the status of primary, as shown in Fig. below. Here, router D loses direct connection to router B and does not have an identified primary route. The estimated FD distance (calculated estimate) for the route from router D to router A is 2, and the announced distance through router C is 3. Since RD is less than the best route metric but greater than FD distance, no back-up route is entered in the TT. Router C has an identified backup route, just like router E, since the route is loop-free, and the distance RD to the next-hop router is less than the FD distance for the primary route. The final result of the DUAL algorithm is shown in the next Fig. The convergence process is described in detail.

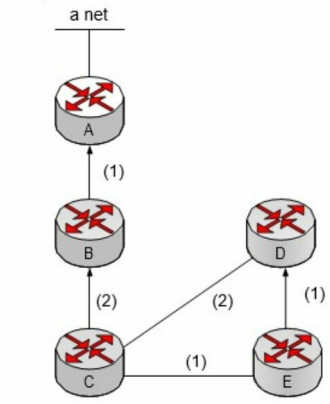
PDM Modules

One of the attractive features of EIGRPP is its modular structure, which provides maximum scalability and adaptability. Support for various network protocols (IP, IPX, AppleTalk) implemented in EIGRP using PDM modules. In fact, EIGRP can be easily adapted to new or modified network protocols (e.g., IPv6) by adding a new PDM module. The following Figure for the next one shows a general diagram of the operation of the PDM module.



C	EIGRP	FD	RD	Topology
a net		3		(FD)
	Because B	3	1	(Successor)
	Because D	4	2	(FS)
	Through E	4	3	
D	EIGRP	FD	RD	Topology
a net		2		(FD)
	Because C	2	1	(Successor)
	Through E	5	3	(Successor)
E	EIGRP	FD	RD	Topology

b)



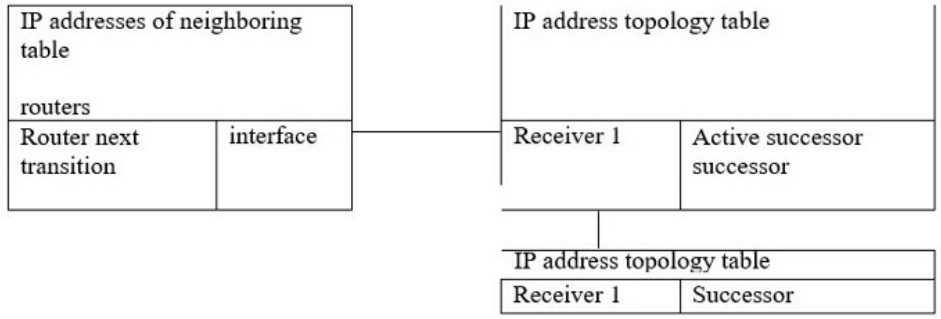
C	EIGRP	FD	RD	Topology
a net		3		(FD)
	Because B	3	1	(Successor)
	Because D			
	Through E			
D	EIGRP	FD	RD	Topology
a net		5		(FD)
	Because C	5	3	(Successor)
	Through E	5	4	(Successor)
E	EIGRP	FD	RD	Topology

An example of the result of the DUAL algorithm: a) network to break the direct connection between the D and B routers; b) the network after such a breach

Each PDM module is responsible for performing all the functions associated with the respective network protocol. In particular, the IP-EIGRPP module is responsible for the following functions:

- Sending and receiving EIGRPP information containing IP protocol data.

- Notification of the DUAL algorithm to receive new information regarding IP routing.
- Support the results of DUAL routing decisions in the IP routing table.
- Further dissemination of route information that has become known to other IP-enabled routing protocols.



EIGRP protocol modules PDM

EIGRPP Package Types

The EIGRP protocol uses several different types of packages to support its various tables and establish complex (complex) connections to neighboring routers. Here are five types of EIGRPP packages:

- Hello packages.
- Acknowledgment packages.
- Update packages.
- Query packages.
- Reply packs. Consider each of these types of packages.

Packages of Greetings

EIGRP uses greetings packets to detect, test, and resume neighboring routers after failures. Re-detection occurs if the routers do not receive greetings from each other during the retention time, but later resume communication.

EIGRP routers send fixed-interval greetings packets (specified in the configuration file), called hello intervals. The default interval is accepted; congratulations depend on the bandwidth of the interface, as shown in the table below. EIGRP uses multicast to send greetings.

Intervals sending packets greeting

Bandwidth	feed Type	The interval for	Retention

		congratulations default	time default
Less than or is equal to 1,544 Mbit / s	Protocol Multipoint Frame Relay	60 seconds	180 seconds
More than 1,544 Mbit / c	Line T1, connection "point - point"	5 seconds	15 seconds

Recall that the router EIGRPP stores information about neighboring devices in the TSP. It has for each neighboring device a serial number field that records the number of the last EIGRPP packet received from this device. Another TSP field is the retention time field, which records the time of receipt of the last packet. For the neighboring router to remain in the passive (reachable and workable) status, at least one packet must be received during the retention period. Otherwise, the EIGRP considers this neighboring router as inoperable, and the DUAL algorithm starts to list the TM. The default hold time is three times the interval of greetings; however, the administrator can configure both timers.

The EIGRP protocol (unlike OSPF) for communication does not have the condition of equality of values of greetings intervals and blocking on neighboring routers. In doing so, the latter learns about the intervals of the greetings timers and use this information to establish stable communication despite the different timer intervals.

Greetings are always sent by non-guaranteed delivery and do not require confirmation.

Confirmation Packages

The EIGRP router uses validation packets to notify other routers of receiving the EIGRPP packet during a "reliable" data exchange session. A robust transport protocol can provide reliable communication between EIGRP nodes. To ensure guaranteed delivery, the receiving node must acknowledge receipt of the message from the source. This is done using acknowledgment packets (which can be called "no data" greetings packages), unlike multicast greetings packets, these packets are unicast. Confirmation can also be made

by combining forward and reverse packet transmissions of other types of EIGRP packets, such as request-response packets.

Route Recovery Packages

Route recovery packets are used when the router detects a new neighboring device. The EIGRP router then sends unicast packet recovery packets to this new adjacent device so that it can add this information to its TT. Note that more than one packet may be required to transmit all topological information to a new neighboring device.

Recovery packets are also used when a router detects a change in network topology, then it sends multicast recovery packets to all its neighbors, alerting them to such a change. All recovery packages are shipped via guaranteed delivery.

Query and Query Packages

The EIGRP Router uses request packets every time it needs specific information from any of its neighboring devices. The answer packet is used to answer the query.

If the primary router disappears from the EIGRP router and cannot find a backup one, the DUAL algorithm puts the route into the active state. The router then sends a multicast request to all its neighbors to find the primary route. Neighboring devices must respond to requests that either provide information about the primary route or report that they do not have such information.

Queries can be multicast and unicast, while queries are always unicast. Both types of packages are shipped via a guaranteed delivery method.

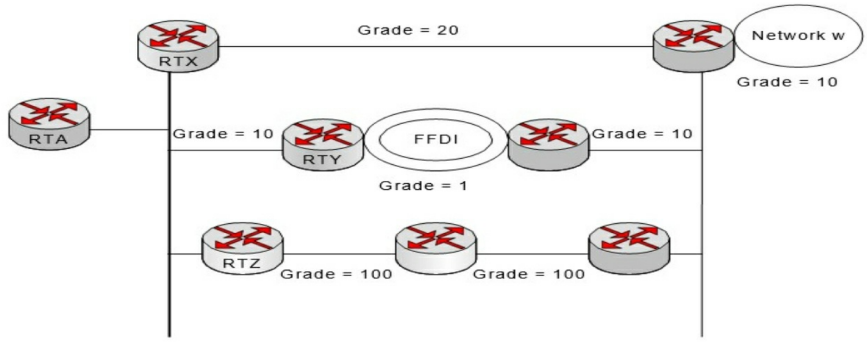
The Convergence of the EIGRP Protocol

The DUAL algorithm ensures a very fast convergence of the EIGRPP protocol. For a better understanding of the convergence process using DUAL, let us consider the scheme shown in Fig. below. An RTA router can access Network w through three different routers: RTX, RTY, or RTZ. To simplify the calculations, the composite metric of the EIGRP protocol was replaced by a channel estimate. The TT of the RTA router contains a list of all the routes announced by neighboring devices.

As shown in the table below, the RTA router stores for each network a real (calculated) estimate of access to that network, as well as an announced

estimate (reported distance) from its neighboring device.

Initially, RTY is the primary route to Network w because it has the lowest computed rating. The smallest calculated RTA metric to Network w (estimated FD distance to Network w) is 31.



Convergence Protocol

EIGRP Composite metric

Neighboring Device	The calculated grade of the route (FD) to the Network w	Reported Distance (RD) Network Network w
RTY	31	21
RTZ	230	220
RTX	40	30

To select a backup route that would be primary to Network w, the RTA router performs a three-step process.

Step 1. Determine which neighboring devices have a distance RD to Network w, less FD distance RTA to Network w. This distance FD equals 31; RD for RTX is 30, and RD for RTZ is 220. Thus, RD for RTX is less than the current FD, while RD for RTZ is greater than the current FD.

Step 2. Determine the minimum computed estimate to Network w of the remaining routes available. The estimated route estimation via RTX is 40, and through RTZ is 230. Thus, RTX provides the lowest calculated estimate.

Step 3. Determine whether the routers meet the criteria of the first and second stages. The RTX router satisfies both, so it is a backup route.

If the RTY router becomes inoperable, the RTA router immediately switches to using the RTX router to send packets to Network w. The ability to

immediately switch to a standby route is a basic prerequisite for very fast convergence of the EIGRPP protocol.

Can RTZ be a backup route?

Using the above three-step process, the RTA finds that RTZ announces an estimate of 220 that is not less than the FD distance for the RTA (31). Therefore, RTZ cannot be a standby route (yet). The FD distance can only change during the transition from the active to the passive state, and this transition has not yet been made, so this distance remains equal to 31. Until that moment, since the transition to the active state has not occurred for Network w, the algorithm DUAL implements a process called local computing.

The RTA cannot find backup routes, so it eventually goes from passive to an active state for Network w and asks its neighboring devices for that network. This process is called diffusion computation. When Network w is switched to an active state, this FD distance is reset, allowing the RTA to accept RTZ as the primary route to Network w eventually.

Now let us return again to the example of the KM and TM of the router R2. If the direct connection between R2 and R3 fails, is there a backup path in the TT of the router R2 to 192.168.1.0? Yes, it is, since the route metric from R1 to network 192.168.1.0 is 2172416, which is less than the route metric from R2 to network 192.168.1.0, which is 3014400 (the presence of a backup path can be viewed by typing show ip eigrp topology R2 on R2 in the Example below). If this condition is not fulfilled, the backup path from the network R2 to the network 192.168.1.0 would not exist, and then a recalculation would be required. In this case, the recalculation is not required, and in case of failure of the main path, the backup will be used immediately.

```
R2 # show ip eigrp topology
  <Output omitted results of>
                . . .
R 192.168.1.0/24, 1 successors, FD is
    3014400 via 192.168.10.10
    (3014400/28160) Serial0 / 0/1 via
    172.16.3.1 (41026560/2172416)
```

Serial0 / 0/1

<Output omitted results of>

Configuring EIGRP for IP

Despite the complexity of the DUAL algorithm, configuring the EIGRP proves to be relatively straightforward. Consider the configuration process in a small example (Fig below).

The following steps must be performed to configure EIGRP for the IP protocol.

Step 1. You must execute the command to enable EIGRP and define the autonomous system

Router (config) # router eigrp autonomous-system-number,

where the parameter autonomous-system-number is the OS identifier that points to all routers that belong to this consolidated network. This value should match all routers in this federated network. For example, for router A this command may be

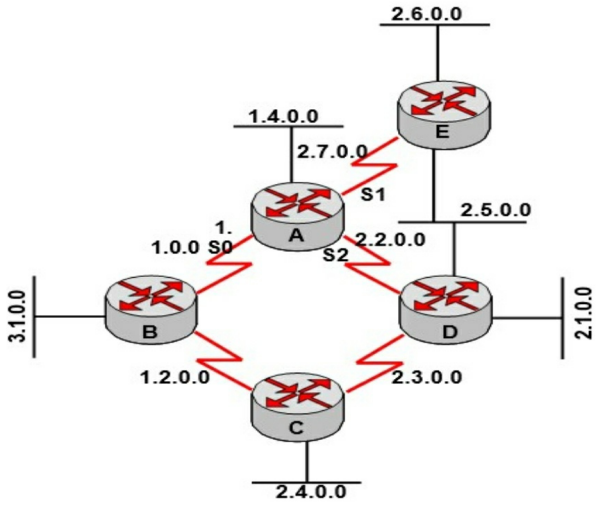
Router_A (config) # router eigrp 13.

Step 2. Specify which networks belong to this EIGRP on the local router using the command

Router (config-router) # network network-number,

where the parameter network-number is the network number. This command specifies which interfaces of this router are involved in the EIGRPP protocol and which networks are announcing it. The network number is given based on the IP address class. For example, 2.2.0.0 and 2.7.0.0 are introduced using the Router_A (config-router) # network 2.0.0.0 command, since they are subsets of 2.0.0.0.

The network command configures only the attached networks. For example, 3.1.0.0 is not directly connected to router A. Therefore, and it is not part of router A.



Configuring EIGRP protocol IP

If you want to specify only subnets for EIGRP, you should use the router (config-router) command # network network-number wildcard mask where wildcard mask - Inverted mask, that is, a 32-bit number that can be obtained by inverting the subnet mask. Bits of the inverted mask indicates whether you have the inverted mask zero and the corresponding bit of the IP address should be checked, and where the individual ones are not.

For example, if only the 2.2.0.0 subnet is specified for EIGRP, the Router_A (config-router) # network 2.2.0.0 0.0.255.255 command should be entered. It is advisable to note that several operating systems allow the introduction of a regular subnet mask instead of an inverted mask. However, before using this feature, you need to find out if this version of the OS supports it.

Step 3. When configuring serial channels using the EIGRPP protocol, it is important to specify a bandwidth on the interface. If it is not changed for such interfaces, the EIGRP protocol accepts the default bandwidth (instead of the true bandwidth). If the channel has a slower speed, the router may not be able to perform convergence, or there may be a loss of routing changes, or a suboptimal route may be selected. The bandwidth value is configured by command

Router (config-if) # bandwidth clock rate

The bandwidth command is the only one used in the routing process and must be set according to the channel speed for the interface.

Step 4. It is also recommended to add the EIGRP command to the configuration of each E1GRP router.

Router (config-if) # EIGRPp log-neighbor-changes.

This command logs changes in contiguity states (adjacent devices) to analyze the stability of the routing system and helps to identify problems that occur.

Configuring Bandwidth on NBMA Networks

When designing an EIGRPP in a nonbroadcast multiaccess - NBMA environment such as the Frame Relay network, the following rules must be followed :

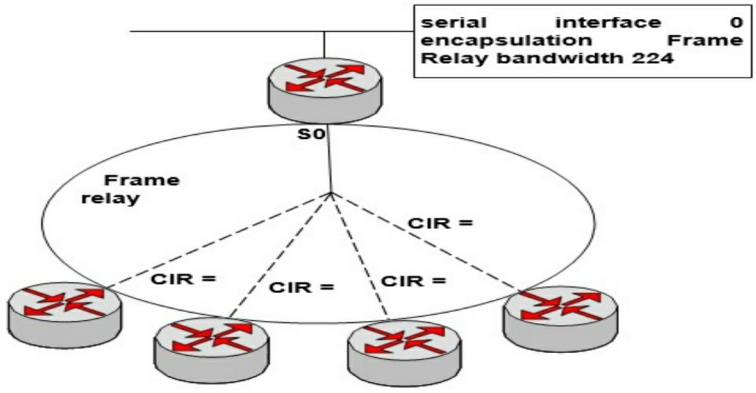
- EIGRP data transmission rate should not exceed the agreed information transfer rate (virtual rate - CIR virtual channel (virtual CVC)).
- The aggregated (aggregate) amount of EIGRPP data, but not all virtual channels should exceed the channel speed at the interface.
- The bandwidth allocated to the EIGRP protocol on each VC channel must be the same in both directions.

Understanding these rules correctly and executing them, E1GRP works effectively in a WAN environment. If no appropriate steps are taken when configuring EIGRPP on the WAN, then EIGRPP data streams may overflow.

Configure Bandwidth in a Multipoint nNetwork

The task of configuring a bandwidth command in an NBMA environment depends on how the VC virtual ropes are designed. If in a multi-point configuration, a serial channel has multiple VC channels and all of these channels share the bandwidth uniformly, the bandwidth command must have a bandwidth equal to the sum of all CIR speeds. For example, in the network In the Fig. below. The CIR speed of each VC channel is 56 Kbps. Since there

are four VC channels, the bandwidth should be set to 224 (4 ☐ 56).

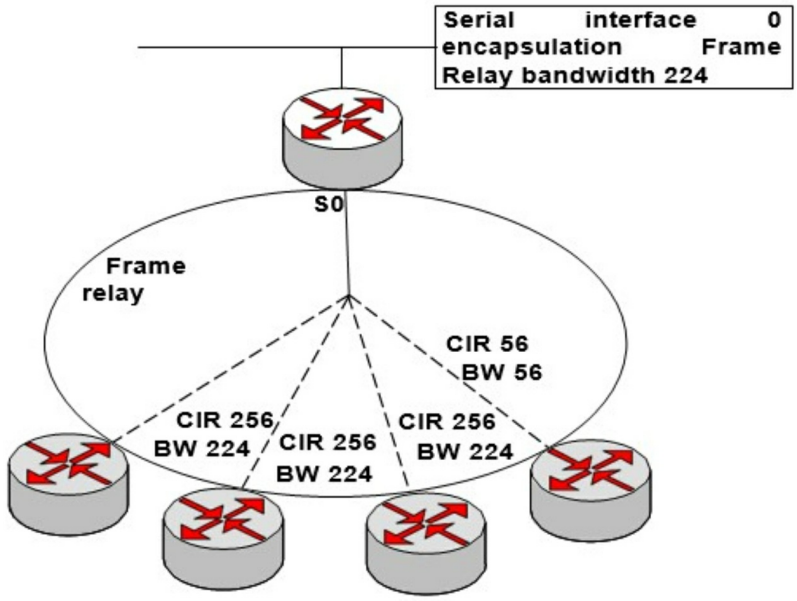


Configuring EIGRP on a Multipoint WAN

Configuring the Bandwidth in a Hybrid Multi-Point Network

If VC channels have different transmission speeds in a multi-point network, then a somewhat more complicated configuration is required. Two basic approaches can be applied.

1. Select the CIR speed that is the lowest for all channels and multiply it by the number of virtual channels (Fig below). This approach is applied to the physical interface. Its disadvantage is that channels with a large bandwidth may be underloaded.

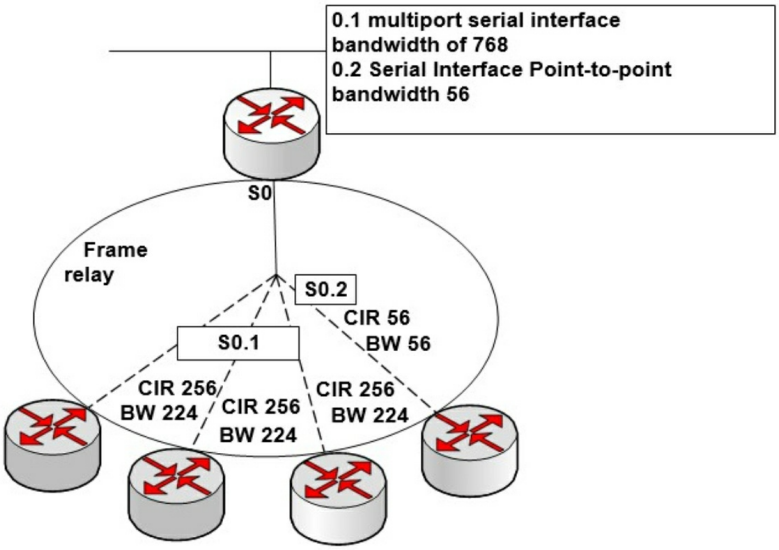


Configuring EIGRP in hybrid multipoint WAN network

2. Using subinterfaces, the bandwidth command can be configured on each sub-interface, allowing different speeds to be used on each VC channel. In this case, the sub-interfaces are configured for channels with different CIR speeds. Channels having the same configured CIR speed are the only bandwidth subinterface that corresponds to the aggregate CIR speed of all channels. In Fig. below the three VC virtual channels have the same CIR of 256 Kbps. They are grouped together as one multi-point serial 0.1. The only remaining VC channel having a CIR less (equal to 56) can be defined as a serial point-to-point sub-interface series 0.2.

Using the IP Bandwidth-Percent Command

The ip bandwidth-percent command specifies the percentage of bandwidth that EIGRPP can use on some interface. By default, EIGRP can use up to 50% of the bandwidth of the interface to exchange routing information. When calculating this percentage, the ip bandwidth-percent command uses the value set by the bandwidth command. The ip bandwidth-percent command should be used when the bandwidth set for the channel does not match its true speed.

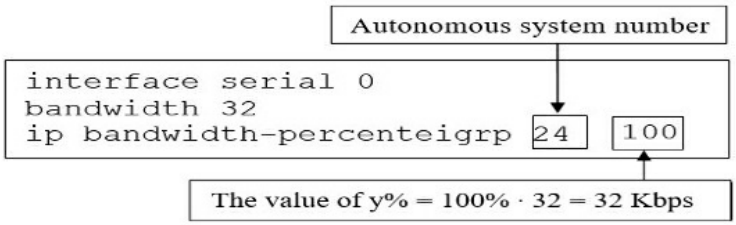


Configuring EIGRP in hybrid multipoint network WAN (best option)

The bandwidth can be artificially lowered for various reasons, in particular, to control the routing metric or to adjust the overload in the multi-point Frame Relay Configuration. Regardless of the cause of the underestimation, the EIGRPP must be configured to replace the artificially lowered bandwidth

with a higher value using the ip bandwidth percent command. In some cases, the value given by this command may even exceed 100%.

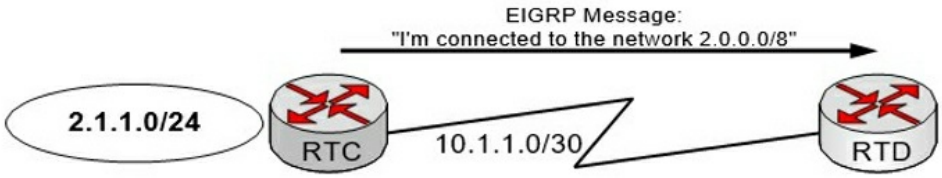
For example, suppose that the real bandwidth of a serial router channel is 64 Kbps; however, its value is artificially lowered to 32 Kbps. Fig below illustrates how EIGRPP should be modified to limit the amount of routing protocol data streams by the real bandwidth of the serial interface. In the above configuration example for an EIGRPP process that operates for autonomous system 24, the bandwidth in percentages for serial 0 is set to 100%. Since 100% of 32 Kbps is 32 Kbps, the EIGRPP protocol provides the opportunity to use half of the real bandwidth equal to 64 Kbps.



Application of the bandwidth-percent ip command to EIGRP

Configure Generalization of EIGRP Routes

The EIGRP protocol automatically generalizes routes on a network boundary that uses IP addresses with classes (that is, on the boundary of a network in which the network address contains an address class). This means that even though the RTC router is only connected to subnet 2.1.1.0, it declares that it is connected to the entire class A. 2.0.0.0 network. In most cases, automatic generalization is useful because it allows making the TM as compact as possible (Fig below).



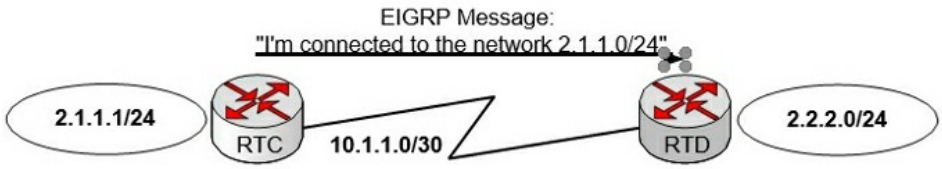
Automatic generalization routes in EIGRP

However, automatic generalization may be undesirable in some circumstances. If there are non-continuous subnets in the network (such as in the next Fig.), the automatic generalization must be disconnected for the proper functioning of the routing mechanism (otherwise the RTD router will not take the route to 2.0.0.0/8 which is connected to RTC, since it is directly

connected to the network 2.0.0.0/8). This disconnection uses the #no auto-summary router (config-router) command.

When using EIGRP, you can manually configure a prefix to use as a generic address. The manual configuration of route generalization is performed separately for each interface, so the first should be the interface that distributes route generalization. The generic address can then be determined using the command

Router(config-if)#ip summary-address eigrp autonomous- system-number ip-address mask administrative-distance.



Automatic generalization protocol EIGRP route network with gaps

Generalized EIGRP default routes have an administrative distance of 5. However, this value can be changed during the configuration to any value from 1 to 255. The RTC router shown in the above Figure can be configured using the commands given in the Example below.

RTC(config)# router eigrp 9

RTC(config-router)#no auto-summary

RTC(config-router)#exit

RTC(config)#interface serial0

RTC(config-if)#ip summary-address eigrp 9 2.1.0.0 255.255.0.0

As a result of executing the commands of this example, RTC will add route D 2.1.0.0/16 is a summary, 00:00:22, Null0 to the table. The generalized route has as its source, not the real interface but Null or 0 since this route is used for announcement purposes only and does not represent the route that the RTC router can choose to reach this network. In the RTC, this route has an administrative distance of 5.

For the RTD router In the . above, route generalization is irrelevant; however, it adopts this route and assigns it the administrative distance of the "normal" EIGRP route (standard 90). In config for the RTC router, automatic route generalization is disabled by the no auto-summary command. If not disabled,

the RTD router would receive two routes: a manually configured generic address (2.1.0.0/16) and assigned automatically using address classes (2.0.0.0/8). In most cases, the no auto-summary command should be used during manual compilation.

Configure Authentication in EIGRP

To increase the security of EIGRP, routers should be configured with authentication. This setup has two steps.

1. Create a key chain that will be used by all your network routers using the commands in the first three lines of Example 4.4. These commands create a key named MY_KEY, set a key number (1), and a key string value (CISCO).
2. Allow MD5 algorithm authentication on the corresponding router interface (s) (last three lines of Example below).

```
Router(config)# key chain MY_KEY
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string CISCO
Router(config-keychain-key)# exit
Router(config-keychain)# exit
Router(config)# interface serial0/0/0
Router(config-if)# ip authentication mode eigrp 1 md5
Router(config-if)# ip authentication key-chain eigrp 1 MY_KEY
```

Testing the Basic EIGRPP Configuration

The Cisco debug IOS feature provides useful EIGRP monitoring commands (Table below).

Basic commands debugging protocol EIGRP

Team	Description
debug eigrp fsm	Let's watch the backup job protocol EIGRP route and verify that the routing process installs and removes renovation Route
debug	Displays transmission and receiving EIGRP protocol packets.

eigrp packet	These packages may be packages greetings, update routes the request or response to the request. In the derivation showing sequential numbers and confirmation numbers used in transportation algorithm of reliable EIGRP protocol

Conclusion

For a long time, the formula "Switch where possible and route only if you have to" was in force. Operators used switches because they were cheaper to implement, provided faster frame forwarding, and supported multiple protocols. Support for multiple protocols was a key element because many L3 protocols were in use (including IP, Novell IPX, Appletalk, Xerox's XNS, etc.) as well as many L2 protocols that could not be routed (including NetBIOS and NetBEUI). The key to success was to understand when routers are needed. The decision was relatively simple - the routers were used in places where it was justified to limit the broadcast domain, e.g., in the case of slow and expensive WAN connections.

Currently, the choice is not so simple, Routing and switching are currently implemented in hardware and have similar performance. Support for many protocols is no longer important because data transfer is almost exclusively using the TCP / IP protocols. Depending on the size and complexity of the network, the operator may prefer the simplicity of layer two switchings, prefer the scalability offered by layer three routing, or choose to take advantage of the benefits of both of these architectures.

Layer 2 Ethernet networks have a flat structure and are designed for broadcasting. The packet to be delivered in the second layer to another device will be forwarded directly to its Ethernet interface (based on MAC address), thanks to the use of the Address Resolution Protocol (ARP).

In contrast, communication in the L3 layer requires routers to pass information between themselves, so-called routing tables so that individual routers know the available routes. When the packet reaches its last hop, the ARP protocol is used to determine the MAC address of the physical interface and then passes the packet to it. The exchange of routing information is done using dynamic routing protocols, such as RIP, OSPF, and less often, IS-IS. The administrator can also configure static routes.

Dynamic routing is much simpler to manage but requires constant information exchange to ensure that routing tables are up to date. Even OSPF, considered an efficient routing protocol, may need up to 2 seconds before it starts forwarding traffic on the new path when the original path is no longer available. In turn, the RIP protocol requires up to 90 seconds,

depending on the type of failure.

However, the question remains whether to use routing protocols in access networks. Experience has shown that small and medium access networks usually have a simple topology (e.g., point-to-point or ring) and converge at one exchange point. In larger networks, there are many exchange points connected with each other through IOF (Inter-Office Facility), which in turn converge in one large data center or operational center.

The structure of the last mile access networks at different access points is subject to conventional Carrier Serving Area guidelines. However, the method of aggregating traffic from terminal equipment depends on the technology used. In the case of the Linear add-drop or tree topology, the matter is quite simple - you can connect as many devices and aggregate their traffic as much as the bandwidth and physical infrastructure allow. However, if the connection or tree fails, the lack of alternative paths will cause a lack of communication felt by clients. Using the optical ring in the last mile, diversified routes to end devices are created. If the structure of the ring is damaged, the movement will be guided by the remaining available paths.

In the event of a ring topology failure, traffic should be sent through the alternative path in the second layer almost instantaneously (time in milliseconds). For L3 routing protocols, you should expect a convergence time of more than a second. This is not a big problem, but end users may notice such a break in communication, e.g., during a VoIP call.

Routers are useful in networks built-in full or partial mesh topology, which is divided by several exchange points, is connected by several paths to the Internet, and traffic requires load balancing between these connections. Small and medium operators hardly use such architecture.

Routing is logically assigned to one point in the access network. The operator will need a large, reliable router that will handle multimedia transmission or will be located at an Internet access point to segment inbound and outbound traffic.

Ethernet technology offers the lowest cost per bit. The use of Ethernet and switching in the second layer means an aggregation of all types of network traffic - VoIP, data, video, etc. This reduces the cost of purchasing equipment and also simplifies network management.

However, even if Ethernet switches are the basis of the access network, this

does not mean that routing will not be needed. A good solution is to use a router in a central location to aggregate L2 access domains if your Ethernet resources are running out. These resources include, among others, MAC address table, IP subnet addressing, bandwidth. By using this model, the operator can exploit the simplicity and performance of layer two switchings as well as the scalability and centralized management of layer three.

Distributed routing in smaller locations will only introduce additional costs and complicate the network structure. With the expansion of access network domains and their increasing number, they can be routed quickly to a central location using core routers. As we have already mentioned, L3 routing is based on alternative paths defined in routing tables. By managing a centralized, scalable router, routing tables are placed at one point (or their number is significantly reduced), which translates into a simplified network structure.

Decisions regarding network design are increasingly one of several solutions. For example, when choosing a broadband access platform, the basic question in the decision-making process is: to choose ATM technology or IP technology? In turn, when making decisions about switching or routing in an access network, it is worth noting that many L2 switching elements are currently available. In addition to the fact that L2 access switches usually offer hardware frame forwarding functions, they also have more advanced mechanisms for deep packet analysis.

Traditionally, L2 switching devices transmit packets across all interfaces, creating a phenomenon known as flooding. This ensures that traffic sent based on VLANs will go to devices that are more often a large array of MAC addresses. This is a forwarding technique useful for data transmission, where all devices connected in the second layer are trusted and "interested" in receiving data. However, flooding is not a desirable phenomenon in access networks. Packets sent by one user should not reach other users. Therefore, L2 switches have solutions that only forward packets to the right user.

You can also enter rules to force all traffic through the router to ensure secure communications. It can be assumed that the use of routers in individual access nodes will eliminate unwanted communication between users, but operators must understand that the only justification for this is to create subnets for individual users. Unfortunately, this has serious disadvantages - a network constructed in such a way scales very hard and has a very large

number of routing paths that need to be managed.

There are also other reasons for creating traffic rules based on the ability to parse TCP or UDP packets. An example is the ability to block protocols, such as IPX, to prevent the commutation of the access network. Clients with experience of using the network can configure WAN connections based on L3 routing in an open network using switching.

In a network with a switch in the second layer, devices in the access network can be automatically detected, which will allow them to be granted access to network services (based on a predefined service model) and will make them work almost immediately. In the case of routed architecture, it is necessary to carefully plan the IP addressing (subnetworks), taking into account the anticipated network expansion. If all subnets are used, additional resources will be needed to manage layer three routings. You should also consider public IP addresses that you may want to use and which must be routed through your operator's private L3 access network. Private IP addressing scales are easy to scale, but planning is required to create IP addresses that are easy to manage.

On the other hand, switching in operator access networks offers efficiency, reliability, lower costs, and simplified addressing. In turn, the central location of tier three routers allows the operator to achieve additional benefits.

Each discussion regarding the comparison of L2 switching with L3 routing in an access network must be preceded by an understanding of the applications and advantages of each of these technologies. Traditionally, switching is used to connect users and network devices with each other efficiently. Switching is, by its very nature, intended for promoting information and sharing services. On the contrary, routing is traditionally used to connect separate network segments and create clear boundaries between networks. The usefulness of routing in access networks is unquestionable - use it to connect separate L2 networks. Also, based on the traditional and current role of routing in communication, it should be centralized rather than distributed between remote locations.

Of course, practical aspects of engineering should also be considered, depending on the size of the access network, user density, and services offered. Smaller networks can certainly benefit from layer two switching.

Resources

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/oer/command/ oer-cr-book/oer-h1.html

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/oer/command/ oer-cr-book/oer-a1.html

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/pfr/command/ pfr-cr-book/pfr-a1.html

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/pfr/command/ pfr-cr-book/pfr-h1.html

https://www.oreilly.com/library/view/advanced-ip-network/1578700973/ 1578700973_ch07lev1sec10.html

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/oer/configuration/ 15-1mt/oer-15-1mt-book/oer-setup-ntwrk.html

https://www.developpez.net/forums/d1607863/systemes/reseaux/ point-to-point-protocol-oe-routeur-cisco-2900-a/

https://www.planet.com.tw/storage/products/48646/EMQ-VC-820M_v2.0.pdf

https://www.academia.edu/11161933/Taller_CCN2Enrutamientocon_RIP_1_

https://flylib.com/books/en/2.8.1.39/1/

https://superuser.com/questions/1120851/ how-does-rip-routing-information-protocol-work

https://networklessons.com/eigrp/eigrp-neighbor-and-topology-table-explained

https://networklessons.com/cisco/ccnp-route/ eigrp-neighbor-and-topology-table-explained

https://packetlife.net/blog/2010/aug/9/eigrp-feasible-successor-routes/

https://ccieblog.co.uk/eigrp/eigrp-query-scoping-using-summarisation

https://studylib.net/doc/9620746/ccna-3-module-3-single

https://networkengineering.stackexchange.com/questions/23682/ this-is-an-eigrp-topology-with-frame-relay-im-not-able-to-figure-out-why-r1s

https://www.auvik.com/franklymsp/blog/first-deployment-eigrp/