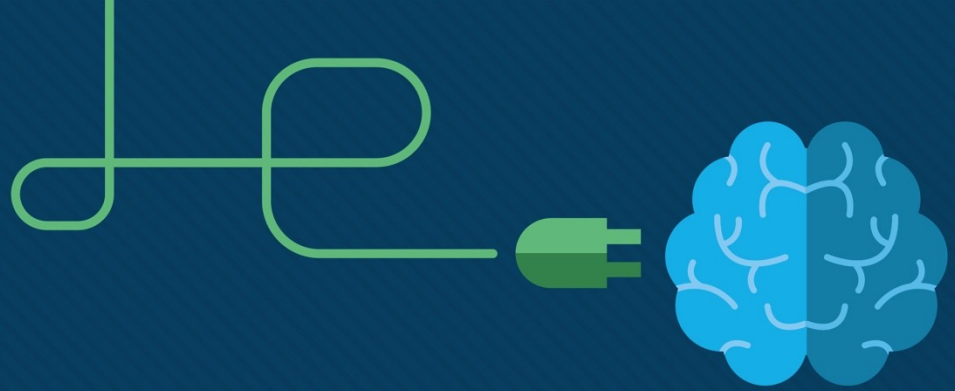


Chapter 4: Access Control Lists

CCNA Routing and Switching

Connecting Networks v6.0

4.1 Standard ACL Operation and Configuration Review

Types of IPv4 ACLs

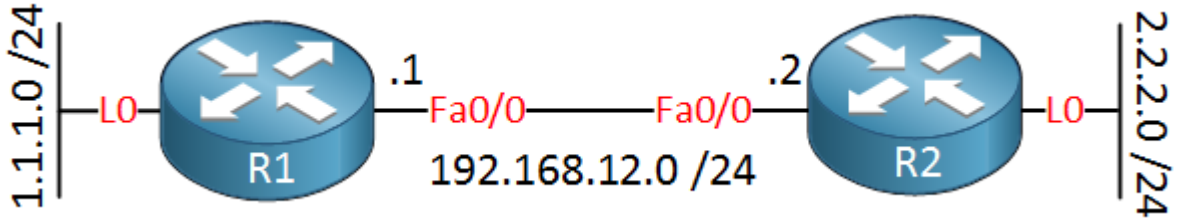
- Standard ACLs filter packets based on the source address only.

```
access-list 10 permit 192.168.30.0 0.0.0.255
```

- Extended ACLs filter packets based on:
  - Protocol type / Protocol number (e.g., IP, ICMP, UDP, TCP, …)
  - Source and destination IP addresses
  - Source and Destination TCP and UDP ports

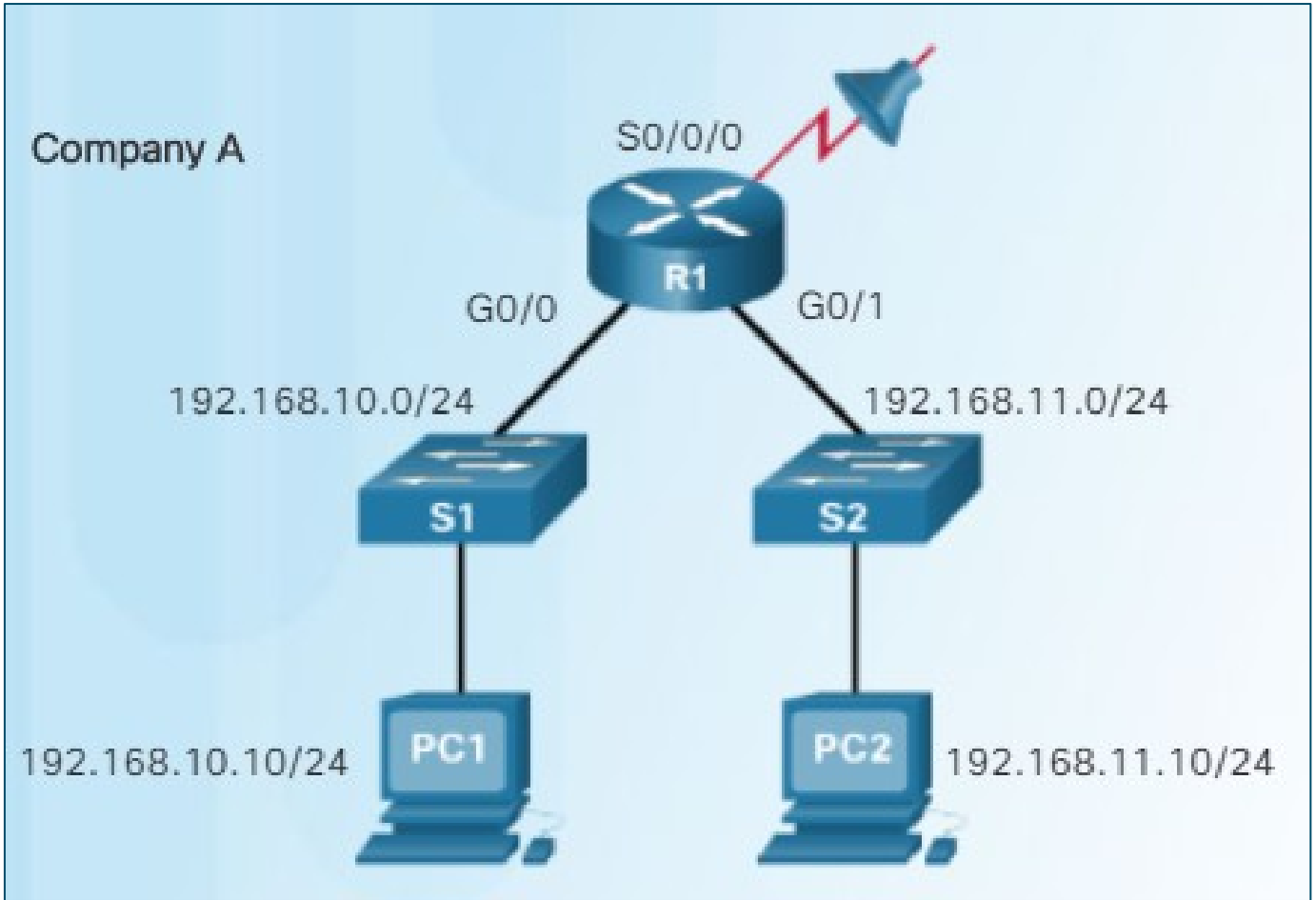
```
access-list 103 permit tcp 192.168.30.0 0.0.0.255 any eq 80
```

Převeďte standardní řešení na rozšířené

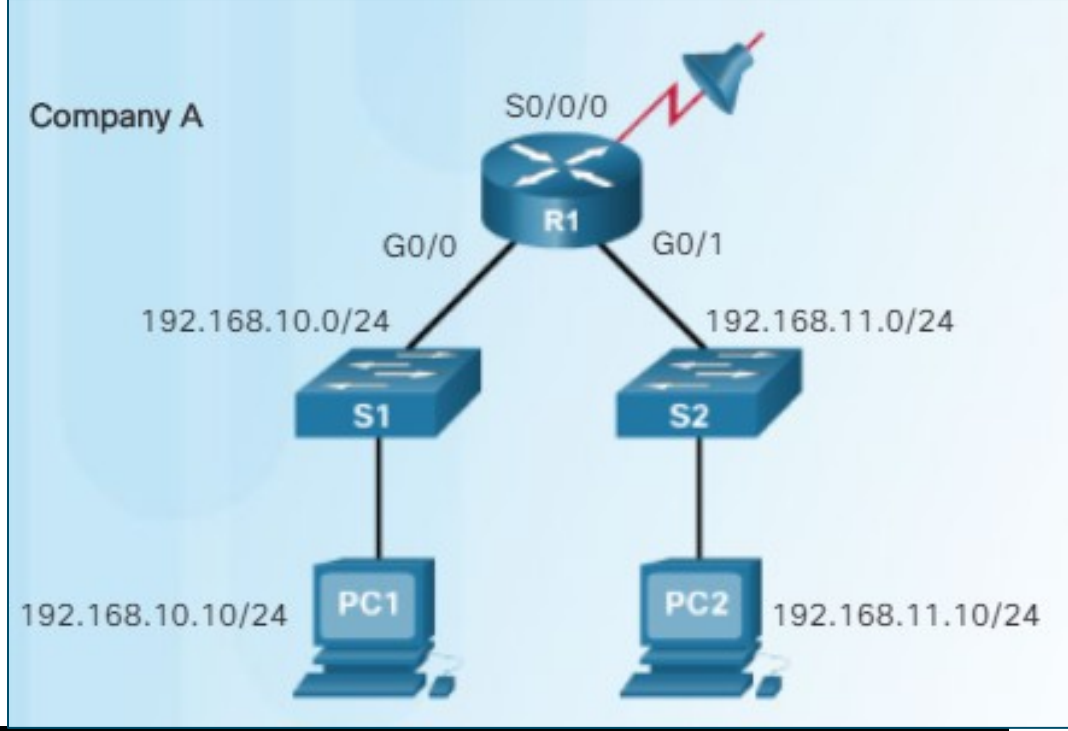


- R1(config)**#ip route 2.2.2.0 255.255.255.0 192.168.12.2**
- R2(config)**#ip route 1.1.1.0 255.255.255.0 192.168.12.1**
- R2(config)**#access-list 1 permit 192.168.12.0 0.0.0.255**
- R2(config)**#interface fastEthernet 0/0**
- R2(config-if)**#ip access-group 1 in**

Povolit ze sítě 192.168.10.0 do sítě za S0/0/0



Řešení




```
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)# interface s0/0/0
R1(config-if)# ip access-group 1 out
```

4.2 Extended IPv4 ACLs

An application can be specified by configuring either:

- The port number

```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 23
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 21
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 20
```

- The name of a well-known port

```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq telnet
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp-data
```

TCP and UDP

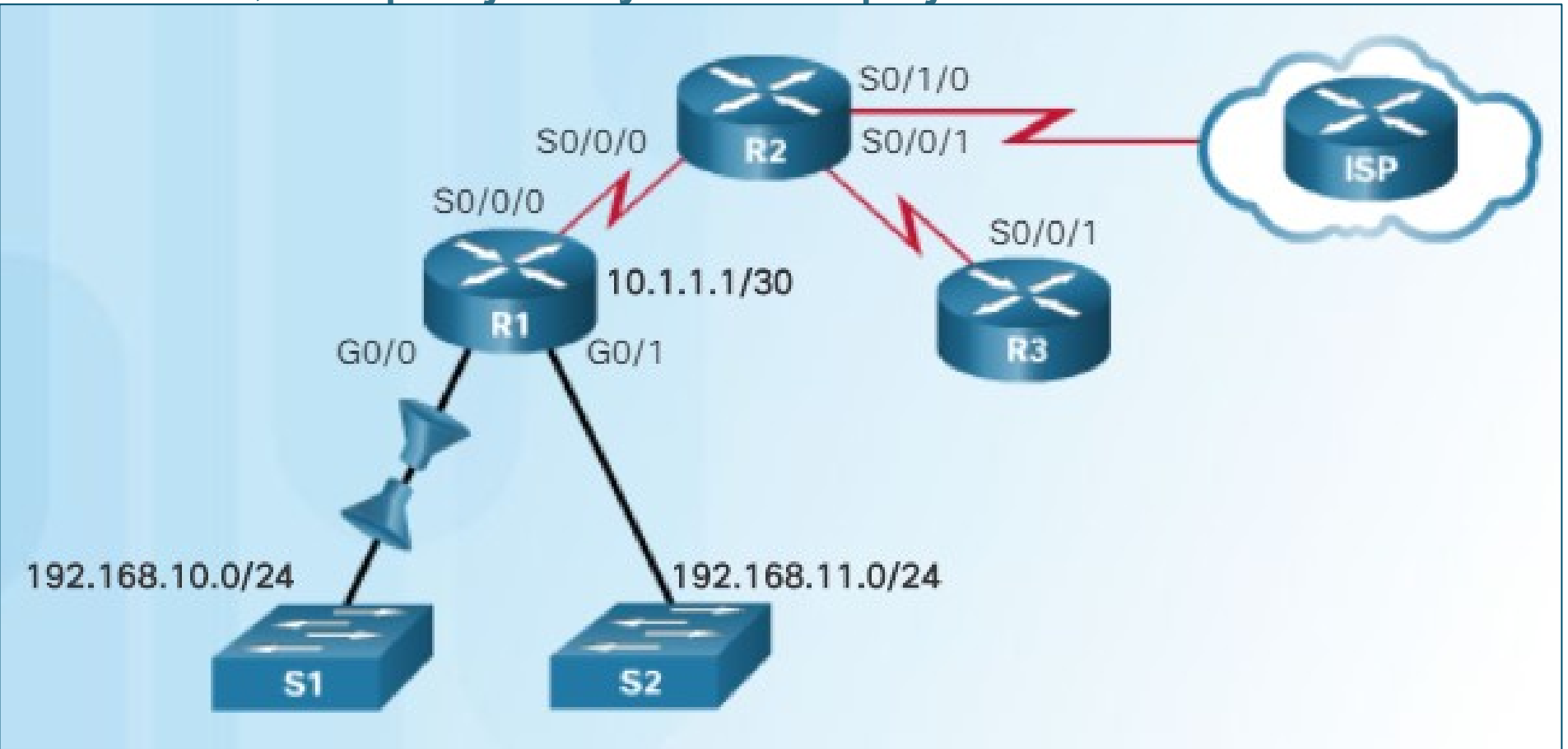
Port Number	Protocol	Application	Acronym
20	TCP	File Transfer Protocol (data)	FTP
21	TCP	File Transfer Protocol (control)	FTP
22	TCP	Secure Shell	SSH
23	TCP	Telnet	–
25	TCP	Simple Mail Transfer Protocol	SMTP
53	UDP, TCP	Domain Name Service	DNS
67	UDP	Dynamic Host Configuration Protocol (server)	DHCP
68	UDP	Dynamic Host Configuration Protocol (client)	DHCP
69	UDP	Trivial File Transfer Protocol	TFTP
80	TCP	Hypertext Transfer Protocol	HTTP
110	TCP	Post Office Protocol version 3	POP3
143	TCP	Internet Message Access Protocol	IMAP
161	UDP	Simple Network Management Protocol	SNMP
443	TCP	Hypertext Transfer Protocol Secure	HTTPS

Pomůcka

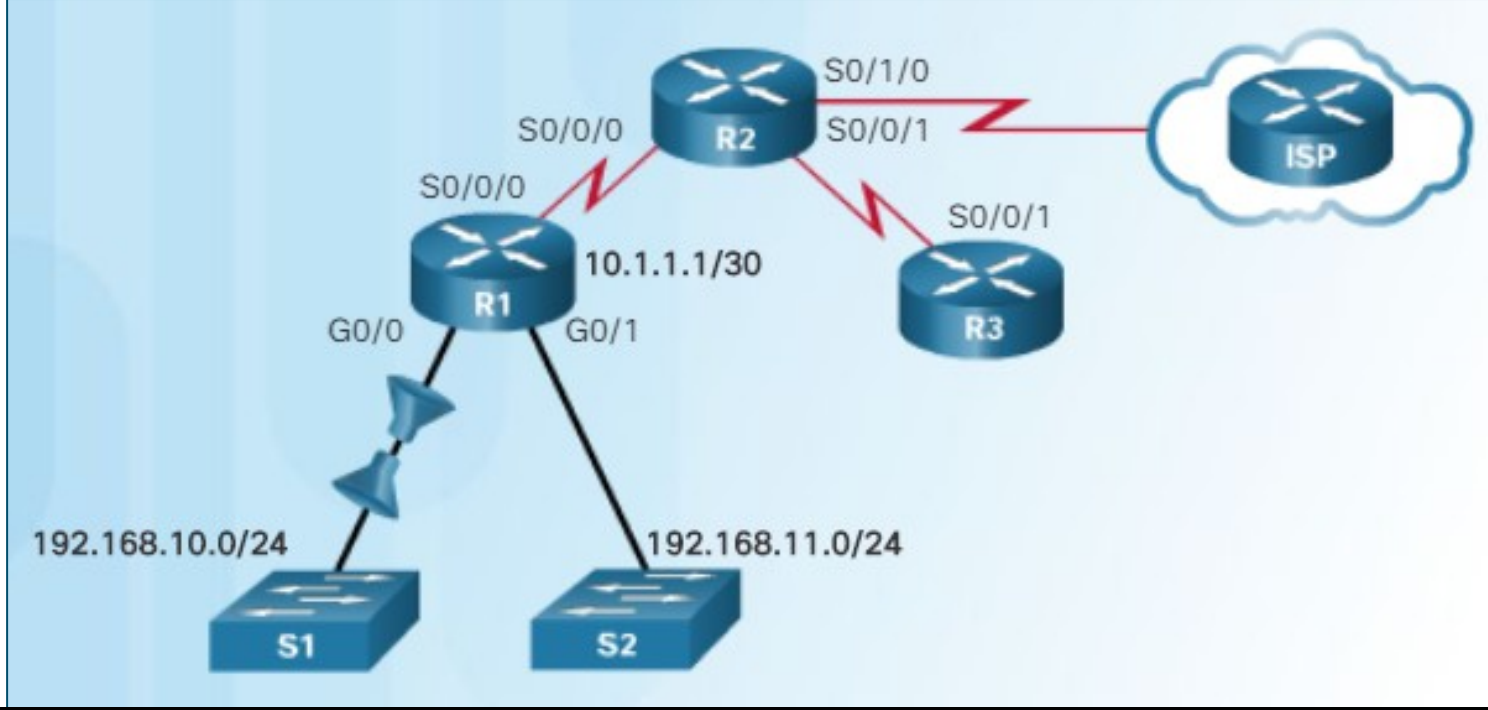
- Use ? to see available well-known port names:

access-list 101 permit tcp any any eq ?

Zadání: povoleno HTTP a HTTPS ze sítě 192.168.10.0 kamkoliv, nazpět jen vyzvaná spojení

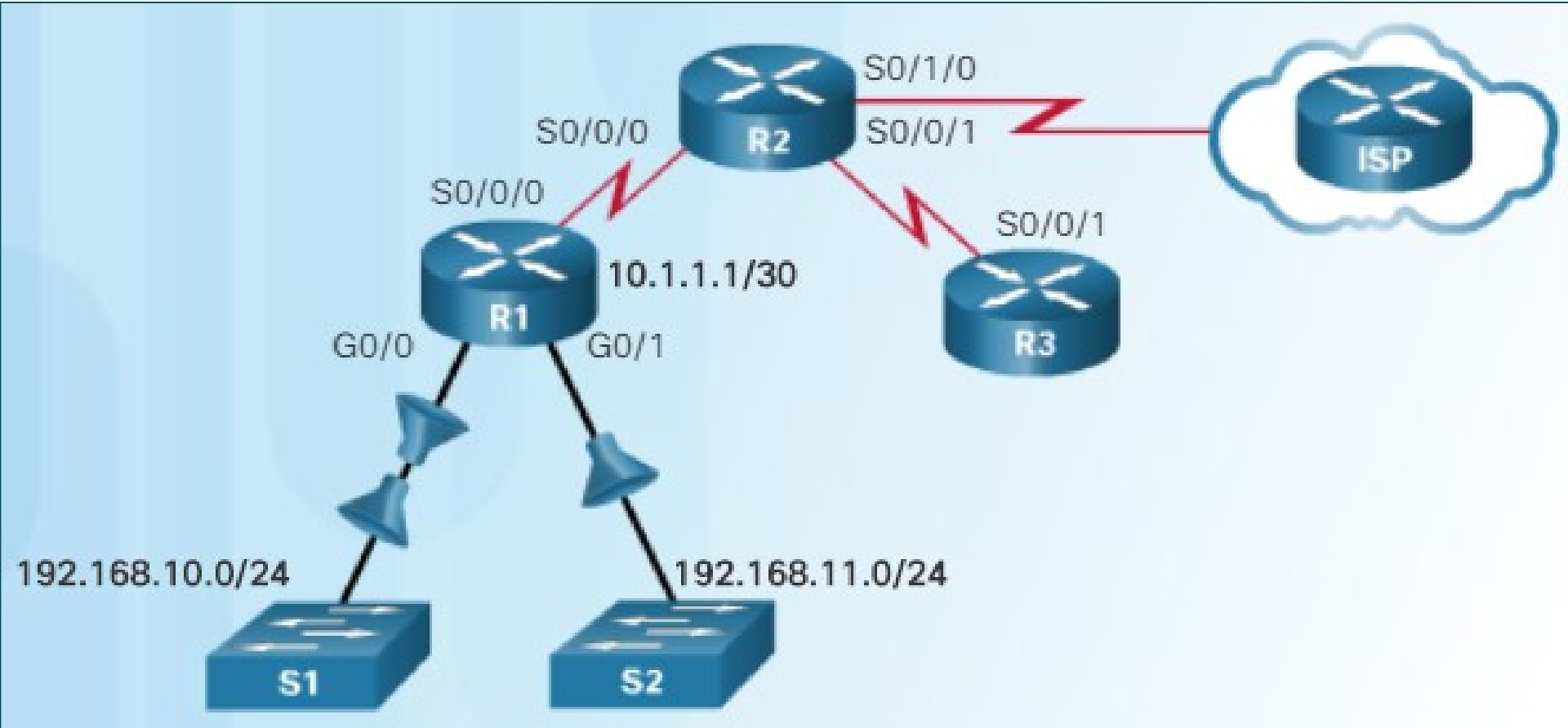


Řešení

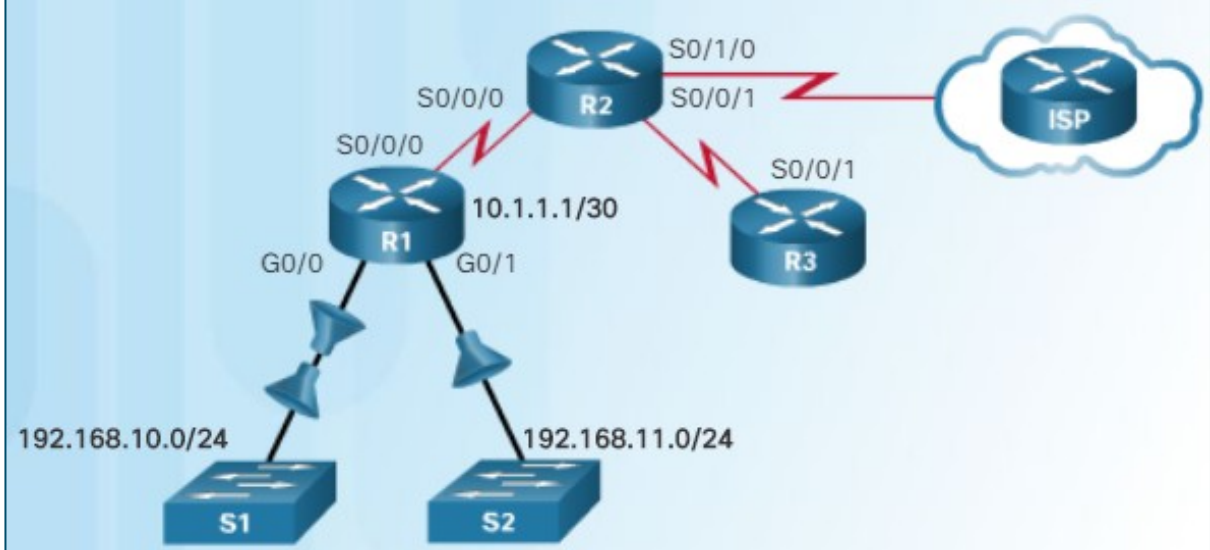



```
R1(config)# access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config)# access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config)# access-list 104 permit tcp any 192.168.10.0 0.0.0.255 established
R1(config)# interface g0/0
R1(config-if)# ip access-group 103 in
R1(config-if)# ip access-group 104 out
```

Zadání: Zákaz ftp ze 192.168.11.0 do 192.168.10.0

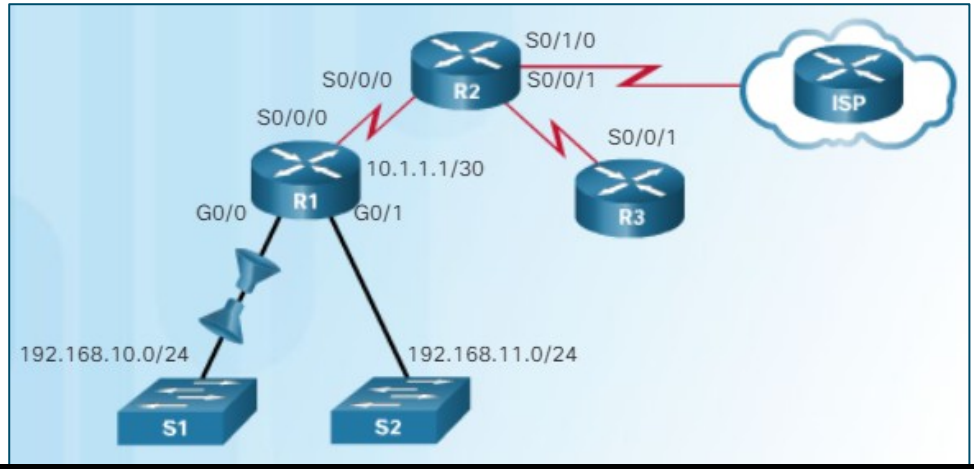


Řešení




```
R1(config)# access-list 101 deny tcp 192.168.11.0 0.0.0.255
192.168.10.0 0.0.0.255 eq ftp
R1(config)# access-list 101 deny tcp 192.168.11.0 0.0.0.255
192.168.10.0 0.0.0.255 eq ftp-data
R1(config)# access-list 101 permit ip any any
R1(config)# interface g0/1
R1(config-if)#ip access-group 101 in
```

Totéž pojmenované



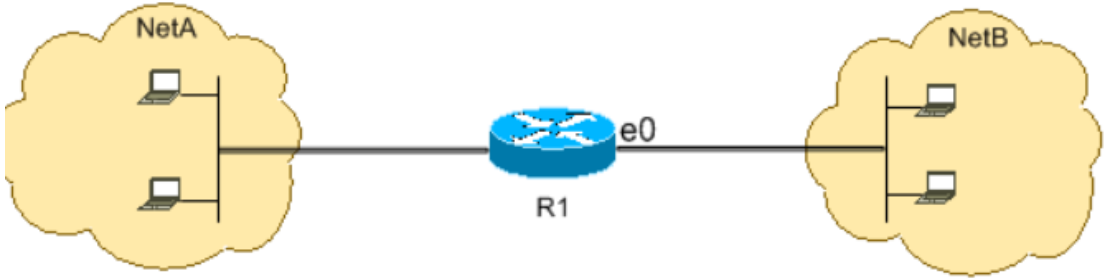

```
R1(config)# ip access-list extended SURFING
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config-ext-nacl)# exit
R1(config)# ip access-list extended BROWSING
R1(config-ext-nacl)# permit tcp any 192.168.10.0 0.0.0.255 established
R1(config-ext-nacl)# exit
R1(config)# interface g0/0
R1(config-if)# ip access-group SURFING in
R1(config-if)# ip access-group BROWSING out
```

A jak je to s routingem?

- access-list 102 permit udp any any eq rip
- access-list 102 permit eigrp any any
- access-list 102 permit ospf any any
- access-list 102 permit tcp any any eq 179
- access-list 102 permit tcp any eq 179 any

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

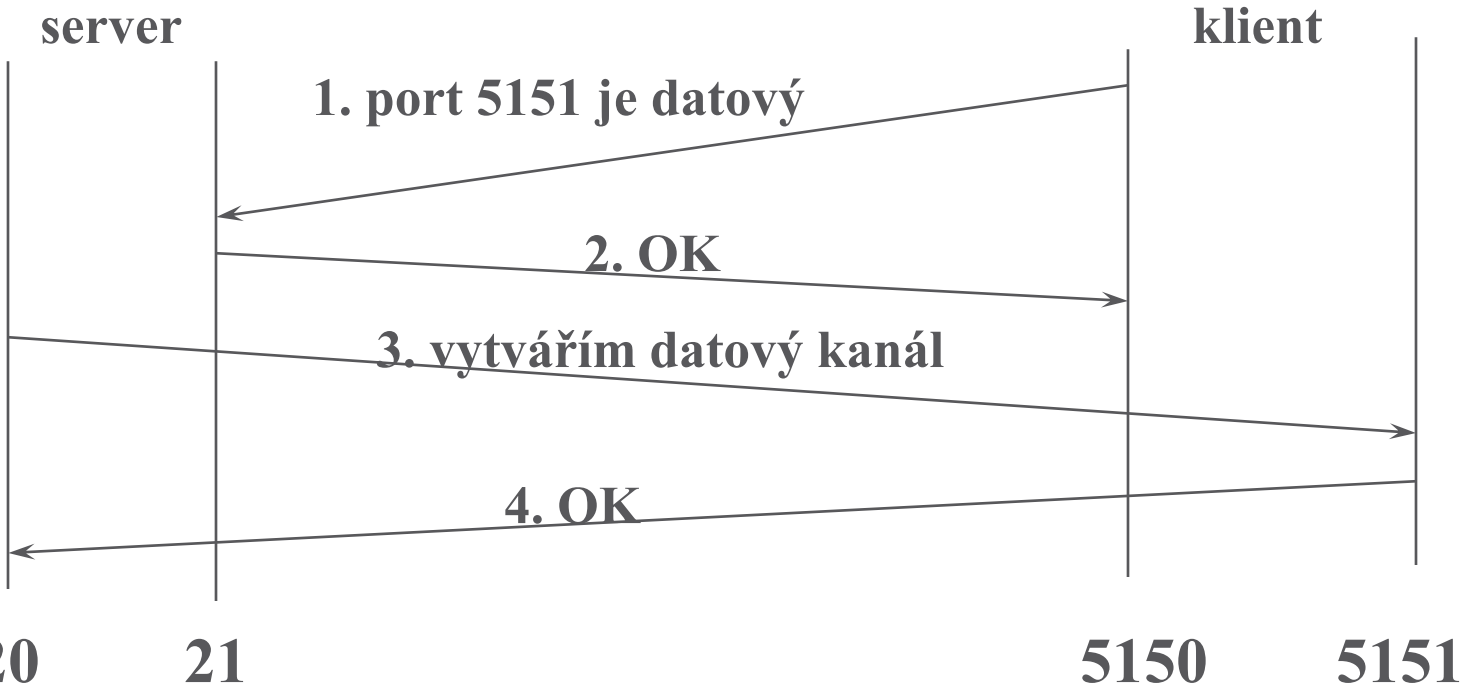
Deny FTP Traffic (TCP, Port 21 řízení, 20 - data)



hostname R1
interface ethernet0
ip access-group 102 in

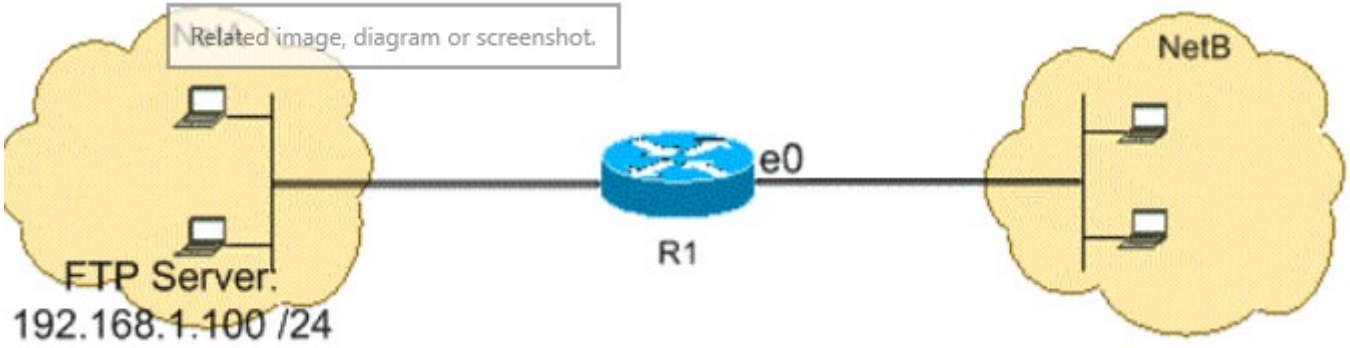
access-list 102 deny tcp any any eq ftp
access-list 102 deny tcp any any eq ftp-data
access-list 102 permit ip any any

FTP - normal mode



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

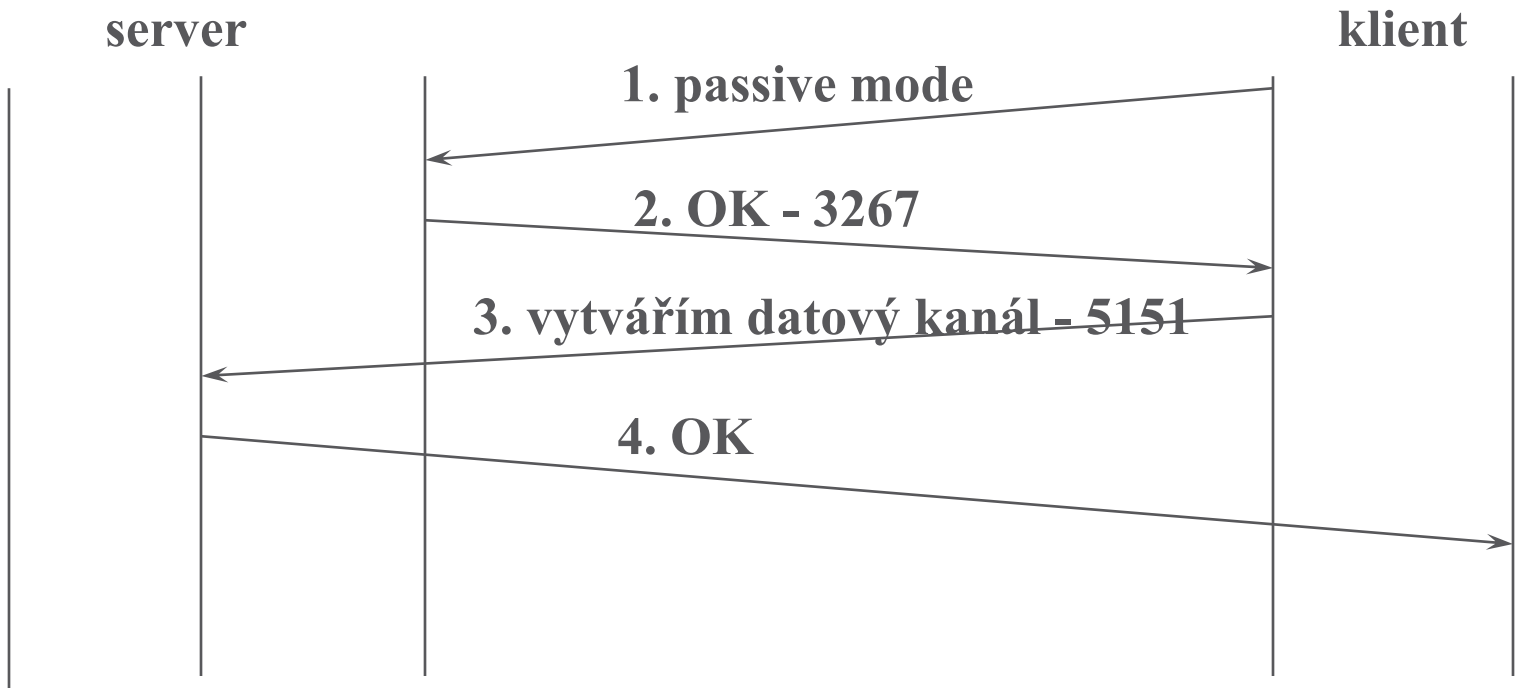
Allow FTP Traffic (Active FTP)



hostname R1
interface ethernet0
ip access-group 102 in
access-list 102 permit tcp any host 192.168.1.100 eq ftp
access-list 102 permit tcp any host 192.168.1.100 eq ftp-data established

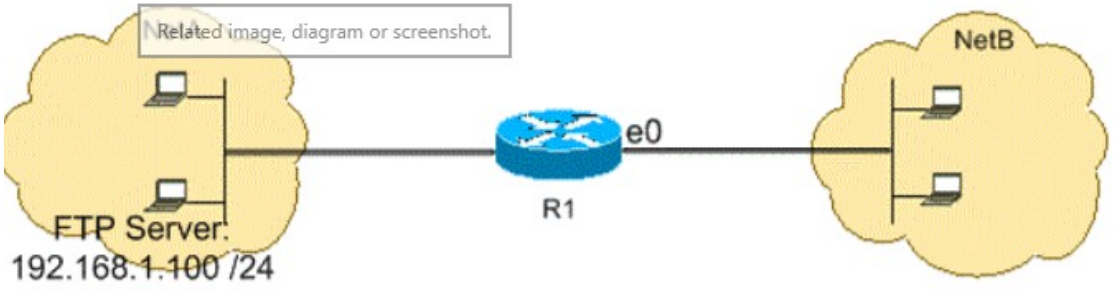
interface ethernet1
ip access-group 110 in
access-list 110 permit host 192.168.1.100 eq ftp any established
access-list 110 permit host 192.168.1.100 eq ftp-data any

FTP - passive mode (prohlížeče)



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Allow FTP Traffic (Passive FTP)



hostname R1
interface ethernet0
ip access-group 102 in
access-list 102 permit tcp any host 192.168.1.100 eq ftp
access-list 102 permit tcp any host 192.168.1.100 gt 1023

interface ethernet1
ip access-group 110 in
access-list 110 permit host 192.168.1.100 eq ftp any established
access-list 110 permit host 192.168.1.100 gt 1023 any established

4.3 IPv6 ACLs

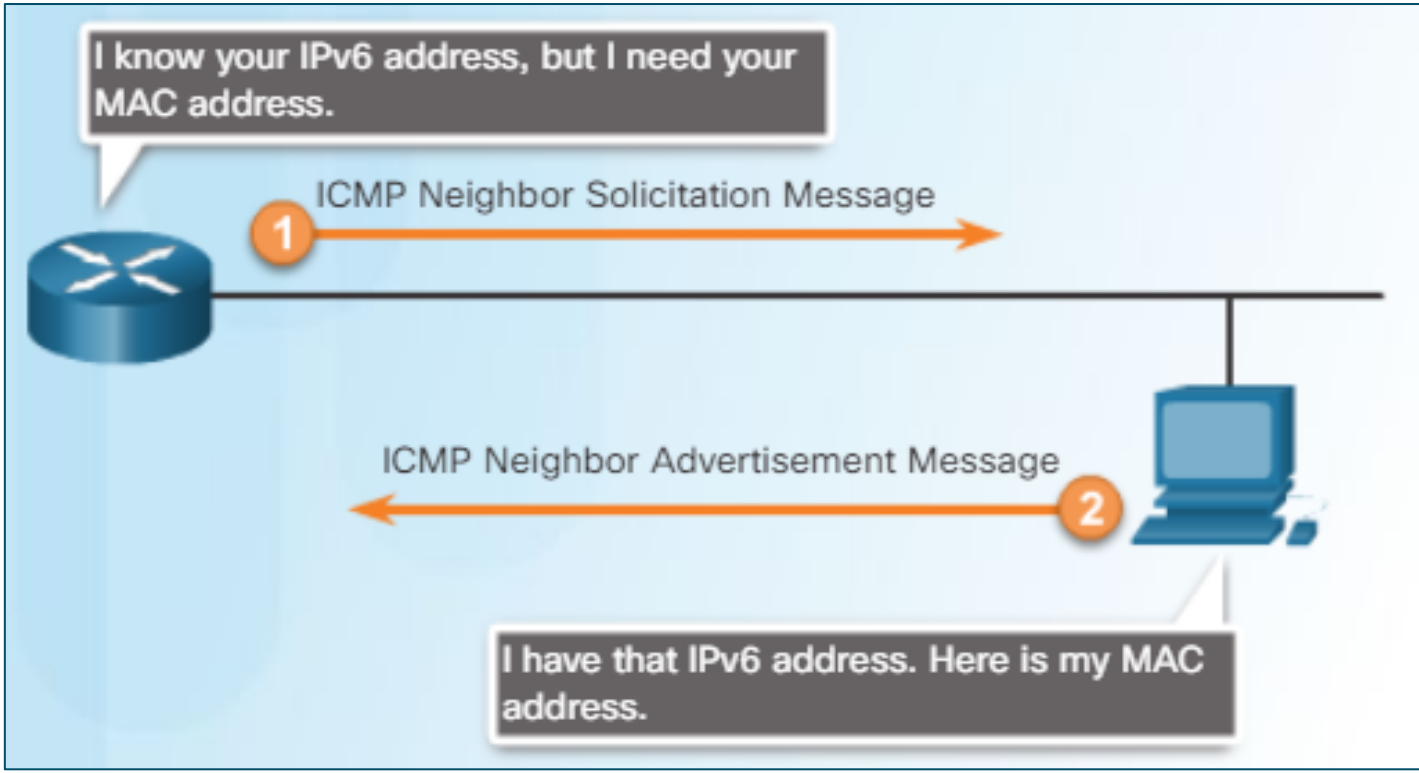
IPv6 ACL Creation

Note: An IPv4 ACL and an IPv6 ACL cannot share the same name.

Three significant differences between IPv4 and IPv6 ACLs

- The command used to apply an IPv6 ACL to an interface is **ipv6 traffic-filter** command.
- IPv6 ACLs do not use wildcard masks but instead specifies the prefix-length.
- An IPv6 ACL adds two implicit permit statements at the end of each IPv6 access list.
  - **permit icmp any any nd-na**
  - **permit icmp any any nd-ns**
  - **deny ipv6 any any statement**

Něco navíc



Two additional statements

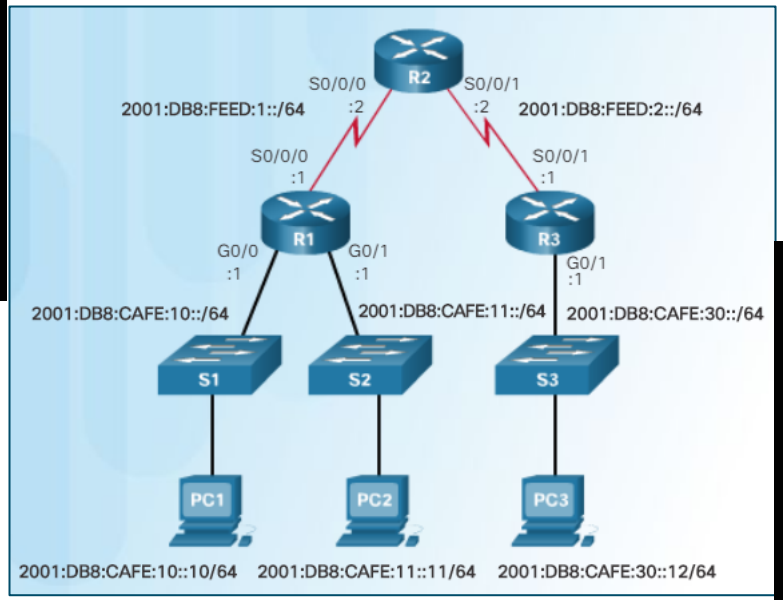
- **permit icmp any any nd-na**
- **permit icmp any any nd-ns**

allow IPv6 ICMP Neighbor Discovery (ND) and Neighbor Solicitation (NS) messages to accomplish the same thing as IPv4 ARP.

Výchozí konfigurace pro příklad

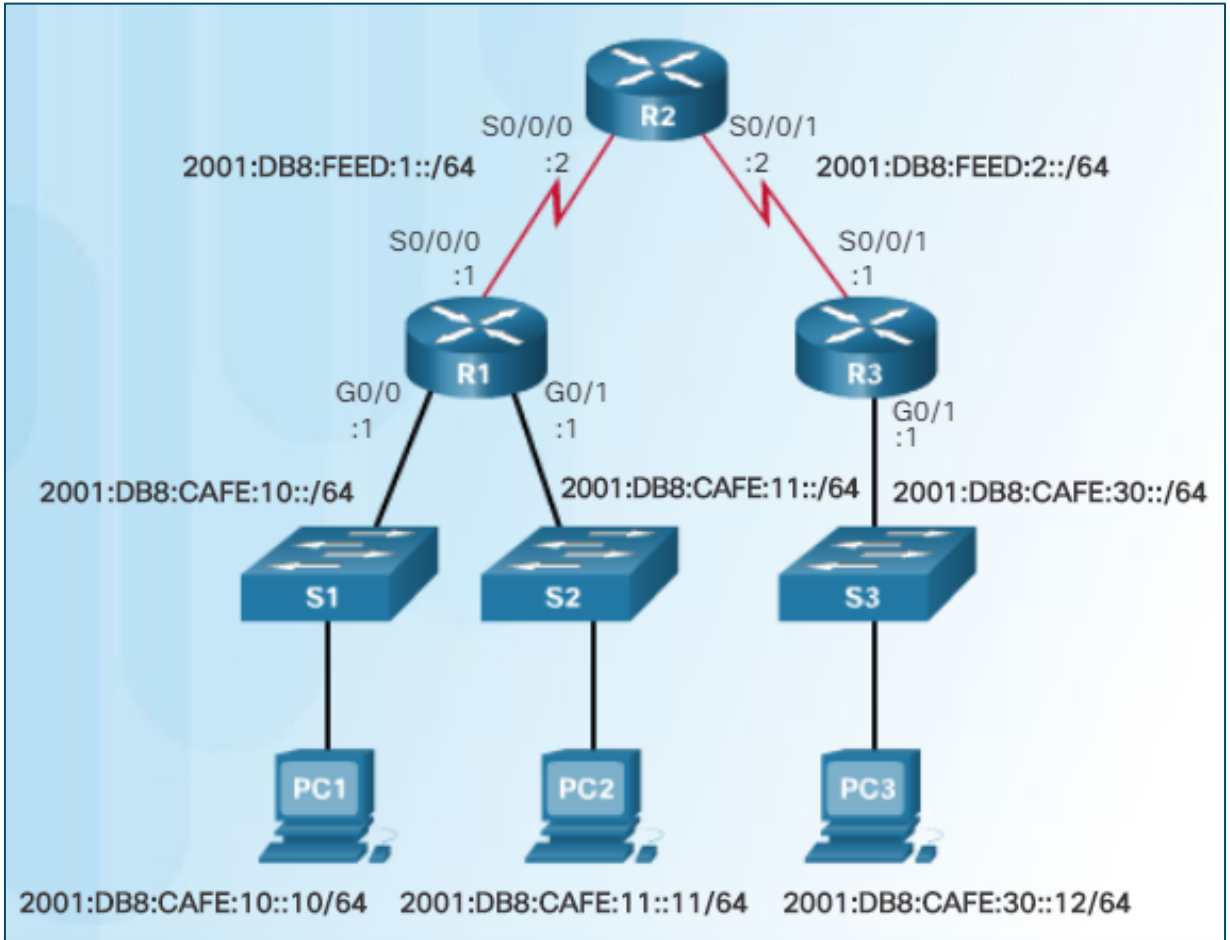
```
R1# show ipv6 interface brief
GigabitEthernet0/0      [up/up]
    FE80::FE99:47FF:FE75:C3E0
    2001:DB8:CAFE:10::1
GigabitEthernet0/1      [up/up]
    FE80::FE99:47FF:FE75:C3E1
    2001:DB8:CAFE:11::1
Serial0/0/0             [up/up]
    FE80::FE99:47FF:FE75:C3E0
    2001:DB8:FEED:1::1
 <output omitted>
R1#
```

```
R2# show ipv6 interface brief
Serial0/0/0             [up/up]
    FE80::FE99:47FF:FE71:78A0
    2001:DB8:FEED:1::2
Serial0/0/1             [up/up]
    FE80::FE99:47FF:FE71:78A0
    2001:DB8:FEED:2::2
 <output omitted>
R2#
```

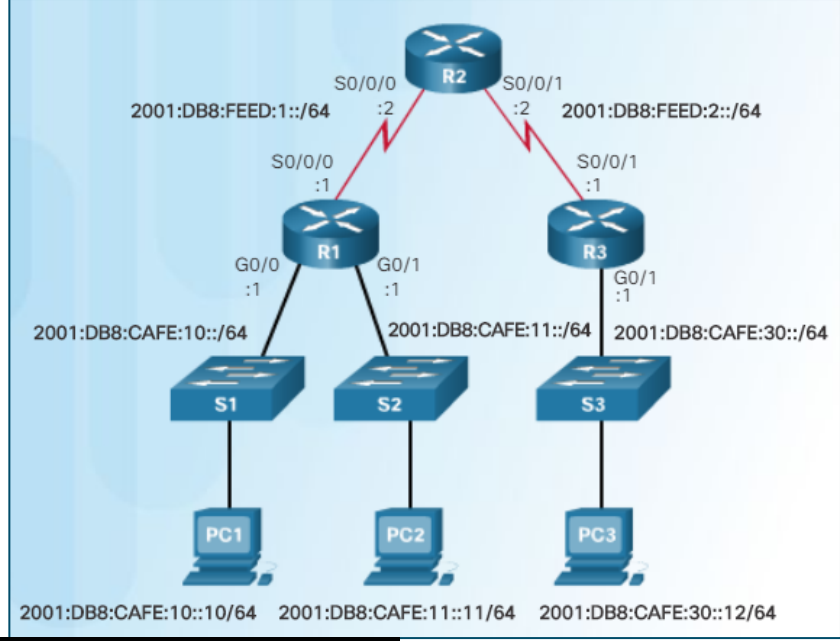



```
R3# show ipv6 interface brief
GigabitEthernet0/0      [up/up]
    FE80::FE99:47FF:FE71:7A20
    2001:DB8:CAFE:30::1
Serial0/0/1             [up/up]
    FE80::FE99:47FF:FE71:7A20
    2001:DB8:FEED:2::1
R3#
```

Zadání: Zákaz ze sítě 2001:DB8:CAFE:30::/64, ostatní povoleny



Řešení: Zákaz ze sítě 2001:DB8:CAFE:30::/64, ostatní povoleny

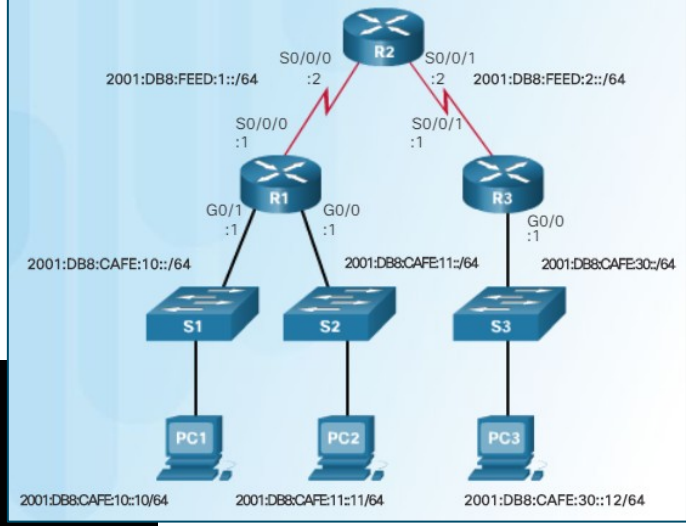



```
R1(config)# ipv6 access-list NO-R3-LAN-ACCESS
R1(config-ipv6-acl)# deny ipv6 2001:db8:cafe:30::/64 any
R1(config-ipv6-acl)# permit ipv6 any any
R1(config-ipv6-acl)# end
R1#

R1(config)# interface s0/0/0
R1(config-if)# ipv6 traffic-filter NO-R3-LAN-ACCESS in
```

All rights reserved. Cisco Confidential

Analyzujte omezení:

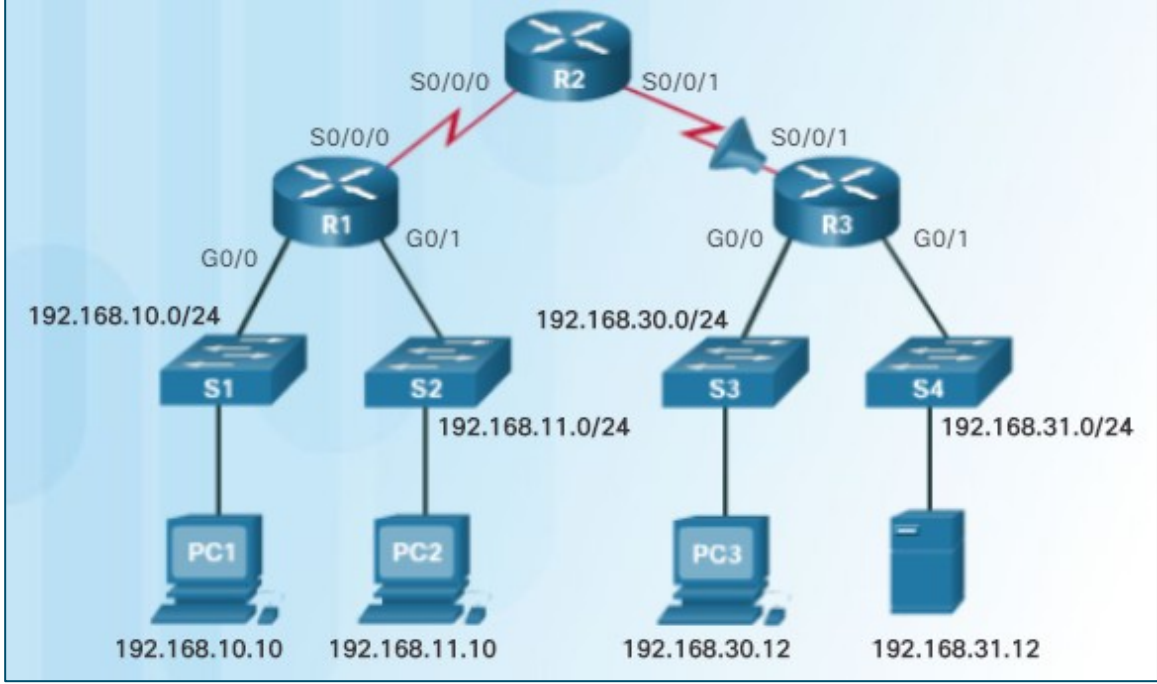



```
R3(config)# ipv6 access-list RESTRICTED-ACCESS
R3(config-ipv6-acl)# remark Permit access only HTTP and HTTPS to Network 10
R3(config-ipv6-acl)# permit tcp any host 2001:db8:cafe:10::10 eq 80
R3(config-ipv6-acl)# permit tcp any host 2001:db8:cafe:10::10 eq 443
R3(config-ipv6-acl)# remark Deny all other traffic to Network 10
R3(config-ipv6-acl)# deny ipv6 any 2001:db8:cafe:10::/64
R3(config-ipv6-acl)# remark Permit PC3 telnet access to PC2
R3(config-ipv6-acl)# permit tcp host 2001:DB8:CAFE:30::12 host 2001:DB8:CAFE:11::11 eq 23
R3(config-ipv6-acl)# remark Deny telnet access to PC2 for all other devices
R3(config-ipv6-acl)# deny tcp any host 2001:db8:cafe:11::11 eq 23
R3(config-ipv6-acl)# remark Permit access to everything else
R3(config-ipv6-acl)# permit ipv6 any any
R3(config-ipv6-acl)# exit
R3(config)# interface g0/0
R3(config-if)# ipv6 traffic-filter RESTRICTED-ACCESS in
R3(config-if)#
```

1
2
3
4
5
6

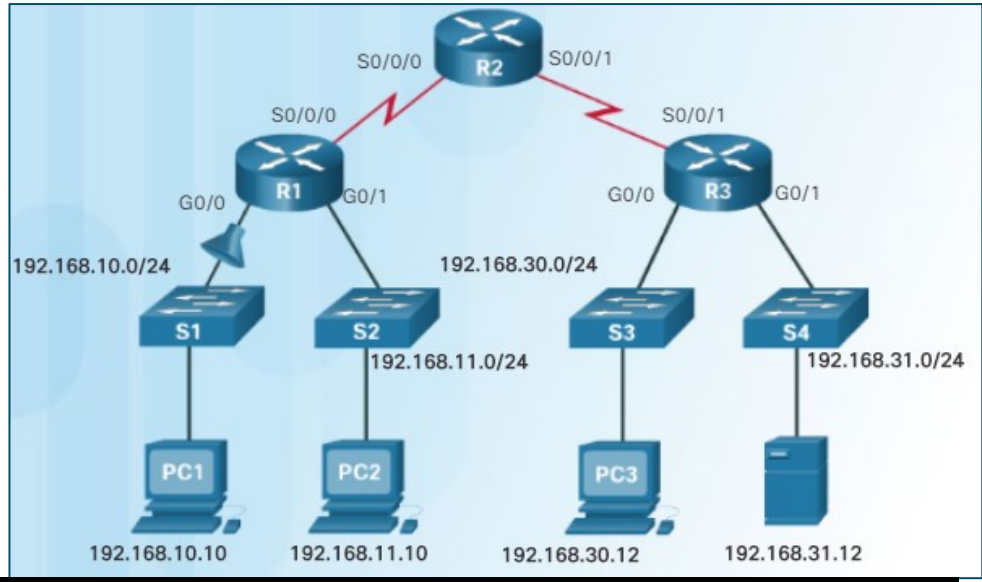
4.4 Troubleshoot ACLs

host 192.168.10.10 has no Telnet connectivity with 192.168.30.12
už je vše zakázáno předchozím pravidlem




```
R3# show access-lists
Extended IP access list 110
    10 deny tcp 192.168.10.0 0.0.0.255 any (12 match(es))
    20 permit tcp 192.168.10.0 0.0.0.255 any eq telnet
    30 permit ip any any
```

Chci TFTP z 192.168.10.0/24 do 192.168.30.0/24

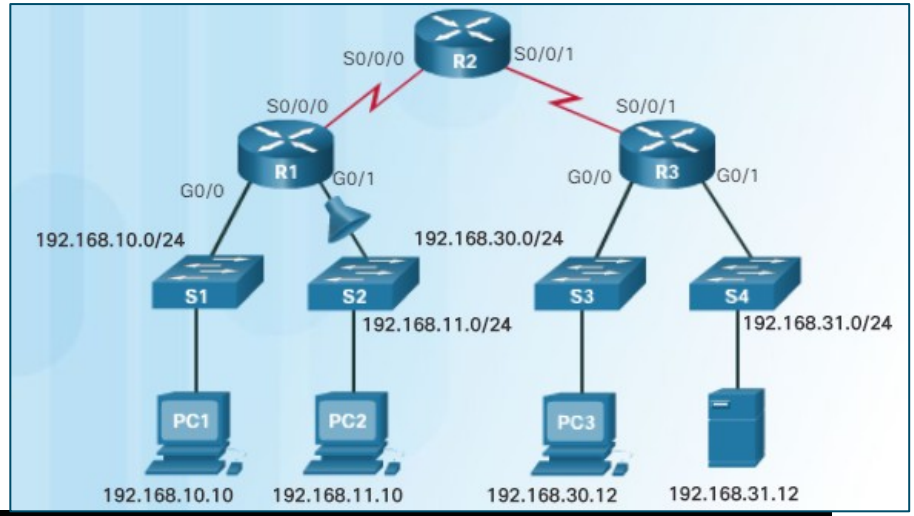


TFTP is over UDP

Statement 30 should be **permit ip any any**.

```
R3# show access-lists 120
Extended IP access list 120
    10 deny tcp 192.168.10.0 0.0.0.255 any eq telnet
    20 deny tcp 192.168.10.0 0.0.0.255 host 192.168.31.12 eq smtp
    30 permit tcp any any
```

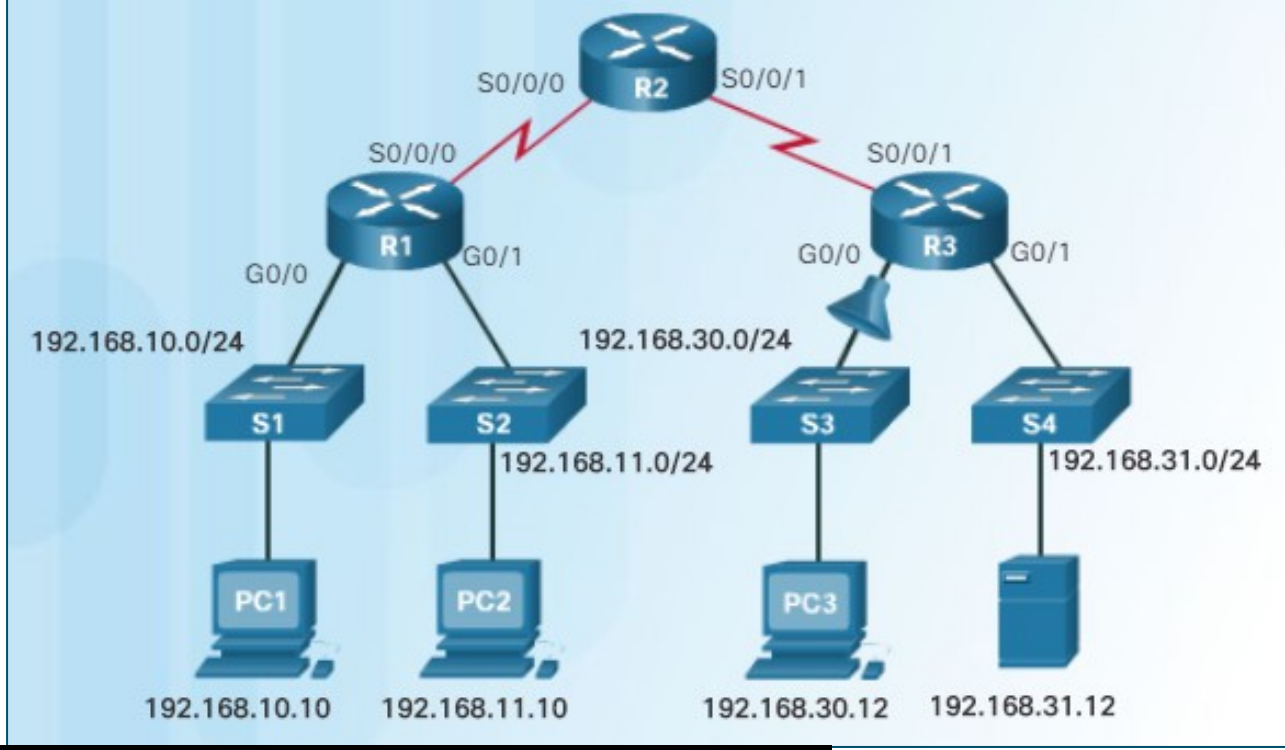
Chci zakázat telnet z 192.168.11.0/24 k 192.168.30.0/24 a nefunguje to




```
R1# show access-lists 130
Extended IP access list 130
  10 deny tcp any eq telnet any
  20 deny tcp 192.168.11.0 0.0.0.255 host 192.168.31.12 eq smtp
  30 permit tcp any any (12 match(es))
```

Řešení: **10 deny tcp 192.168.11.0 0.0.0.255 192.168.30.0 0.0.0.255 eq telnet**.

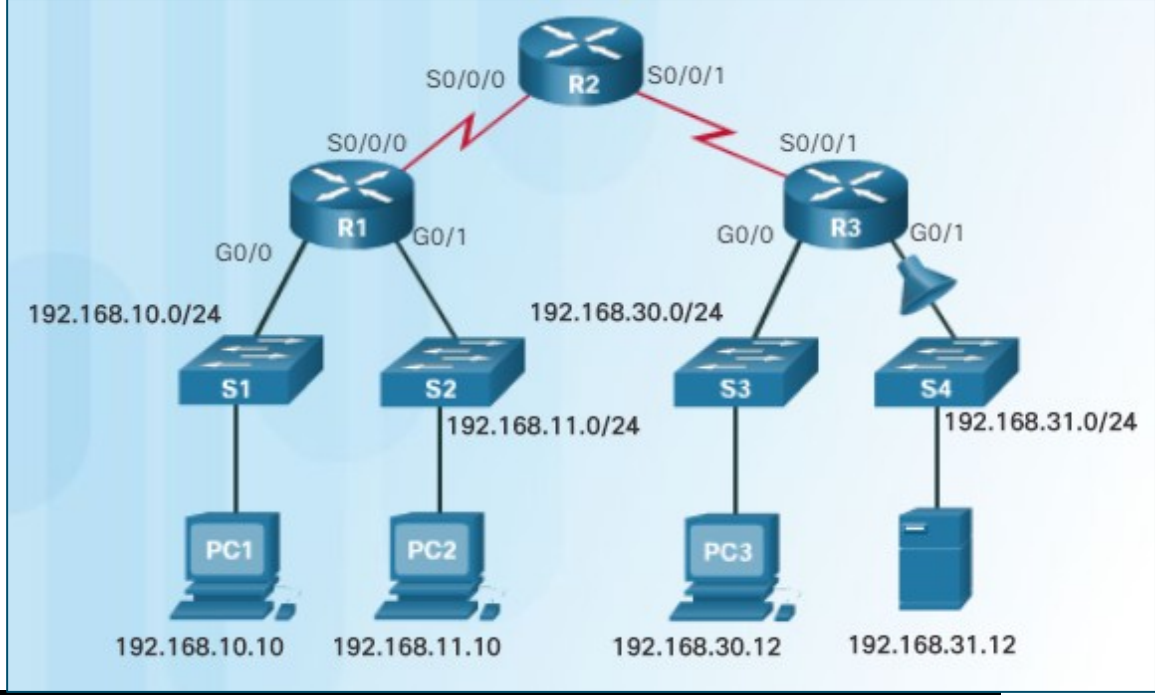
Zákaz se má týkat
192.168.30.12
a ne 192.168.30.1
je třeba přepsat




```
R3# show access-lists 140
Extended IP access list 140
    10 deny tcp host 192.168.30.1 any eq telnet
    20 permit ip any any (5 match(es))
```

Chci zákaz telnetu z 192.168.30.12 na 192.168.31.12

Řešení: dát ho na G0/1 u R3

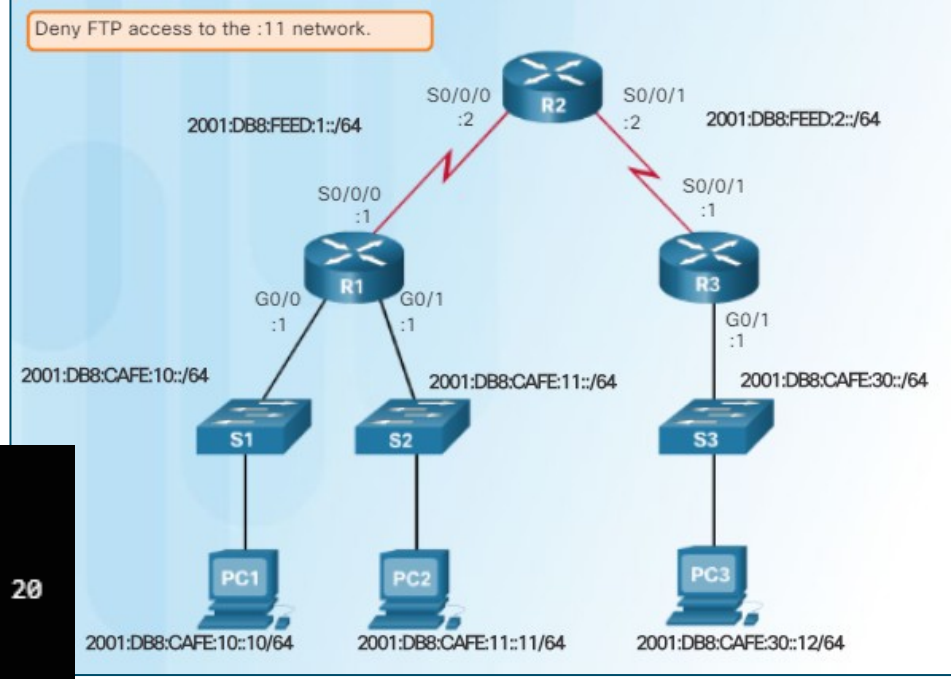



```
R2# show access-lists 150
Extended IP access list 150
        10 deny tcp any host 192.168.31.12 eq telnet
        20 permit ip any any
```

Chci zákaz FTP z :10 na network to the :11

- **Chyba: špatný směr.**
- **Oprava:**

no ipv6 traffic-filter NO-FTP-TO-11 out
ipv6 traffic-filter NO-FTP-TO-11 in.



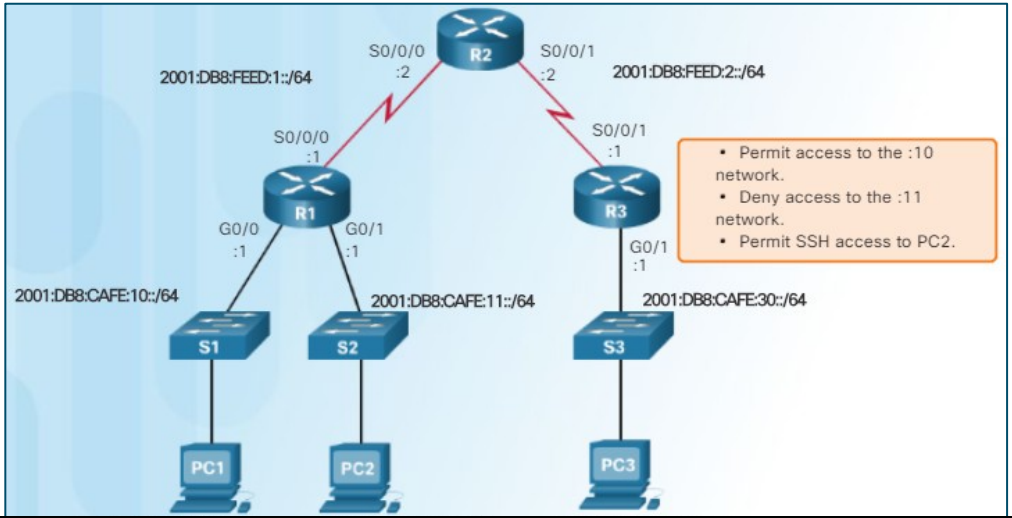

```
R1# show ipv6 access-list
IPv6 access list NO-FTP-TO-11
    deny tcp any 2001:DB8:CAFE:11::/64 eq ftp sequence 10
    deny tcp any 2001:DB8:CAFE:11::/64 eq ftp-data sequence 20
    permit ipv6 any any (11 matches) sequence 30
R1# show running-config | begin interface G
interface GigabitEthernet0/0
 no ip address
 ipv6 traffic-filter NO-FTP-TO-11 out
 duplex auto
 speed auto
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:1:10::1/64
 ipv6 eigrp 1
<output omitted>
R1#
```

permit access to network :10, deny access to the network :11, permit SSH to PC 2001:DB8:CAFE:11::11

Problem: PC3 cannot reach network10 or 11 and SSH to 2001:DB8:CAFE:11::11.

Solution:

- remove the host argument and change the prefix to /64. You can do this without removing the ACL by replacing the ACE using the sequence number 10.
- remove the statements first, and then enter them in the correct order.

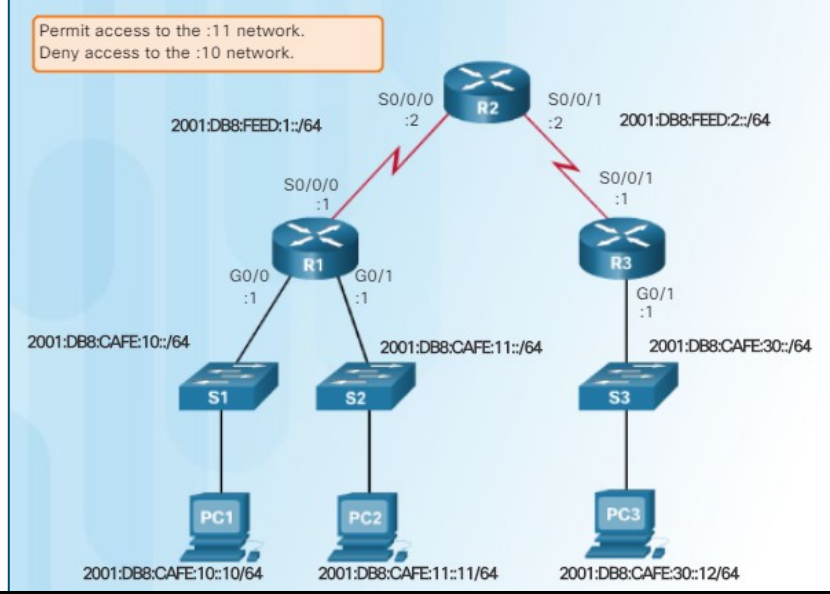



```
R3(config)# ipv6 access-list RESTRICTED-ACCESS
R3(config-ipv6-acl)# permit ipv6 any 2001:db8:cafe:10::/64 sequence 10
R3(config-ipv6-acl)# end
R3# show access-list
IPv6 access list RESTRICTED-ACCESS
    permit ipv6 any 2001:DB8:CAFE:10::/64 sequence 10
    deny ipv6 any 2001:DB8:CAFE:11::/64 sequence 20
    permit tcp any host 2001:DB8:CAFE:11::11 eq 22 sequence 30
R3#
```

R1 DENY-ACCESS
permit access from network :30 to network :11, but deny to network:10.

Problem: from 30 to :10 is reachable.
Solution:

- Location ACL move closest to the source of the traffic.
- Remove the ACL on R1 and apply on R3.




```
R1(config)# no ipv6 access-list DENY-ACCESS
R1(config)# interface g0/1
R1(config-if)# no ipv6 traffic-filter DENY-ACCESS out
R1(config-if)#
!-----------------------------------------------------
R3(config)# ipv6 access-list DENY-ACCESS
R3(config-ipv6-acl)# permit ipv6 any 2001:DB8:CAFE:11::/64
R3(config-ipv6-acl)# deny ipv6 any 2001:DB8:CAFE:10::/64
R3(config-ipv6-acl)# exit
R3(config)# interface g0/0
R3(config-if)# ipv6 traffic-filter DENY-ACCESS in
R3(config-if)#
```

```
R1# show access-list
IPv6 access list DENY-ACCESS
    permit ipv6 any 2001:DB8:CAFE:11::/64 sequence 10
    deny ipv6 any 2001:DB8:CAFE:10::/64 sequence 20
R1# show running-config | section interface GigabitEthernet0/1
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:CAFE:11::1/64
 ipv6 eigrp 1
 ipv6 traffic-filter DENY-ACCESS out
R1#
```

Allow DNS and HTTP(S) protocols to Internet

Outgoing direction

- `access-list 103 permit udp any any eq 53`
- `access-list 103 permit tcp any any eq 53`
- `access-list 103 permit tcp any any eq 80`
- `access-list 103 permit tcp any any eq 443`

Incoming direction

- `access-list 104 permit udp any eq 53  any`
- `access-list 104 permit tcp any eq 53  any established`
- `access-list 104 permit tcp any eq 80  any established`
- `access-list 104 permit tcp any eq 443 any established`

Deny ICMP traffic for network 10.0.20.0/24 except usage of command ping to public network

Outgoing direction

- `access-list 105 permit icmp 10.0.20.0 **0.0.0.255** any **echo**`
- `access-list 105 deny icmp 10.0.20.0 **0.0.0.255** any`
- `access-list 105 permit ip any any`

Incoming direction

- `access-list 106 permit icmp any 10.0.20.0 **0.0.0.255 echo-reply**`
- `access-list 106 deny icmp any 10.0.20.0 **0.0.0.255**`
- `access-list 106 permit ip any any`

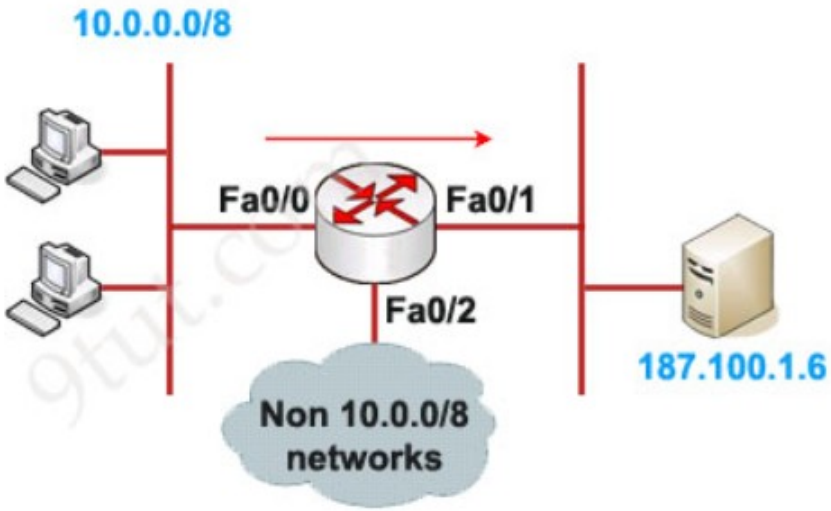
Allow the access from outside to POP3 servers in network 100.70.20.40/30 and to SMTP server 100.70.20.45

Outgoing direction

- access-list 107 permit tcp 100.70.20.40 **0.0.0.3** eq 110 any **established**
- access-list 107 permit tcp host 100.70.20.45 eq 25 any **established**
- access-list 107 permit tcp host 100.70.20.45 any eq 25
- (rules allowing the access to DNS servers should follow)

Incoming direction

- access-list 108 permit tcp any 100.70.20.40 **0.0.0.3** eq 110
- access-list 108 permit tcp any host 100.70.20.45 eq 25
- access-list 108 permit tcp any eq 25 host 100.70.20.45 **established**
- (rules allowing the access to DNS servers should follow)



Router(config)#access-list 1 permit 10.0.0.0 0.255.255.255
Router(config)#interface fa0/1
Router(config-if)#ip access-group 1 out