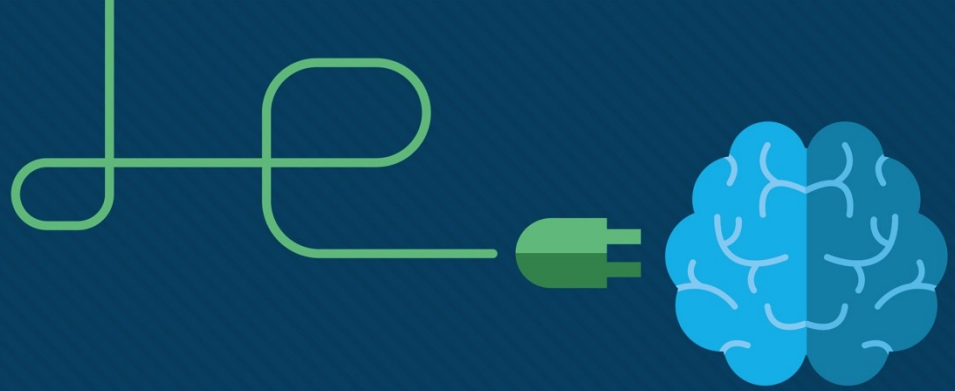


Module 14: Routing Concepts

Instructor Materials

Switching, Routing, and Wireless Essentials v7.0 (SRWE)

- Téma 14.1
- Jak bychom mohli využít pravidla nejdelší shody k naší výhodě a zmenšit velikost směrovací tabulky?
- Proč si myslíte, že jsou do směrovací tabulky přidány přímo připojené sítě?

- Téma 14.2
- Co se v paketu/rámci musí změnit pokaždé, když se paket pohybuje směrovačem?
- Jaká je primární odpovědnost routeru v procesu předávání paketů?

- Téma 14.3
- Jaký je rozdíl v informacích, které vám dávají příkazy `show interface` a `show ip interface`?

- Téma 14.4
- Zeptejte se studentů na jejich vlastní analogii toho, co je administrativní vzdálenost.
- Požádejte studenty, aby vysvětlili označení /0 pro výchozí trasu vlastními slovy.

- Téma 14.5
- Směrovací protokoly jsou obecně kategorizovány jako IGP nebo EGP. Jaký je v tom rozdíl?
- Požádejte studenty, aby vysvětlili zjišťování vzdálených sítí jejich vlastními slovy.

Module Objectives

Module Title: Routing Concepts

Module Objective: Explain how routers use information in packets to make forwarding decisions.

Topic Title	Topic Objective
Path Determination	Explain how routers determine the best path.
Packet Forwarding	Explain how routers forward packets to the destination.
Basic Router Configuration Review	Configure basic settings on a router.
IP Routing Table	Describe the structure of a routing table.
Static and Dynamic Routing	Compare static and dynamic routing concepts.

14.1 Path Determination

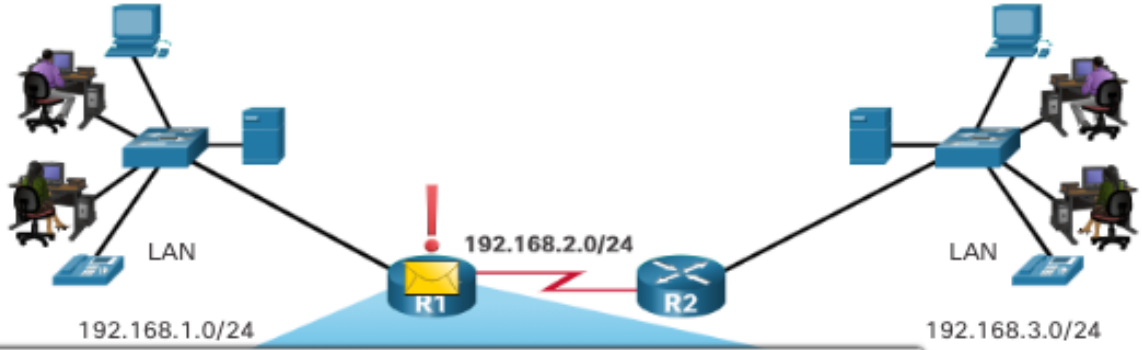
Two Functions of a Router

When a router receives an IP packet on one interface, it determines which interface to use to forward the packet to the destination. This is known as routing. The interface that the router uses to forward the packet may be the final destination, or it may be a network connected to another router that is used to reach the destination network. Each network that a router connects to typically requires a separate interface, but this may not always be the case.

The primary functions of a router are to determine the best path to forward packets based on the information in its routing table, and to forward packets toward their destination.

Router Functions Example

The router uses its IP routing table to determine which path (route) to use to forward a packet. R1 and R2 will use their respective IP routing tables to first determine the best path, and then forward the packet.




```
R1# show ip route
Codes:
C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default
U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
S    192.168.3.0/24 [1/0] via 192.168.2.2
```

Routers use the routing table like a map to discover the best path for a given network.

Best Path Equals Longest Match

- The best path in the routing table is also known as the longest match.
- The routing table contains route entries consisting of a prefix (network address) and prefix length. For there to be a match between the destination IP address of a packet and a route in the routing table, a minimum number of far-left bits must match between the IP address of the packet and the route in the routing table. The prefix length of the route in the routing table is used to determine the minimum number of far-left bits that must match.
- The longest match is the route in the routing table that has the greatest number of far-left matching bits with the destination IP address of the packet. The longest match is always the preferred route.

Note: The term prefix length will be used to refer to the network portion of both IPv4 and IPv6 addresses.

IPv4 Longest Match Example

In the table, an IPv4 packet has the destination IPv4 address 172.16.0.10. The router has three route entries in its IPv4 routing table that match this packet: 172.16.0.0/12, 172.16.0.0/18, and 172.16.0.0/26. Of the three routes, 172.16.0.0/26 has the longest match and would be chosen to forward the packet. For any of these routes to be considered a match there must be at least the number of matching bits indicated by the subnet mask of the route.

Destination IPv4 Address		**Address in Binary**
172.16.0.10		**10101100.00010000.00000000.00**001010
Route Entry	Prefix/Prefix Length	Address in Binary
1	172.16.0.0**/12**	**10101100.0001**0000.00000000.00001010
2	172.16.0.0**/18**	**10101100.00010000.00**000000.00001010
3	172.16.0.0**/26**	**10101100.00010000.00000000.00**001010

IPv6 Longest Match Example

An IPv6 packet has the destination IPv6 address 2001:db8:c000::99. This example shows three route entries, but only two of them are a valid match, with one of those being the longest match. The first two route entries have prefix lengths that have the required number of matching bits as indicated by the prefix length. The third route entry is not a match because its /64 prefix requires 64 matching bits.

Destination	**2001:db8:c000::99/48**	
Route Entry	Prefix/Prefix Length	Does it match?
1	**2001:db8:c0**00::**/40**	Match of 40 bits
2	**2001:db8:c000**::**/48**	Match of 48 bits (longest match)
3	**2001:db8:c000**:5555::**/64**	Does not match 64 bits

Build the Routing Table

Directly Connected Networks: Added to the routing table when a local interface is configured with an IP address and subnet mask (prefix length) and is active (up and up).

Remote Networks: Networks that are not directly connected to the router. Routers learn about remote networks in two ways:

- **Static routes** - Added to the routing table when a route is manually configured.
- **Dynamic routing protocols** - Added to the routing table when routing protocols dynamically learn about the remote network.

Default Route: Specifies a next-hop router to use when the routing table does not contain a specific route that matches the destination IP address. The default route can be entered manually as a static route, or learned automatically from a dynamic routing protocol.

- A default route has a /0 prefix length. This means that no bits need to match the destination IP address for this route entry to be used. If there are no routes with a match longer than 0 bits, the default route is used to forward the packet. The default route is sometimes referred to as a gateway of last resort.

14.2 Packet Forwarding

Packet Forwarding Decision Process

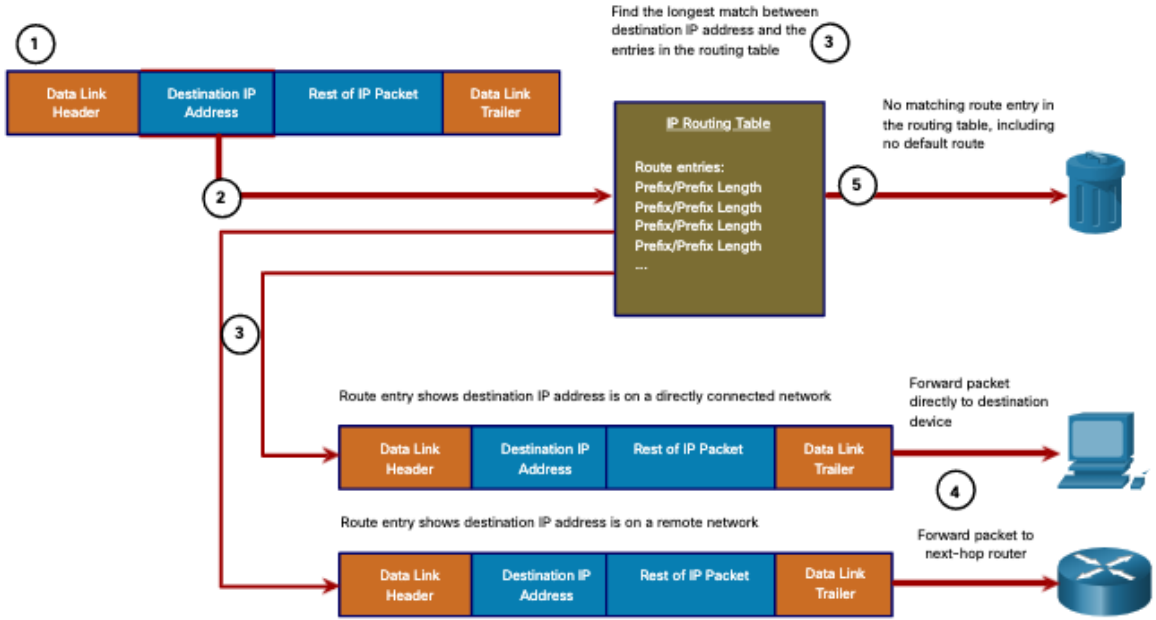
1. The data link frame with an encapsulated IP packet arrives on the ingress interface.

2. The router examines the destination IP address in the packet header and consults its IP routing table.

3. The router finds the longest matching prefix in the routing table.

4. The router encapsulates the packet in a data link frame and forwards it out the egress interface. The destination could be a device connected to the network or a next-hop router.

5. However, if there is no matching route entry the packet is dropped.



Packet Forwarding Decision Process (Cont.)

After a router has determined the best path, it could do the following:

Forward the Packet to a Device on a Directly Connected Network

- If the route entry indicates that the egress interface is a directly connected network, the packet can be forwarded directly to the destination device. Typically this is an Ethernet LAN.
- To encapsulate the packet in the Ethernet frame, the router needs to determine the destination MAC address associated with the destination IP address of the packet. The process varies based on whether the packet is an IPv4 or IPv6 packet.

Packet Forwarding Decision Process (Cont.)

After a router has determined the best path, it could do the following:

Forward the Packet to a Next-Hop Router

- If the route entry indicates that the destination IP address is on a remote network, meaning a device on network that is not directly connected. The packet must be forwarded to the next-hop router. The next-hop address is indicated in the route entry.
- If the forwarding router and the next-hop router are on an Ethernet network, a similar process (ARP and ICMPv6 Neighbor Discovery) will occur for determining the destination MAC address of the packet as described previously. The difference is that the router will search for the IP address of the next-hop router in its ARP table or neighbor cache, instead of the destination IP address of the packet.

Note: This process will vary for other types of Layer 2 networks.

Packet Forwarding Decision Process (Cont.)

After a router has determined the best path, it could do the following:

Drop the Packet - No Match in Routing Table

- If there is no match between the destination IP address and a prefix in the routing table, and if there is no default route, the packet will be dropped.

End-to-End Packet Forwarding

The primary responsibility of the packet forwarding function is to encapsulate packets in the appropriate data link frame type for the outgoing interface. For example, the data link frame format for a serial link could be Point-to-Point (PPP) protocol, High-Level Data Link Control (HDLC) protocol, or some other Layer 2 protocol.

Packet Forwarding Mechanisms

The primary responsibility of the packet forwarding function is to encapsulate packets in the appropriate data link frame type for the outgoing interface. The more efficiently a router can perform this task, the faster packets can be forwarded by the router.

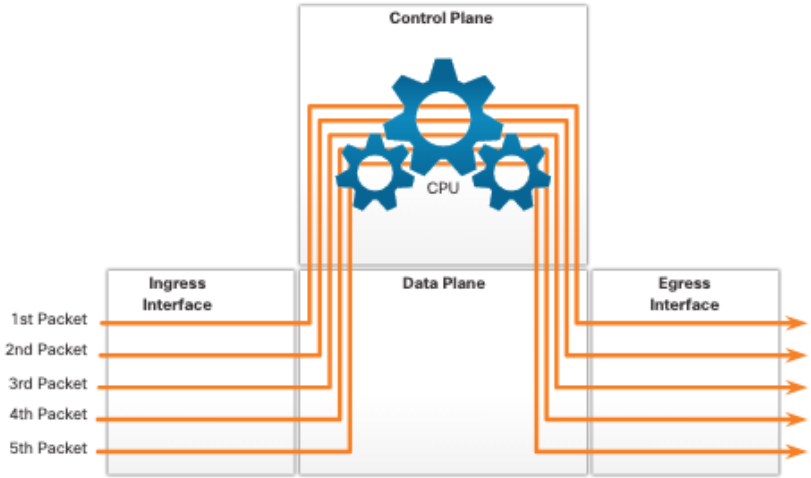
Routers support the following three packet forwarding mechanisms:

- Process switching
- Fast switching
- Cisco Express Forwarding (CEF)

Packet Forwarding Mechanisms (Cont.)

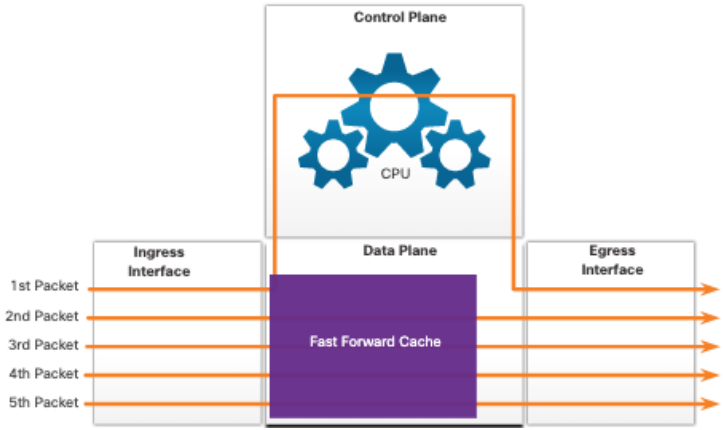
Process Switching: An older packet forwarding mechanism still available for Cisco routers. When a packet arrives on an interface, it is forwarded to the control plane where the CPU matches the destination address with an entry in its routing table, and then determines the exit interface and forwards the packet.

It is important to understand that the router does this for every packet, even if the destination is the same for a stream of packets.



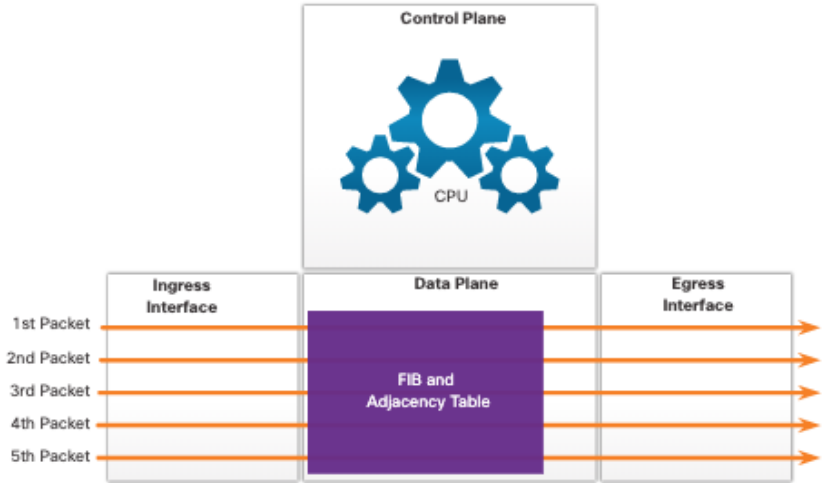
Packet Forwarding Mechanisms (Cont.)

- **Fast Switching:** Another, older packet forwarding mechanism which was the successor to process switching. Fast switching uses a fast-switching cache to store next-hop information. When a packet arrives on an interface, it is forwarded to the control plane where the CPU searches for a match in the fast-switching cache.
- If it is not there, it is process-switched and forwarded to the exit interface. The flow information for the packet is then stored in the fast-switching cache. If another packet going to the same destination arrives on an interface, the next-hop information in the cache is re-used without CPU intervention.



Packet Forwarding Mechanisms (Cont.)

- **Cisco Express Forwarding (CEF):** The most recent and default Cisco IOS packet-forwarding mechanism. CEF builds a Forwarding Information Base (FIB), and an adjacency table.
- The table entries are not packet-triggered like fast switching but change-triggered, such as when something changes in the network topology. When a network has converged, the FIB and adjacency tables contain all the information that a router would have to consider when forwarding a packet.




```
Router(config)#ip cef
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

```
Router#sh ip cef
Prefix Next Hop Interface
0.0.0.0/0 drop Null0 (default route handler entry)
0.0.0.0/8 drop
0.0.0.0/32 receive
127.0.0.0/8 drop
224.0.0.0/4 drop
224.0.0.0/24 receive
240.0.0.0/4 drop
255.255.255.255/32 receive
Router#
```

Adjacency table (tabulka sousedství)

Cache adjacency: Tento typ záznamu obsahuje správné odchozí rozhraní a správnou adresu MAC pro jeho záznam FIB. Eliminuje nutnost ARPu.

Receive adjacency: Tento typ vstupu zpracovává pakety, jejichž konečné cíle zahrnují samotný směrovač. To zahrnuje pakety, jejichž adresy IP jsou přiřazeny samotnému směrovači, vysílací pakety a vícesměrové vysílání, které jako jeden z cílů nastavily samotný směrovač.

Null adjacency: Pakety s položkami FIB ukazujícími na NULL adjacencies budou normálně zahozeny.

Punt adjacency (výkop): Zabývá se pakety, které vyžadují speciální zacházení nebo je nelze přepnout pomocí CEF. Takové pakety jsou předávány do další přepínací vrstvy (obvykle rychlé přepínání), kde je lze správně přeposílat.

Glean adjacency (sběr): Je vytvořena, když router ví, že buď je podsíť cílové IP přímo připojena k samotnému routeru a nezná MAC adresu cílového zařízení, nebo router zná IP adresu routeru, na který má předat paket pro cíl, ale neví MAC adresu routeru. Pakety, které aktivují tuto položku, vygenerují požadavek ARP.

Discard adjacency: FIB položky ukazující na tento typ sousedství budou zahozeny.

Drop adjacency: Pakety směřující na tuto položku jsou zahozeny, ale předpona zkontrolována.

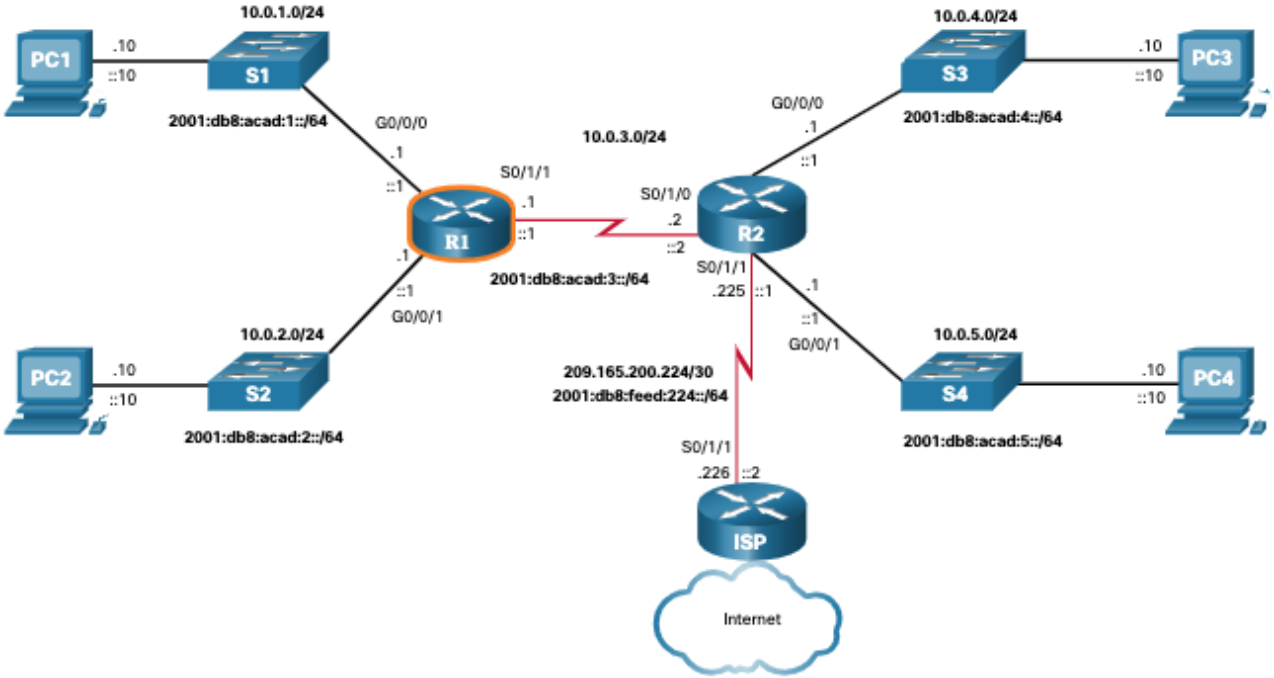
CEF Load-Balancing – vyrovnávání zátěže

- load balancing per-destination (defaultní)
- load balancing per-packet

14.3 Basic Router Configuration Review

Topology

The topology in the figure will be used for configuration and verification examples. It will also be used in the next topic to discuss the IP routing table.



Configuration Commands

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line. End with
CNTL/Z.
Router(config)# hostname R1
R1(config)# enable secret class
R1(config)# line console 0
R1(config-line)# logging synchronous
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# transport input ssh telnet
R1(config-line)# exit
R1(config)# service password-encryption R1(config)#
banner motd #
Enter TEXT message. End with a new line and the #
**********************************************
WARNING: Unauthorized access is prohibited!
**********************************************
#
```

```
R1(config)# ipv6 unicast-routing
R1(config)# interface gigabitethernet 0/0/0
R1(config-if)# description Link to LAN 1
R1(config-if)# ip address 10.0.1.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# ipv6 address fe80::1:a link-local
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface gigabitethernet 0/0/1
R1(config-if)# description Link to LAN 2
R1(config-if)# ip address 10.0.2.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# ipv6 address fe80::1:b link-local
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface serial 0/1/1
R1(config-if)# description Link to R2
R1(config-if)# ip address 10.0.3.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:3::1/64
R1(config-if)# ipv6 address fe80::1:c link-local
R1(config-if)# no shutdown
R1(config-if)# exit
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

login

```
R2(config)#line vty 0 4
R2(config-line)#no login

R2(config)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#transport input telnet
R2(config-line)#login local

R2(config)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#transport input ssh
R2(config-line)#login local
R2(config)#crypto key generate rsa modulus 1024
R2(config)#username admin privilege 15 secret heslo
R2(config)# ip domain-name muni.cz

……
R2(config-line)#do show run | sec vty
```

Verification Commands

Common verification commands include the following:

- **show ip interface brief**
- **show running-config interface** *interface-type number*
- **show interfaces**
- **show ip interface**
- **show ip route**
- **ping**

In each case, replace **ip** with **ipv6** for the IPv6 version of the command.

Rozdíl sh int a sh ip int

sh int s1/0/0

Serial1/0/0 is up, line protocol is up
  Hardware is cyBus Serial
  Description: T1 connection
  Internet address is 192.168.1.1/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, crc 16, loopback not set
  Keepalive set (10 sec)
  Restart-Delay is 0 secs
  LCP Open
  Open: IPCP, CDPCP
  Last input 00:00:03, output 00:00:03, output hang never
  Last clearing of "show interface" counters 8w3d
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    7517564 packets input, 1383633996 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    433 input errors, 429 CRC, 0 frame, 1 overrun, 0 ignored, 3 abort
    7363054 packets output, 2531859256 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions
    RTS up, CTS up, DTR up, DCD up, DSR up

sh ip int s1/0/0

Serial1/0/0 is up, line protocol is up
  Internet address is 192.168.1.1/30
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  Peer address is 192.168.10.10
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined:
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is enabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP Distributed switching is enabled
  IP Feature Fast switching turbo vector
  IP Feature CEF switching turbo vector
  IP multicast fast switching is enabled
  .....
  RTS up, CTS up, DTR up, DCD up, DSR up

Filter Command Output

Filtering commands can be used to display specific sections of output. To enable the filtering command, enter a pipe (|) character after the **show** command and then enter a filtering parameter and a filtering expression.

The filtering parameters that can be configured after the pipe include:

- **section** - This displays the entire section that starts with the filtering expression.
- **include** - This includes all output lines that match the filtering expression.
- **exclude** - This excludes all output lines that match the filtering expression.
- **begin** - This displays all the output lines from a certain point, starting with the line that matches the filtering expression.

Note: Output filters can be used in combination with any **show** command.

Packet Tracer - Basic Router Configuration Review

In this Packet Tracer, you will do the following:

- Configure Devices and Verify Connectivity
- Display Router Information

14.4 IP Routing Table

Route Sources

A routing table contains a list of routes to known networks (prefixes and prefix lengths). The source of this information is derived from the following:

- Directly connected networks
- Static routes
- Dynamic routing protocols

The source for each route in the routing table is identified by a code. Common codes include the following:

- **L** - Identifies the address assigned to a router interface.
- **C** - Identifies a directly connected network.
- **S** - Identifies a static route created to reach a specific network.
- **O** - Identifies a dynamically learned network from another router using the OSPF routing protocol.
- ***** - This route is a candidate for a default route.

Routing Table Principles

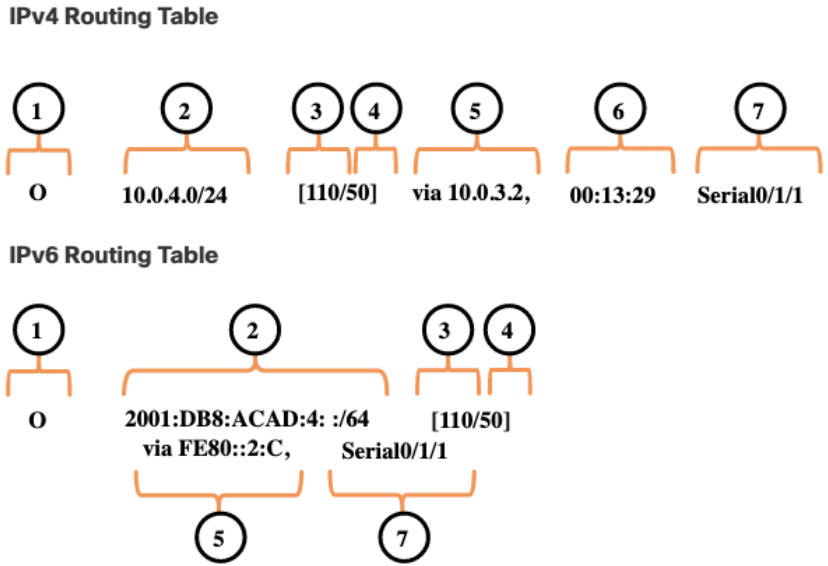
There are three routing table principles as described in the table. These are issues that are addressed by the proper configuration of dynamic routing protocols or static routes on all the routers between the source and destination devices.

Routing Table Principle	Example
Every router makes its decision alone, based on the information it has in its own routing table.	•R1 can only forward packets using its own routing table. •R1 does not know what routes are in the routing tables of other routers (e.g., R2).
The information in a routing table of one router does not necessarily match the routing table of another router.	Just because R1 has route in its routing table to a network in the internet via R2, that does not mean that R2 knows about that same network.
Routing information about a path does not provide return routing information.	R1 receives a packet with the destination IP address of PC1 and the source IP address of PC3. Just because R1 knows to forward the packet out its G0/0/0 interface, doesn't necessarily mean that it knows how to forward packets originating from PC1 back to the remote network of PC3

Routing Table Entries

In the figure, the numbers identify the following information:

- **Route source** - This identifies how the route was learned.
- **Destination network (prefix and prefix length)** - This identifies the address of the remote network.
- **Administrative distance** - This identifies the trustworthiness of the route source. Lower values indicate preferred route source.
- **Metric** - This identifies the value assigned to reach the remote network. Lower values indicate preferred routes.
- **Next-hop** - This identifies the IP address of the next router to which the packet would be forwarded.
- **Route timestamp** - This identifies how much time has passed since the route was learned.
- **Exit interface** - This identifies the egress interface to use for outgoing packets to reach their final destination.



Note: The prefix length of the destination network specifies the minimum number of far-left bits that must match between the IP address of the packet and the destination network (prefix) for this route to be used.

Directly Connected Networks

To learn about any remote networks, the router must have at least one active interface configured with an IP address and subnet mask (prefix length). This is known as a directly connected network or a directly connected route. Routers add a directly connected route to its routing table when an interface is configured with an IP address and is activated.

- A directly connected network is denoted by a status code of **C** in the routing table. The route contains a network prefix and prefix length.
- The routing table also contains a local route for each of its directly connected networks, indicated by the status code of **L**.
- For IPv4 local routes the prefix length is /32 and for IPv6 local routes the prefix length is /128. This means the destination IP address of the packet must match all the bits in the local route for this route to be a match. The purpose of the local route is to efficiently determine when it receives a packet for the interface instead of a packet that needs to be forwarded.

Static Routes

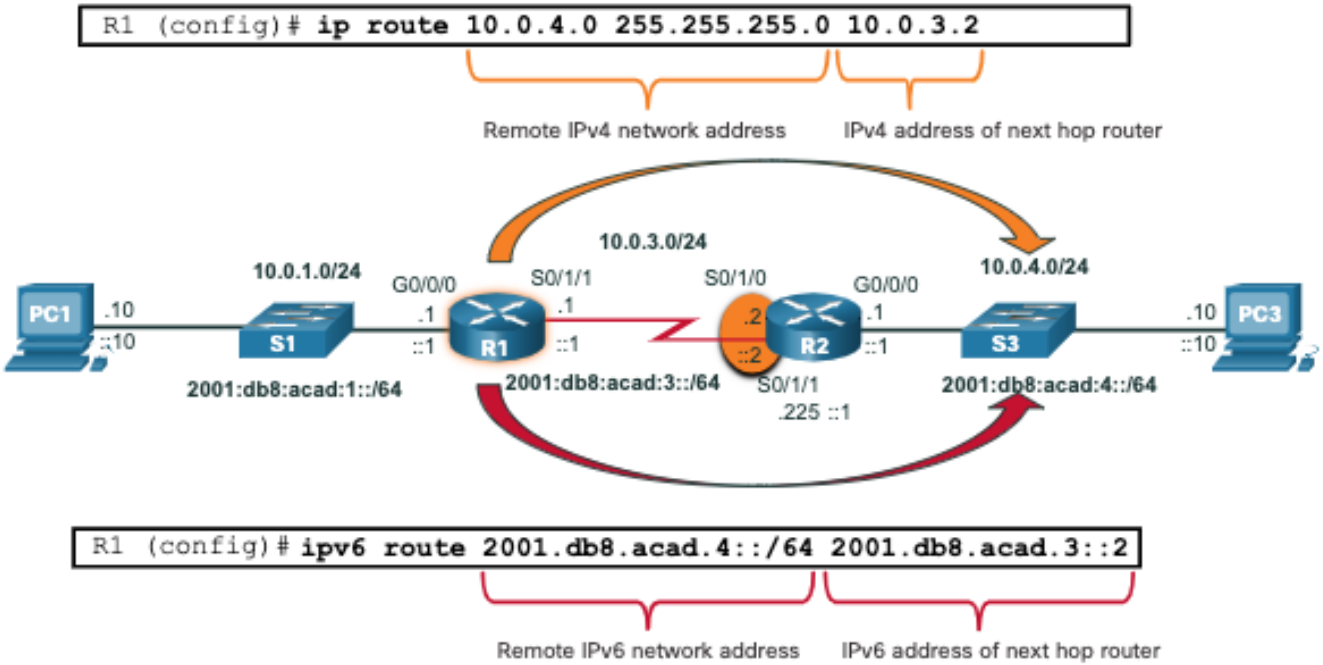
After directly connected interfaces are configured and added to the routing table, static or dynamic routing can be implemented for accessing remote networks. Static routes are manually configured. They define an explicit path between two networking devices. They are not automatically updated and must be manually reconfigured if the network topology changes.

Static routing has three primary uses:

- It provides ease of routing table maintenance in smaller networks that are not expected to grow significantly.
- It uses a single default route to represent a path to any network that does not have a more specific match with another route in the routing table. Default routes are used to send traffic to any destination beyond the next upstream router.
- It routes to and from stub networks. A stub network is a network accessed by a single route, and the router has only one neighbor.

Static Routes in the IP Routing Table

The topology in the figure is simplified to show only one LAN attached to each router. The figure shows IPv4 and IPv6 static routes configured on R1 to reach the 10.0.4.0/24 and 2001:db8:acad:4::/64 networks on R2.

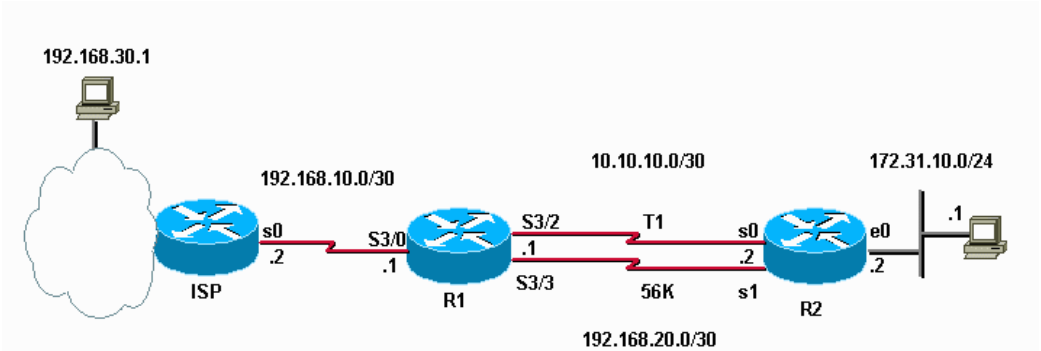


Rekurzivní statický routing: dvojí průchod tabulkou 1. S řádek, 2. L řádek

```
R1(config)#do sh ip route

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.10.1.0/24 is directly connected, FastEthernet0/0
L        10.10.1.1/32 is directly connected, FastEthernet0/0
S     192.168.1.0/24 [1/0] via 10.10.1.2
S     192.168.2.0/24 [1/0] via 10.10.1.2
```

Rekurzivní statický routing



Router R1 má nakonfigurovanou následující výchozí statickou cestu.

IP route 0.0.0.0 0.0.0.0 S3/0

Má také následující cestu do LAN mimo R2 přes linku T1 a plovoucí statickou elektřinu přes pomalejší linku 56K, aby byla chráněna před selháním linky T1.

IP route 172.31.10.0 255.255.255.0 10.10.10.2
IP route 172.31.10.0 255.255.255.0 192.168.20.2 200

Pokud nyní vypneme Serial 3/2, očekávali byste, že R1 použije záložní cestu k 172.31.10.0/24, ale nepoužije.

Proč ne?

Je to proto, že statické trasy mají rekurzivní povahu, když zadáte adresu IP jako další směrování.

V tomto příkladu se R1 podívá na směrovací tabulku pro cestu k 10.10.10.2 a protože existuje výchozí cesta k ISP, bude předpokládat, že cesta existuje a trasa k 172.31.10.0/24 zůstane ve směrovací tabulce směřující k 10.10.10.2.

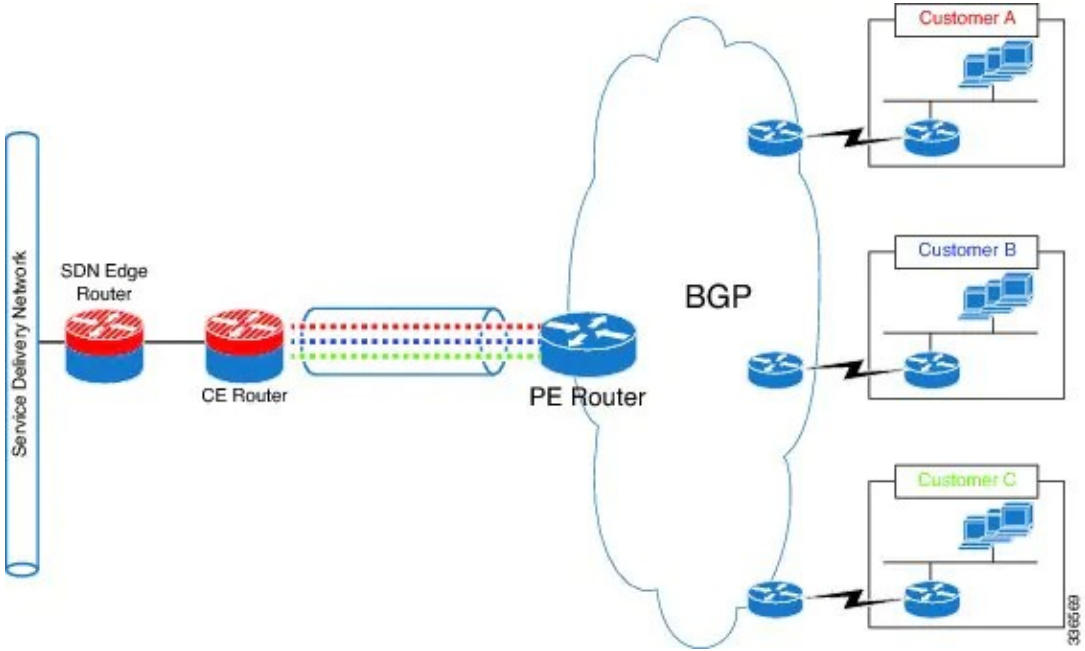
K překonání tohoto problému nasměrujte trasu na rozhraní a IP adresu. Tím je zajištěno, že pokud nelze zjistit další adresu směrování, zadané rozhraní nebude trasa umístěna do směrovací tabulky.

IP cesta 172.31.10.0 255.255.255.0 Serial3/2 10.10.10.2

IP cesta 172.31.10.0 255.255.255.0 Serial3/3 192.168.20.2 200

Packet Tracer nezajišťuje ani toto.

Na problém s rekurzí statického routingu narazíte i u BGP



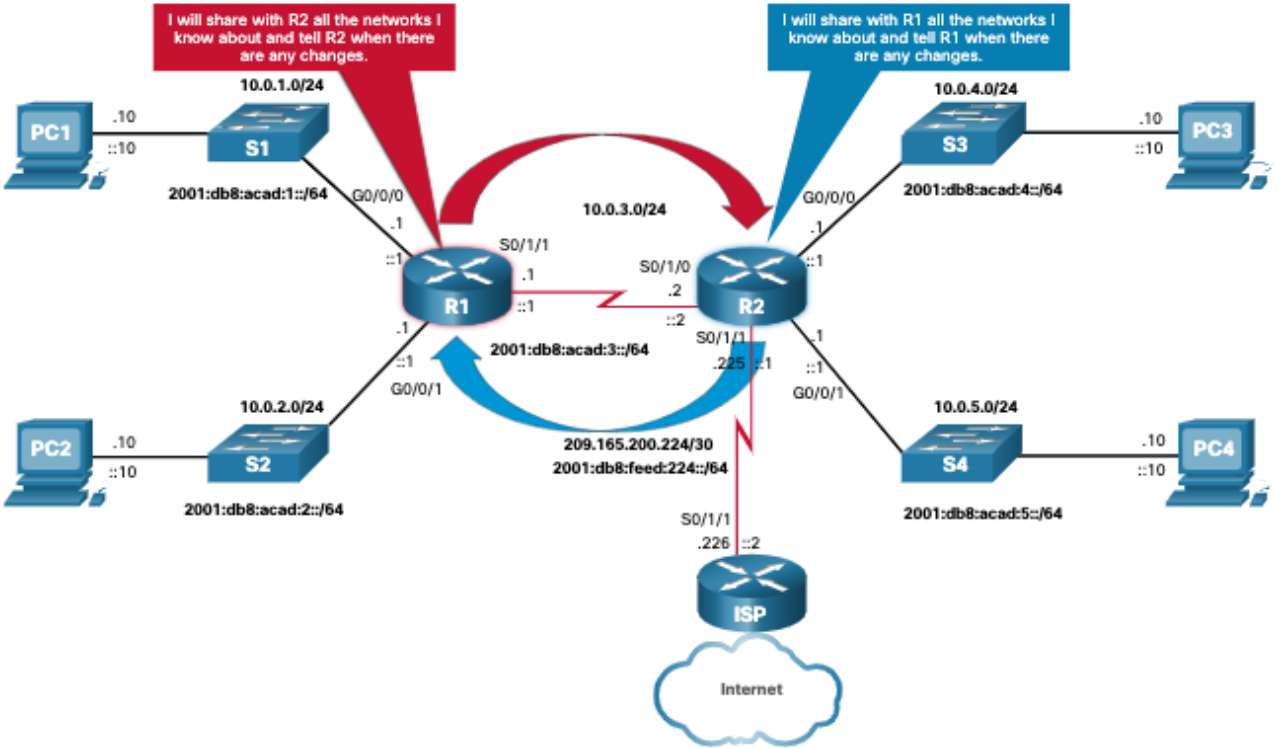
Řešení:

- VRF
- Route map

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_pi/configuration/15-s/iri-15-s-book/iri-rec-stat-route.html

Dynamic Routing Protocols

Dynamic routing protocols are used by routers to automatically share information about the reachability and status of remote networks. Dynamic routing protocols perform several activities, including network discovery and maintaining routing tables.



Dynamic Routes in the Routing Table

OSPF is now being used in our sample topology to dynamically learn all the networks connected to R1 and R2. The routing table entries use the status code of **O** to indicate the route was learned by the OSPF routing protocol. Both entries also include the IP address of the next-hop router, via *ip-address*.

Note: IPv6 routing protocols use the link-local address of the next-hop router.

Note: OSPF routing configuration for IPv4 and IPv6 is beyond the scope of this course.

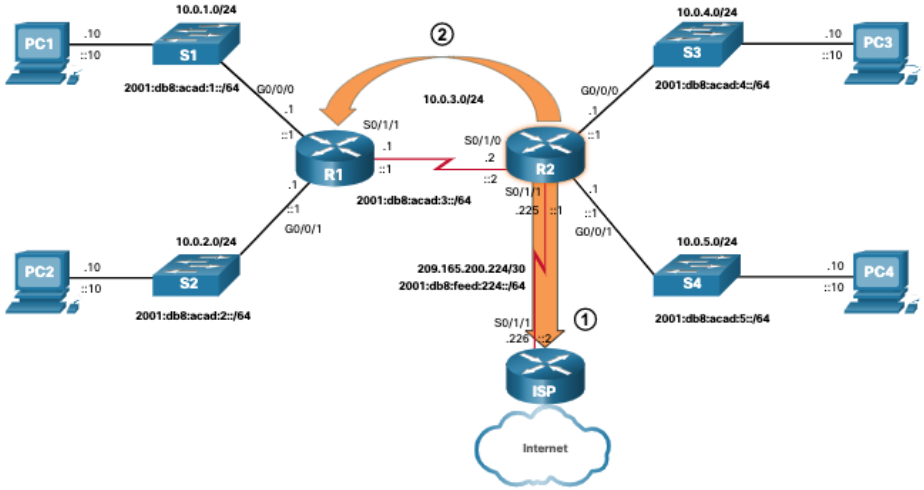
```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP D - EIGRP,
EX - EIGRP external, O - OSPF, IA - OSPF inter area
(output omitted for brevity)
O 10.0.4.0/24 [110/50] via 10.0.3.2, 00:24:22, Serial0/1/1
O 10.0.5.0/24 [110/50] via 10.0.3.2, 00:24:15, Serial0/1/1
R1# show ipv6 route
IPv6 Routing Table - default - 10 entries
(Output omitted)
NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
O 2001:DB8:ACAD:4::/64 [110/50]
   via FE80::2:C, Serial0/1/1
O 2001:DB8:ACAD:5::/64 [110/50]
   via FE80::2:C, Serial0/1/1
```

Default Route

The default route specifies a next-hop router to use when the routing table does not contain a specific route that matches the destination IP address.

A default route can be either a static route or learned automatically from a dynamic routing protocol.

A default route has an IPv4 route entry of 0.0.0.0/0 or an IPv6 route entry of ::/0. This means that zero or no bits need to match between the destination IP address and the default route.



1) **Default Gateway** (*ip default-gateway x.x.x.x*)

Tento příkaz slouží nesměrovacímu síťovému zařízení, které potřebuje dosáhnout jakékoli sítě mimo vlastní podsíť nebo mimo místní síť. Příkaz má fungovat, když síťové zařízení není v režimu směrování. Příkaz obvykle existuje u přepínačů **vrstvy 2** nebo přepínačů, které jsou pouze v režimu přemostění.

Aby tento příkaz fungoval ve směrovači, musí být zakázáno směrování IP (**no ip routing**). Když je směrování IP zakázáno, router se stane pouze hostitelem, podobně jako běžné PC. K dosažení jakékoli sítě mimo vlastní podsíť nebo mimo místní síť musí mít zařízení výchozí bránu.

2) **Default Network** (*ip default-network a.b.c.d*)

Tento příkaz vytvoří defaultní (výchozí)í podsíť nebo síť pro konkrétní směrovací zařízení. Proto musí být na zařízení nastaven **ip routing**.

Po zavedení tohoto příkazu bude síťové zařízení **vrstvy 3** ve skutečnosti směrovat pakety na rozdíl od příkazu *default-gateway*. Za druhé tento příkaz neurčuje další adresu směrování, určuje síť, která má být považována za výchozí. Aby tento příkaz nastavil výchozí síť, musíte mít ve své směrovací tabulce již statickou trasu. Můžete zjistit, zda to funguje, pomocí příkazu sh ip.

3) **Gateway of Last Resort** brána poslední instance“. (*ip route 0.0.0.0 0.0.0.0 next-hop-ip/exit-interface*)

Tento příkaz také vyžaduje nastavení **ip routing**. Tento příkaz nastaví výchozí trasu pro cokoli, co není ve směrovací tabulce. Po zadání tohoto příkazu se zobrazí „gateway of last resort neboli brána poslední instance“ nakonfigurovaná ve směrovací tabulce.

Structure of an IPv4 Routing Table

IPv4 was standardized using the now obsolete classful addressing architecture. The IPv4 routing table is organized using this same classful structure. Although the lookup process no longer uses classes, the structure of the IPv4 routing table still retains in this format.

An indented entry is known as a child route. A route entry is indented if it is the subnet of a classful address (class A, B or C network). Directly connected networks will always be indented (child routes) because the local address of the interface is always entered in the routing table as a /32. The child route will include the route source and all the forwarding information such as the next-hop address. The classful network address of this subnet will be shown above the route entry, less indented, and without a source code. That route is known as a parent route.

Structure of an IPv4 Routing Table

- An indented entry is known as a **child route**. A route entry is indented if it is the subnet of a classful address (class A, B or C network).
- Directly connected networks will always be indented (child routes) because the local address of the interface is always entered in the routing table as a /32.
- The child route will include the route source and all the forwarding information such as the next-hop address.
- The classful network address of this subnet will be shown above the route entry, less indented (odsazené), and without a source code. That route is known as a **parent route.**

```
Router# show ip route
(Output omitted)
   192.168.1.0/24 is variably..
C     192.168.1.0/24 is direct..
L     192.168.1.1/32 is direct..
O     192.168.2.0/24 [110/65]..
O     192.168.3.0/24 [110/65]..
   192.168.12.0/24 is variab..
C     192.168.12.0/30 is direct..
L     192.168.12.1/32 is direct..
   192.168.13.0/24 is variably..
C     192.168.13.0/30 is direct..
L     192.168.13.1/32 is direct..
   192.168.23.0/30 is subnette..
O     192.168.23.0/30 [110/128]..
Router#
```

Structure of an IPv6 Routing Table

The concept of classful addressing was never part of IPv6, so the structure of an IPv6 routing table is very straight forward. Every IPv6 route entry is formatted and aligned the same way.

```
R1# show ipv6 route
(output omitted for brevity)
OE2 ::/0 [110/1], tag 2
   via FE80::2:C, Serial0/0/1
C 2001:DB8:ACAD:1::/64 [0/0]
   via GigabitEthernet0/0/0, directly connected
L 2001:DB8:ACAD:1::1/128 [0/0]
   via GigabitEthernet0/0/0, receive
C 2001:DB8:ACAD:2::/64 [0/0]
  via GigabitEthernet0/0/1, directly connected
L 2001:DB8:ACAD:2::1/128 [0/0]
   via GigabitEthernet0/0/1, receive
C 2001:DB8:ACAD:3::/64 [0/0]
   via Serial0/1/1, directly connected
L 2001:DB8:ACAD:3::1/128 [0/0]
   via Serial0/1/1, receive
O 2001:DB8:ACAD:4::/64 [110/50]
   via FE80::2:C, Serial0/1/1
O 2001:DB8:ACAD:5::/64 [110/50]
   via FE80::2:C, Serial0/1/1
L FF00::/8 [0/0]
   via Null0, receive
R1#
```

Administrative Distance

A route entry for a specific network address (prefix and prefix length) can only appear once in the routing table. However, it is possible that the routing table learns about the same network address from more than one routing source. Except for very specific circumstances, only one dynamic routing protocol should be implemented on a router. Each routing protocol may decide on a different path to reach the destination based on the metric of that routing protocol.

This raises a few questions, such as the following:

- How does the router know which source to use?
- Which route should it install in the routing table?

Cisco IOS uses what is known as the administrative distance (AD) to determine the route to install into the IP routing table. The AD represents the "trustworthiness" of the route. The lower the AD, the more trustworthy the route source.

Administrative Distance (Cont.) Cisco a Juniper

Route Source	Administrative Distance
Directly connected	0
Static route	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170
Internal BGP	200

Route Source	Default Distance
Connected interface	0
Static route	1
Internal access route	2
Access route	3
External BGP	20
OSPF	110
IS-IS	115
RIP	120
Internal BGP	200
Unknown	255

Porovnání

PROTOCOL	CISCO	JUNIPER
Connected / Direct	0	0
Static	1	5
EIGRP Summary	5	-
OSPF Internal	-	10
IS-IS Level 1 Internal	-	15
IS-IS Level 2 Internal	-	18
BGP External	20	-
EIGRP Internal	90	-
OSPF All	110	-
IS-IS All	115	-
RIP	120	100
OSPF External	-	150
IS-IS Level 1 External	-	160
IS-IS Level 2 External	-	165
EIGRP External	170	-
BGP All	-	170

14.5 Static and Dynamic Routing

Static or Dynamic?

Static and dynamic routing are not mutually exclusive. Rather, most networks use a combination of dynamic routing protocols and static routes.

Static routes are commonly used in the following scenarios:

- As a default route forwarding packets to a service provider
- For routes outside the routing domain and not learned by the dynamic routing protocol
- When the network administrator wants to explicitly define the path for a specific network
- For routing between stub networks

Static routes are useful for smaller networks with only one path to an outside network. They also provide security in a larger network for certain types of traffic, or links to other networks that need more control.

Static or Dynamic? (Cont.)

Dynamic routing protocols are implemented in any type of network consisting of more than just a few routers. Dynamic routing protocols are scalable and automatically determine better routes if there is a change in the topology.

Dynamic routing protocols are commonly used in the following scenarios:

- In networks consisting of more than just a few routers
- When a change in the network topology requires the network to automatically determine another path
- For scalability. As the network grows, the dynamic routing protocol automatically learns about any new networks.

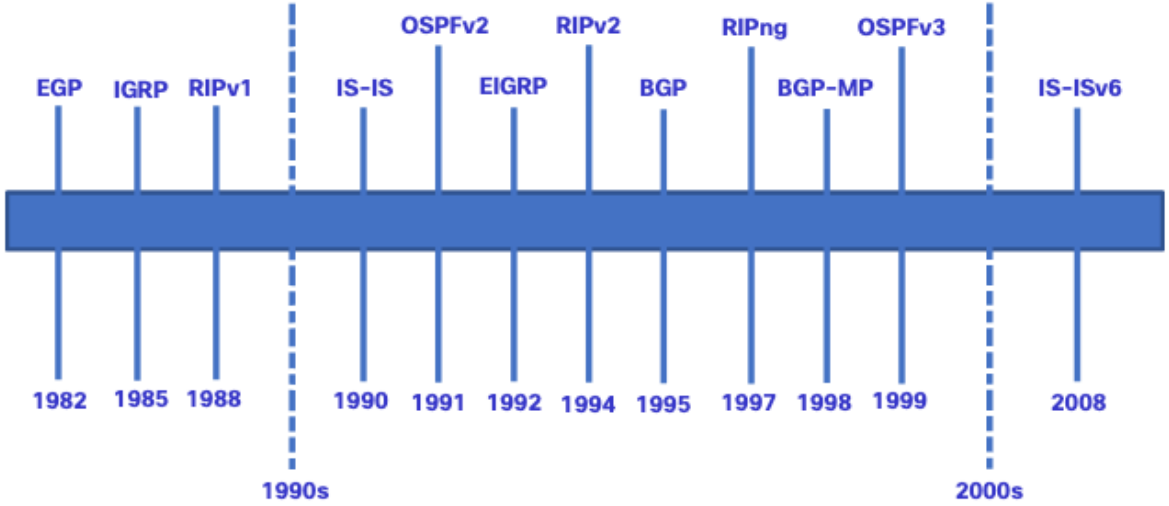
Static or Dynamic? (Cont.)

The table shows a comparison of some the differences between dynamic and static routing.

Feature	Dynamic Routing	Static Routing
Configuration complexity	Independent of network size	Increases with network size
Topology changes	Automatically adapts to topology changes	Administrator intervention required
Scalability	Suitable for simple to complex network topologies	Suitable for simple topologies
Security	Security must be configured	Security is inherent (sobě vlastní)
Resource Usage	Uses CPU, memory, and link bandwidth	No additional resources needed
Path Predictability	Route depends on topology and routing protocol used	Explicitly defined by the administrator

Dynamic Routing Evolution

Dynamic routing protocols have been used in networks since the late 1980s. One of the first routing protocols was RIP. RIPv1 was released in 1988, but some of the basic algorithms within the protocol were used on the Advanced Research Projects Agency Network (ARPANET) as early as 1969. As networks evolved and became more complex, new routing protocols emerged.



Dynamic Routing Evolution (Cont.)

The table classifies the current routing protocols. Interior Gateway Protocols (IGPs) are routing protocols used to exchange routing information within a routing domain administered by a single organization. There is only one EGP and it is BGP. BGP is used to exchange routing information between different organizations, known as autonomous systems (AS). BGP is used by ISPs to route packets over the internet. Distance vector, link-state, and path vector routing protocols refer to the type of routing algorithm used to determine best path.

	Interior Gateway Protocols				**Exterior Gateway Protocols**
	Distance Vector		Link-State		Path Vector
IPv4	RIPv2	EIGRP	OSPFv2	IS-IS	BGP-4
IPv6	RIPng	EIGRP for IPv6	OSPFv3	IS-IS for IPv6	BGP-MP

Dynamic Routing Protocol Concepts

A routing protocol is a set of processes, algorithms, and messages that are used to exchange routing information and populate the routing table with the choice of best paths. The purpose of dynamic routing protocols includes the following:

- Discovery of remote networks
- Maintaining up-to-date routing information
- Choosing the best path to destination networks
- Ability to find a new best path if the current path is no longer available

Dynamic Routing Protocol Concepts (Cont.)

The main components of dynamic routing protocols include the following:

- **Data structures -** Routing protocols typically use tables or databases for their operations. This information is kept in RAM.
- **Routing protocol messages -** Routing protocols use various types of messages to discover neighboring routers, exchange routing information, and other tasks to learn and maintain accurate information about the network.
- **Algorithm -** An algorithm is a finite list of steps used to accomplish a task. Routing protocols use algorithms for facilitating routing information and for the best path determination.

Routing protocols determine the best path, or route, to each network. That route is then offered to the routing table. The route will be installed in the routing table if there is not another routing source with a lower AD.

Best Path

The best path is selected by a routing protocol based on the value or metric it uses to determine the distance to reach a network. A metric is the quantitative value used to measure the distance to a given network. The best path to a network is the path with the lowest metric.

Dynamic routing protocols typically use their own rules and metrics to build and update routing tables. The following table lists common dynamic protocols and their metrics.

Routing Protocol	Metric
Routing Information Protocol (RIP)	•The metric is “hop count”. •Each router along a path adds a hop to the hop count. •A maximum of 15 hops allowed.
Open Shortest Path First (OSPF)	•The metric is “cost” which is the based on the cumulative bandwidth from source to destination. •Faster links are assigned lower costs compared to slower (higher cost) links.
Enhanced Interior Gateway Routing Protocol (EIGRP)	•It calculates a metric based on the slowest bandwidth and delay values. •It could also include load and reliability into the metric calculation.

Load Balancing

When a router has two or more paths to a destination with equal cost metrics, then the router forwards the packets using both paths equally. This is called equal cost load balancing.

- The routing table contains the single destination network, but has multiple exit interfaces, one for each equal cost path. The router forwards packets using the multiple exit interfaces listed in the routing table.
- If configured correctly, load balancing can increase the effectiveness and performance of the network.
- Equal cost load balancing is implemented automatically by dynamic routing protocols. It is enabled with static routes when there are multiple static routes to the same destination network using different next-hop routers.

Note: Only EIGRP supports unequal cost load balancing.

14.6 Module Practice and Quiz

- Téma 14.1
- Jak bychom mohli využít pravidla nejdelší shody k naší výhodě a zmenšit velikost směrovací tabulky?
- Proč si myslíte, že jsou do směrovací tabulky přidány přímo připojené sítě?

- Téma 14.2
- Co se v paketu/rámci musí změnit pokaždé, když se paket pohybuje směrovačem?
- Jaká je primární odpovědnost routeru v procesu předávání paketů?

- Téma 14.3
- Jaký je rozdíl v informacích, které vám dávají příkazy `show interface` a `show ip interface`?

- Téma 14.4
- Zeptejte se studentů na jejich vlastní analogii toho, co je administrativní vzdálenost.
- Požádejte studenty, aby vysvětlili označení /0 pro výchozí trasu vlastními slovy.

- Téma 14.5
- Směrovací protokoly jsou obecně kategorizovány jako IGP nebo EGP. Jaký je v tom rozdíl?
- Požádejte studenty, aby vysvětlili zjišťování vzdálených sítí jejich vlastními slovy.

What Did I Learn In This Module?

- The primary functions of a router are to determine the best path to forward packets based on the information in its routing table, and to forward packets toward their destination.
- The best path in the routing table is also known as the longest match. The longest match is the route in the routing table that has the greatest number of far-left matching bits with the destination IP address of the packet.
- Directly connected networks are networks that are configured on the active interfaces of a router. A directly connected network is added to the routing table when an interface is configured with an IP address and subnet mask (prefix length) and is active (up and up).
- Routers learn about remote networks in two ways: static routes and with dynamic routing protocols.
- After a router determines the correct path, it can forward the packet on a directly connected network, it can forward the packet to a next-hop router, or it can drop the packet.
- Routers support three packet forwarding mechanisms: process switching, fast switching, and CEF.
- There are several configuration and verification commands for routers, including **show ip route, show ip interface, show ip interface brief and show running-config**.

What Did I Learn In This Module? (Cont.)

- A routing table contains a list of routes known networks (prefixes and prefix lengths). The source of this information is derived from directly connected networks, static routes, and dynamic routing protocols.
- Every router makes its decision alone, based on the information it has in its own routing table. The information in a routing table of one router does not necessarily match the routing table of another router.
- Routing information about a path does not provide return routing information.
- Routing table entries include the route source, destination network, AD, metric, next-hop, route timestamp, and exit interface.
- Static routes are manually configured and define an explicit path between two networking devices.
- Dynamic routing protocols can discover a network, maintain routing tables, select a best path, and automatically discover a new best path if the topology changes.
- The default route specifies a next-hop router to use when the routing table does not contain a specific route that matches the destination IP address. A default route can be either a static route or learned automatically from a dynamic routing protocol.

What Did I Learn In This Module? (Cont.)

- IPv4 routing tables still have a structure based on classful addressing represented by levels of indentation. IPv6 routing tables do not use the IPv4 routing table structure.
- Cisco IOS uses what is known as the administrative distance (AD) to determine the route to install into the IP routing table. The AD represents the "trustworthiness" of the route. The lower the AD, the more trustworthy the route source.
- Static routes are commonly used as a default route forwarding packets to a service provider, for routes outside the routing domain and not learned by the dynamic routing protocol, when the network administrator wants to explicitly define the path for a specific network, or for routing between stub networks.
- Dynamic routing protocol are commonly used in networks consisting of more than just a few routers, when a change in the network topology requires the network to automatically determine another path, and for scalability. As the network grows, the dynamic routing protocol automatically learns about any new networks.
- Current routing protocols include IGPs and EGPs. IGPs exchange routing information within a routing domain administered by a single organization. The only EGP is BGP. BGP exchanges routing information between different organizations.BGP is used by ISPs to route packets over the internet.

What Did I Learn In This Module? (Cont.)

- Distance vector, link-state, and path vector routing protocols refer to the type of routing algorithm used to determine best path.
- The main components of dynamic routing protocols are data structures, routing protocol messages, and algorithms.
- The best path is selected by a routing protocol based on the value or metric it uses to determine the distance to reach a network. The best path to a network is the path with the lowest metric.
- When a router has two or more paths to a destination with equal cost metrics, then the router forwards the packets using both paths equally. This is called equal cost load balancing.


CISCO