

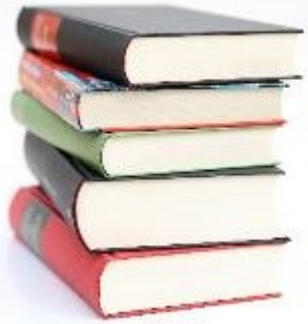


UNIVERSITY OF ŽILINA
Faculty of Management Science
and Informatics

Konektivita zákazník / ISP – PPPoE a external BGP (eBGP)

Pavel Segeč
Katedra informačných sietí
Fakulta riadenia a informatiky, ŽU





Čo bude v prednáške

- PPPoE
 - Cisco a PPPoE
- External BGP (eBGP)
 - V single homed zapojení



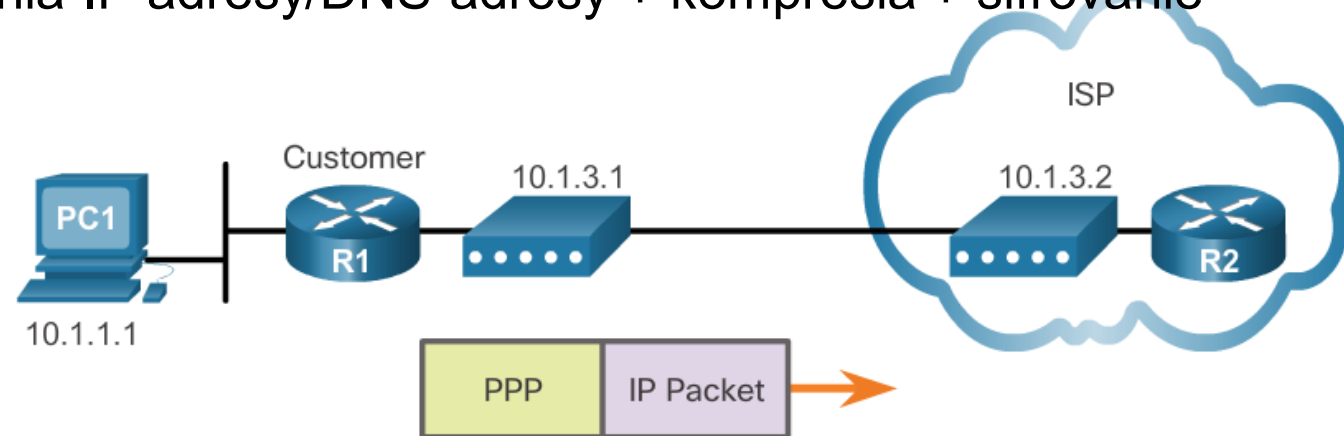
PPP over Ethernet (PPPoE)

PPP over Ethernet (PPPoE) – motivácia

- PPP - L2 p2p technológia nad analógovým dial-up, ISDN, sériové WAN linky
 - Primárne využívaná ISP
 - Má niektoré zaujímavé vlastnosti:
 - Schopnosť prideliť IP adresu cez PPP linku na diaľku (nie DHCP)
 - Podpora autentifikácie (CHAP + PAP)
- Súčasnosť => Ethernet => dominantne rozšírený
 - Populárny aj na prístupe do WAN
 - Ale napr. nemá podporu autentifikácie
- Idea, skombinuj Ethernet a PPP
 - => vznik PPP over Ethernet (PPPoE)
 - [Štandard RFC2516](#)

PPP over Ethernet (PPPoE) – kto ho využíva?

- PPPoE = enkapsulácia PPP v Ethernet (PPPoE + Ethernet = PPPoE)
 - Vytvára P-2-P prepoj cez BMA Ethernet
 - Je nástupcom PPPoverATM (PPPoA)
- PPP over Ethernet (PPPoE) – kto ho využíva?
 - ISP, ktorý získa
 - Možnosť autentifikácie viac klientov na jednom rozhraní PPPoE servera cez Ethernet
 - Každý klient bude mať svoje virtuálne rozhranie
 - Pozn. PPPoE Server má viac mien
 - AC - Access concentrator, BNG – Broadband Network Gateway, BRAS – Broadband Access Server
 - Využitie PPP autentifikácie + pridelenia IP adresy/DNS adresy + kompresia + šifrovanie
- Implementované primárne
 - WAN rozhrania
 - DSL a káblové modemy
 - Wireless



Dashboard > Security Fabric > Network > Interfaces

Name: port2
 Alias: WAN1
 Type: Physical Interface
 Role: WAN
 Estimated bandwidth: 0 kbps Upstream / 0 kbps Downstream

Addressing mode: Manual DHCP **PPPoE**

Status: Initializing...

Username: _____
 Password: _____

Unnumbered IP: 0.0.0.0
 Initial Disc Timeout: 1
 Initial PADT Timeout: 1

Retrieve default gateway from server:

FortiGate VCF_Fortigate
 Status: Up
 MAC address: 00:0c:29:e9:83:e4

Documentation: Online Help, Video Tutorials

OK Cancel

PPPoE na WAN rozhraní

Basic Information

Enable WAN:

Encapsulation Mode: IPoE PPPoE

Protocol Type: IPv4/IPv6

WAN Mode: Route WAN

Service Type: INTERNET

Enable VLAN:

VLAN ID: 82 (1-4094)

802.1p Policy: Use the specified value

802.1p: 0

MRU: 1462 (1280-1540)

User Name: username15

Password:

Enable LCP Detection:

Binding Options: LAN1 LAN2 LAN3 LAN4
 SSID1 SSID2 SSID3 SSID4

IPv4 Information

IP Acquisition Mode: Static DHCP PPPoE

Enable NAT:

NAT type: Port-restricted cone NAT

Enable DNS Override:

Multicast VLAN ID: _____ (0-4094; 0 indicates untagged VLAN.)

IPv6 Information

Prefix Acquisition Mode: DHCPv6-PD Static None

IP Acquisition Mode: DHCPv6 Automatic Static None

Prefix Mask: _____ (IPv6 address/64)

Multicast VLAN ID: _____ (0-4094; 0 indicates untagged VLAN.)

Apply Cancel

BASIC LAN PRIMARY WAN WI-FI SECURITY / APP VISIBILITY

WAN Configuration

WAN Type *
 Interface *

DNS / IP Address

Get DNS Server info directly from ISP

Get IP automatically from ISP

Enable NAT

Profile

Access Point Name (APN) *

Configure username and password if provided by service

< LAN SETTINGS

Interface <pppoe-out1>

General Dial Out Status Traffic

Service: _____
 AC Name: _____

User: mikrotik_wan
 Password:

Profile: default

Keepalive Timeout: 60

Dial On Demand
 Use Peer DNS
 Add Default Route

Default Route Distance: 0

- Allow
 pap chap
 mschap1 mschap2

OK Cancel Apply Disable Comment Copy Remove Torch PPPoE Scan

PPPoE fázy

■ Fáza Active Discovery

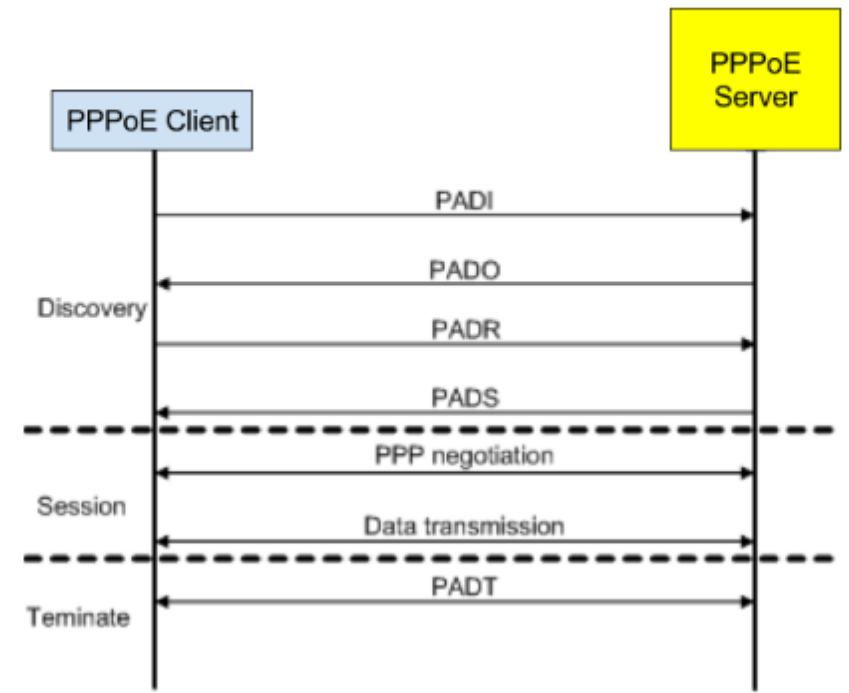
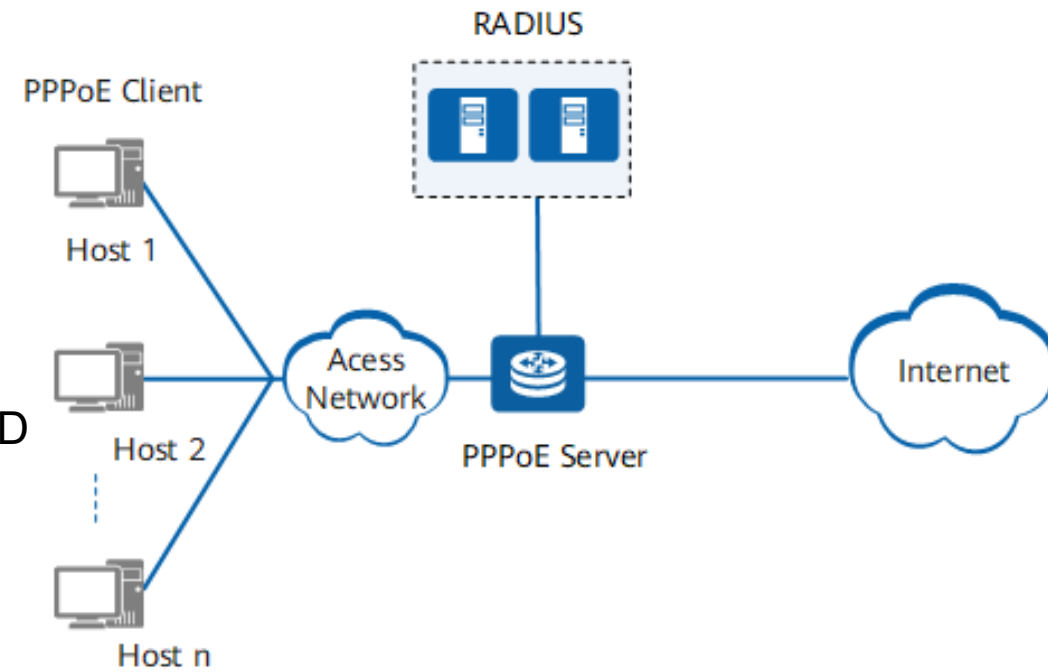
- Účel: klient lokalizuje PPPoE server (*Access concentrator*) a zistí jeho MAC adresu, založí s AC spojenie, získa Session ID
- Discovery proces má 4 kroky
 - Klient> Inicializácia komunikácie: klient odošle **PPPoE Active Discovery Initiation (PADI)** broadcast paket, ktorý obsahuje žiadosť o službu (spojenie)
 - AC> odpovie **PPPoE Active Discovery Offer (PADO)**: ten obsahuje meno AC + detaily o službe.
 - Klient> vyberie si Offer (môže byť od viac AC) a požiada oň cez **PPPoE Active Discovery Request (PADR)**
 - AC> potvrdí spojenie odoslaním **PPPoE Active Discovery Session-confirmation (PADS)** paketu + **pridelí Session ID** (aby AC vedel s kým komunikuje)
- Klient vždy používa svoju Session ID + MAC address AC

■ Fáza PPP Session

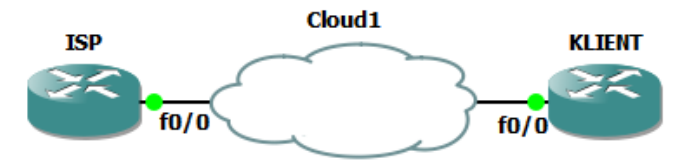
- Sú dojednané voliteľné nastavenia spojenia
- Vykoná sa autentifikácia

■ Fáza ukončenia

- **PPPoE Active Discovery Terminate (PADT)**



Založenie PPPoE



ppp or pppoe or pppoeo or pppoes or icmp

Time	Source	Destination	Protocol	Length	Info	
11 40.144189	ca:02:9e:fa:00:08	Broadcast	PPPoED	60	Active Discovery Initiation (PADI)	PPPOE FÁZA PADI
12 40.149952	ca:01:9c:3a:00:08	ca:02:9e:fa:00:08	PPPoED	63	Active Discovery Offer (PADO) AC-Name='ISP'	PADO
14 42.188192	ca:02:9e:fa:00:08	ca:01:9c:3a:00:08	PPPoED	63	Active Discovery Request (PADR) AC-Name='ISP'	PADR
15 42.224243	ca:01:9c:3a:00:08	ca:02:9e:fa:00:08	PPPoED	63	Active Discovery Session-confirmation (PADS) AC-Name='ISP'	PADS
16 42.329232	ca:02:9e:fa:00:08	ca:01:9c:3a:00:08	PPP LCP	60	Configuration Request	PPP – ZALOŽ. LINKY
17 42.345105	ca:01:9c:3a:00:08	ca:02:9e:fa:00:08	PPP LCP	60	Configuration Request	
18 42.345144	ca:01:9c:3a:00:08	ca:02:9e:fa:00:08	PPP LCP	60	Configuration Ack	
19 42.359455	ca:02:9e:fa:00:08	ca:01:9c:3a:00:08	PPP LCP	60	Configuration Ack	
20 42.395517	ca:01:9c:3a:00:08	ca:02:9e:fa:00:08	PPP CHAP	60	Challenge (NAME='ISP', VALUE=0x7fe39ba70da9310da5e9ad0ab5e644f6)	
21 42.409824	ca:02:9e:fa:00:08	ca:01:9c:3a:00:08	PPP CHAP	60	Response (NAME='Pouzivatel_1', VALUE=0x558b4db060c579457d03d0208d2d8fd1)	
22 42.647298	ca:01:9c:3a:00:08	ca:02:9e:fa:00:08	PPP CHAP	60	Success (MESSAGE='')	PPP CHAP AUTENT.
23 42.657424	ca:01:9c:3a:00:08	ca:02:9e:fa:00:08	PPP IPCP	60	Configuration Request	
24 42.711886	ca:02:9e:fa:00:08	ca:01:9c:3a:00:08	PPP IPCP	60	Configuration Request	
25 42.711916	ca:02:9e:fa:00:08	ca:01:9c:3a:00:08	PPP CDPCP	60	Configuration Request	PPP NCP FÁZA
26 42.727952	ca:01:9c:3a:00:08	ca:02:9e:fa:00:08	PPP IPCP	60	Configuration Nak	
27 42.727988	ca:01:9c:3a:00:08	ca:02:9e:fa:00:08	PPP LCP	60	Protocol Reject	
28 42.742103	ca:02:9e:fa:00:08	ca:01:9c:3a:00:08	PPP IPCP	60	Configuration Ack	
29 42.742135	ca:02:9e:fa:00:08	ca:01:9c:3a:00:08	PPP IPCP	60	Configuration Request	
30 42.748175	ca:01:9c:3a:00:08	ca:02:9e:fa:00:08	PPP IPCP	60	Configuration Ack	
33 52.566141	ca:01:9c:3a:00:08	ca:02:9e:fa:00:08	PPP LCP	60	Echo Request	UDRŽIAVANIE LINKY
34 52.570402	ca:02:9e:fa:00:08	ca:01:9c:3a:00:08	PPP LCP	60	Echo Reply	
35 52.671110	ca:02:9e:fa:00:08	ca:01:9c:3a:00:08	PPP LCP	60	Echo Request	
36 52.676950	ca:01:9c:3a:00:08	ca:02:9e:fa:00:08	PPP LCP	60	Echo Reply	
40 62.564793	ca:01:9c:3a:00:08	ca:02:9e:fa:00:08	PPP LCP	60	Echo Request	

PPPoE - Fáza Active Discovery

PADI

- ▼ PPP-over-Ethernet Discovery
 - 0001 = Version: 1
 - 0001 = Type: 1
 - Code: Active Discovery Initiation (PADI) (0x09)
 - Session ID: 0x0000
 - Payload Length: 16
 - ▼ PPPoE Tags
 - Host-Uniq: a900000100000ea4

PADR

- PPP-over-Ethernet Discovery
 - 0001 = Version: 1
 - 0001 = Type: 1
 - Code: Active Discovery Request (PADR) (0x19)
 - Session ID: 0x0000
 - Payload Length: 43
 - ▼ PPPoE Tags
 - Host-Uniq: a900000100000ea4
 - AC-Name: ISP
 - AC-Cookie: d5824df956eef48688be9ee3507061e8

PADO

- PPP-over-Ethernet Discovery
 - 0001 = Version: 1
 - 0001 = Type: 1
 - Code: Active Discovery Offer (PADO) (0x07)
 - Session ID: 0x0000
 - Payload Length: 43
 - ▼ PPPoE Tags
 - Host-Uniq: a900000100000ea4
 - AC-Name: ISP
 - AC-Cookie: d5824df956eef48688be9ee3507061e8

PADS

- PPP-over-Ethernet Discovery
 - 0001 = Version: 1
 - 0001 = Type: 1
 - Code: Active Discovery Session-confirmation (PADS) (0x65)
 - Session ID: 0x0002
 - Payload Length: 43
 - ▼ PPPoE Tags
 - Host-Uniq: a900000100000ea4
 - AC-Name: ISP
 - AC-Cookie: d5824df956eef48688be9ee3507061e8

CHAP Autentifikácia

```
ca:01:9c:3a:00:08 ca:02:9e:fa:00:08 PPP CHAP 60 Challenge (NAME='ISP', VALUE=0x7fe39ba70da9310da5e9ad0ab5e644f6)
ca:02:9e:fa:00:08 ca:01:9c:3a:00:08 PPP CHAP 60 Response (NAME='Pouzivatel_1', VALUE=0x558b4db060c579457d03d0208d2d8fd1)
ca:01:9c:3a:00:08 ca:02:9e:fa:00:08 PPP CHAP 60 Success (MESSAGE='')
```

▼ PPP-over-Ethernet Session

```
0001 .... = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x0002
Payload Length: 26
```

▼ Point-to-Point Protocol

```
Protocol: Challenge Handshake Authentication Protocol (0xc223)
```

▼ PPP Challenge Handshake Authentication Protocol

```
Code: Challenge (1)
Identifier: 1
Length: 24
```

▼ Data

```
Value Size: 16
Value: 7fe39ba70da9310da5e9ad0ab5e644f6
Name: ISP
```

> PPP-over-Ethernet Session

> Point-to-Point Protocol

▼ PPP Challenge Handshake Authentication Protocol

```
Code: Response (2)
Identifier: 1
Length: 33
```

▼ Data

```
Value Size: 16
Value: 558b4db060c579457d03d0208d2d8fd1
Name: Pouzivatel_1
```

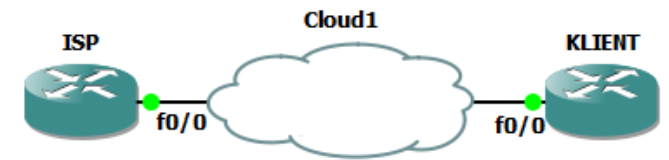
> PPP-over-Ethernet Session

> Point-to-Point Protocol

▼ PPP Challenge Handshake Authentication Protocol

```
Code: Success (3)
Identifier: 1
Length: 4
```

Ukončenie PPPoE



87	132.701484	ca:01:9c:3a:00:08	ca:02:9e:fa:00:08	PPP LCP	60 Echo Request
89	142.702167	ca:01:9c:3a:00:08	ca:02:9e:fa:00:08	PPP LCP	60 Echo Request
91	152.782522	ca:01:9c:3a:00:08	ca:02:9e:fa:00:08	PPP LCP	60 Termination Request
92	152.822881	ca:01:9c:3a:00:08	ca:02:9e:fa:00:08	PPPoED	60 Active Discovery Terminate (PADT)

Ukončenie spojenia

Frame 92: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface -, id 0
Ethernet II, Src: ca:01:9c:3a:00:08 (ca:01:9c:3a:00:08), Dst: ca:02:9e:fa:00:08 (ca:02:9e:fa:00:08)

PPP-over-Ethernet Discovery

0001 = Version: 1

.... 0001 = Type: 1

Code: Active Discovery Terminate (PADT) (0xa7)

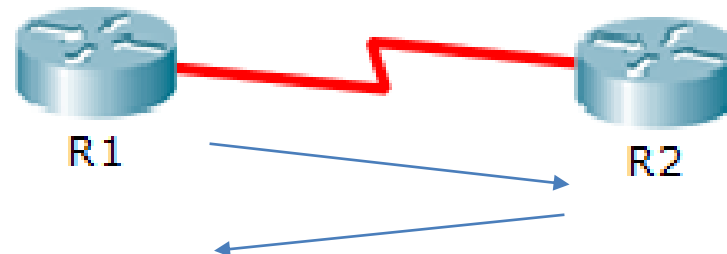
Session ID: 0x0002

Payload Length: 0

Základná **PPP** konfigurácia

```
! R1 („server“)  
---  
username R2 password 0 R2pass  
!  
interface Serial10/0/0  
 ip address 10.0.0.1 255.0.0.0  
 encapsulation ppp  
 ppp authentication pap
```

```
! R2 (klient)  
---  
!  
interface Serial10/0/0  
 ip address 10.0.0.2 255.0.0.0  
 encapsulation ppp  
 ppp pap sent-username R2 password 0  
 R2pass
```



Pozn. Ide aj v PT.

PPP konfigurácia s pridelením adresy a D.R. cez PPP

```
! R1 - prideli IP
! ---
username R2 password 0 R2pass
!
ip local pool PPP_Pool 10.0.0.10 10.0.0.20
!
interface Serial10/0
 ip address 10.0.0.1 255.0.0.0
 encapsulation ppp
 peer default ip address pool PPP_Pool
 ppp authentication pap
```

```
! R2 - dostane IP
! ---

!
interface Serial10/0
 ! Vypytaj si IPcku
 ip address negotiated
 encapsulation ppp
 ppp pap sent-username R2 password 0 R2pass
 ! Instaluj po aktivacii linky
 ! def. route, comm prepise inu def. route
 ppp ipcp route default
```



PPPoE konfigurácia v Cisco IOS

- PPPoE prístupový koncentrátor
 - Môže a bude obsluhovať veľa klientov
- Cisco separuje konfiguráciu pre vyššiu flexibilitu na:
 - Tzv. **Šablóny** (templates) s parametrami
 - Vytvárajú a rušia sa z nich Virtuálne rozhrania ako sa pripájajú/odpájajú klienti
 - PPPoE **BBA profily** skupín (BBA – BroadBand Aggregator)
 - Jedno zariadenie môže mať viac profilov s rôznymi parami
 - Každý profil môže mať viac šablón rozhraní

PPPoE konfigurácia v Cisco IOS - príklad

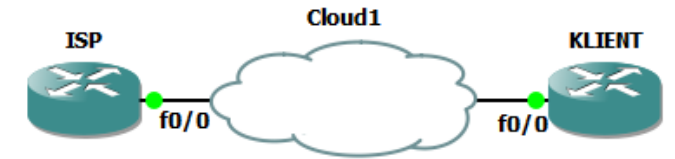
PPPoE prístupový koncentrátor - ISP

- Vytvor lokálnu DB mien a hesiel zákazníkov
- Vytvor pool IP adries na pridelovanie zákazníkom
- Vytvor konfiguračný template pre virtuálne rozhrania
 - Každý pripojený zákazník bude mať z neho jedno Virtual Access (VA) rozhranie
 - Vytvorené/zrušené na požiadavku dynamicky
 - V ňom
 - Nastav mu IP adresu
 - Nastav, ktorý adresný pool sa bude používať
 - Zníž MTU na 1492
 - Nastav autentifikáciu, a iné param, napr. DNS, def. route
- Asociuj virtuálny template s PPPoE grupou (PPPoE koncentrátorom)
- Spusti PPPoE na Ethernet rozhraní k zákazníkovi

PPPoE klient (dialer) – zákazník

- Vytvor virtuálne *interf dialer NUM* rozhranie
 - Nastav v ňom
 - Enkapsuláciu na PPP
 - Vyžiadanie IP adresy od ISP
 - Zníž MTU na 1492 aby sa do ethernet rámca zmestili PPP hlavičky
 - Vytvor dialer pool
 - Nastav autentifikáciu, napr. CHAP, a nastav meno/heslo získané od ISP
- Aktivuj PPPoE klienta a dialer pool na rozhraní vedúcom k ISP

Router ako dialer – PPPoE klient



■ PPPoE prístupový koncentrátor (server)

```

!ISP (PPPOE server):
!---
Int lo 0
  ip address 10.0.0.254 255.255.255.0

! Local DB hesiel pre autentifikáciu
username Pouzivatel_1 password ciscoppoe
username Pouzivatel_1 autocommand logout

! Pool adres pre klientov
ip local pool PPPoE-POOL 10.0.0.1 10.0.0.10

! Virtual template
interface virtual-template 1
  ip unnumbered loop 0
  mtu 1492
  ppp mtu adaptive
  ip tcp adjust-mss 1452
  peer default ip address pool PPPoE-POOL
  ppp authentication chap
  ppp ipcp dns 8.8.8.8

! Asociuj template s PPPoE grupou
! Bba - Broadband aggregator
bba-group pppoe global
  virtual-template 1

! Nastav template na INPUT rozhranie smerom k zakaznik.
interface fa0/0
  pppoe enable group global
  
```

■ PPPoE Dialer (klient)

```

!Klient (customer 1):
!---
interface dialer 1
  encapsulation ppp
  ip address negotiated
  mtu 1492
  dialer pool 1

  ppp chap hostname Pouzivatel_1
  ppp chap password ciscoppoe

  ! Instaluj def. route po uspesnej inicializácii
  ppp ipcp route default

  ! Aby relacia po uplynuti casovaca nepadala
  ! dialer persistent

! Or pouzi staticku def. route
! ip route 0.0.0.0 0.0.0.0 dialer 1

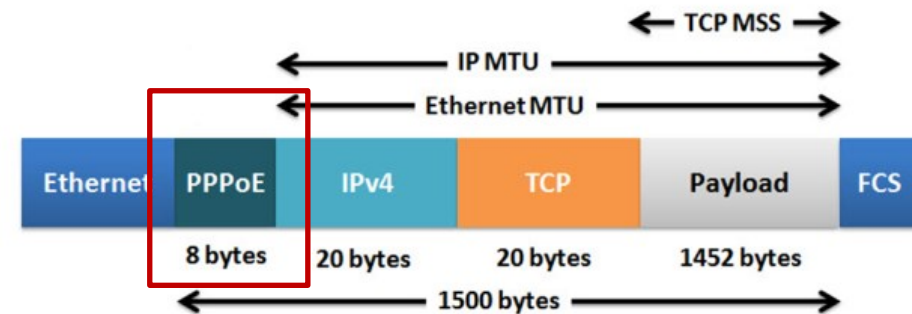
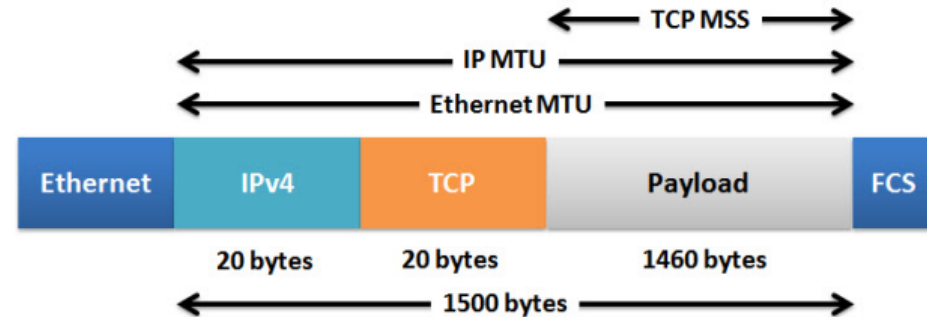
! Aktivuj PPPoE na OUTPUT rozhraní k ISP
interface fa0/0
  no ip address
  pppoe enable group global
  pppoe-client dial-pool-number 1
  no shut
!
  
```

Prečo ponížiť MTU

- MSS: maximum segment size
- MTU: maximum transmission unit
- Nezníženie MTU pod 1500 spôsobí čo ...?

Fragmentáciu!

- `ip tcp adjust-mss` *max-segment-size*
 - Prispôsobí TCP MSS hodnotu počas TCP 3-way handshake

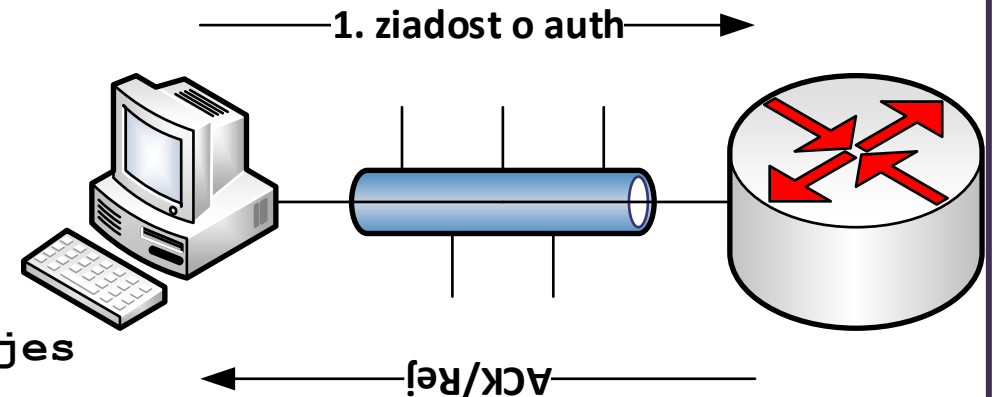


PPPoE access koncentrátor s PC Win 7/10 ako klient

```
interface Loopback0
  ip address 10.255.255.1 255.255.255.255
!
! Spusti ppoe server
! Tzv. Broadband agregator
bba-group ppoe global
  virtual-template 1
  ! Umravni aktivne Windows
  ! pps (sec) cas merania) kolko sekund ingorujes
  sessions per-mac throttle 100 1 2

! Pool adries pre klientov
ip local pool Adresy-PPPoE-Klientov 192.168.1.1 192.168.1.254

! Vytvor virtual template s parametrami
interface Virtual-Template1
  ip unnumbered Loopback0
  peer default ip address pool Adresy-PPPoE-Klientov
  mtu 1492
  ppp mtu adaptive
  ip tcp adjust-mss 1452
  ppp authentication ms-chap-v2 ms-chap chap
  ppp ipcp dns 158.193.152.2
```



PPPoE access koncentrátor s PC Win 7/10 ako klient (2.)

```
! Aktivacia PPPoE servera na ethernetovom rozhrani
interface FastEthernet0/0
  pppoe enable group global
  no shutdown

! Username-y pre PPPoE autentifikáciu
! logout command je aby sa dany clovek s danym kontom
! nemohol prihlasit napr. na
! konzolu, ak je na nej login local
username someuser1 privilege 0 password 0 h3s10
username someuser1 autocommand logout
username someuser2 privilege 0 password 0 in3h3s10
username someuser2 autocommand logout
```

===== WIN 7 / 10 =====

```
! Wo windows 7 treba ist do network center a v nom vybrat „setup new connection“, vybrat
„connect to internet“, vybrat „setup new connection“ a ten hned ponukne Broadband PPPoE
```



PPPoE - overenie a diagnostika

Overenie PPPoE

- **show ip interface brief**
 - či sme dostali správnu IP adresu
- **show interface dialer**
 - zobrazí, či je MTU a PPP enkapsulácia konfigurovaná na dialer rozhraní
- **show pppoe session**
 - Zobrazí info o aktívnych PPPoE reláciach

```
ISP# show pppoe session
  1 session in LOCALLY_TERMINATED (PTA) State
  1 session total
```

Uniq ID	PPPoE	RemMAC	Port	VT	VA	State
	SID	LocMAC			VA-st	Type
3	3	ca02.9efa.0008	Fa0/0	1	Vi2.1	PTA
		ca01.9c3a.0008			UP	

```
KLIENT# show pppoe session
  1 client session
```

Uniq ID	PPPoE	RemMAC	Port	VT	VA	State
	SID	LocMAC			VA-st	Type
N/A	3	ca01.9c3a.0008	Fa0/0	Di1	Vi2	UP
		ca02.9efa.0008			UP	

Show ip int brie

```
KLIENT#show ip int brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	unset	up	up
FastEthernet0/1	unassigned	YES	unset	administratively down	down
Serial1/0	unassigned	YES	unset	administratively down	down
Serial1/1	unassigned	YES	unset	administratively down	down
Serial1/2	unassigned	YES	unset	administratively down	down
Serial1/3	unassigned	YES	unset	administratively down	down
Dialer1	10.0.0.3	YES	IPCP	up	up
Virtual-Access1	unassigned	YES	unset	up	up
Virtual-Access2	unassigned	YES	unset	up	up

```
ISP#show ip int brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	unset	up	up
FastEthernet0/1	unassigned	YES	unset	administratively down	down
Serial1/0	unassigned	YES	unset	administratively down	down
Serial1/1	unassigned	YES	unset	administratively down	down
Serial1/2	unassigned	YES	unset	administratively down	down
Serial1/3	unassigned	YES	unset	administratively down	down
Loopback0	10.0.0.254	YES	manual	up	up
Virtual-Access1	unassigned	YES	unset	down	down
Virtual-Access2	unassigned	YES	unset	up	up
Virtual-Access2.1	10.0.0.254	YES	unset	up	up
Virtual-Template1	10.0.0.254	YES	unset	down	down

Show int dialer 1

```
KLIENT# show interfaces dialer 1
Dialer1 is up, line protocol is up (spoofing)
  Hardware is Unknown
  Internet address is 10.0.0.3/32
  MTU 1492 bytes, BW 56 Kbit/sec, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Closed, loopback not set
  Keepalive set (10 sec)
  DTR is pulsed for 1 seconds on reset
  Interface is bound to Vi2
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 00:40:52
  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
    7 packets input, 538 bytes
    228 packets output, 4256 bytes
Bound to:
V, 0 output buffers swapped out
  0 carrier transitions
irtual-Access2 is up, line protocol is up
  Hardware is Virtual Access interface
  MTU 1492 bytes, BW 56 Kbit/sec, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
```

→→

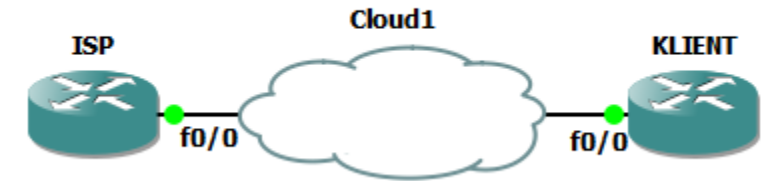
→→

```
Encapsulation PPP, LCP Open
  Stopped: CDPCP
  Open: IPCP
  PPPoE vaccess, cloned from Dialer1
  Vaccess status 0x44, loopback not set
  Keepalive set (10 sec)
  Interface is bound to Di1 (Encapsulation PPP)
  Last input 00:00:04, output never, output hang never
  Last clearing of "show interface" counters 00:34:09
  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
    200 packets input, 2805 bytes, 0 no buffer
  Received 0 broadcasts (0 IP multicasts)
  0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored,
0 abort
  199 packets output, 2802 bytes, 0 underruns
  0 output errors, 0 collisions, 0 interface resets
  0 unknown protocol drops
  0 output buffer failures
```

PPPoE diagnostika

- Chyba pri PPPoE môže byť v:
 - Chyba v PPP negociácii (spomínate na LCP/NCP??)
 - Možné chyby
 - Nie je odpoveď od ISP
 - LCP neprebehol
 - Chyba autentifikácie
 - Chyba IPCP
 - **debug ppp negotiation**
 - Chyba v PPP autentifikácii
 - Možné chyby
 - Nenakonfigurovanie, preklep, navzájom nezhodná metóda
 - **debug ppp authentication**
 - **debug ppp negotiation**
 - Chyba v prispôbení TCP segmentov

Chyba v PPP negociácii – zlé heslo



```

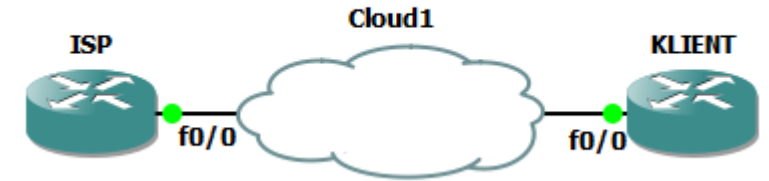
KLIENT(config-if)#do debug ppp negotiation
PPP protocol negotiation debugging is on
KLIENT(config-if)#no shut
KLIENT(config-if)#

*Mar 22 09:19:05.863: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state
to up
*Mar 22 09:19:06.863: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up
*Mar 22 09:19:12.379: %DIALER-6-BIND: Interface Vi2 bound to profile Di1
*Mar 22 09:19:12.391: %LINK-3-UPDOWN: Interface Virtual-Access2, changed state
to up
*Mar 22 09:19:12.395: Vi2 PPP: Sending cstate UP notification
*Mar 22 09:19:12.399: Vi2 PPP: Processing CstateUp message
*Mar 22 09:19:12.439: PPP: Alloc Context [699FF068]
*Mar 22 09:19:12.439: ppp12 PPP: Phase is ESTABLISHING
*Mar 22 09:19:12.443: Vi2 PPP: Using dialer call direction
*Mar 22 09:19:12.443: Vi2 PPP: Treating connection as a callout
*Mar 22 09:19:12.447: Vi2 PPP: Session handle[7400000C] Session id[12]
*Mar 22 09:19:12.447: Vi2 LCP: Event[OPEN] State[Initial to Starting]
*Mar 22 09:19:12.447: Vi2 PPP: No remote authentication for call-out
*Mar 22 09:19:12.451: Vi2 LCP: O CONFREQ [Starting] id 1 len 14
*Mar 22 09:19:12.451: Vi2 LCP: MRU 1492 (0x010405D4)
*Mar 22 09:19:12.455: Vi2 LCP: MagicNumber 0x02CDFA2F (0x050602CDFA2F)
*Mar 22 09:19:12.455: Vi2 LCP: Event[UP] State[Starting to REQsent]
*Mar 22 09:19:12.503: Vi2 LCP: I CONFREQ [REQsent] id 1 len 19
*Mar 22 09:19:12.503: Vi2 LCP: MRU 1492 (0x010405D4)
*Mar 22 09:19:12.507: Vi2 LCP: AuthProto CHAP (0x0305C22305)
*Mar 22 09:19:12.507: Vi2 LCP: MagicNumber 0x01D31B68 (0x050601D31B68)
*Mar 22 09:19:12.507: Vi2 LCP: O CONFACK [REQsent] id 1 len 19
*Mar 22 09:19:12.511: Vi2 LCP: MRU 1492 (0x010405D4)
*Mar 22 09:19:12.511: Vi2 LCP: AuthProto CHAP (0x0305C22305)
*Mar 22 09:19:12.511: Vi2 LCP: MagicNumber 0x01D31B68 (0x050601D31B68)
    
```

```

*Mar 22 09:19:12.511: Vi2 LCP: Event[Receive ConfReq+] State[REQsent to ACKsent]
*Mar 22 09:19:12.511: Vi2 LCP: I CONFACK [ACKsent] id 1 len 14
*Mar 22 09:19:12.511: Vi2 LCP: MRU 1492 (0x010405D4)
*Mar 22 09:19:12.511: Vi2 LCP: MagicNumber 0x02CDFA2F (0x050602CDFA2F)
*Mar 22 09:19:12.511: Vi2 LCP: Event[Receive ConfAck] State[ACKsent to Open]
*Mar 22 09:19:12.527: Vi2 PPP: Phase is AUTHENTICATING, by the peer
*Mar 22 09:19:12.527: Vi2 LCP: State is Open
*Mar 22 09:19:12.535: Vi2 CHAP: I CHALLENGE id 1 len 24 from "ISP"
*Mar 22 09:19:12.543: Vi2 CHAP: Using hostname from interface CHAP
*Mar 22 09:19:12.543: Vi2 CHAP: Using password from interface CHAP
*Mar 22 09:19:12.543: Vi2 CHAP: O RESPONSE id 1 len 33 from "Pouzivatel_1"
*Mar 22 09:19:12.559: Vi2 CHAP: I FAILURE id 1 len 25 msg is "Authentication
failed"
*Mar 22 09:19:12.559: Vi2 PPP DISC: We failed authentication
*Mar 22 09:19:12.563: PPP: NET STOP send to AAA.
*Mar 22 09:19:12.563: Vi2 LCP: I TERMREQ [Open] id 2 len 4
*Mar 22 09:19:12.563: Vi2 PPP: Phase is TERMINATING
*Mar 22 09:19:12.567: Vi2 LCP: O TERMACK [Open] id 2 len 4
*Mar 22 09:19:12.571: Vi2 LCP: Event[Receive TermReq] State[Open to Stopping]
*Mar 22 09:19:12.583: %DIALER-6-UNBIND: Interface Vi2 unbound from profile Di1
*Mar 22 09:19:12.591: Vi2 PPP: Block vaccess from being freed [0x10]
*Mar 22 09:19:12.595: %LINK-3-UPDOWN: Interface Virtual-Access2, changed state
to down
*Mar 22 09:19:12.603: Vi2 PPP: Sending cstate DOWN notification
*Mar 22 09:19:12.607: Vi2 PPP: Processing CstateDown message
*Mar 22 09:19:12.607: Vi2 LCP: Event[CLOSE] State[Stopping to Closing]
*Mar 22 09:19:12.615: Vi2 LCP: Event[DOWN] State[Closing to Initial]
*Mar 22 09:19:12.619: Vi2 PPP: Unlocked by [0x10] Still Locked by [0x0]
*Mar 22 09:19:12.619: Vi2 PPP: Free previously blocked vaccess
*Mar 22 09:19:12.619: Vi2 PPP: Phase is DOWN
    
```

Chyba v PPPautentifikácii



```

KLIENT# debug ppp authentication
PPP authentication debugging is on
  
```

```

KLIENT#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
KLIENT(config)#int fa 0/0
KLIENT(config-if)#no shutdown
KLIENT(config-if)#
  
```

```

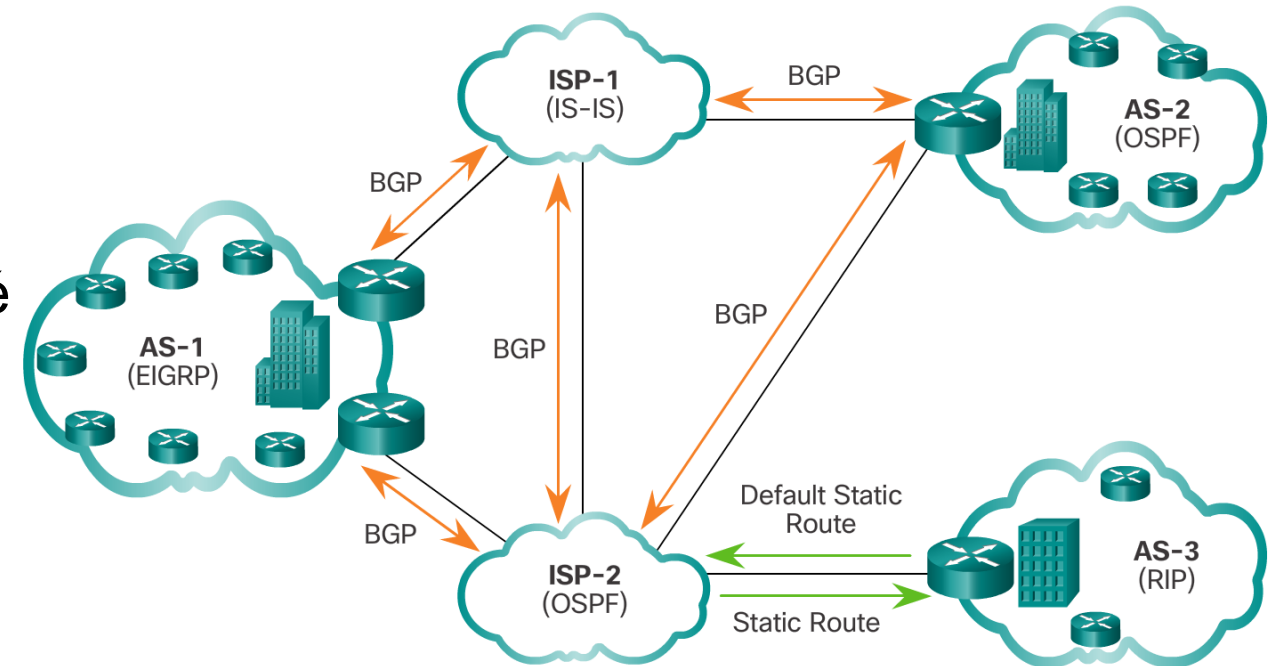
*Mar 22 09:15:57.135: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 22 09:15:58.135: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up
*Mar 22 09:16:00.291: %DIALER-6-BIND: Interface Vi2 bound to profile Di1
*Mar 22 09:16:00.303: %LINK-3-UPDOWN: Interface Virtual-Access2, changed state to up
*Mar 22 09:16:00.351: Vi2 PPP: Using dialer call direction
*Mar 22 09:16:00.351: Vi2 PPP: Treating connection as a callout
*Mar 22 09:16:00.355: Vi2 PPP: Session handle[4F000004] Session id[4]
*Mar 22 09:16:00.431: Vi2 PPP: No authorization without authentication
*Mar 22 09:16:00.467: Vi2 CHAP: I CHALLENGE id 1 len 24 from "ISP"
*Mar 22 09:16:00.471: Vi2 PPP: Sent CHAP SENDAUTH Request
*Mar 22 09:16:00.475: Vi2 PPP: Received SENDAUTH Response FAIL
*Mar 22 09:16:00.475: Vi2 CHAP: Using hostname from interface CHAP
*Mar 22 09:16:00.475: Vi2 CHAP: Using password from interface CHAP
*Mar 22 09:16:00.475: Vi2 CHAP: O RESPONSE id 1 len 33 from "Pouzivatel 1"
*Mar 22 09:16:00.491: Vi2 CHAP: I FAILURE id 1 len 25 msg is "Authentication failed"
*Mar 22 09:16:00.543: %DIALER-6-UNBIND: Interface Vi2 unbound from profile Di1
KLIENT(config-if)#
  
```



eBGP – external Border Gateway Protocol

Dynamické smerovacie protokoly - logický pohľad na Internet

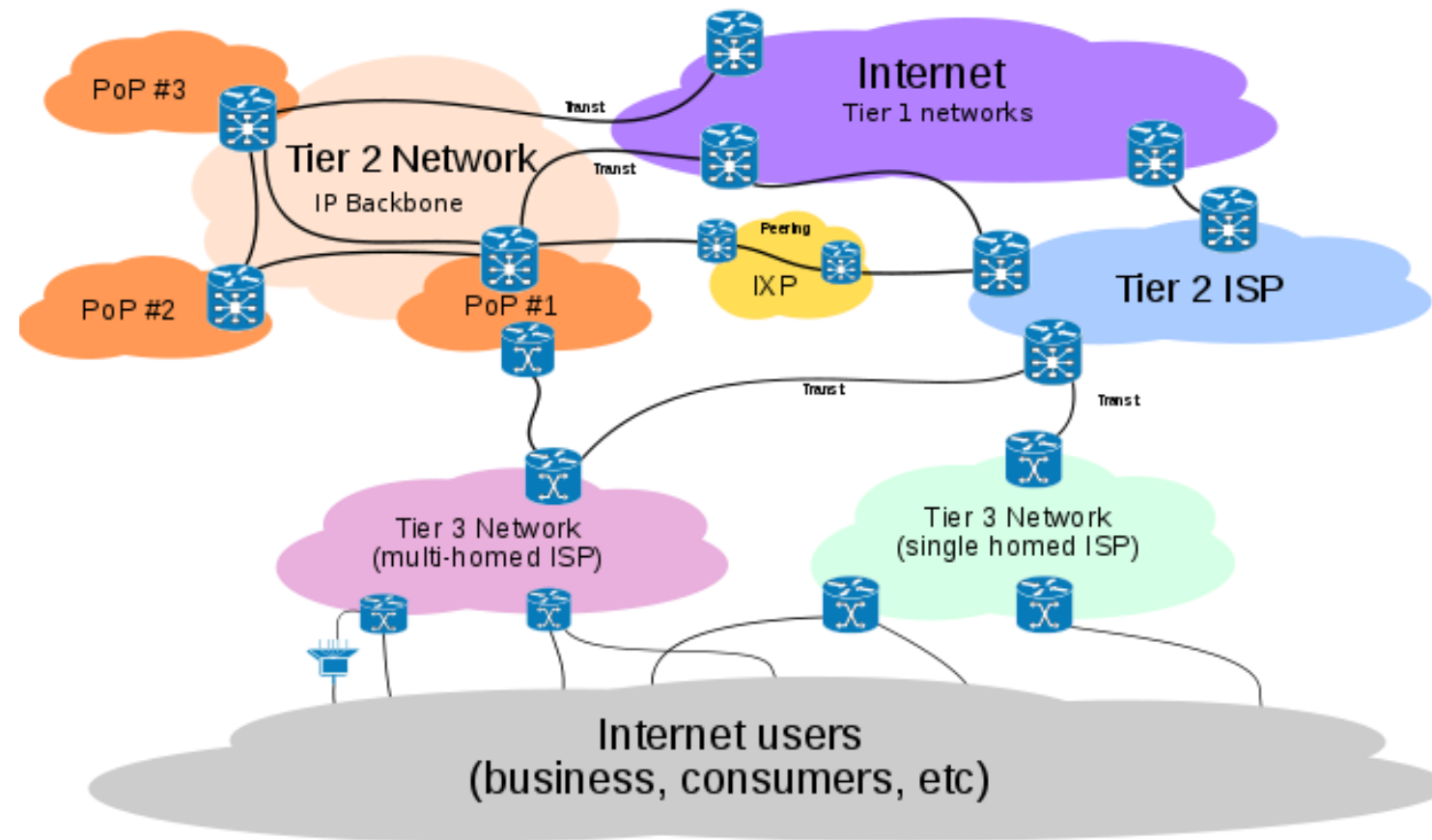
- Internet je skupina navzájom poprepájaných Autonómnych systémov (AS)
 - je skupina sietí a smerovačov, ktoré používajú spoločnú smerovaciu politiku a patria pod spoločnú administratívnu doménu
 - **Smerovacia politika**: spôsob výberu ciest do rôznych cieľov, filtrovanie smerovacích informácií, oznamovanie smerov...
 - **Administratívna doména**: dosah administratívnej právomoci správcu



- Zjednodušenie
 - AS je buď ISP alebo firma
 - Zvonku je AS vnímaný ako jedna nerozdelená entita

Štruktúra Internetu - AS infraštruktúra

- Jednotlivé AS (ISP AS) sa prepájajú cez Internet Packet Exchange (IPX) Gateways
 - v tzv. Internet Exchange Points (IXP)
- IXP je priamy prepoj, cez ktorý si ISP vymieňajú navzájom svoje dáta
 - A redukujú množstvo, ktoré musia poslať cez svojich tranzitných providerov
 - Peering: dobrovoľný prepoj AS za účelom vzájomnej výmeny dát („ak prepošleš moje ja prepošlem tvoje“)




Európske IXP




IXP na Slovensku - historicky


- Slovensko má troch IXP providerov (BA a KE)
 - Six.sk (nasjtaráš), Nix.sk, peering.cz
- Slovak IXP (SIX) – www.six.sk
 - Špičková prevádzka – 2023/501Gbit/s
 - 2020/233,4Gbps, 2018/223,2 Gbps, 2017/212Gbps
 - Priemer: okolo 60 Gbps
 - Peerov:
 - https://www.six.sk/index.php?page=pripojene_siete
 - 2020/59, 2018/58, 2016/61



The Slovak Internet eXchange

PEERING DOKUMENTY LINKY ENGLISH VERSION

 **BRATISLAVA**


 **KOŠICE**


Prehľad aktívnych peeringov
Prehľad záťaže liniek
Looking glass

Prehľad aktívnych peeringov
Prehľad záťaže liniek
Looking glass

Stalo sa...

Stalo sa...





Centrum výpočtovej techniky STU
Nám. slobody 17, 812 43 Bratislava
tel.: 02/524 51 301, 02/529 61 573,
fax: 02/524 94 351, e-mail: six-ba@six.sk

Ústav výpočtovej techniky TU Košice
B. Nemcovej 3, 042 01 Košice
tel.: 055/602 51 56, 055/602 50 00,
fax: 055/625 35 82, e-mail: six-ke@six.sk

Webstránky používajú kódovanie UTF-8

Pripojené siete IPv4

Tabuľka dostupná ako: [JSON](#) | [CSV](#)

Pripojené siete IPv4

Pripojené siete IPv6

Názov firmy	ASN	Route server	Peeringová politika	Detail
ACS	12905	✓	Otvorená	📄 🗑️
ActiveNet	209998	✓	Otvorená	📄 🗑️
AIRNET	201603	✓	Otvorená	📄
Antik	42841	✓	Otvorená	📄 🗑️
BONET	44185	✓	Otvorená	📄 🗑️
CNC	50128	✓	Otvorená	📄 🗑️
DataNetworks	48326	✓	Otvorená	📄 🗑️
Detronics	56656	✓	Otvorená	📄 🗑️

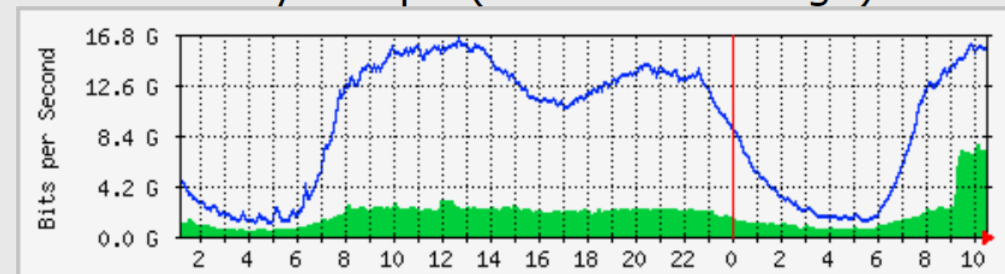
Summary Traffic Analysis for SANET connections

System: SIX-SANET-gw

Max Speed: 200 Gbit/s

The statistics were last updated **Wednesday, 22 March 2023 at 10:30**

`Daily' Graph (5 Minute Average)

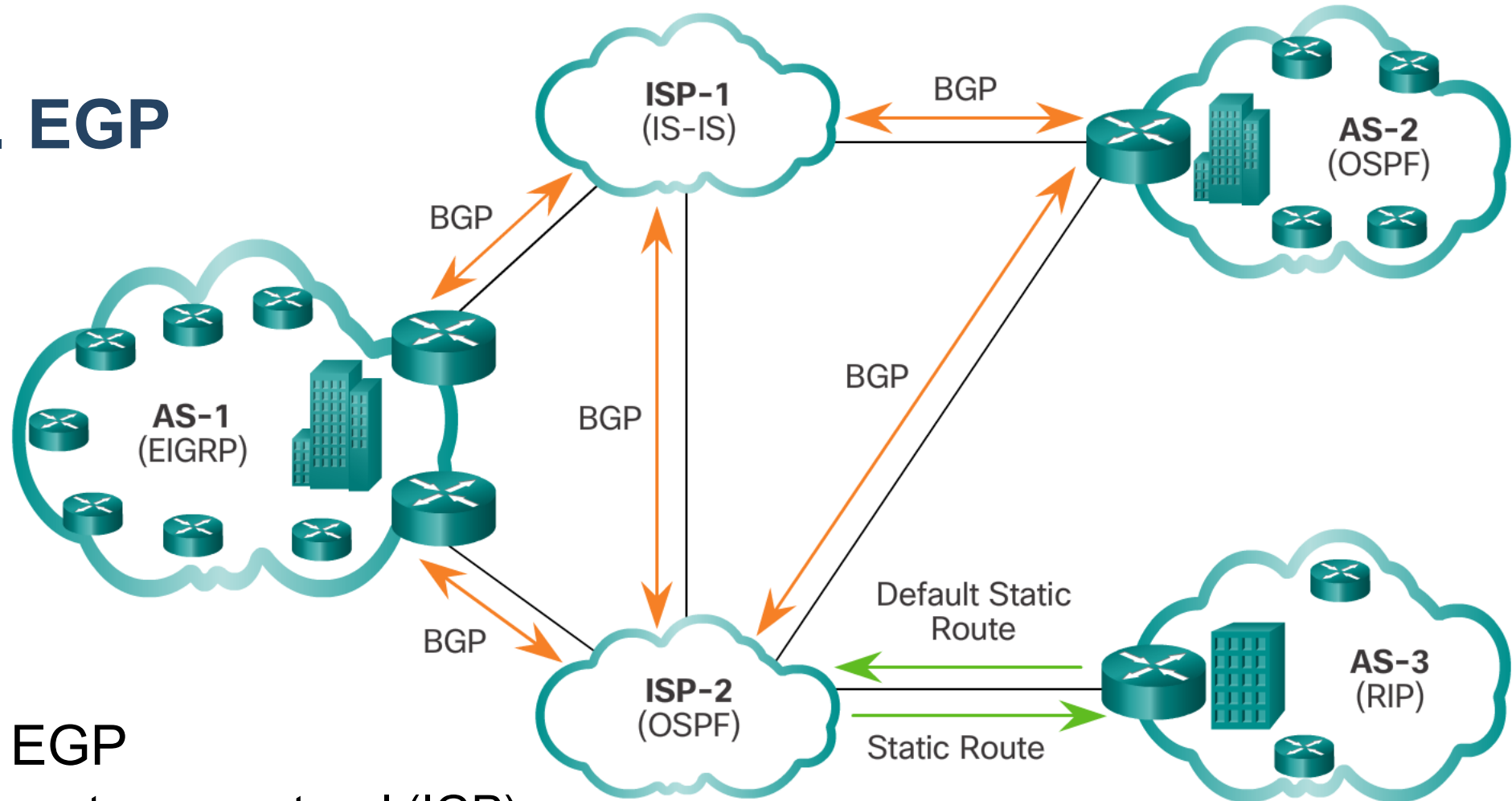


Max Average Current

In 7662.9 Mb/s (3.8%) 1788.0 Mb/s (0.9%) 6803.5 Mb/s (3.4%)

Out 16.4 Gb/s (8.2%) 9084.5 Mb/s (4.5%) 15.3 Gb/s (7.7%)

IGP vs. EGP



■ IGP vs EGP

■ Interior gateway protocol (IGP)

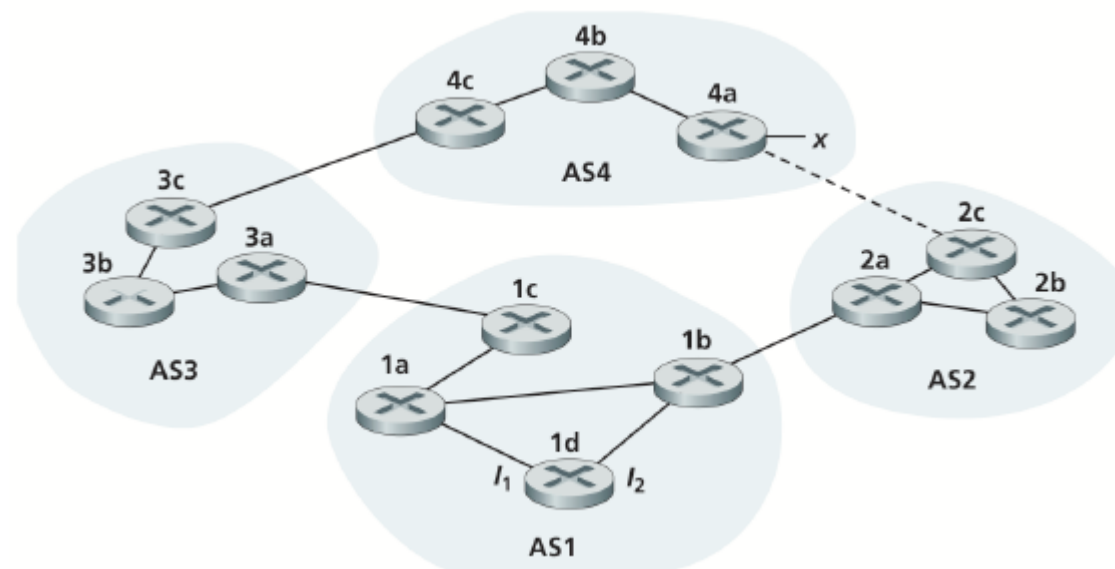
- Smerovací protokol pracujúci vo vnútri Autonomous System (AS).
 - Napr. RIP, OSPF, a EIGRP

■ Exterior gateway protocol (EGP) = defacto rovná sa BGP

- Smerovací protokol pracujúci medzi rôznymi AS

Smerovanie medzi AS vs. vnútri AS

- Smerovanie medzi AS sa zásadne líši od smerovania vo vnútri AS
- **IGP protokoly:**
 - Susedné smerovače sa navzájom objavujú automaticky
 - Snahou IGP je vymeniť si čo najkompletnejšiu informáciu o vnútornej topológii AS a jeho členských sieťach
 - Svet za hranicami AS je „zahmlený“
 - Nahradený sumárnymi smermi alebo využitím default route, vždy bez topologickej predstavy
 - Metrika odráža výhodnosť trasy na základe počtu hopov, prenosovej rýchlosti, oneskorenia, záťaže, teda jej prenosové vlastnosti

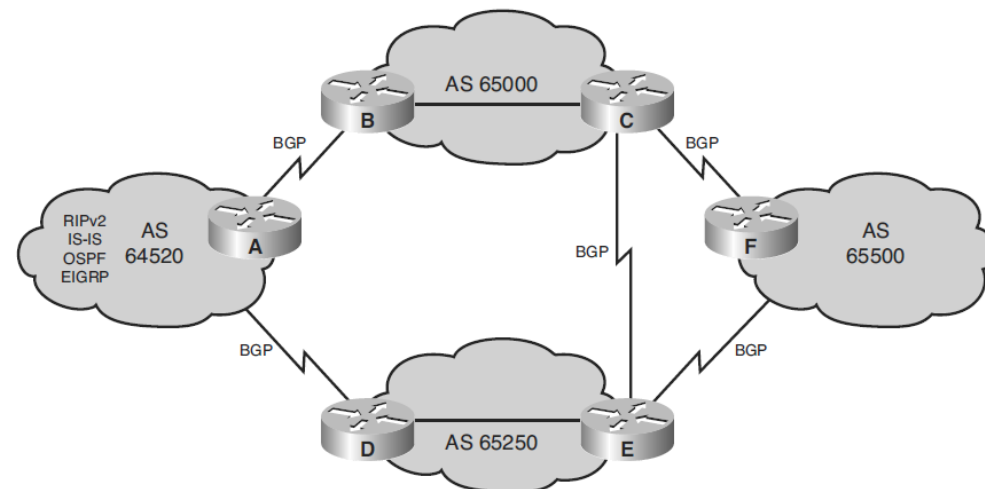


Smerovanie medzi AS vs. vnútri AS

- Smerovanie medzi AS sa zásadne líši od smerovania vo vnútri AS
- **EGP protokoly (BGP):**
 - Susedné smerovače musia pre vzájomnú komunikáciu byť **explicitne nakonfigurované** na základe dohody správcov
 - EGP protokoly sa **nezaujímajú o vnútornú topológiu** AS
 - Riešenie vnútornej dosiahnuteľnosti prenechávajú IGP
 - EGP protokoly sa **zaujímajú o hraničné smerovače** na okrajoch AS a o vzájomné prepojenie AS medzi sebou
 - Metrika sa skladá z parametrov, ktoré vyjadrujú pôvod siete a cestu cez tranzitné AS (Path), jej lokálnu preferenciu
 - neodráža nutne fyzický charakter cesty, ale jej administratívne vlastnosti;

Smerovanie medzi AS

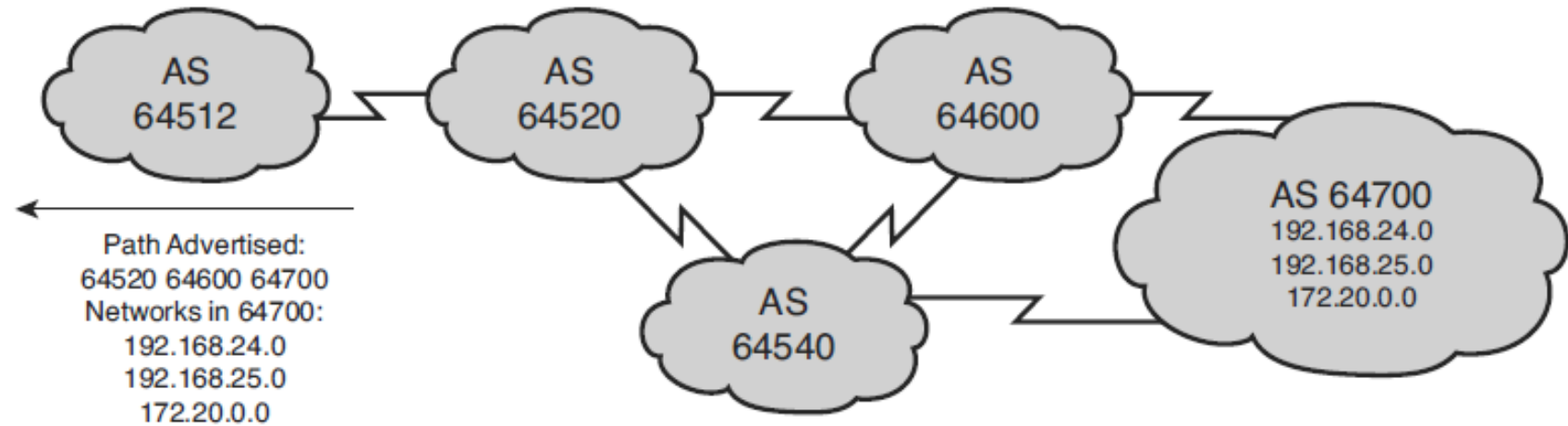
- Smerovanie medzi AS musí byť zaručene bezslučkové
- Objem vymieňaných informácií je obrovský – desiatky až stovky megabajtov informácií obsiahnutých v smerovacích tabuľkách (100tis. ciest cca 70MB)
 - <http://bgp.potaroo.net/>
 - Internet Core (<http://www.cidr-report.org/>)
 - IPv6 => 81479 v 2020
 - IPv4 => 819535 v 2020 (725555 v 2018 (636106 v 2016 (529 189 v 2014, (482.880 v 2013 (407.000 v 2012)))))) CIDR položiek
 - AS => 68178 v 2020 (61257 v 2018 (55542 v 2016 (48 913 v 2014 (45.592 v 2013 (40659 v 2012))))))
- Výber ciest sa nerealizuje na základe metriky,
- ale na základe dohodnutých smerovacích politík, administratívnych rozhodnutí a atribútov



Border Gateway Protocol

- BGP je v súčasnosti prakticky jediný používaný smerovací protokol pre inter-AS smerovanie
 - T.j. výmenu sieťových prefixov v daných AS a optimalizáciu smerovania cez tzv. atribúty cesty
 - Je typu **Path vector**, vymieňajú sa zoznamy ciest
 - **Garantuje bezslučkovú výmenu** smerovacích informácií
 - **Dve AD**
 - eBGP AD=20
 - iBGP AD = 200
 - BGP **beží nad TCP** protokolom, cieľový port 179
 - Preto BGP nepotrebuje vlastné error recovery mechanizmy
- Aktuálna verzia: **BGPv4** špecifikovaná v RFC 4271
 - Početné ďalšie RFC rozširujú schopnosti BGP o smerovanie multicastov, podporu MPLS a ďalšie
 - = veľmi, veľmi,, veľmi komplexný protokol s mnohými oblasťami využitia
 - ISP routing, DC, ISP VPN

BGP Path Vector



- IGP fungujú na princípe oznámenia zoznamu sietí a zoznamu parametrov (atribútov) o ceste do nich (metrika)
- BGP používa informácie o atribúte smerovanej cesty (volaných **path vector**) a k nej patriacich prefixov
 - Path vector informácie zahŕňajú napr.
 - Zoznam BGP AS čísel (hop by hop) potrebných traverzovať na dosiahnutie cieľovej siete
 - A iné atribúty
 - Napr. IP adresa Next Hop ako sa dostať do ďalšieho AS (*next-hop attribute*), ako sa dostali koncové siete do BGP (origin code attribute)
 - Textové značky
 - Preferencie smerovania dnu a von z AS apod.

BGP update – příklad

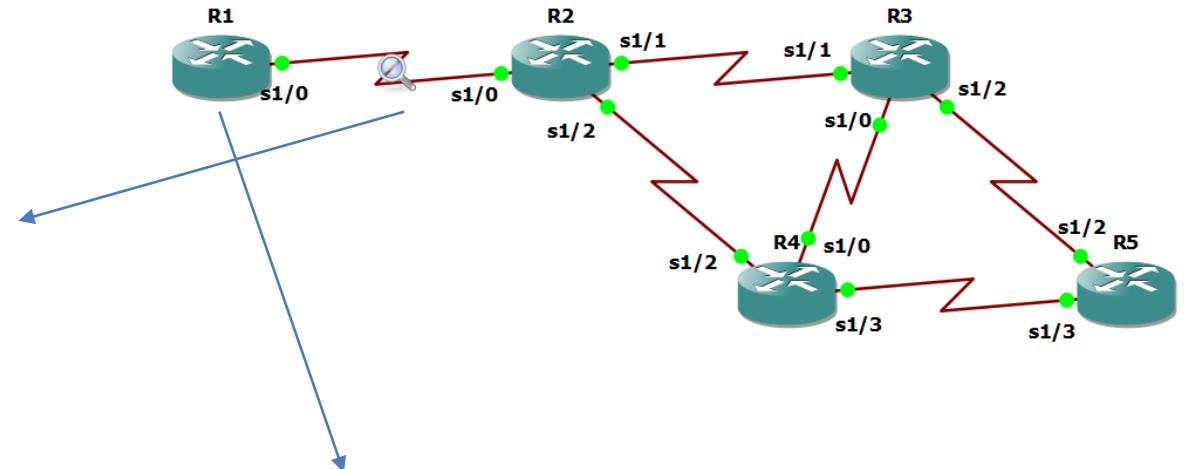
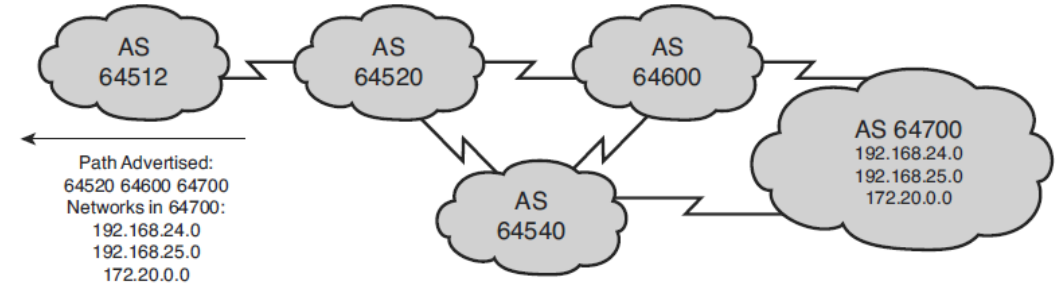
- > Frame 87: 152 bytes on wire (1216 bits), 152 bytes captured (1216 bits) on interface -, id 0
- > Cisco HDLC
- > Internet Protocol Version 4, Src: 10.12.0.2, Dst: 10.12.0.1
- > Transmission Control Protocol, Src Port: 51231, Dst Port: 179, Seq: 100, Ack: 77, Len: 108
- ▼ Border Gateway Protocol - UPDATE Message

Marker: ffffffffffffffffffffffffffffffffff
Length: 62
Type: UPDATE Message (2)
Withdrawn Routes Length: 0
Total Path Attribute Length: 28

- ▼ Path attributes
 - ▼ Path Attribute - ORIGIN: IGP
 - > Flags: 0x40, Transitive, Well-known, Complete
 - Type Code: ORIGIN (1)
 - Length: 1
 - Origin: IGP (0)
 - ▼ Path Attribute - AS_PATH: 64520 64540 64700
 - > Flags: 0x40, Transitive, Well-known, Complete
 - Type Code: AS_PATH (2)
 - Length: 14
 - > AS Path segment: 64520 64540 64700
 - ▼ Path Attribute - NEXT_HOP: 10.12.0.2
 - > Flags: 0x40, Transitive, Well-known, Complete
 - Type Code: NEXT_HOP (3)
 - Length: 4
 - Next hop: 10.12.0.2

- ▼ Network Layer Reachability Information (NLRI)
 - ▼ 172.20.0.0/16
 - NLRI prefix length: 16
 - NLRI prefix: 172.20.0.0
 - > 192.168.24.0/24
 - > 192.168.25.0/24

- > Border Gateway Protocol - ROUTE-REFRESH Message
- > Border Gateway Protocol - UPDATE Message

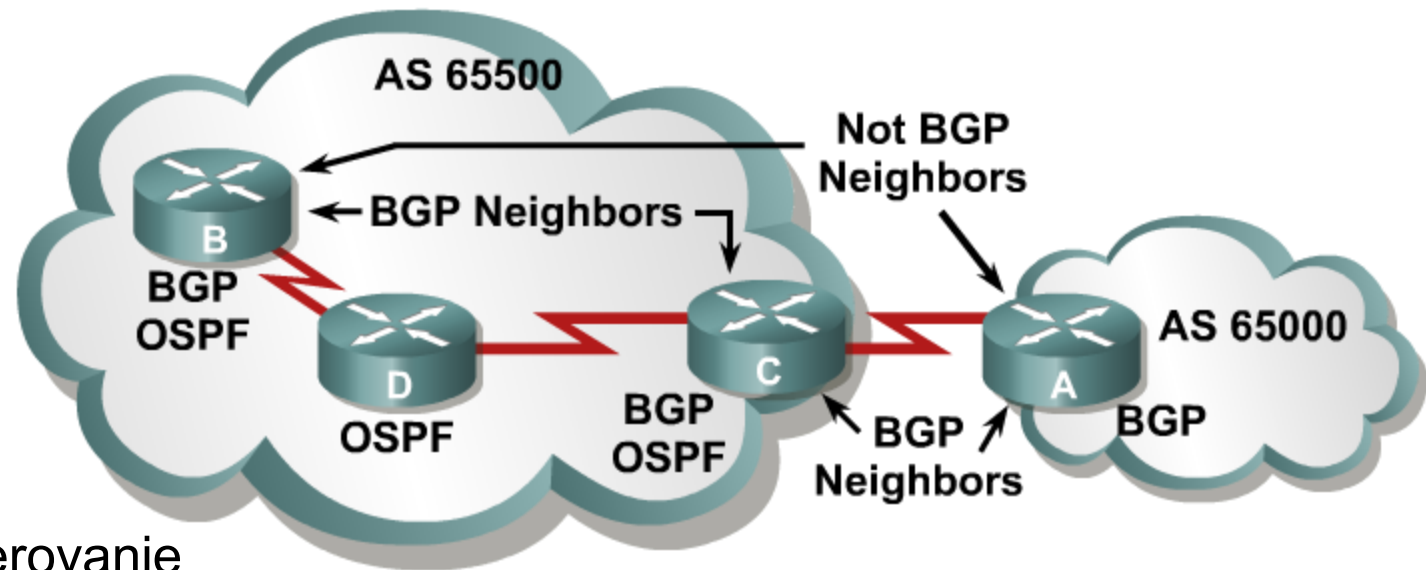


```
R1(config-router)#do sh ip route
...
Gateway of last resort is not set

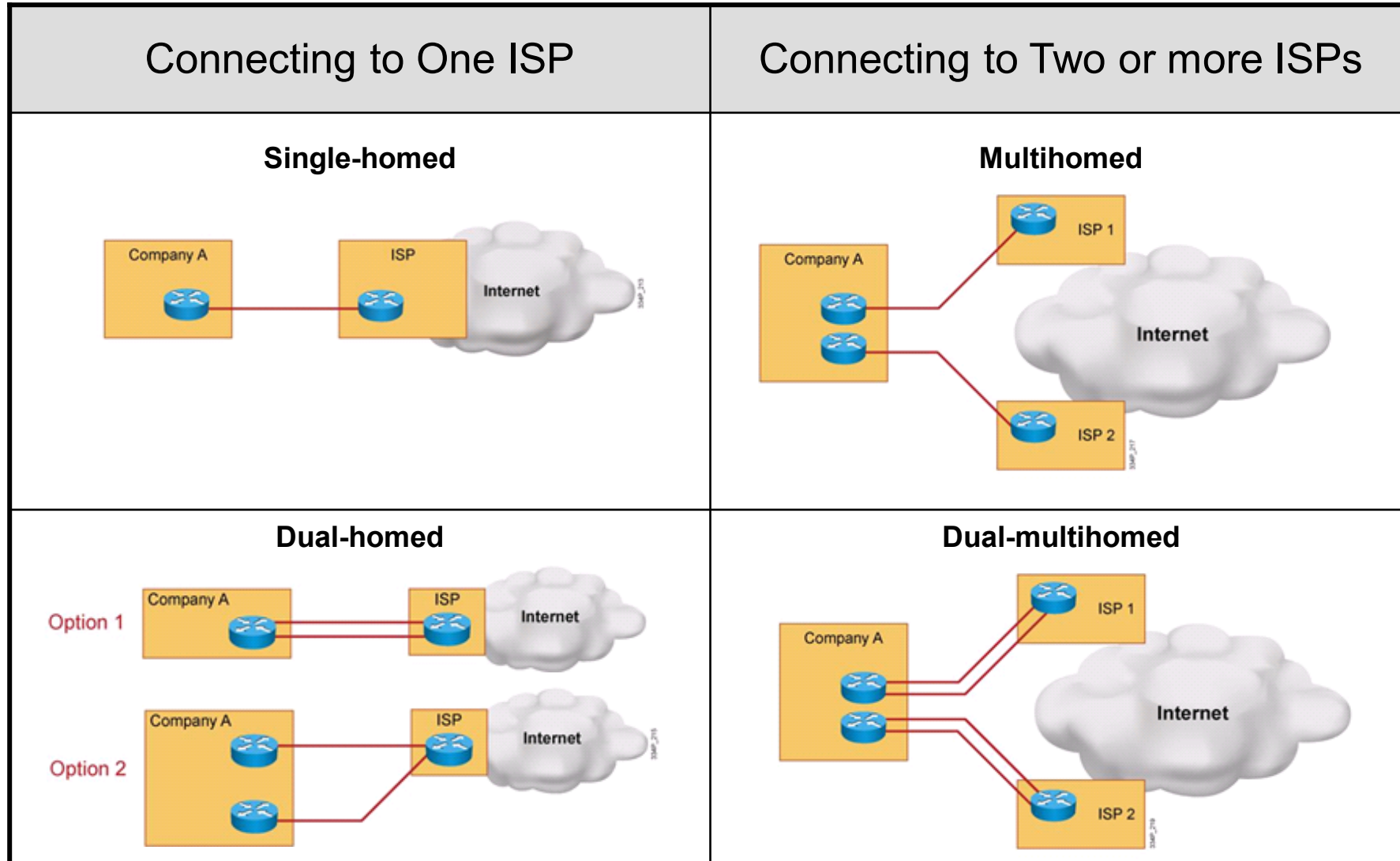
    10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.12.0.0/24 is directly connected, Serial1/0
L       10.12.0.1/32 is directly connected, Serial1/0
B       172.20.0.0/16 [20/0] via 10.12.0.2, 00:01:28
B       192.168.24.0/24 [20/0] via 10.12.0.2, 00:01:28
B       192.168.25.0/24 [20/0] via 10.12.0.2, 00:01:28
R1(config-router)#
```

BGP komponenty

- BGP sa z hľadiska činnosti delí na
 - **External BGP (eBGP)**
 - Činnosť BGP zameraná na smerovanie medzi BGP smerovačmi (BGP peer), ktoré sú v rôznych AS.
 - **Internal BGP (iBGP)**
 - Činnosť BGP zameraná na smerovanie medzi BGP smerovačmi (BGP peer), ktoré sú v tom istom AS.
- Pojmy
 - BGP speaker = každý router, ktorý hovorí BGP protokolom
 - T.j. je na ňom spustený BGP
 - BGP peers or neighbors (susedia) = dvojica vzájomne komunikujúcich BGP speakerov
- CCNA kurz sa zameriaval chvíľu len na eBGP



Prepojenie firmy s ISP

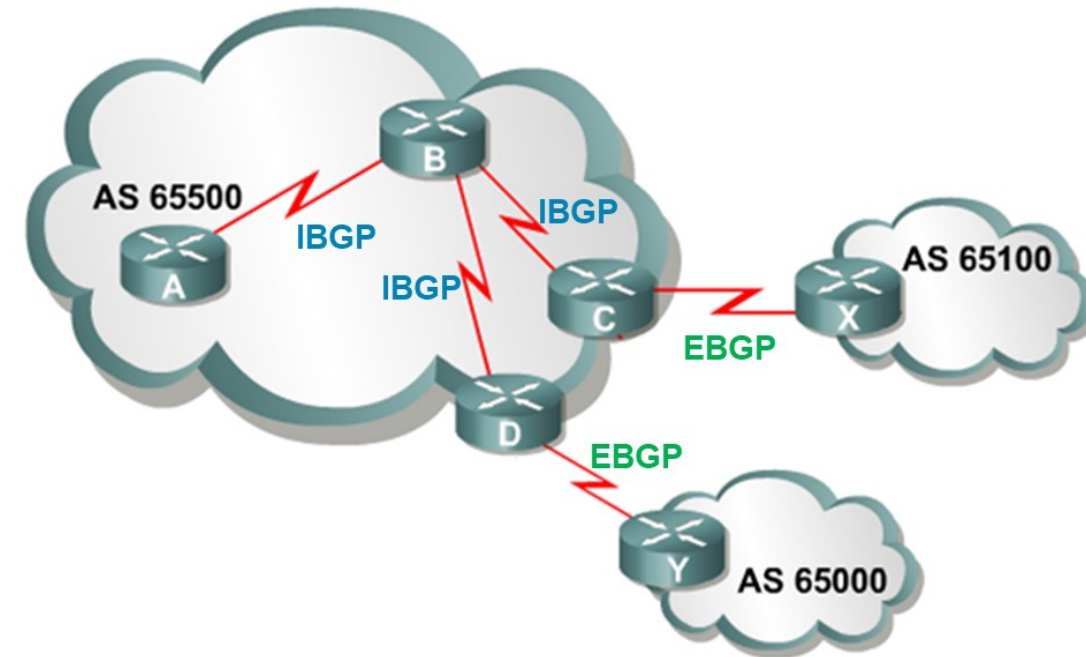


Druhy autonómnych systémov

- Autonómne systémy sa tradične rozdeľujú na 3 druhy
 - Single-homed
 - AS, ktorý má jediný hraničný router do ostatného sveta
 - Single-homed AS častokrát vôbec nepotrebujú EGP routing
 - Typicky firma/podnik
 - Multihomed
 - AS, ktorý má viacero hraničných routerov do ostatného sveta
 - Napriek tomu, že sa pripája viacerými výstupnými bodmi, nedovoľuje, aby cez neho tiekla cudzia prevádzka
 - Transit
 - AS, ktorý má viacero hraničných routerov do ostatného sveta a slúži na prenos tranzitnej prevádzky (medzi inými AS)
 - Typicky AS ISP

Možnosti prepojenia zákazníka a ISP na úrovni eBGP smerovania

- Prepojenie medzi zákazníkom a ISP na úrovni eBGP je možné typicky riešiť tromi spôsobmi
 - **Prijatie len Default Route**
 - Najjednoduchšia metóda, zákazník dostane len default route, nízke nároky na zdroje smerovača.
 - Môže viesť k neoptimálnemu smerovaniu mimo sieť zákazníka.
 - **Default Route a siete zákazníkov daného ISP**
 - Zákazník môže optimalizovať smerovanie do sietí iných zákazníkov toho istého ISP
 - Zvyšok sveta nahradený Default route - Môže viesť k neoptimálnemu smerovaniu mimo sieť zákazníka a ISP
 - **Prijatie všetkých ciest**
 - Zákazník dostane úplnú smerovaciu tabuľku celého internetu, najpresnejšie smerovanie kamkoľvek, pozor na nároky na HW smerovača (600tisíc položiek len pre IPv4)



Kedy použiť/nepoužiť BGP v mojom AS

- Použiť BGP
 - Najvhodnejšie ak je jasný prínos nasadenia BGP a existuje najmenej jedna z nasledujúcich situácií
 - „Naše“ AS má viaceré prepojenia na iné AS
 - „Naše“ AS umožňuje tranzit paketom cez seba na ceste do iných AS
 - Je potrebná manipulácia s výberom smerovacích ciest pre pakety opúšťajúce AS
 - Firma chce odlíšiť svoju prevádzku od prevádzky ISP
- Nepoužiť BGP
 - Ak existuje najmenej jedna z nasledujúcich situácií
 - Jedno pripojenie na Internet alebo AS
 - Slabé zariadenie na pozícii okrajových smerovačov
 - Malo pamäte, nízky výkon
 - „Slabé vedomosti o filtrácii ciest a činnosti BGP“ (dnes odstránime)
 - V týchto prípadoch výhodné nasadenie statických ciest or default smerovania

eBGP – jednoduchá konfigurácia

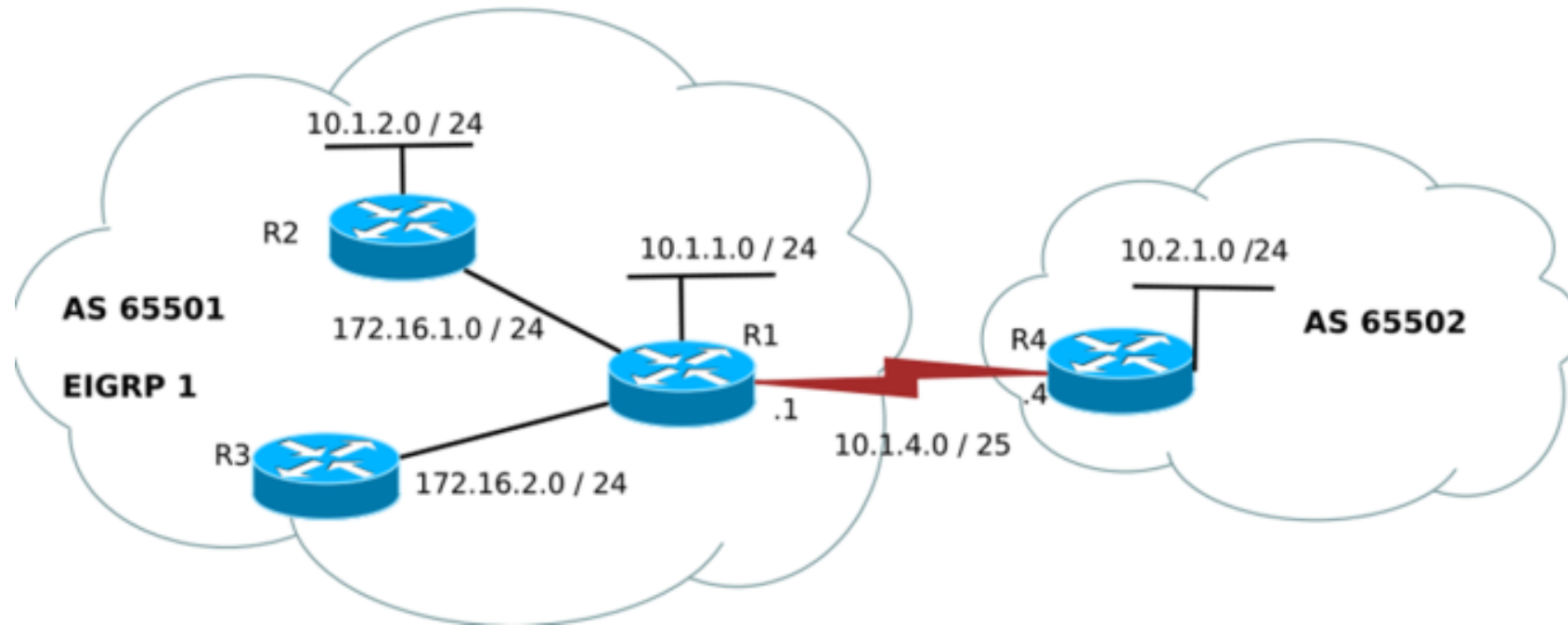
- Tri jednoduché kroky:
 - **Step 1:** spusti BGP proces
 - **Step 2:** explicitne konfiguruj BGP neighbor(s) (peering)
 - Susedia musia byť jednoznačne nakonfigurovaný
 - Neexistuje auto objavovanie ako v IGP
 - **Step 3:** ohlás svoje siete (tie, ktoré pochádzajú z tvojho AS a sú v tvojej smerovacej tabuľke. nielen na rozhraniach)

Command	Description
Router(config)# router bgp <i>as-number</i>	Enables a BGP routing process, and places the router in router configuration mode.
Router(config-router)# neighbor <i>ip-address remote-as as-number</i>	Specifies a BGP neighbor. The as-number is the neighbor's AS number.
Router(config-router)# network <i>network-address [mask network-mask]</i>	Advertises a network address to an eBGP neighbor as being originated by this AS. The network-mask is the subnet mask of the network.

BGP – overenie

- Over suseda
 - `Show ip bgp neighbor`
 - `Show ip bgp summary`
- Over BGP pracovnú databázu (BGP FIB)
 - `Sh ip bgp`
- Over smerovaciú tabuľku (RT)
 - `Show ip route bgp`

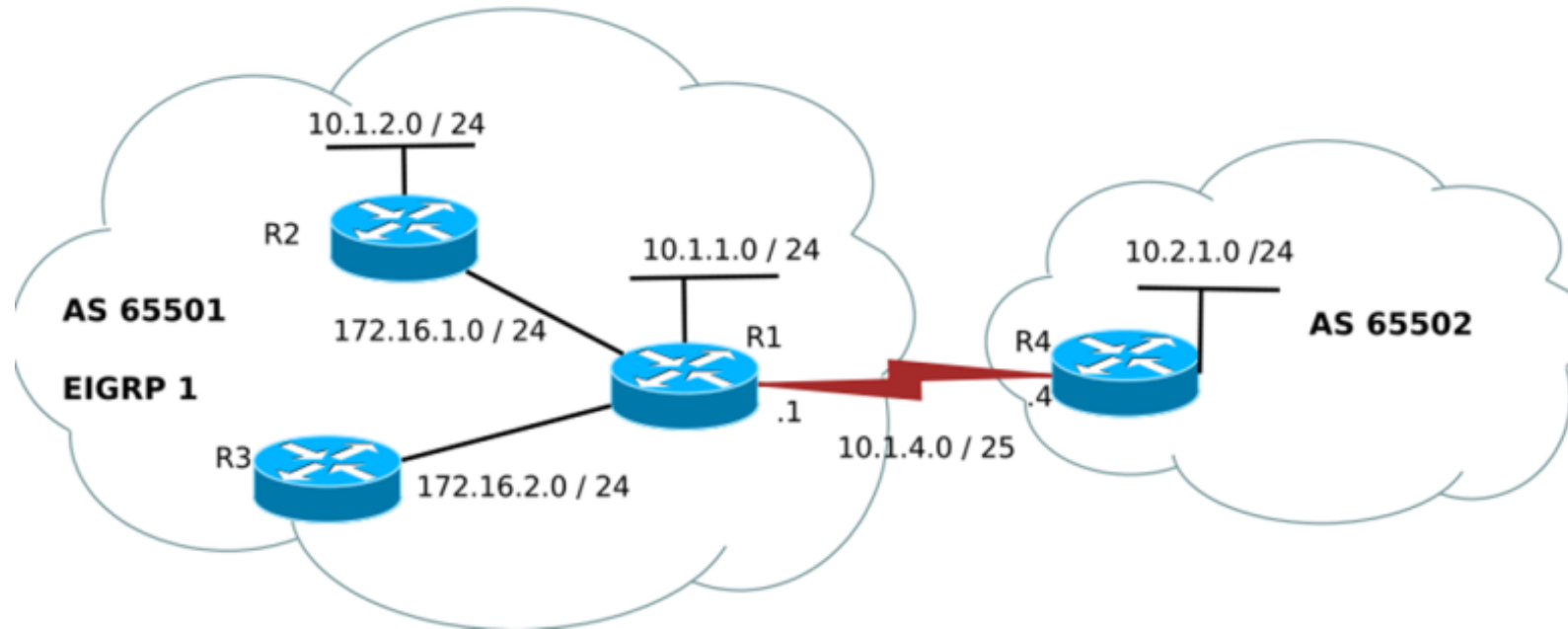
eBGP – Príklad jednoduchej konfigurácie



- Scenár:
 - Považuj 10.0.0.0 adresy ako Public – budú ohlásené mimo AS cez BGP
 - Považuj 172.16.0.0 adresy ako Private – nebudú ohlasované mimo AS
- Úloha:
 - R1 ohlási R4 siete 10.1.1.0/24 a 10.1.2.0 / 24
 - R4 ohlási R1 sieť 10.2.1.0 /24

Neighbors configuration and verification:

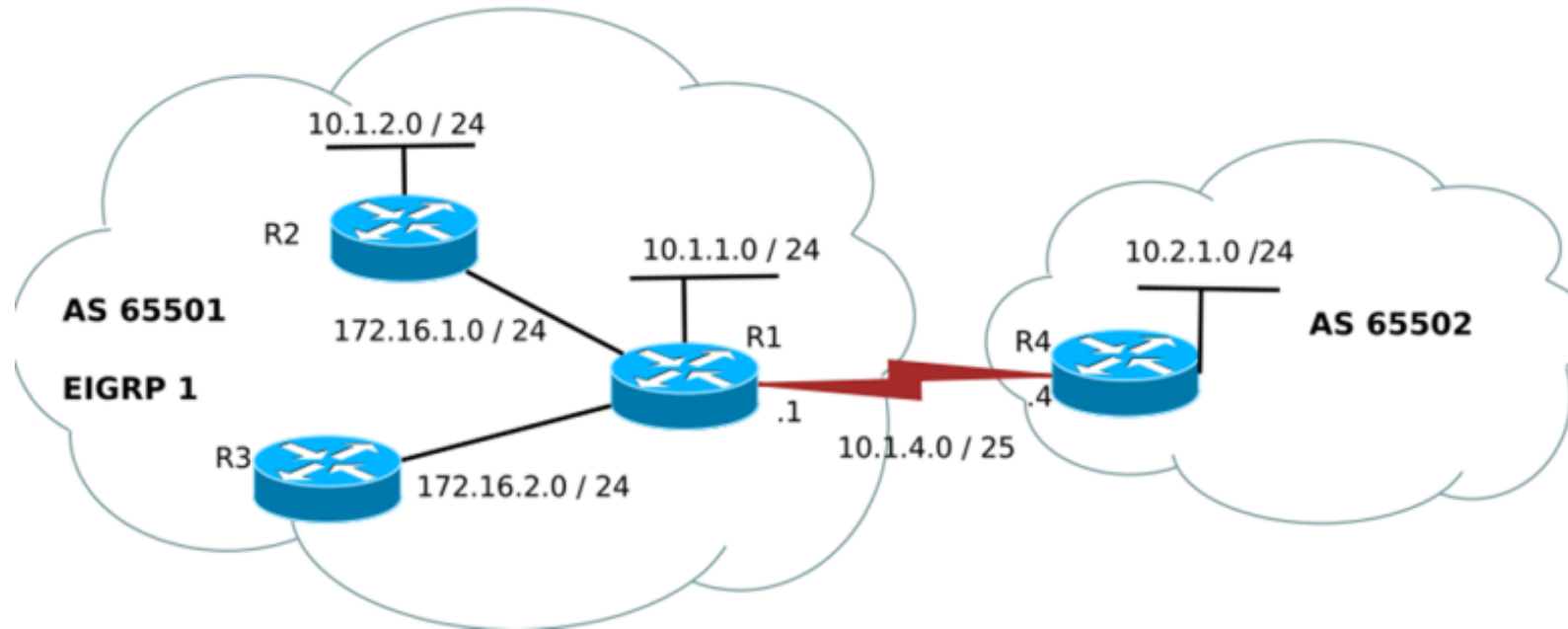
eBGP – Príklad jednoduchej konfigurácie



```
!R1
router eigrp 1
  network 10.0.0.0
  network 172.16.0.0
  passive-interface Serial1/0
!
router bgp 65501
  neighbor 10.1.4.4 remote-as 65502
```

```
!R4
router bgp 65502
  neighbor 10.1.4.1 remote-as 65501
```

eBGP – Overenie susedov



```
R1# show ip bgp neighbors
```

```
BGP neighbor is 10.1.4.4, remote AS 65502,
external link
```

```
  BGP version 4, remote router ID 10.2.1.4
```

```
  BGP state = Established, up for 00:07:17
```

```
... (output omitted)
```

```
R4#show ip bgp neighbors
```

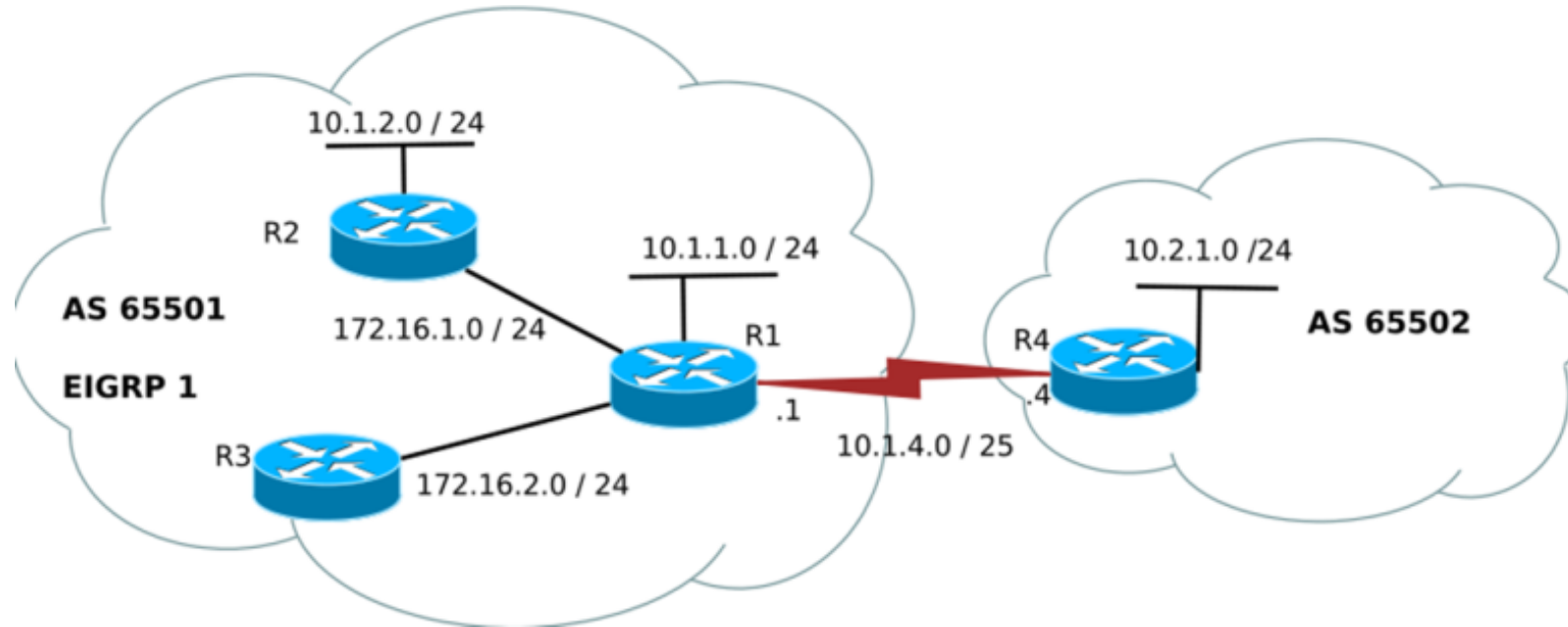
```
BGP neighbor is 10.1.4.1, remote AS 65501,
external link
```

```
  BGP version 4, remote router ID 10.1.1.1
```

```
  BGP state = Established, up for 00:08:04
```

```
... (output omitted)
```

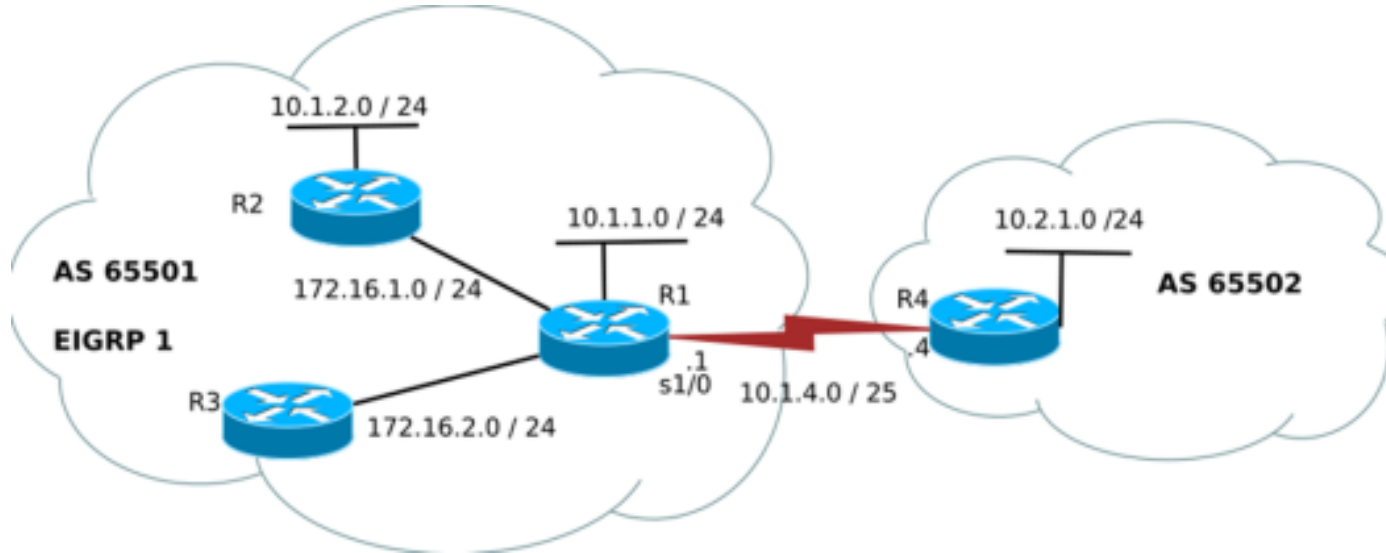
eBGP – ohlásenie sietí a overenie



```
! Siete musia byt v smerovacej tabulke
! + presna maska
R1(config)# router bgp 65501
  network 10.1.1.0 mask 255.255.255.0
  network 10.1.2.0 mask 255.255.255.0
```

```
!
!
R4(config)# router bgp 65502
  network 10.2.1.0 mask 255.255.255.0
```

eBGP – overenie BGP pracovnej databázy



Kód/symbol

- * Dostupná cesta, BGP ju nevybral na použitie
- *> naj cesta vybratá BGP. Bude ponúknutá do smerovacej tabuľky
- **Next Hop** – nasledujúci smerovač
 - = 0.0.0.0 som ním ja

! R1 - vidi siet z R4 + dve svoje

R1# **show ip bgp**

BGP table version is 8, local router ID is 10.1.1.1

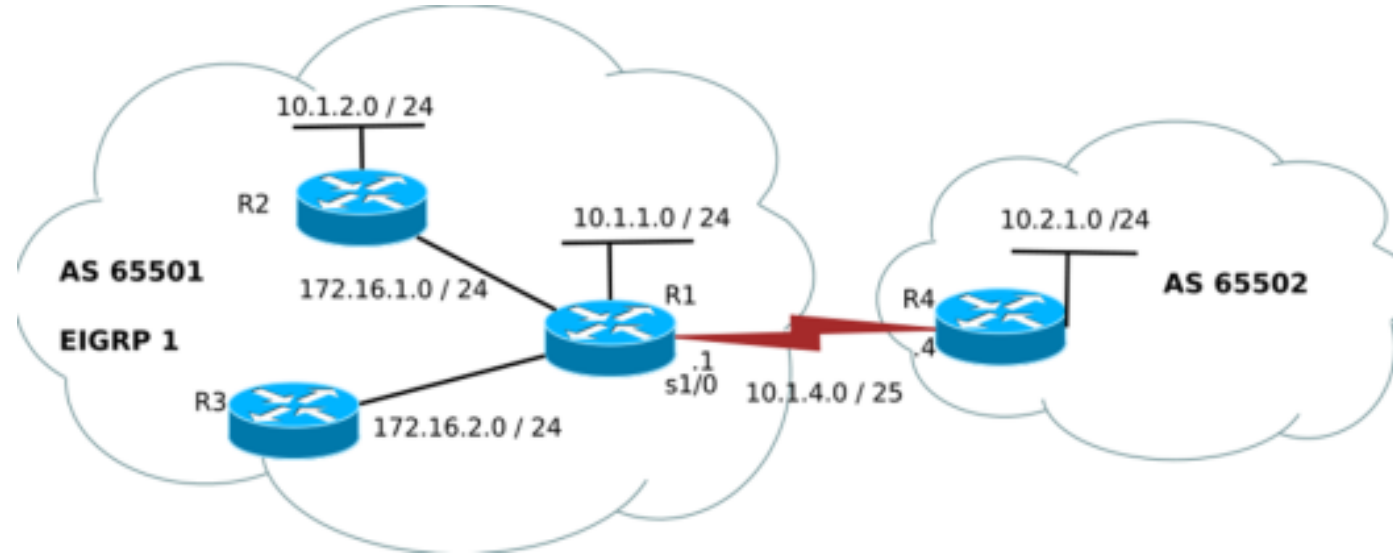
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed,

Origin codes: i - IGP, e - EGP, ? - incomplete

RPKI validation codes: V valid, I invalid, N Not found

	Network	Next Hop	Metric	LocPrf	Weight	Path
*>	10.1.1.0/24	0.0.0.0	0		32768	i
*>	10.1.2.0/24	172.16.1.2	156160		32768	i
*>	10.2.1.0/24	10.1.4.4	0		0	65502 i

eBGP – overenie BGP pracovnej databázy



! R4 vidi obe siete z R1 + jednu svoju

R4# **show ip bgp**

BGP table version is 8, local router ID is 10.2.1.4

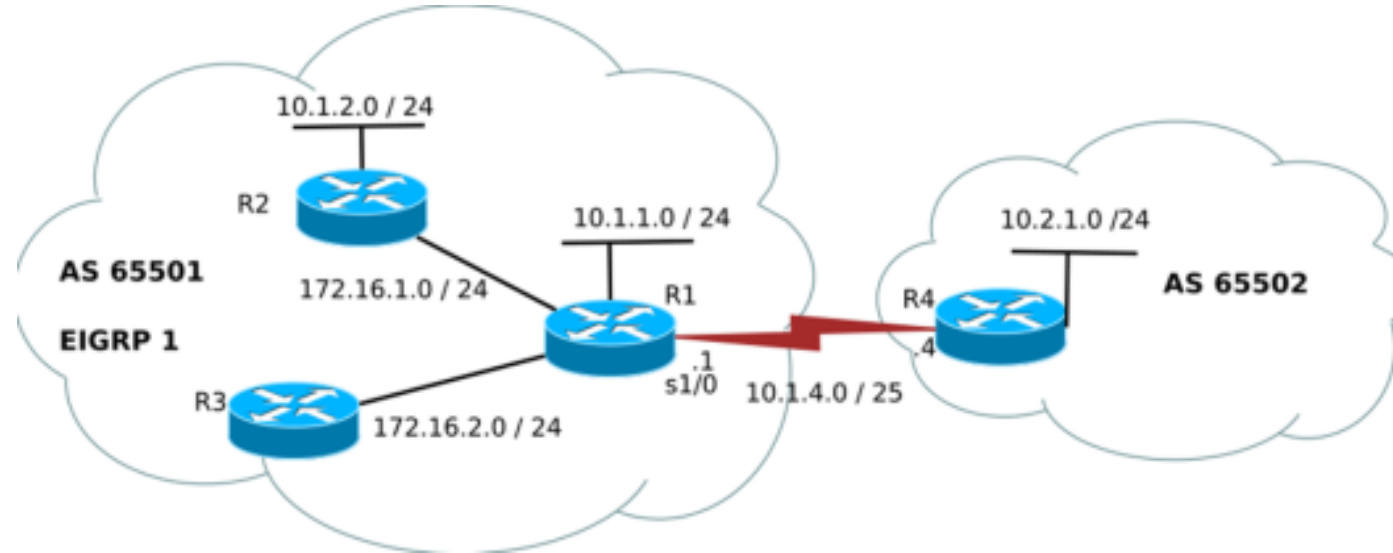
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed,

Origin codes: i - IGP, e - EGP, ? - incomplete

RPKI validation codes: V valid, I invalid, N Not found

	Network	Next Hop	Metric	LocPrf	Weight	Path
*>	10.1.1.0/24	10.1.4.1	0	0	0	65501 i
*>	10.1.2.0/24	10.1.4.1	156160	0	0	65501 i
*>	10.2.1.0/24	0.0.0.0	0	0	32768	i

Ako zabezpečiť smerovanie z R3 a R2 von z AS?



- V reále sú dve možnosti
 - R1 bude default router, ktorý sa ohlási cez EIGRP
 - Redistribúcia BGP ciest do EIGRP
 - Závisí od množstva ciest prijatých od ISP AS
 - Spomeň na možnosti BGP prepojenia zákazníka a ISP
 - Posledná možnosť – všetky cesty - je vražda EIGRP



UNIVERSITY OF ŽILINA
Faculty of Management Science
and Informatics



Ďakujem za pozornosť !



Ohodnot' našu CAN na google:

- <https://goo.gl/maps/BAnFvQKYCBpffcEX7>



Networking
Academy