



Computer Networks Laboratory

www.cnl.tuke.sk

Počítačové siete 12.

Ing. František Jakab, PhD.

frantisek.jakab@tuke.sk

KPI FEI TU

Úvod

- Primárna téma prezentácie:
Medzisieťová komunikácia
- Záznam z prednášky:
<http://www.cnl.tuke.sk>

Ciele prezentácie

- Konceptcia smerovačov, ich funkcionality
- Princíp práce smerovačov
- ACL

Smerovanie (Routing)

- Množina smerov, podľa ktorej router rozhoduje o (ne)dostupnosti jednotlivých priamo aj nepriamo (ne)pripojených sietí :-)
- **Statické**
 - konfigurované manuálne administrátorom
- **Dynamické**
 - „naučené“ automaticky smerovacím protokolom (RIP, IGRP, OSPF, EIGRP, BGP, ISIS, ...)
 - dynamicky prispôsobované aktuálnej topológii a vytáženiu liniek

Static Routes

Static routes between networks are manually configured by an administrator. Static routes are added with the following command:

```
Router(config)# ip route 192.168.2.0 255.255.255.0 E0
```

Network Address

Subnet Mask

Gateway

This command sets a **default route** on a router:

```
Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

Static routes to **next hop addresses** have **administrative distance of 1**.

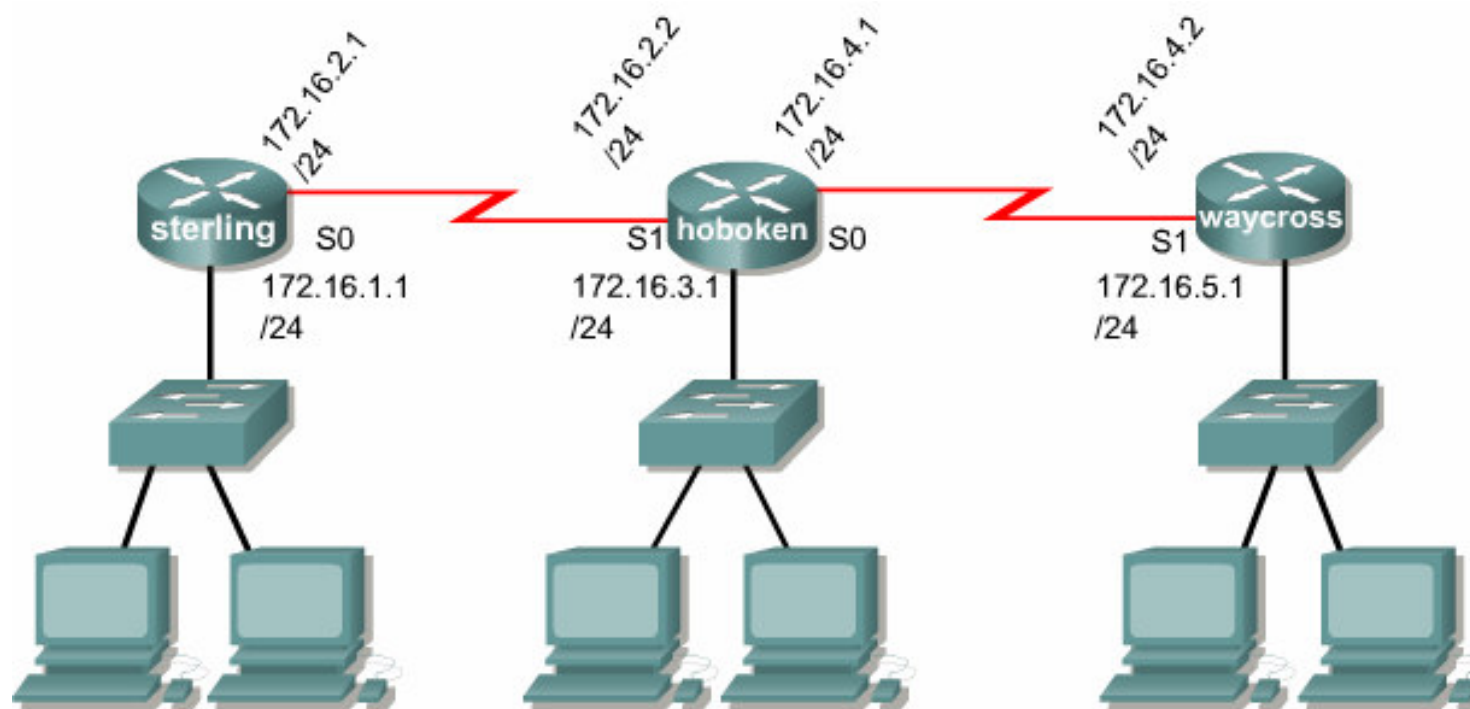
Static routes out **interfaces** have an **administrative distance of 0**.

You can specify a non-default administrative distance for a static route:

```
Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.1 130
```

Statické smerovanie

- Adresovanie nepriamo pripojených sietí



```
Hoboken(config)#ip route 172.16.1.0 255.255.255.0 172.16.2.1
                    command destination sub mask gateway
                    network
Hoboken(config)#ip route 172.16.5.0 255.255.255.0 172.16.4.2
                    command destination sub mask gateway
                    network
```

Administratívna vzdialenosť

AV (AD) miera „spoľahlivosti“ cesty
(informácie o ceste)

Nižšia hodnota – väčšia
dôverihodnosť

Pre rôzne smerovacie protokoly má
rôzné hodnoty

Do smerovacej tabuľky sa dostane
cesta s najnižšou hodnotou AD

Connected	0
Static	1
EIGRP (summary route)	5
eBGP	20
EIGRP (Internal)	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP (External)	170
iBGP (External)	220

Default route & troubleshooting

- Množina smerov, podľa ktorej router rozhoduje o (ne)dostupnosti jednotlivých (ne)zapojených sietí
- **ip route 0.0.0.0 0.0.0.0 Serial 0/1** ← outgoing interface
- **ip route 0.0.0.0 0.0.0.0 10.22.54.35** ← next hop IP
- **Troubleshooting:**
 - show ip route (výpis aktuálnej routing table)
 - show running-config (výpis aktuálnej konfigurácie routra)
 - ping (testovanie dostupnosti hostov ICMP paketmi)
 - **!** – successful reply
 - **U** – destination unreachable
 - **A** – destination administratively prohibited
 - **.** – no reply received

Troubleshooting (2)

- traceroute (získovanie trasy k hostu)
 - 10ms 10ms 10ms – Round Trip Time 10ms (korektná odpoveď)
 - * * * – žiaden z troch paketov sa nevrátil (prerušená linka na ceste, firewall, prípadne vypnutý cieľový host/router)

```
swr#traceroute www.cvut.cz
Translating "www.cvut.cz"...domain server (147.232.22.65) [OK]
```

```
Type escape sequence to abort.
Tracing the route to www.cvut.cz (147.32.3.39)
```

```
 1 swr-fei.cn1.tuke.sk (147.232.48.1) 0 msec 0 msec 4 msec
 2 vku-lin.fei.tuke.sk (147.232.40.25) 0 msec 4 msec 0 msec
 3 swr-uvt.tuke.sk (147.232.10.1) 0 msec 0 msec 4 msec
 4 fw2.tuke.sk (147.232.249.3) 0 msec 0 msec 0 msec
 5 TU-Kosice.sanet2.sk (147.232.14.41) 4 msec 4 msec 0 msec
 6 CVT-Bratislava.sanet2.sk (194.160.8.150) 8 msec 8 msec 8 msec
 7 195.113.179.165 8 msec 8 msec 12 msec
 8 r92-r105.cesnet.cz (195.113.156.126) 12 msec 12 msec 12 msec
 9 r92-cvut.cesnet.cz (195.113.144.174) 12 msec 12 msec 16 msec
10 p1-r1de.net.cvut.cz (147.32.252.50) 12 msec 12 msec 12 msec
11 www.cvut.cz (147.32.3.39) 12 msec 12 msec 12 msec
```

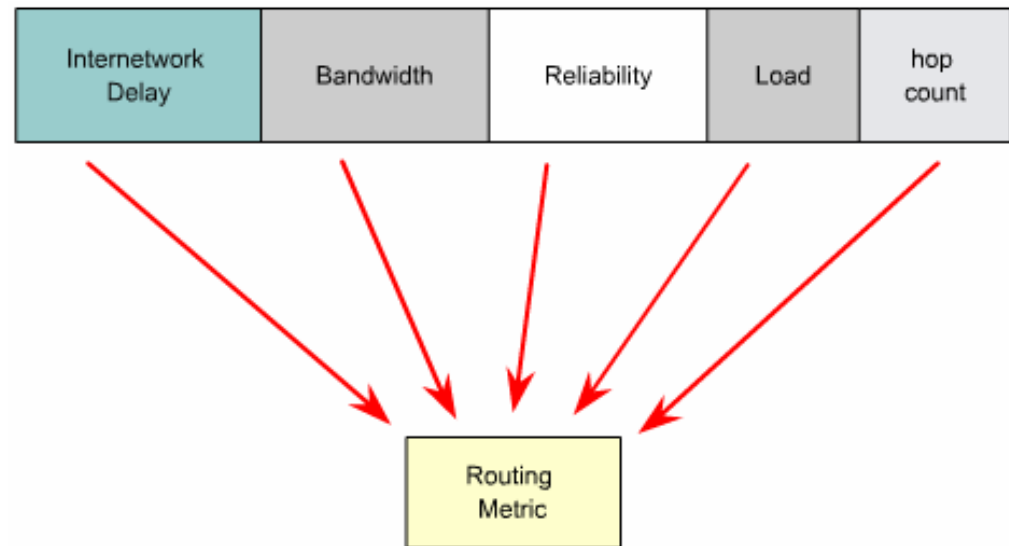
```
swr#
```

Dynamické smerovanie (1)

- **Protokoly**
 - **routing** (smerovacie)
 - „budujú“ smerovaciu tabuľku
 - RIP, IGRP, OSPF, EIGRP, BGP, ISIS, ...
 - **routed** (smerované)
 - riadia sa podľa už vybudovanej tabuľky
 - IP (celý internet), IPX (staršie Novell siete), DECnet ...
- **Routing prokoly**
 - distance vector (RIP, IGRP, BGP)
 - link-state (OSPF)
 - hybrid (EIGRP)
- **Routing protokoly**
 - interiérové (RIP, IGRP, OSPF, EIGRP)
 - exteriérové (BGP, ISIS)

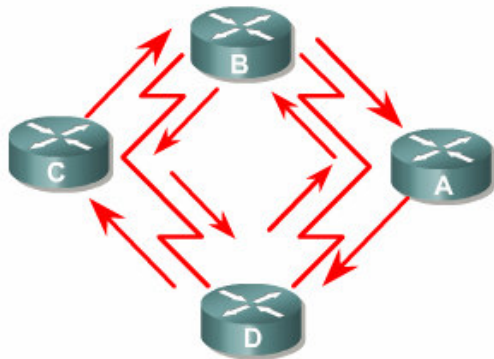
Dynamické smerovanie (2)

- **Routing** protokoly sa rozhodujú o výhodnosti **cesty** na základe metriky
- Routing protokoly používajú jeden alebo viacej parametrov na vypočítanie metriky (~ metriky)
 - RIP – hop count
 - IGRP – **delay, bandwidth, reliability, load**
 - OSPF – bandwidth
 - EIGRP – **delay, bandwidth, reliability, load**



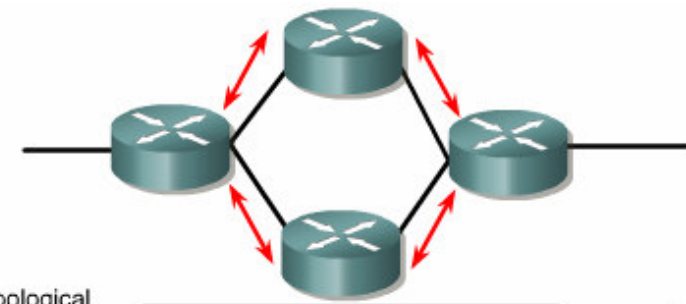
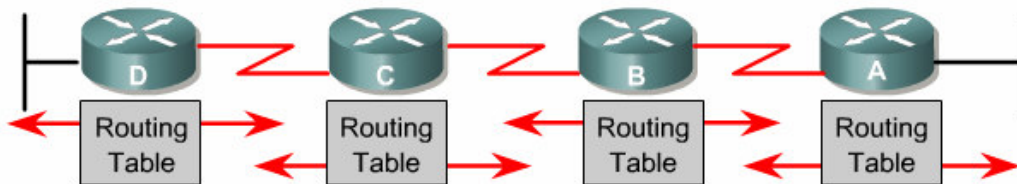
```
Router#sh int fa0/1
FastEthernet0/1 is up, line protocol is up (connected)
Hardware is Fast Ethernet, address is 0013.1aac.c481 (bia 0013.1aac.c481)
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 6/255
```

Distance vector vs. link-state



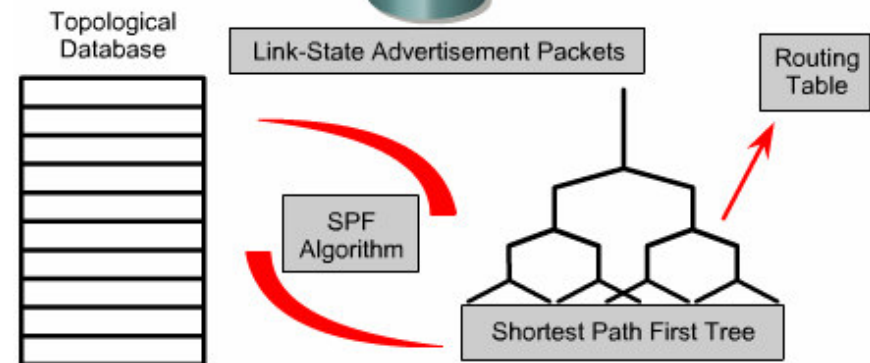
Distance vector:

- Každý router vie iba o existencii susedných, ďalej topológiu nepozná
- Tabuľku buduje na základe pravidelných updatov od susedných routrov



Link-state:

- Každý router pozná topológiu celej siete
- Tabuľku si vybuduje na základe naučenej topológie



Nekonzistentne smerovacie tabuľky

- **Routing loops**

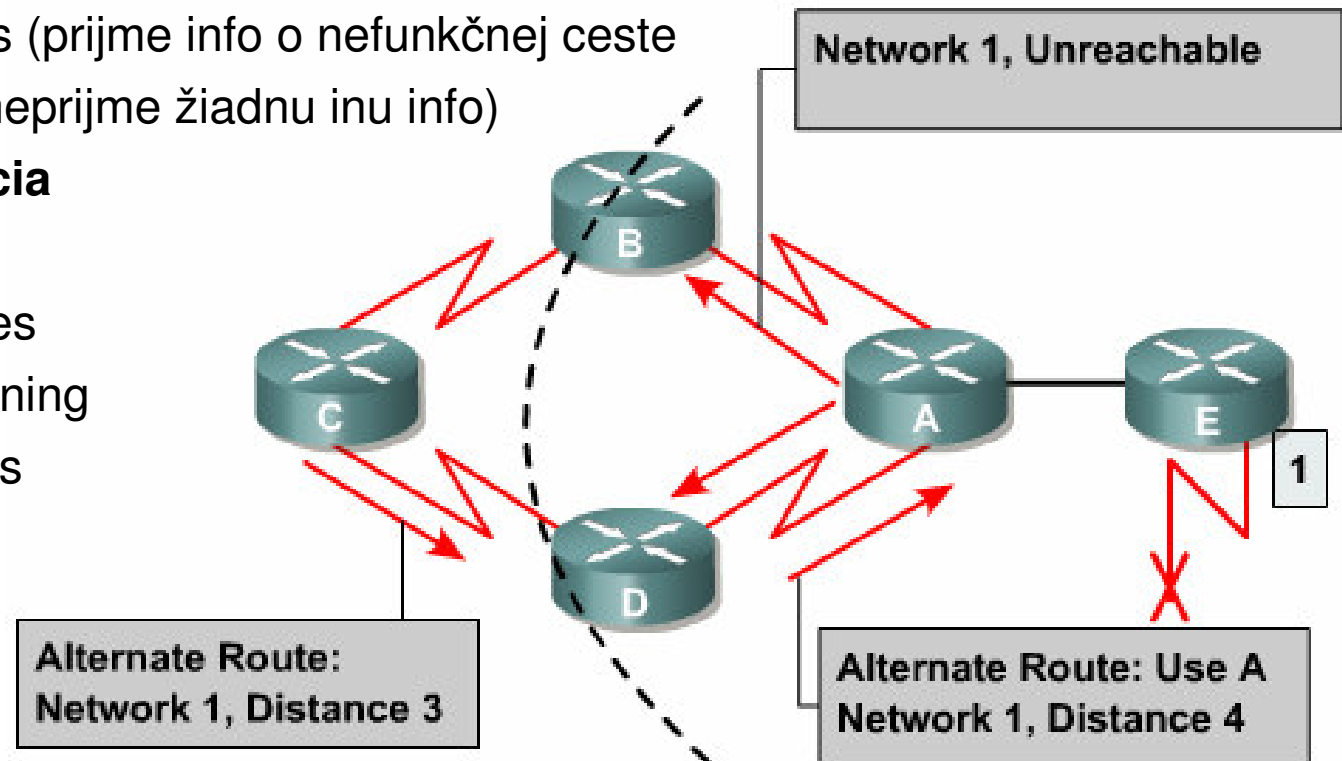
- **Riešenie**

- split horizon
 - holddown timers (prijme info o nefunkčnej ceste - od toho času neprijme žiadnu inu info)

- **Rýchlejšia konvergencia**

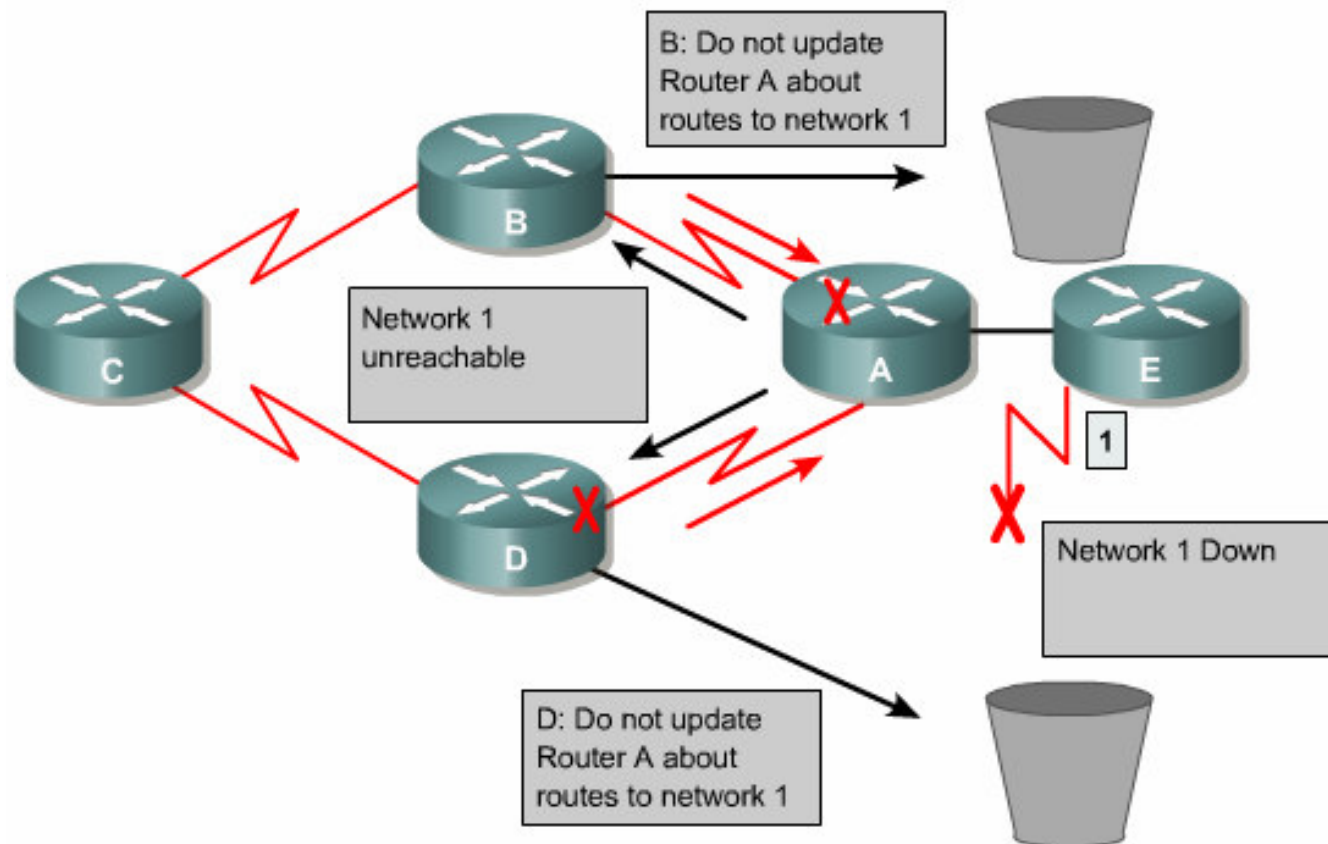
- **Riešenie**

- triggered updates
 - route poisoning
 - flash updates



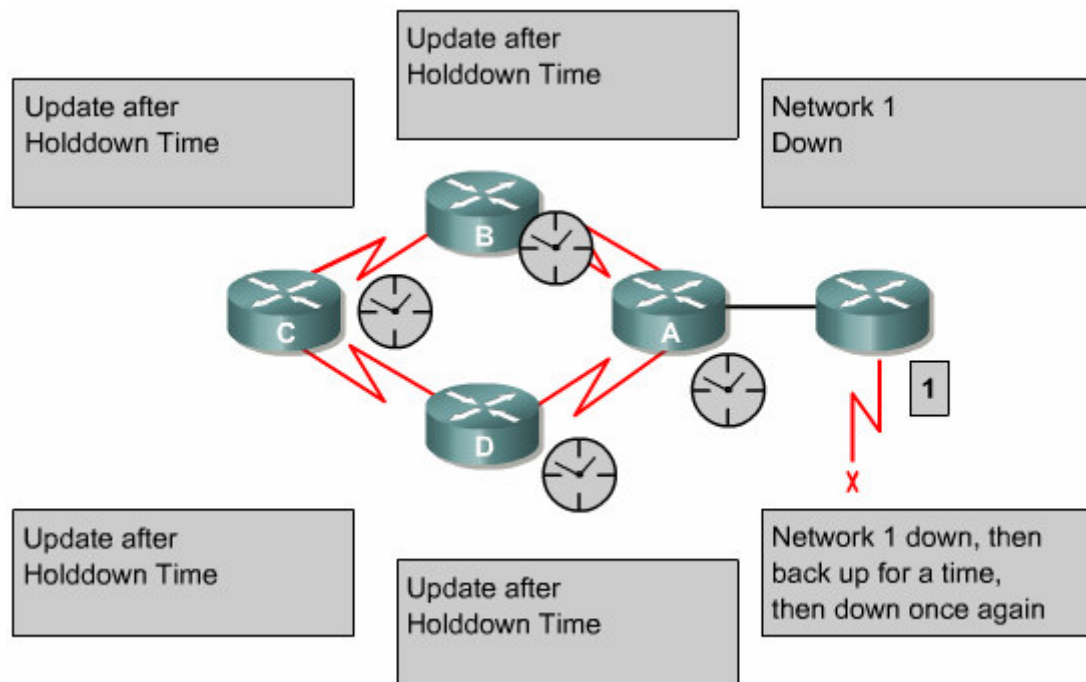
Split horizon

- Ak sa dozviem o dostupnosti siete „1“ cez pravý interface routra „D“, tak sieť „1“ nezahrňam do updatov vysielaných cez pravý interface



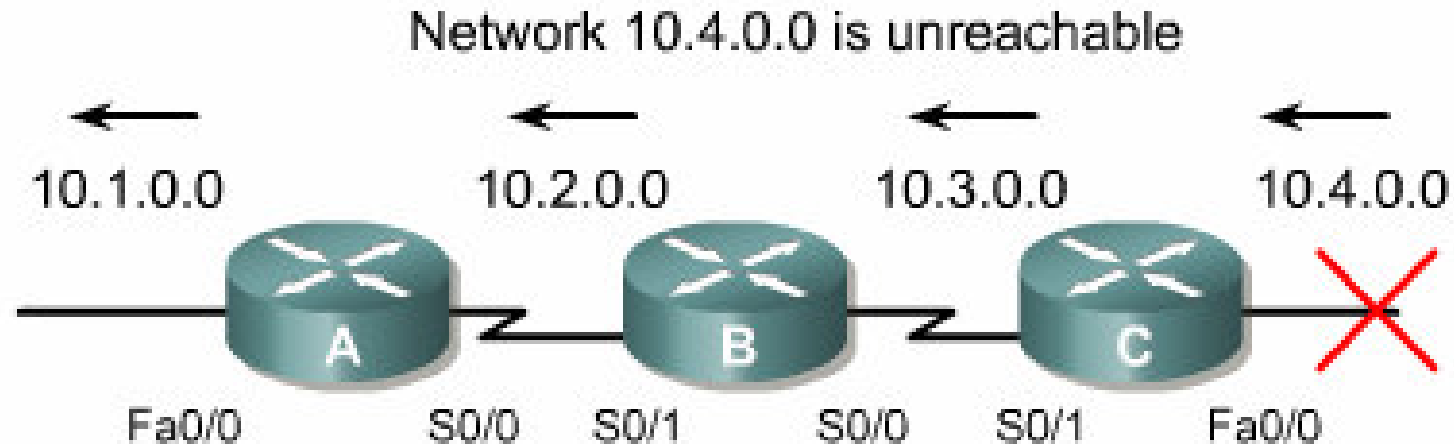
Holddown timers

- Ak router dostane info o nedostupnosti siete, vyradí ju zo routovacej tabuľky
- Istý čas si ju však ešte routing proces pamätá
 - ak dostane update o danej sieti cez iný interface s **lepšou** metrikou, routu **vloží** do tabuľky a holddown stav končí
 - ak dostane update o danej sieti cez iný interface s **horšou** metrikou, update **ignoruje** (v snahe zabrániť slučkám a nekonvergovanej sieti)



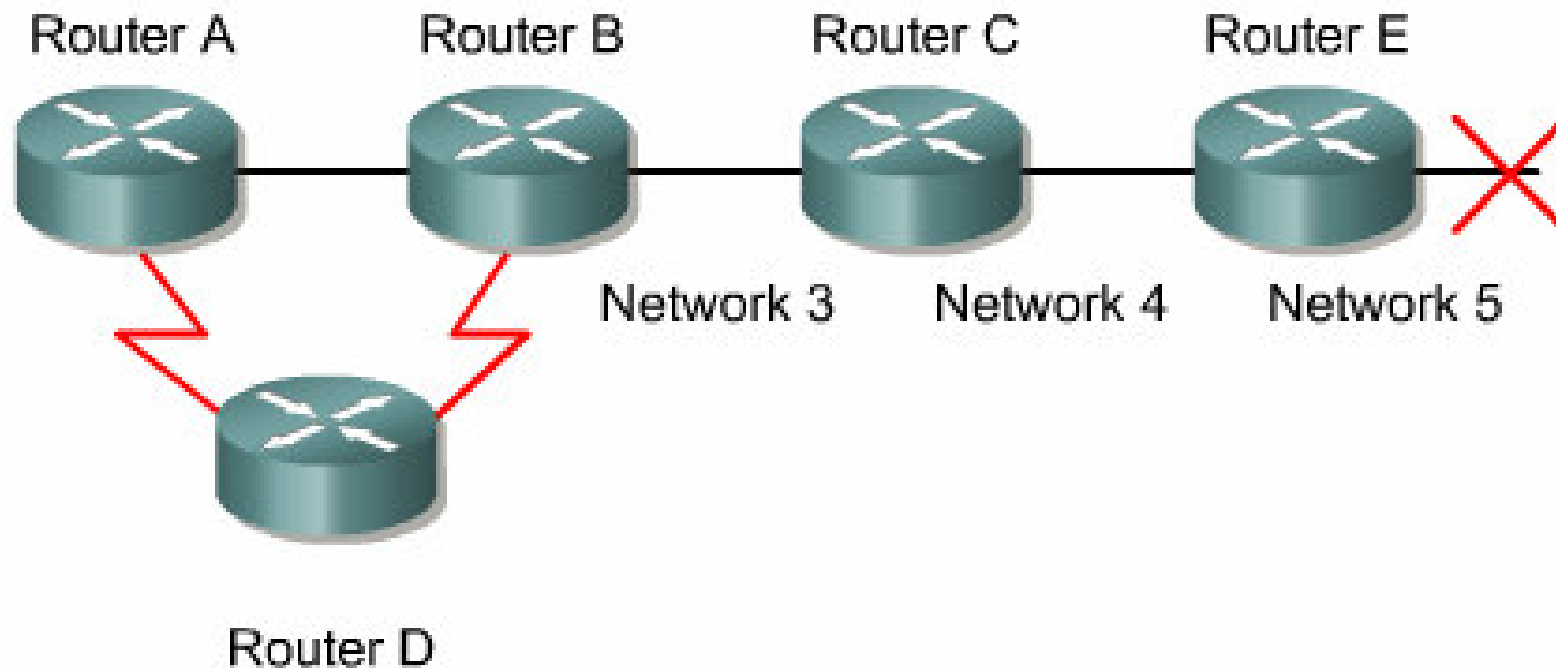
Triggered updates

- Updaty iniciované zmenou stavu siete
 - interface UP/DOWN
 - preposlanie prijatého triggered updatu
- Nečakajú na pravidelný plánovaný interval, sú posielané hneď
- Urýchľujú konvergenciu smerovacích tabuliek v sieti



Route poisoning

- Ak router E zistí nedostupnosť siete, okamžite (bez čakania na pravidelný update interval) pošle informáciu o nedostupnosti siete
 - Pošle update „infinite metric“ pre danú sieť (pri RIP je to 16)

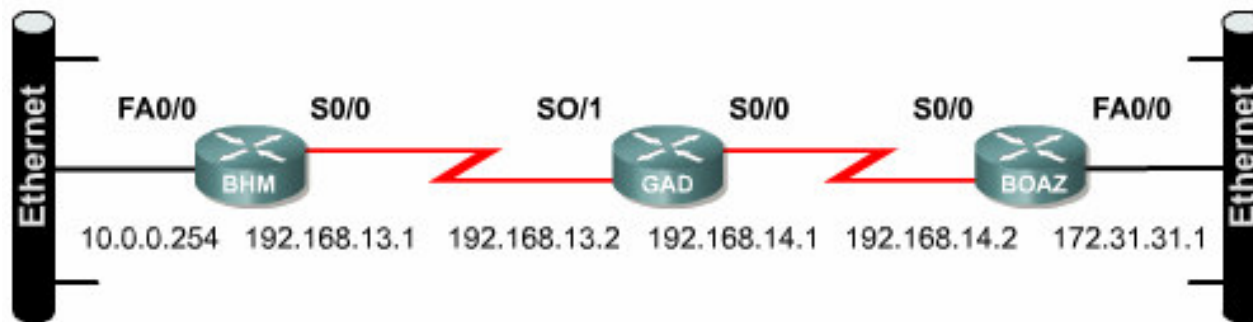


RIP (Routing Information Protocol)

- Distance vector routing protokol
- Ako metriku používa (iba) **hop count**
 - hop = prechod ďalším routrom
 - maximálny hop count je 15
 - 16 znamená, že sieť je nedostupná
- Routing updates posiela každých 30 sekúnd
- RIP version 2
 - classless/VLSM, authentication
 - inteligentnejšie posielanie updatov (mcast, prenos masky, ...)

Základná konfigurácia RIP

- Ak chcem, aby interface vysielal a prijímal routing updates musím ho prostredníctvom príkazu **network** zahrnúť do konfigurácie



```
BHM(config)#router rip
BHM(config-router)#network 10.0.0.0
BHM(config-router)#network 192.168.13.0
```

```
GAD(config)#router rip
GAD(config-router)#network 192.168.14.0
GAD(config-router)#network 192.168.13.0
```

```
BOAZ(config)#router rip
BOAZ(config-router)#network 192.168.14.0
BOAZ(config-router)#network 172.31.0.0
```

RIP Configuration Issues

Convergence is when all routers in the Internetwork have the same routing information. **Slow convergence** of DV protocols results in **inconsistencies**.

RIPs performance can be tuned to improve convergence time:

To disable split horizon: `GAD (config-if) # no ip split-horizon`

The default holddown is **180 secs**. Decrease it to speed up convergence. Set the timer just longer than the longest possible update time for the network:

```
GAD (config-router) # timers basic 30 180 180 240
```

Update Invalid Holdtime Flush



Invalid – ak žiadny upd o danej ceste nepride, tak je označena za „invalid“
Holdtime – ak je cesta označena za nedosiahnuteľnú, začína počítať
Flush – čas, po ktorom sa odstráni cesta úplne

The default RIP update interval is 30 secs. Longer intervals can conserve bandwidth, shorter intervals may decrease convergence time:

```
GAD (config-router) # update-timer 40
```

To disable sending routing updates on specified interfaces:

```
GAD (config-router) # passive-interface f0/0
```

Verifying RIP Configuration

```
Dublin# show ip protocols
```

RIP routing is configured

```
Routing Protocol is "rip"
```

```
Sending updates every 30 seconds, next due in 14 seconds  
Invalid after 180 seconds, hold down 180, flushed after 240  
Outgoing update filter list for all interfaces is not set  
Incoming update filter list for all interfaces is not set  
Redistributing: rip
```

```
Default version control: send version 1, receive any version
```

Interface	Send	Recv	Triggered	RIP	Key-chain
FastEthernet0/0	1	1	2		

Interfaces sending and receiving RIP updates

```
Automatic network summarization is in effect
```

```
Maximum path: 4
```

```
Routing for Networks:
```

Router is advertising the correct networks

```
11.0.0.0  
12.0.0.0
```

```
Routing Information Sources:
```

Gateway	Distance	Last Update
11.0.0.2	120	00:01:16

```
Distance: (default is 120)
```

```
Dublin#
```

Examining the Routing Table

Routing tables are stored using on-board DRAM.

A routing table contains a list of the best available routes.

Routers use routing tables to make packet forwarding decisions.

```
Dublin# 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
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    12.0.0.0/24 is directly connected, FastEthernet0
C    11.0.0.0/30 is subnetted, 1 subnets
     11.0.0.0 is directly connected, Serial0
R    13.0.0.0/24 [120/11] via 11.0.0.2, 00:00:02, Serial0

Dublin#
```

Networks being advertised

FastEthernet0

Out interface

Serial0

Serial0

Codes, how the routes were learnt

Administrative Distance

Metric

Next Hop

Time since last update

Troubleshooting RIP

Typical RIP configuration errors:

- incorrect network statement
- discontinuous subnets
- split horizons

To analyse RIP update issues:

```
Pretoria# debug ip rip
01:04:44: RIP: sending v1 update to 255.255.255.255 via Serial0 (192.168.15.2)
01:04:44: RIP: build update entries
01:04:44:      network 192.168.13.0 metric 1
01:04:44:      network 192.168.16.0 metric 1
01:04:44: RIP: sending v1 update to 255.255.255.255 via Serial1 (192.168.13.2)
```

Other commands to troubleshoot RIP:

Command	Definition
<code>show ip rip database</code>	Summary of entries in RIP routing database
<code>show ip protocols</code>	Data for each routing protocol active on router
<code>show ip route</code>	View the routing table
<code>debug ip rip {events}</code>	Check routing updates are being sent
<code>show ip interface brief</code>	Summary of interface status and parameters

Determining the Gateway of Last Resort

Default routes are used when there isn't a more specific entry in routing table.

The router uses the default route to reach the gateway of last resort.

Default routes reduce the size of routing tables.

Default routes are established either:

- Statically by an administrator

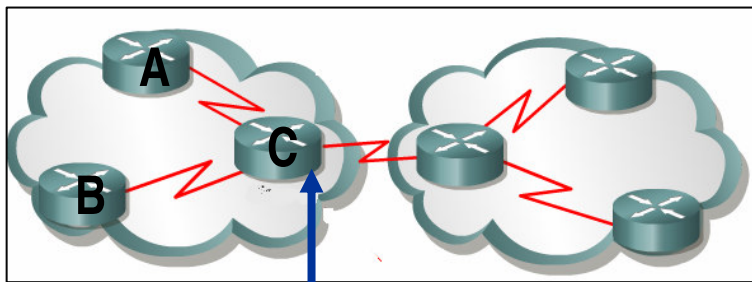
or

- Dynamically learned using a routing protocol.

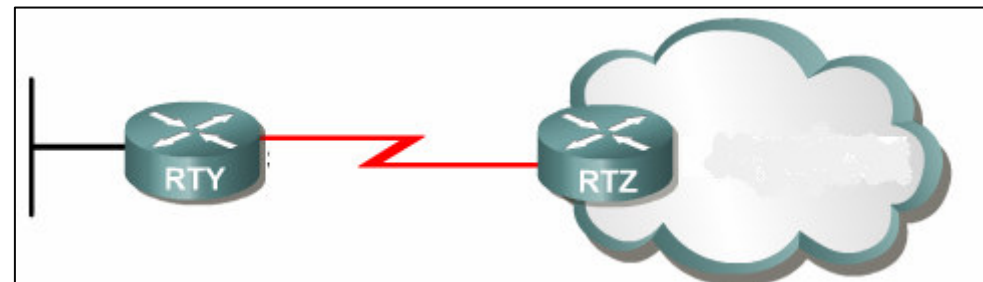
Use one of the following commands to statically configure a default route:

```
RTR(config) # ip default-network [network address] ←  
RTR(config) # ip route 0.0.0.0 0.0.0.0 [next hop IP address or exit interface]
```

Tells router to advertise default route via dynamic routing protocols.
Any known route to this network is flagged as a candidate default route.



`ip default-network` on C
information is advertised to A and B.



`ip route 0.0.0.0 0.0.0.0 s0`
on RTY configures a default router to RTZ.

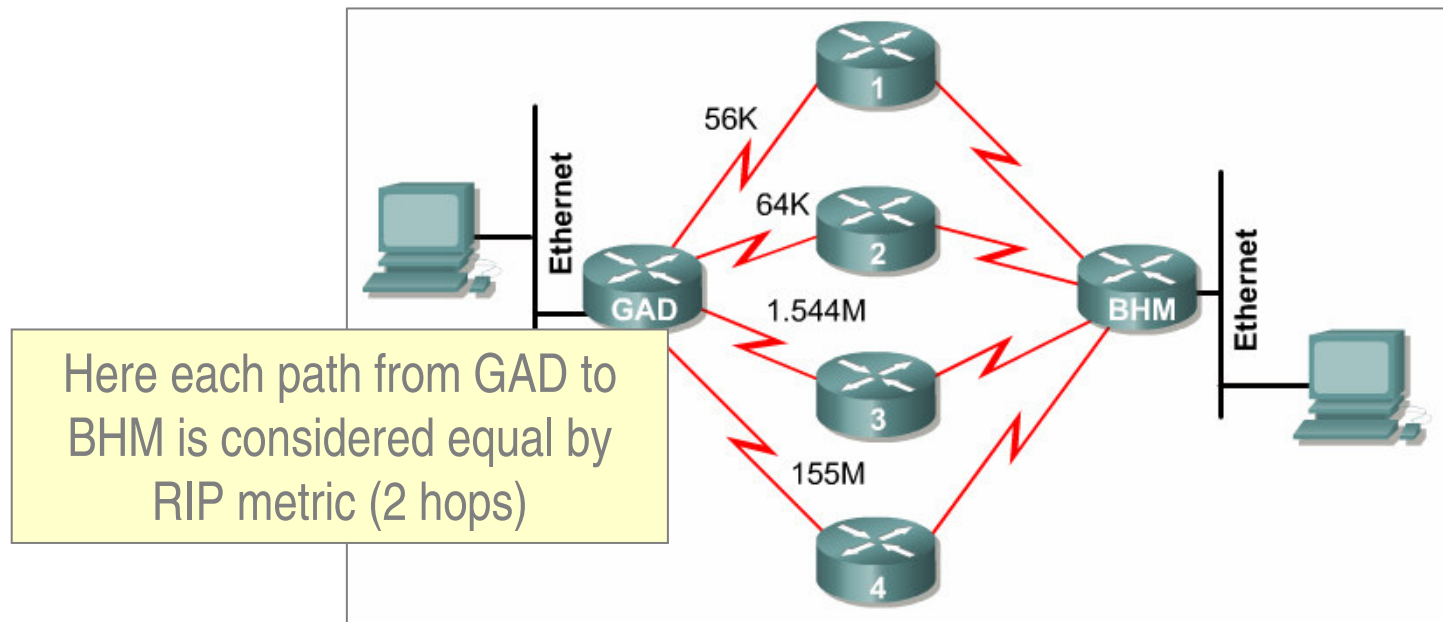
RIP Load Balancing

Load balancing allows a router to **simultaneously** use **multiple paths** to a destination. RIP can load balance over **6 equal-cost paths**, (default 4 paths).

```
Router(config-router)# maximum-paths 5
```

RIP performs what is referred to as “**round robin**” load balancing:

- If **process switching** is enabled, paths alternate on a **per-packet** basis.
- If **fast switching** is enabled, paths alternate on a **per-destination** basis.



Equal cost routes can be found by using `#show ip route`.

Each route is represented by a **routing descriptor block**.

An asterisk (*) next to one of the entries corresponds to the **active route**. 25

Redistributing Static Routes into RIP

1. Static routes are important for destinations not included in dynamic routing processes. They are also useful for specifying a **default route**.
2. Each dynamic routing protocol has a default **administrative distance (AD)**.
3. A static route can be defined as less desirable than a dynamically learned route if its **AD** is higher than the dynamic route's.
4. If a static route points to an interface that is not part of the RIP process (as defined with a **network** command) RIP will not advertise the route unless configured to:

```
Router(config)# router rip  
Router(config-router)# redistribute static
```

5. **Floating Static routes** are routes with an AD set greater than the AD of the dynamic routing protocol in use.
6. Static routes are removed from the routing table when their corresponding interface **goes down** or when the next hop is **no longer valid**.
7. Static routes can be removed using the **no ip route** global configuration command.

ACL - Access Control Lists

- **ACLs nám umožňujú**
 - **Filtrovanie sieťovej premávky (pri routovaní)**
 - **Obmedzenie prístupu k zdrojom routra**
- **ACL je sada (zoznam) podmienok, ktorý (ak je správne aplikovaný) vie na základe informácií z hlavičky L2/L3/L4 rozhodnúť o pustení alebo zahodení paketu**
 - podmienky (riadky) sú vyhodnocované sekvenčne až po prvú zhodu, daná podmienka určí, čo s paketom (**deny, permit**).
 - **T.j. podmienka pozostáva z L2/L3/L4 informácií a osudu, ktorý postihne paket, ktorý vyhoví zadaným informáciám**
 - ak sa v ACL nenájde vyhovujúca podmienka (riadok), uplatní sa implicitná podmienka zahadzujúca pakety (**implicit deny**)

What are ACLs?

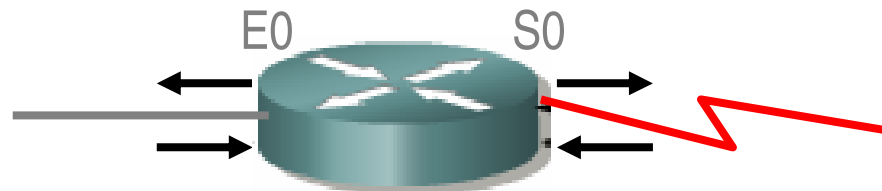
ACLs provide basic **traffic filtering** capabilities.

ACLs enable **management** of traffic and **secure access** to and from a network.

ACLs can be created for various network protocols; IP, IPX, or AppleTalk.

The router examines each packet and either **forwards or drops** it.

Example:



This router has one Ethernet interface and one Serial interface.

Each interface can have one ACL inbound and one ACL outbound

This router is configured for three routed protocols: IP, AppleTalk, IPX.

Maximum no. of ACLs that can be configured:

$$(\text{No. of interfaces}) \times 2 \times (\text{no. of routed protocols}) = 12$$

Forwarding decision can be based on a packets:

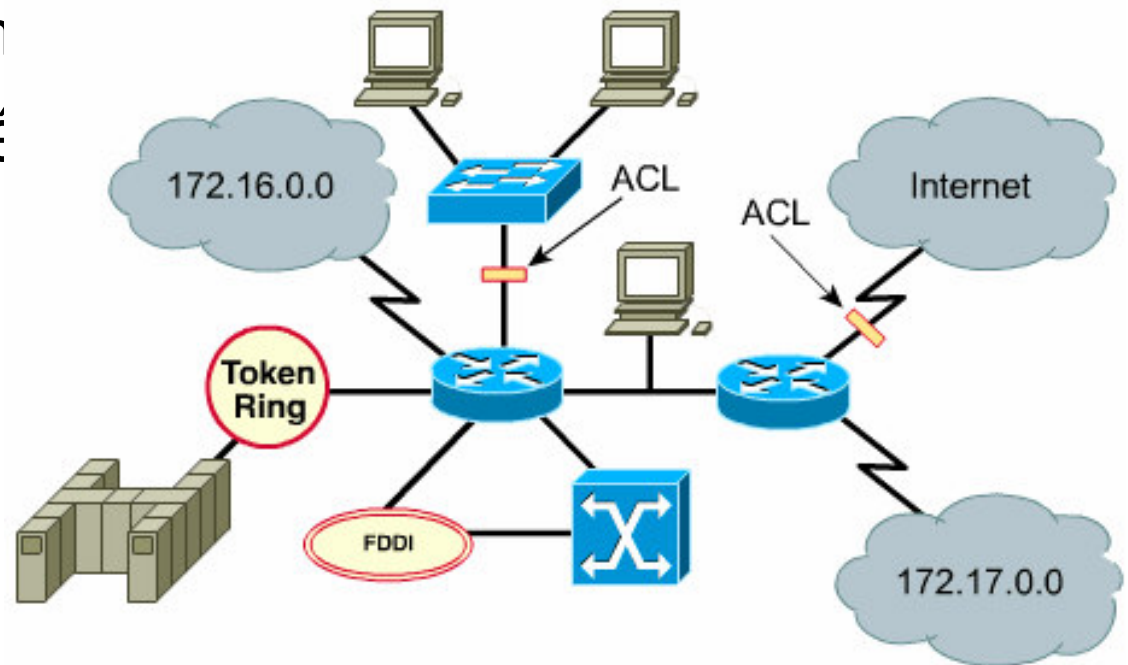
- Source address
- Destination address
- Protocol
- Port number

Why use ACLS?

- Limit network traffic to increase network performance .
- Provide traffic flow control by restricting the delivery of routing updates .
- Security - allow one host access but prevent another.
- Control which types of traffic are forwarded or blocked by the router.
- Ability to control which areas a client can access.
- Restrict user access to only certain types of files ,
(eg. Web pages).
- If ACLs are not configured, all packets passing through the router will be allowed onto all parts of the network.

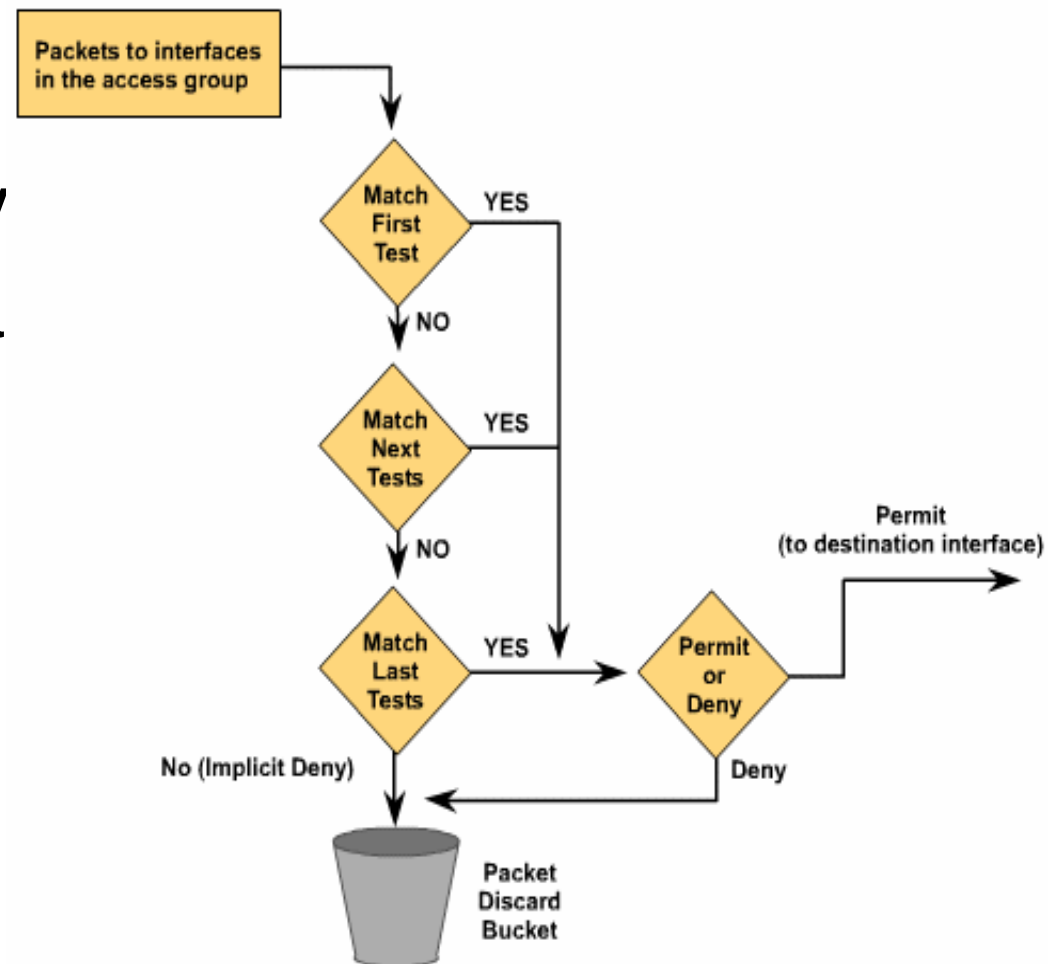
ACL – access control list

- možnosti filtrovania dátového toku
 - Vstupného, výstupného
- Aplikácia na príslušné rozhranie smerovača
- Použitie na smerovateľné protokoly (IP, IPX)



Posudzovanie paketov podľa ACL

- Poradie výrazov v ACL je dôležité
- Pri zmene položky ACL treba prepísa celý ACL
- Na konci je „deny any“



Wildcard maska

128 64 32 16 8 4 2 1

↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓

Octet bit position and address value for bit

Examples

0 0 0 0 0 0 0 0 =	Check all address bits (match all)
0 0 1 1 1 1 1 1 =	Ignore last 6 address bits
0 0 0 0 1 1 1 1 =	Ignore last 4 address bits
1 1 1 1 1 1 0 0 =	Check last 2 address bits
1 1 1 1 1 1 1 1 =	Do not check address (ignore bits in octet)

Wildcard maska

- Sieť sa v ACL **ne**definuje klasickým spôsobom **sieťová adresa + sieťová maska**, ale pomocou kombinácie **sieťová adresa + wildcard maska**
- Wildcard maska = invertovaná sieťová maska
- Príklady

192.168.1.0	255.255.255.0
192.168.1.0	0.0.0.255

147.232.22.64	255.255.255.224
147.232.22.64	0.0.0.31

10.20.30.0	255.255.255.240
10.20.30.0	0.0.0.15

172.16.152.0	255.255.248.0
172.16.152.0	0.0.7.255

Jednoduché počty:

255.255.255.255
- 255.255.248.0
<hr/>
0 . 0 . 7 .255

← sieťová maska
← wildcard maska

Špeciálne wildcard masky a skratky

- **Any** – znamená akúkoľvek IP adresu/sieť

0.0.0.0 255.255.255.255 = any

- **Host** – znamená jeden host (jednu IP)

192.168.1.100 0.0.0.0 =

host 192.168.1.100 =

192.168.1.100

Zisťovanie zhody

- Pri porovnávaní sa bude ignorovať tá časť sieťovej adresy, na ktorej sa vo wildcard maske nachádzajú **jednotky**

192.168.100.96 / 255.255.255.224 (t.j. 96 - 127)
192.168.100.96 / 0 . 0 . 0 . 31

192.168.100. 96	<u>11000000.10101000.01100100.01100000</u>	
0 . 0 . 0 . 31	00000000.00000000.00000000.00011111	
192.168.100. 99	11000000.10101000.01100100.01100011	PASS
192.168.100.117	11000000.10101000.01100100.01110101	PASS
192.168.100.130	11000000.10101000.01100100. <u>100</u> 00010	FAIL

Pri porovnávaní sa musia zhodovať **červené** časti adresy

Číslované ACL

- Číslom na začiatku podmienky identifikujem aký ACL hodlám zadávať do routra

Protocol	Range
IP	1-99, 1300-1999
Extended IP	100-199, 2000-2699
AppleTalk	600-699
IPX	800-899
Extended IPX	900-999
IPX Service Advertising Protocol	1000-1099

Creating ACLs

There are many different types of ACLs.

Each ACL is uniquely identified by assigning a **number** (or a name) to it.

This number identifies the **type of access list** created and must fall within the specific range of numbers:

```
Rio(config)# access-list ?
```

```
<1-99>          IP standard access list
<100-199>       IP extended access list
<200-299>       Protocol type-code access list
<300-399>       DECnet access list
<600-699>       Appletalk access list
<700-799>       48-bit MAC address access list
<800-899>       IPX standard access list
<900-999>       IPX extended access list
<1000-1099>     IPX SAP access list
<1100-1199>     Extended 48-bit MAC address access list
<1200-1299>     IPX summary address access list
<1300-1999>     IP standard access list (expanded range)
<2000-2699>     IP extended access list (expanded range)
```

Štandardný ACL

- Pracuje na základe zdrojovej adresy
 - Adresa siete, podsiete alebo počítača
- Povolí alebo blokuje celý príslušný protokol

- **Definovanie**

```
Router(config)# access-list access-list-number {deny | permit} source [source-wildcard ] [log]
```

(správa pri prvom pak. + kazdych 5 min.)

- **Použitie**

```
Router(config-if)#ip access-group access-list-number {in | out}
```

- In/out – vstupné alebo výstupné rozhranie – default je out
- Na rozhraní je povolený 1 ACL pre každý protokol a smer

Štandardný ACL – príklad

- **Filtrovanie jedného PC**

```
access-list 1 deny host 172.16.4.13
```

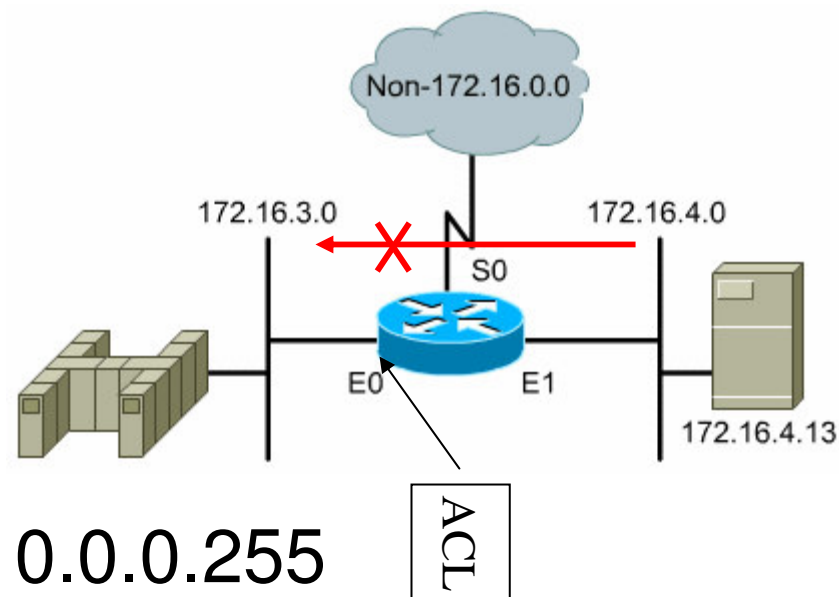
```
access-list 1 permit any  
(implicit deny any)
```

```
interface ethernet 0
```

```
ip access-group 1 out
```

- **Filtrovanie celej siete**

```
access-list 1 deny 172.16.4.0 0.0.0.255
```



Standard ACLs

Standard IP ACLs check only the source address of packets to be routed.

```
Rio(config)# access-list 50 deny 172.16.1.1 [ ]
Rio(config)# access-list 50 permit 172.16.0.0 0.0.255.255
```

Number between 1 and 99,
or 1300 to 1999 (recent IOS)

Deny or Permit

No WM specified,
∴ mask = 0.0.0.0

Wildcard Mask

Extended ACLs

Extended ACLs check the source and destination packet addresses as well as being able to check for protocols and port numbers.

	Protocol	Source	Destination	Port
1.	access-list 101 permit ip	host 10.0.0.1	any	
2.	access-list 101 deny ip	10.0.0.0 0.0.0.255	any	
3.	access-list 101 deny tcp	host 172.16.6.1	192.168.1.0 0.0.0.255	eq 23
4.	access-list 101 permit tcp	172.16.6.0 0.0.0.255	any	eq telnet

1. Specifically permit all IP traffic from this host (only) to any other network or host
2. More general statement denying other traffic from 10.0.0.0/24 network
3. Specifically denies host 172.16.6.1 (only) telnet access to 192.168.1.0/24 network
4. More general statement permitting telnet from all other hosts on 172.16.6.0/24 network

Konfigurácia ACL

- **Definovanie ACL**
 - **číselné (ACL)**
 - `access-list 10 permit host 147.232.22.65`
`access-list 10 permit 147.232.48.32 0.0.0.31`
 - **pomenované (named ACL)**
 - `ip access-list extended Povoľ_Telnet`
`permit tcp any any eq 23`
`deny any any log`
- **Priradenie ACL**
 - **na sieťové rozhranie v požadovanom smere (filtrovanie routovaných paketov)**
 - `interface Ethernet 0`
`access-group 10 in`
 - **na niektorý z prostriedkov poskytovaných samotným routrom**
 - **virtuálnu linku (telnet, SSH), SNMP prístup, HTTP prístup routra**
 - `line vty 0 4`
`access-class 10 in`

Štandardné ACL

```
access-list 2 deny 172.16.1.1
access-list 2 permit 172.16.1.0 0.0.0.255
access-list 2 deny 172.16.0.0 0.0.255.255
access-list 2 permit 172.0.0.0 0.255.255.255
```

- Access list number range of 1 - 99 and 1300 - 1999
- Filter only on source IP address
- Wildcard masks
- Applied to interface closest to destination

```
ip access-list 64 permit 192.168.100.0 0.0.0.255
```

Štandardné ACL

	identifikácia ACL	osud	informácia o zdroji (SRC)
ip access-list	64	permit	192.168.100.0 0.0.0.255
ip access-list	50	deny	147.232.22.1 0.0.0.0
ip access-list	10	permit	host 147.232.22.1
ip access-list	99	deny	10.1.1.64 0.0.0.31

Rozšířený ACL

- Pracuje na základe zdrojovej aj cieľovej adresy
- Povolí alebo blokuje špecifický protokol alebo číslo portu
- Pre jeden ACL možno definovať viacero pravidiel

- **Definovanie**

```
router(config)# access-list access-list-number  
{permit| deny} protocol source  
[source-mask destination destination-mask  
operator operand] [established]
```

- **Použitie**

```
ip access-groupaccess-list-number { in| out}
```

Rozšířený ACL

- Poznať porty známych služieb
- Operátory
 - Lt – menší než
 - Gt – väčší než
 - Eq – rovný
 - Neq – nerovný
- Protokoly – eigrp, gre, icmp, igmp, igrp, ip (znamená ICMP, TCP a UDP), ospf, tcp, udp

Porty TCP a UDP:

- **TCP a UDP využívajú porty pri komunikácií medzi koncovými stanicami.**
 - Služby transportnej vrstvy môžu byť volané prostredníctvom ich čísiel portov.
- **Teda ak koncova stanica chce preniesť súbor prostredníctvom FTP**
 - využíva TCP port 20 pre prenos dát
 - TCP porty 20 & 21 su označované ako “Well Known Port Numbers” pretože aplikácie predpokladajú, že FTP služby budú poskytované prostredníctvom týchto portov
 - **využíva TCP port 21 pre zriadenie a riadenie spojenia**
- **Ďalšie “Well Known” porty sú:**
 - TCP Port 23 - Telnet, TCP Port 25 - SMTP (email)
 - TCP Port 53 – DNS, TCP Port 80 - HTTP web serv.
 - UDP Port 53 – DNS, UDP Port 69 - TFTP
 - UDP Port 161 - SNMP

Rozšířený ACL – příklad

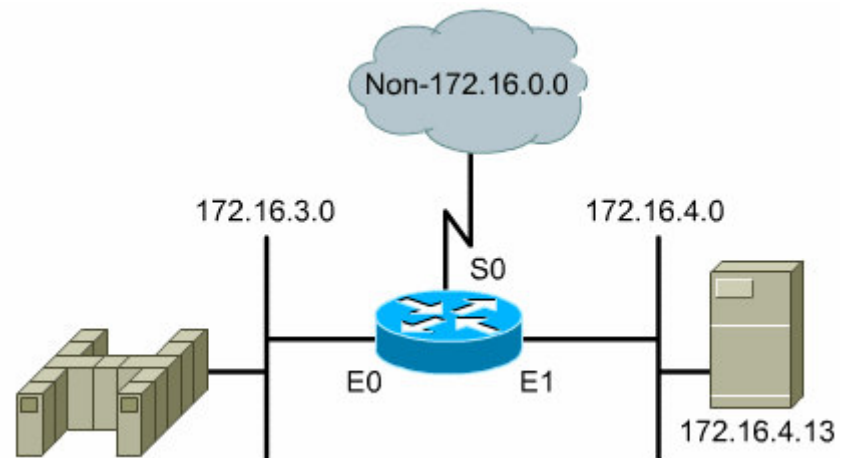
Blokovanie ftp príkazov (a teda aj prenosov)

```
Access-list 101 deny tcp 172.16.4.0 0.0.0.255  
172.16.3.0 0.0.0.255 eq 21
```

```
Access-list 101 permit ip any any  
(Implicit deny any)
```

Interface ethernet 1

```
Ip access-group 101 out
```



FTP



47

Príklady

Umožniť telnet pre host 223.8.151.10 zo siete 195.5.5.0
ale zakázať všetky ostatne a taktiež umožniť akykoľvek iný
vstup do uvedenej siete:

```
Access-list 101 permit tcp 195.5.5.0 0.0.0.255  
223.8.151.10 0.0.0.0 eq 23
```

```
Access-list 101 deny tcp 195.5.5.0 0.0.0.225  
223.8.151.0 0.0.0.255
```

```
Access-list 101 permit ip any any
```

```
Interface e0
```

```
IP access-group 101 in
```

Príklady

Ktorá sieť bude zakázaná:

Access-list 24 deny 157.118.237.0 7.63.0.0

Odpoved': 152-159.64-127.237.0

Access-list 25 deny 84.7.109.0 63.3.0.63

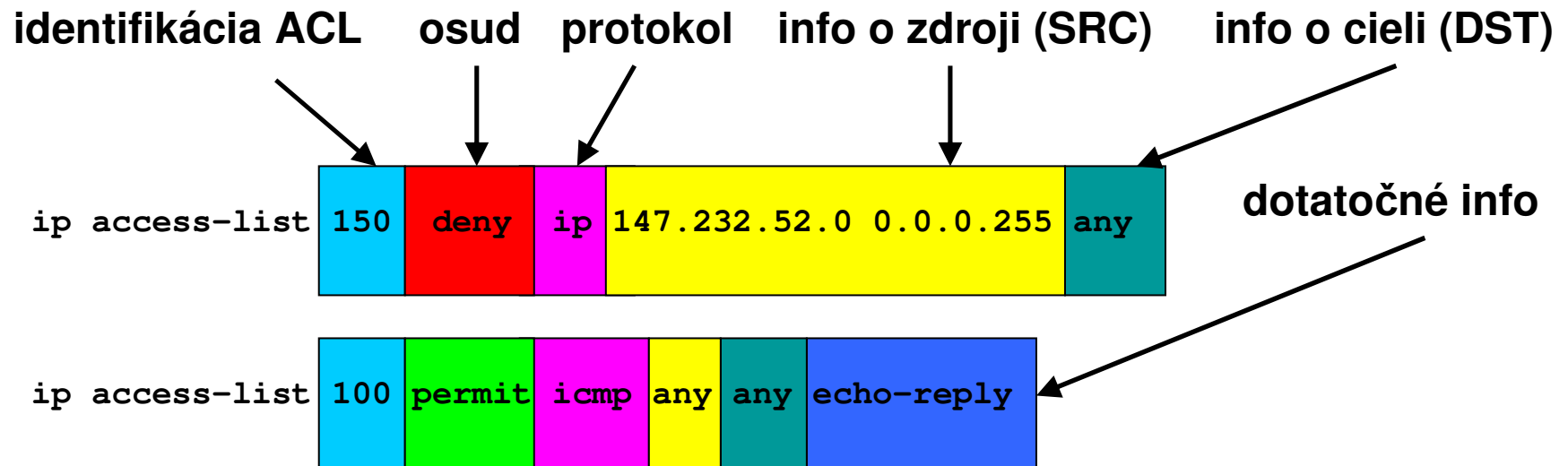
Odpoved': 64-127.4-7.109.0-63

Extended ACL

```
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq telnet
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq ftp
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq ftp-data
```

- Access list number range of 100 - 199 and 2000 to 2699
- Source destination IP address
- Layer 4 protocol number
- Applied to port closest to source host

Extended ACL



Pomenované ACL

- Vhodné pre individuálne modifikovanie položiek ACL bez jeho zmazania
- Ak máme viac ACL ako povoľuje číselný rozsah

- **Definovanie**

```
router(config)# ip access-list{standard | extended}  
name
```

- **Použitie**

```
router(config)# deny{source [source-wildcard] | any}
```

Alebo

```
router(config)# permit{source [source-wildcard] | any}
```

Pomenované ACL – príklad

```
ip access-list standard Internetfilter  
deny 192.5.34.0 0.0.0.255  
permit 128.88.0.0 0.0.255.255  
permit 36.0.0.0 0.255.255.255
```

```
Interface ethernet 0
```

```
Ip access-group Internetfilter out
```

Pomenované ACL

- **Príklady**

- `ip access-list standard VTY_pristup`
`permit host 147.232.22.70`
`permit host 147.232.22.65`
`deny any any log`
- Aplikujem v „line vty 0 4“:
`access-group VTY_pristup in`

- `ip access-list extended webServer`
`permit tcp any host 147.232.33.4 eq 80`
`permit tcp any host 147.232.33.4 eq 443`
`permit icmp any host 147.232.33.4`
`deny any any`
- Aplikujem v „interface FastEthernet 0/0“
`access-group webServer out`

Named ACLs

IP named ACLs were introduced in Cisco IOS Software Release 11.2.

Advantages are:

- Intuitively identify ACLs using **names** (not just numbers).
- **Extend possibilities** beyond 798 simple and 799 extended ACLs
- **Modification** of a NACL without deleting and reconfiguring it.

NACLs allow individual statements to be deleted without losing whole list.

It is still only possible to **add statements** to the **end of a list**.

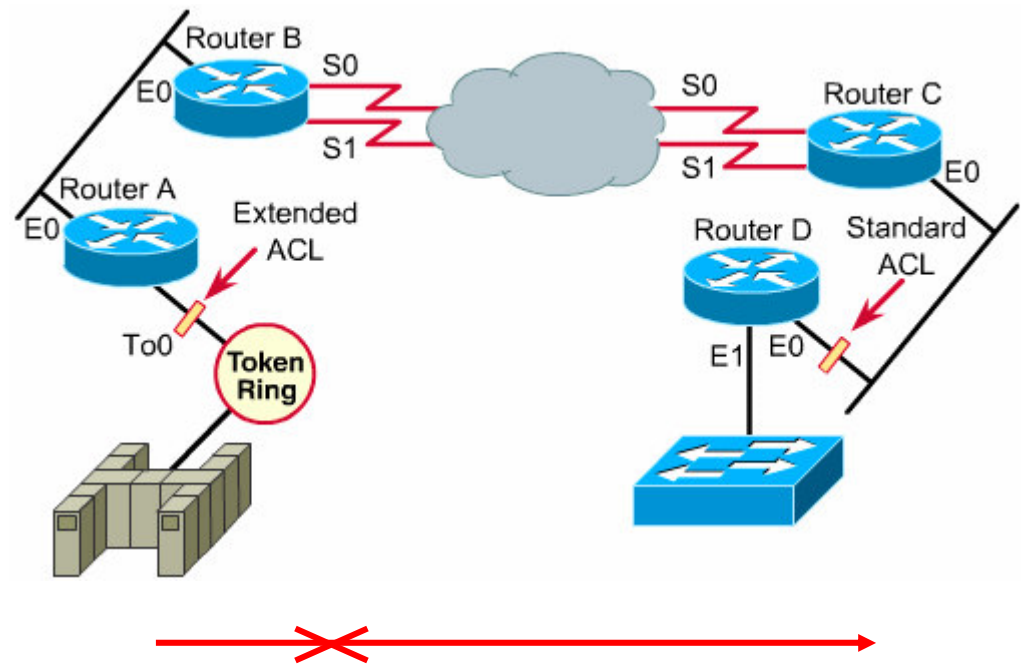
Standard or Extended

Administrator assigned name

```
Rio(config)# ip access-list extended Server-Access
Rio(config-ext-nacl)# permit tcp any host 10.0.0.2 eq smtp
Rio(config-ext-nacl)# permit udp any host 10.0.0.2 eq 53
Rio(config-ext-nacl)# [Control + Z]
Rio(config)# interface f 0/0
Rio(config-if)# ip access-group Server-Access out
```

Umiestnenie ACL

- rozšírený ACL umiestňovať čo najbližšie k zdroju blokovaných dát
- Štandardný ACL umiestňovať čo najbližšie k cieľu

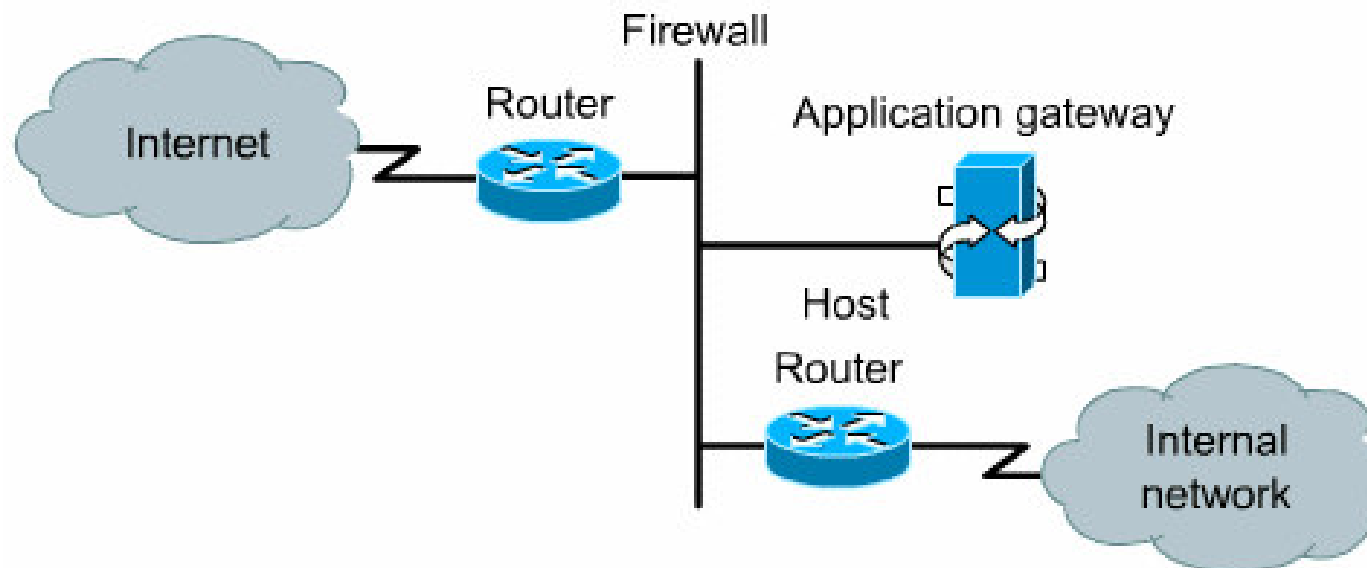


Zdroj pred
Routrom A

Cieľ za
routrom B

Umiestnenie ACL – firewall

- ACL Minimálne na okrajových smerovačoch
- ACL pre každý smerovaný protokol
- Filtrovanie na vstupnom i výstupnom rozhraní
- Vnútorňý smerovač prijíma pakety len od aplikačnej brány
- Vonkajší smerovač chráni aplikačnú bránu



Overovanie činnosti ACL

- Príkazy

Show ip interface

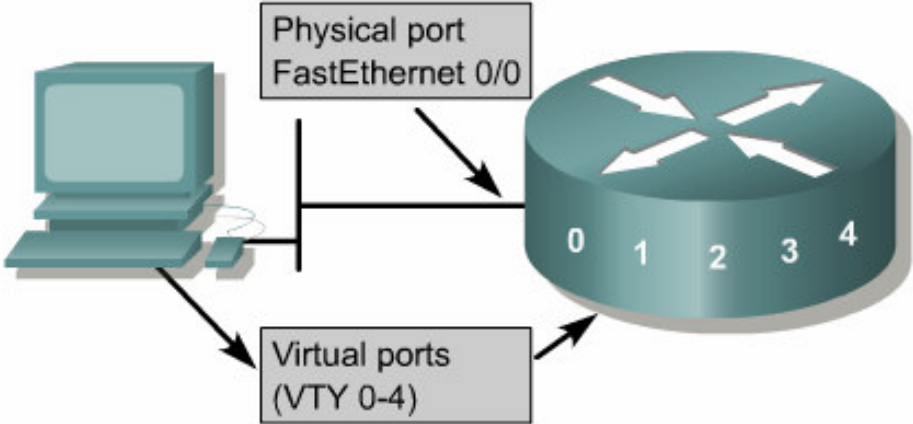
Show access-list

– Prípadne zadať číslo ACL

Obmedzenie telnet pristupu

Cisco - Hyperterminal

```
Creating the standard list:  
  
Rt1(config)#access-list 2 permit 172.16.1.0 0.0.0.255  
R11(config)#access-list 2 permit 172.16.2.0 0.0.0.255  
R11(config)#access-list 2 deny any  
  
Applying the access list:  
  
Rt1(config)#line vty 0 4  
Rt1(config)#login  
Rt1(config)#password secret  
Rt1(config)#access-class 2 in
```



Physical port
FastEthernet 0/0

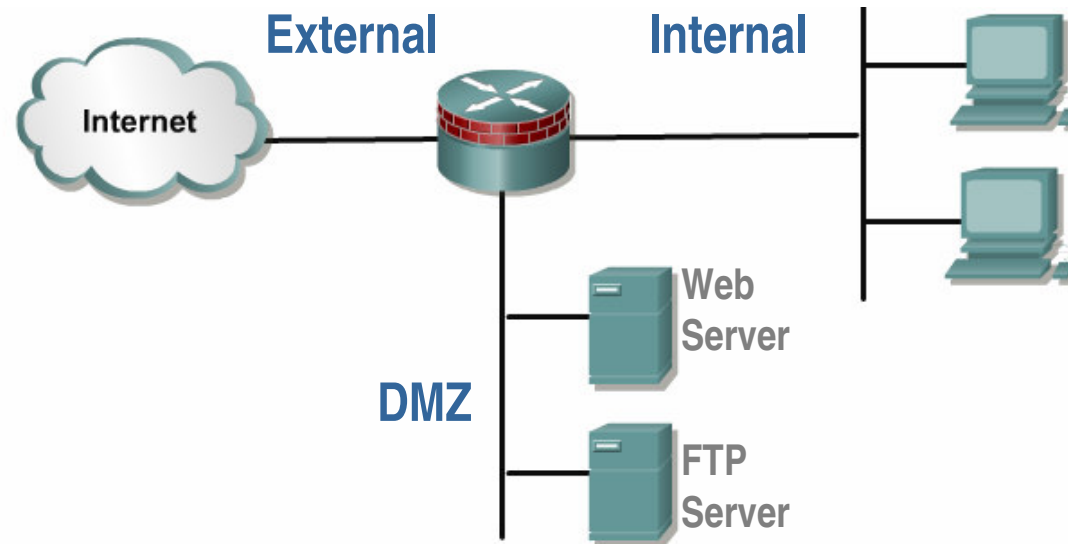
Virtual ports
(VTY 0-4)

ACL Rules

1. One access list per protocol , per interface , per direction .
2. Standard access lists should be applied closest to the destination .
3. Extended access lists should be applied closest to the source .
4. Use the inbound or outbound interface reference as if looking at the port from inside the router .
5. The implicit deny at the end of all access lists will not appear in the configuration listing.
6. Access list entries should filter in the order from specific to general .
7. The permit or deny is examined ONLY if the match is true .
8. New lines are always added to the end of the access list.
9. **no access-list** [number] will remove the whole list.
10. It is not possible to selectively add and remove lines with numbered ACLs.
11. An IP ACL will send ICMP host unreachable to sender of rejected packet.
12. In some situations, removing an access list may result in a default 'deny any' being applied to the interface.
13. Outbound filters do not affect traffic originating at the local router .

Firewalls

A network firewall can be one or several machines working together to prevent unwanted access.



Firewalls control access to services both into and from the internal network. ACLs are used in firewalls between the **internal** and **external** network. A **De-Militarised Zone** contains network services available to Internet traffic. The firewall router provides **isolation** for the internal network and the DMZ. Border routers (at the edge of a network) use ACLs to provide security benefits.

Restricting VTY Access

A router has both physical ports (Fa0/0, S0/0) and virtual ports.

These virtual ports are called vtv lines.

There are five such vty lines, numbered 0 to 4 (0 to 15 on later IOS).

VTY access can be restricted on routers by using access lists.

Access to vty is accomplished using Telnet.

Identical restrictions should be placed on all vty lines as it is not possible to control which line a user will connect on.

The process of creating a vty access list is the same as for an interface.

Applying the ACL to a terminal line (vty, aux or con) requires the command access-class instead of access-group.

Only numbered ACLs can be applied to vty lines.

```
Rio(config)# line vty 0 4
Rio(config-line)# login
Rio(config-line)# password Cisco
Rio(config-line)# access-class 2 in
Rio(config-line)# end
Rio#
```



Technická univerzita
v Košiciach



Fakulta elektrotechniky
a informatiky



Katedra počítačov
a informatiky