MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY

Konektivita vzdialených pobočiek

CN (ccna4) – Chapter 3 - CCNA, v6

Katedra informačných sietí

Fakulta riadenia a informatiky, ŽU

Čo bude v prednáške

- Riešenia vzdialeného prístupu a širokopásmové technológie
- PPPoE
  - Cisco a PPPoE
- VPNs
- GRE tunely
- External BGP (eBGP)
  - V single homed zapojení

Riešenia vzdialeného prístupu (Remote Access Connections)

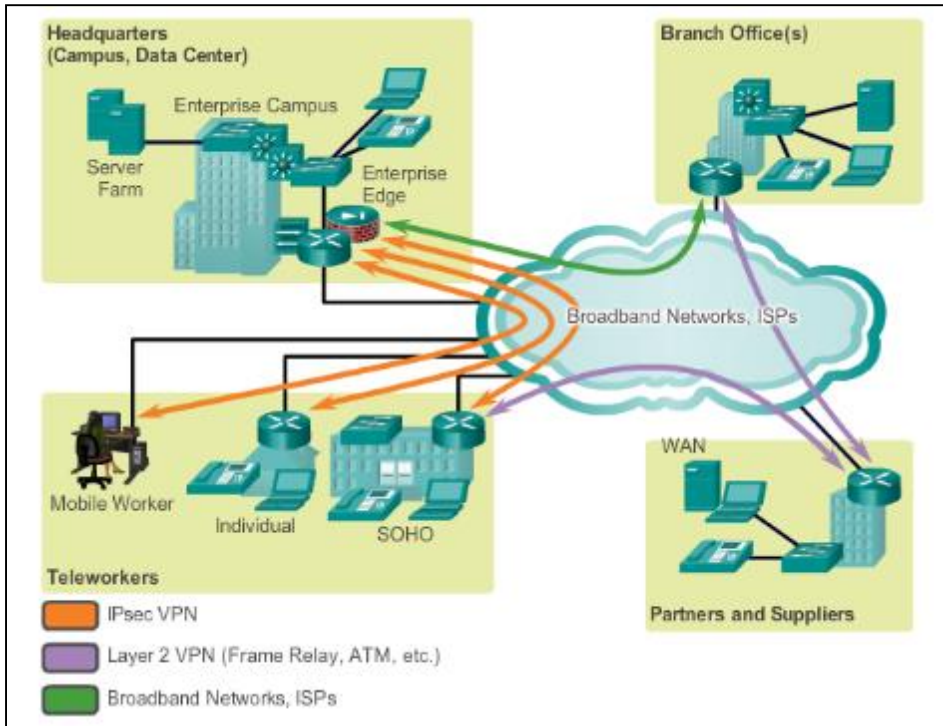
Prečo treba vzdialený prístup?

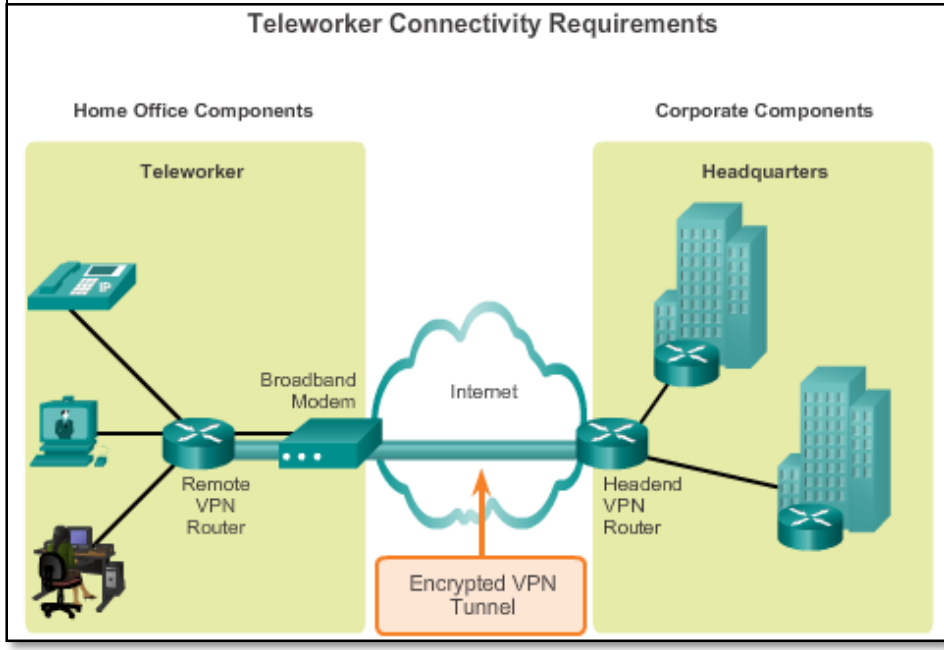
- Firmy potrebujú typicky riešiť vzdialený prístup z dôvodov:
  - **Integrácia sietí pobočiek s centrálou**
    - Napr. prístup zo siete/sietí pobočky k službám centrály (interné služby a servery)
  - **Prístup zákazníkov** k interným službám firmy
    - Napr. rôzne systémy výroby pri dodávkach tovarov a služieb
  - **Teleworking/Homeworking**
    - Umožnenie pracovať zamestnancom z domu
    - Freelancing

Požiadavky na riešenie

- Každé riešenie z predchádzajúcich možností vyžaduje:
  - Širokopásmový/rýchly prístup
    - Rôzne služby (VoIP, TelePresence, zdieľanie apod.)
  - Bezpečný prístup

- Riešenia širokopásmového a rýchleho prístupu
  - Rýchlosť vyššia 200kbps
    - Cable / DSL / WiMAX / Fiber („Always-on“ technológie)
  - Je potrebné pri výbere zvažovať
    - Cena, rýchlosť
    - Bezpečnosť
    - Jednoduchosť a spoľahlivosť
- Riešenie bezpečného prístupu
  - IPsec VPNs cez verejnú WAN
  - Privátne VPN služby
    - napr. VPLS cez MPLS na SK, Frame Relay a podobne

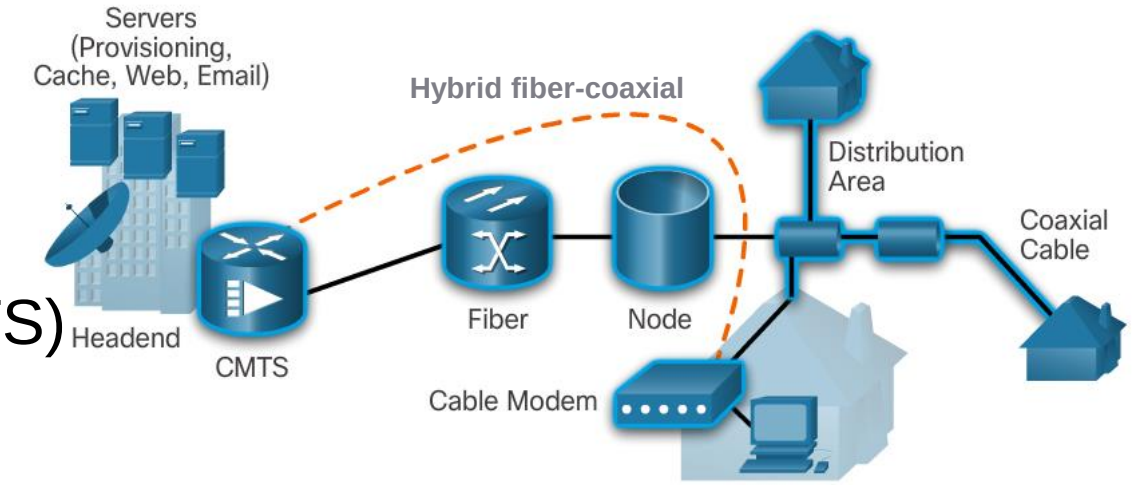




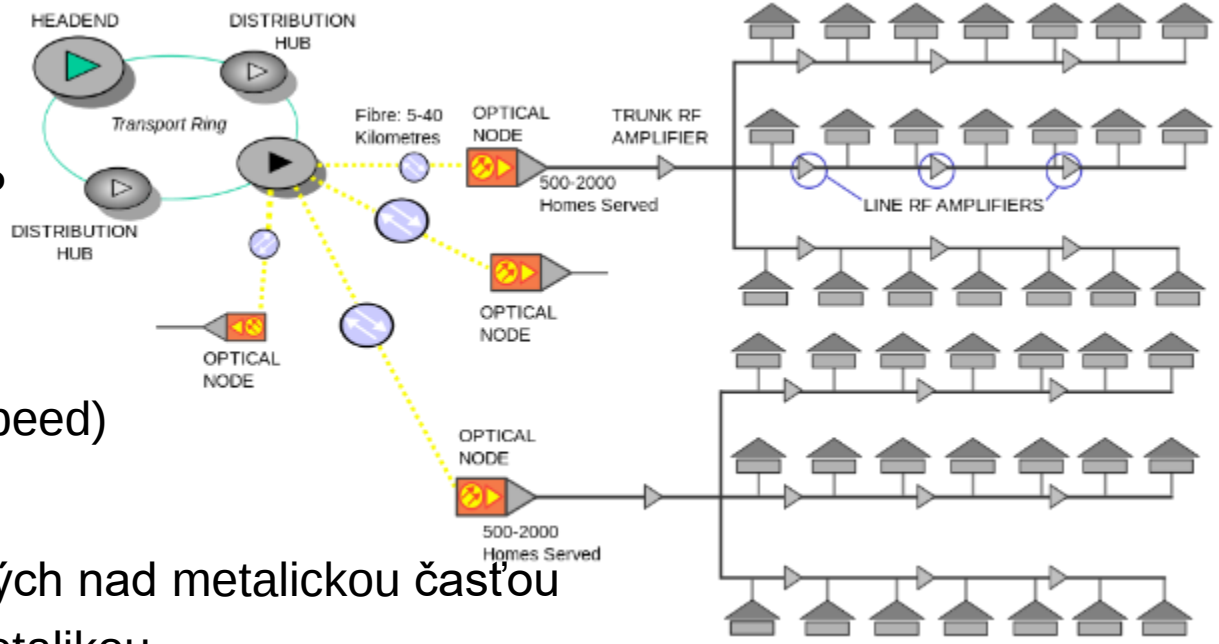
Internet cez káblové TV rozvody (Cable System)

- TV rozvody = Community Antenna Television (CATV)
  - História od roku 1948
- Štandard pre rozšírenie CATV o distribúciu dát a riešenie IP prístupu
  - Data-over-Cable Service Interface Specification (DOCSIS) od CableLabs
  - Špecifikuje OSI Layer 1 a Layer 2
    - Layer 1: frekvencie kanálov, techniky modulácie
    - Layer 2 (MAC Layer): Metódy pre prístup k médiu – MAC (TDM, Synchronous Code DMA)
- Káblové systémy
  - Používajú sa existujúce coax rozvody systémov káblovej TV
  - Rýchlosť:
    - Do ***160 Mb/s downstream***, a do ***120 Mb/s upstream***
    - Nový štandard v3.1: 10Gbps/1Gbps Down/UP
  - POZOR: kapacita sa zdieľa medzi používateľmi
    - Predpoklad od 500 do 2000 používateľov (subscibers) na jednom distribučnom systéme
  - Častokrát ponúkané v rámci TriplePlay služieb
    - Telefón, vysoko rýchlostný internet, digitálna TV

Komponety DOCSIS

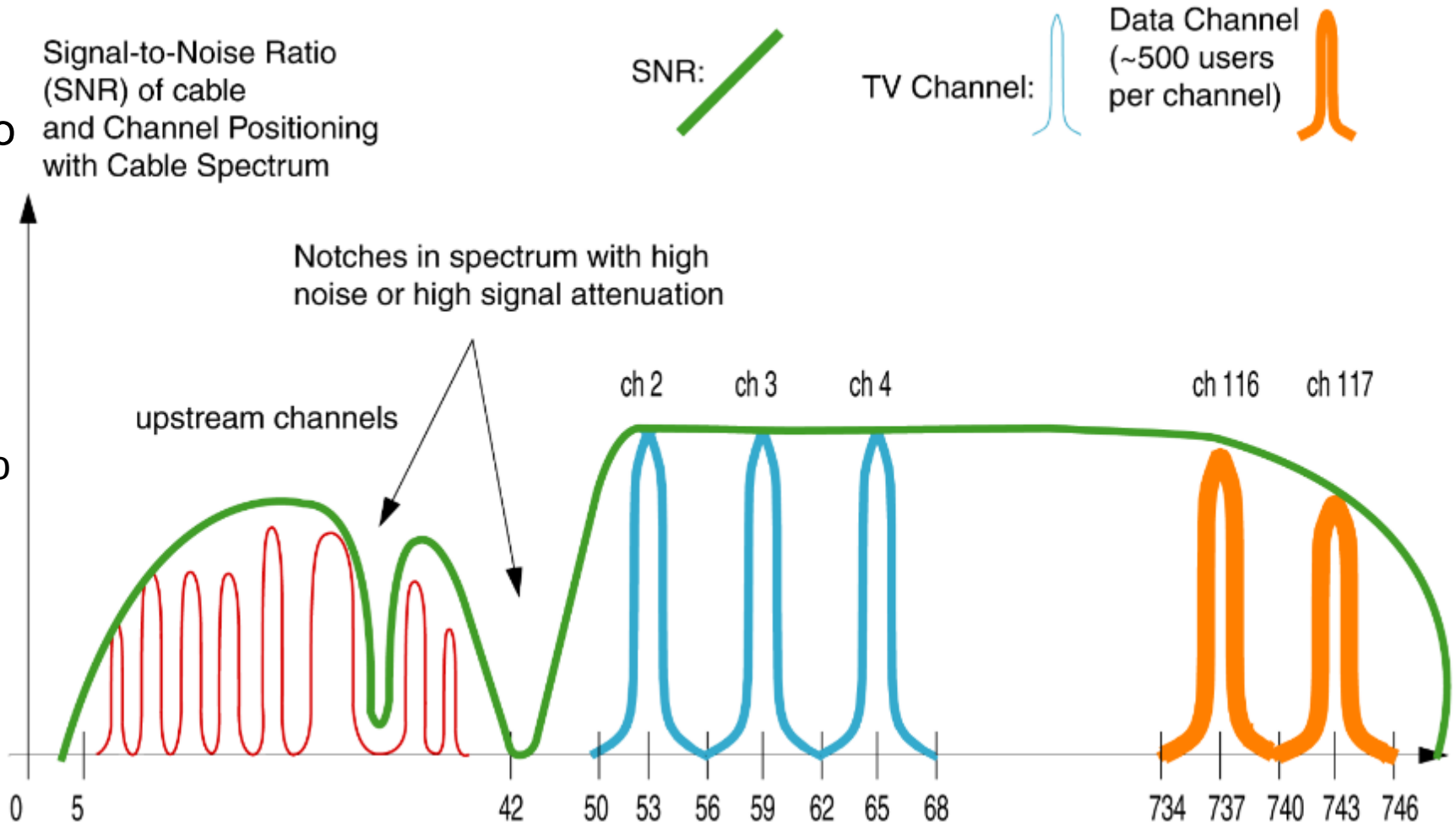


- Cable Modem Termination System (CMTS)
  - Zariadenie na strane operátora (headend router)
  - Rieši komunikáciu s CM u zákazníkov
  - Autentifikuje a autorizuje CM od jednotlivých používateľov
- Cable modem (CM)
  - Zariadenie u používateľov (router)
  - Pripája LAN sieť používateľa na coax rozvod SP
- Hybrid fiber-coaxial (HFC)
  - Mixovaná metalicko-optická distribučná sieť
  - Riešená ako strom s optickými trunkami (high speed)
- Node (Uzol)
  - Konvertuje dáta z optiky do frekvencií prenášaných nad metalickou časťou
  - Pripája vo vetvách používateľov prepojených metalikou
- Distribučná oblasť
  - Zdieľané coax rozvody k používateľom



Princíp činnosti

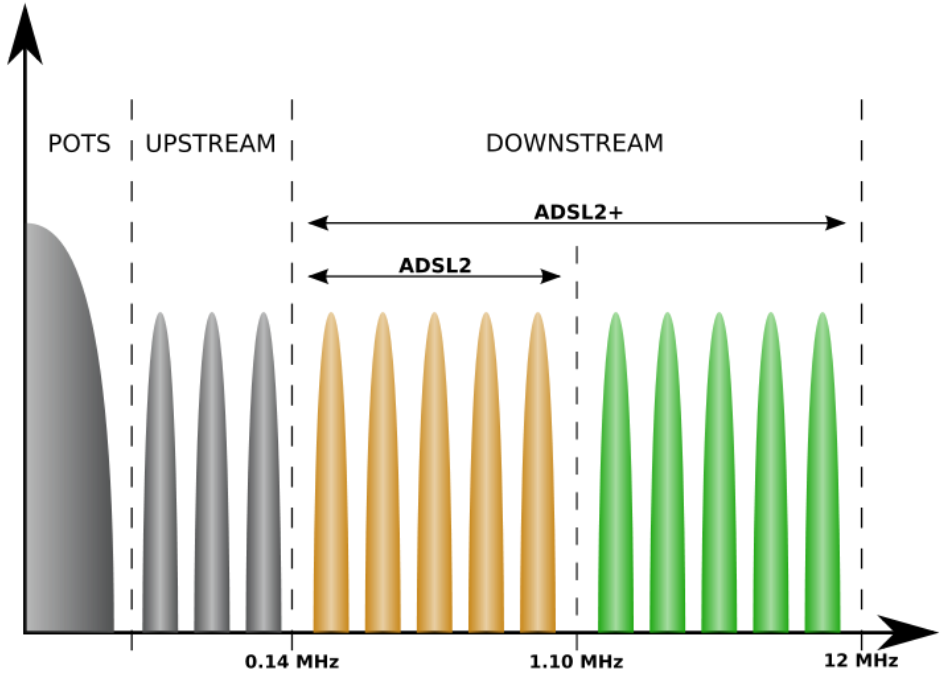
- Rozdelenie frekvenčného pásma
  - TV na jedných frekvenciách, hlas na druhých a dáta na iných
- Frekvenčné rozsahy
  - Donwstream (headend to subscriber)
    - Od 50 do 860 MHz.
  - Upstream (subscriber to headend)
    - Od 5 do 42 MHz.



Zdroj: Venkata C. Majeti

Digital Subscriber Line (DSL)

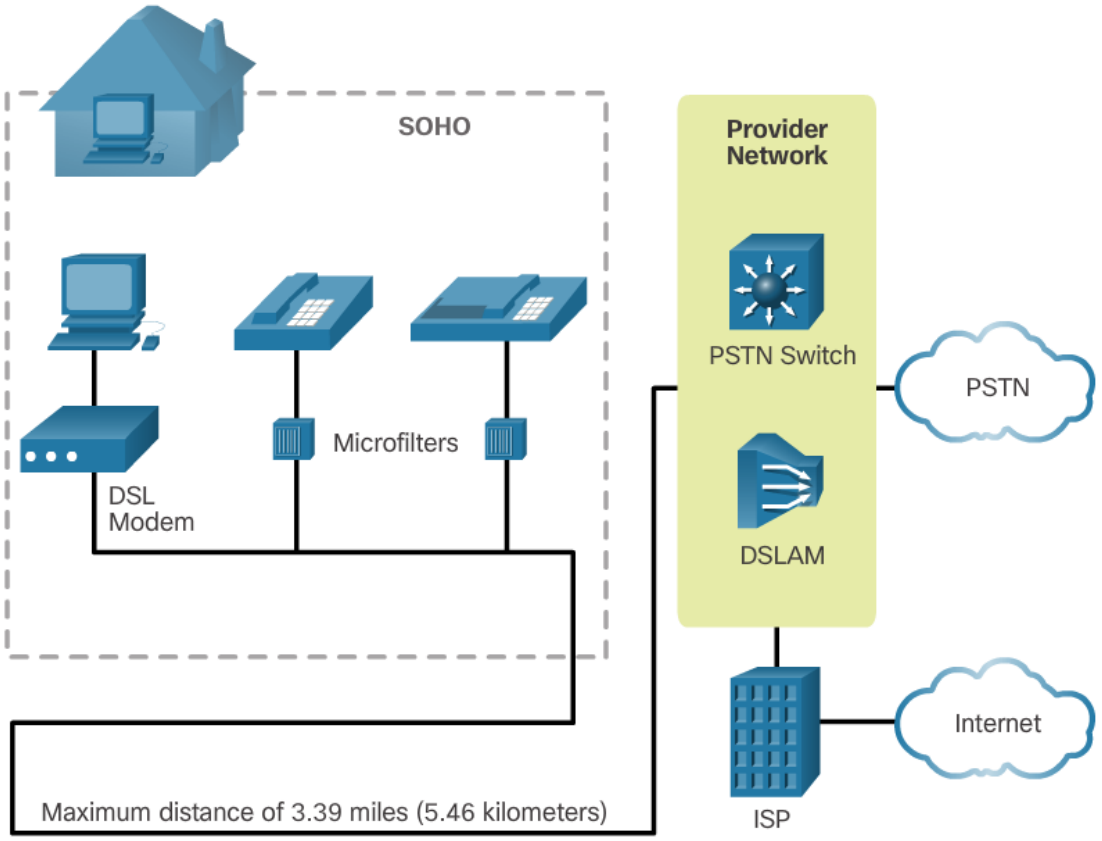
- DSL poskytuje high-speed pripojenie cez existujúcu sieť metalických dvojlinkových rozvodov (pôvodne pre analog. telefón)
  - Max dĺžka poslednej míle (Local loop) je obmedzená
  - Zároveň čím dlhšie vedenie, tým je finálne nižšia rýchlosť
- Existuje viacero DSL technológií sumárne označovaných ako ***xDSL*** (ADSL/2/2+, VDSL, SDSL, HDSL)
- Dva základné typy:
  - Asymetrické DSL (ADSL)
    - Používa frekvencie 20 kHz to 1 MHz.
    - Rozdiel vo väčšom Downstream voči Upstream
    - Max dĺžka poslednej míle (Local loop) nesmie prekročiť 5.46 km
  - Symetrické DSL (SDSL)
    - Rovnaká kapacita Up aj Down obojsmerne
    - Do 40Mbps podľa vzdialenosti
- Podobne aj tu je princíp frekvenčného oddelenia hlasu od dátovej prevádzky



DSL Type	Max. Send Speed	Max. Receive Speed	Max. Distance	Lines Required	Phone Support
ADSL	800 Kbps	8 Mbps	18,000 ft (5,500 m)	1	Yes
HDSL	1.54 Mbps	1.54 Mbps	12,000 ft (3,650 m)	2	No
IDSL	144 Kbps	144 Kbps	35,000 ft (10,700 m)	1	No
MSDSL	2 Mbps	2 Mbps	29,000 ft (8,800 m)	1	No
RADSL	1 Mbps	7 Mbps	18,000 ft (5,500 m)	1	Yes
SDSL	2.3 Mbps	2.3 Mbps	22,000 ft (6,700 m)	1	No
VDSL	16 Mbps	52 Mbps	4,000 ft (1,200 m)	1	Yes

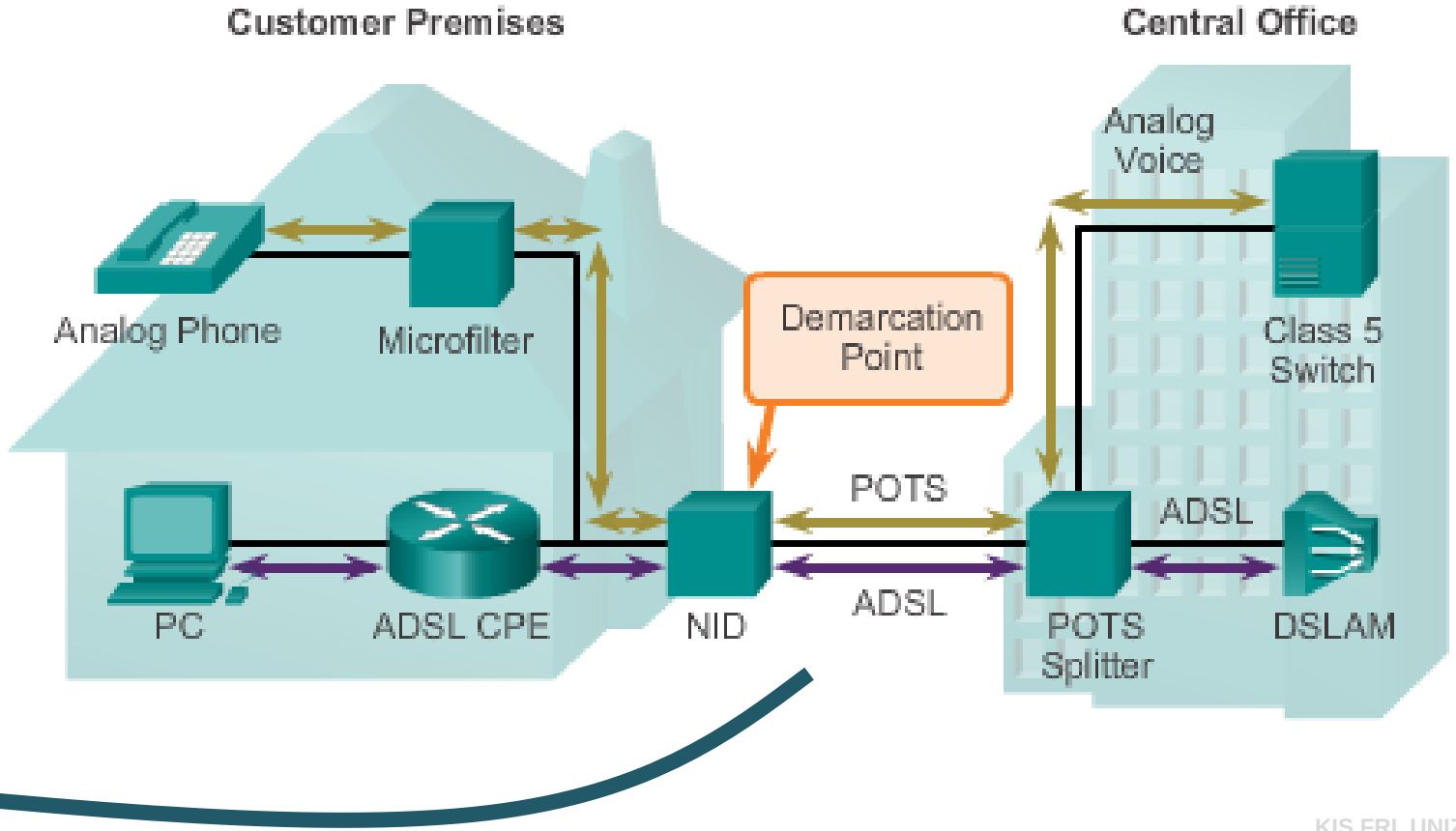
DSL komponenty

- DSL spojenie je medzi dvomi DSL modemami
  - Oddelenie dátovej a hlasovej prevádzky je riešené cez frekvenčné filtre
- Dva kľúčové komponenty DSL sú:
  - **Transceiver**
    - DSL modem, samostatný alebo súčasť domáceho smerovača
    - Pripája používateľov do siete
  - **DSL access multiplexer** (DSLAM)
    - „Modemová banka“ umiestnená v Central office (ústredňa)
    - Býva súčasť agregačného smerovača
    - Pripája:
      - na jednej strane point-to-point jednotlivých zákazníkov
      - Na druhej je vysokorýchlostné rozhranie do IP siete ISP



Oddelenie hlasu do dát

- Network Interface Device (NDI)
  - Bod vstupu, súčasťou je frekvenčný filter
- Na káblovom zväzku je kvôli presluchom obmedzený počet využiteľných párov



Bezdrôtové širokopásmové technológie

- Narastajú na popularite
- Patria sem napr.:
  - **Mestské/obecné WiFi siete** (Municipal Wi-Fi/Muni Wi-Fi/Muni-Fi)
    - Bezdrôtové siete vo forme Mesh, poskytujúce WiFi prístup
    - Budované lokálnymi úradmi zvyčajne s bezplatným prístupom (služba občanom)
    - Využívajú desiatky/stovky WiFi AP v zastavaných územiach
  - **Satelitný Internet**
    - Služba prístupu v riedko zastavaných oblastiach
    - Vďaka použitiu satelitov veľmi dobré pokrytie, rýchlosť down od 5Mbps do 25Mbps
    - Rôzne služby (one-way multicast, one-way terrestrial return, two-way satellite Internet)
  - **Mobilný prístup na internet**
    - Využitie mobilných sietí 3G/4G sietí s LTE (Long-Term Evolution) (<450Mbps, reálne ďaleko nižšie)
      - Pomocou mobilov a tethering-u
      - Pomocou smerovačov s gsm rozhraním a SIM
    - Stávajú sa v súčasnosti silnou alternatívou k fix prístupu

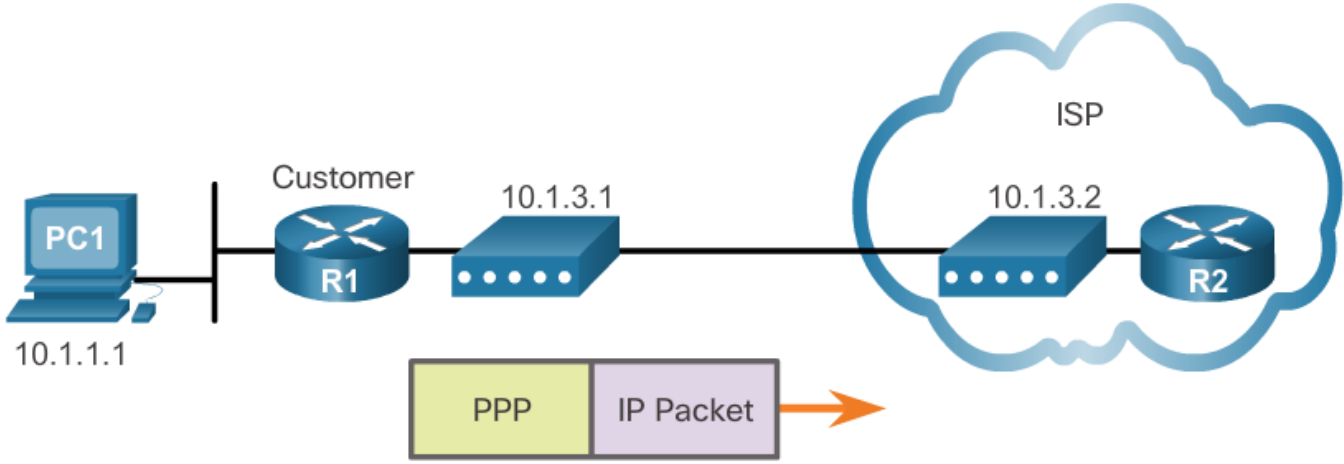
Porovnanie riešení širokopásmového prístupu

- Každé zo spomínaných riešení ma svoje výhody aj nevýhody
  - Cable
    - Zdieľaná kapacita, s množstvom pripojených a v silných hodinách klesá
    - Typicky asymetrické (symetrické oveľa drahšie)
  - DSL
    - Obmedzená rýchlosť a kapacita na zväzku, vzdialenosťou rýchlosť klesá, typicky asymetrická služba
  - Fiber-to-the-Home
    - Populárne v husto obývaných oblastiach, potreba doviesť optiku až domov
  - Cellular/Mobile
    - Otázne pokrytie (dostupnosť), ktoré sa líši podľa operátora, typicky asymetrická služba, zahusťovaním počtu pripojených rýchlosť klesá
  - Muni Wi-Fi Mesh
    - Nie každé mesto investuje, nelicencované pásmo, zahusťovaním počtu pripojených rýchlosť klesá
  - Satellite
    - Drahé, limitovaná kapacita, dobrá dostupnosť

PPP over Ethernet (PPPoE)

PPP over Ethernet (PPPoE) – motivácia

- PPP - L2 technológia nad analógovým dial-up, ISDN, sériové WAN linky
  - Dosť využívaná ISP
  - Má niektoré zaujímavé vlastnosti:
    - Schopnosť prideliť IP adresu cez PPP linku na diaľku (nie DHCP)
    - Podpora autentifikácie (CHAP + PAP)
- Rozšírený Ethernet napr. nemá podporu autentifikácie
  - Idea, využi na to PPP => vznik PPP over Ethernet (PPPoE)
  - PPPoE = vytvorenie PPP tunela cez Ethernet (PPPoE + Ethernet = PPPoE)
    - Využitie pridelenie IP adresy +
    - autentifikácia



Na pripomenutie

Základná PPP konfigurácia

```
R1
---
username R2 password 0 R2pass
!
interface Serial0/0/0
 ip address 10.0.0.1 255.0.0.0
 encapsulation ppp
 ppp authentication pap
 ppp pap sent-username R1 password 0
R1pass
```

```
R2
---
username R1 password 0 R1pass
!
interface Serial0/0/0
 ip address 10.0.0.2 255.0.0.0
 encapsulation ppp
 ppp authentication pap
 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 Serial0/0
 ip address 10.0.0.1 255.0.0.0
 encapsulation ppp
 peer default ip address pool PPP_Pool
 ppp authentication pap
 ppp pap sent-username R1 password 0 R1pass
```

```
R2 – dostane IP
---
username R1 password 0 R1pass
!
interface Serial0/0
 ip address negotiated
 encapsulation ppp
 ppp authentication pap
 ppp pap sent-username R2 password 0 R2pass
 ppp ipcp route default
```

PPPoE konfigurácia

PPPoE prístupový koncentrátor - ISP

- Vytvor lokálnu DB mien a hesiel zákazníkov
- Vytvor pool IP adries na prideľovanie zákazníkom
- Vytvor virtuálne rozhranie s konfiguračným template
- V ňom
  - 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 rozhraní k zákazníkovi

PPPoE klient (dialer) – zákazník

- Vytvor virtuálne *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 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 autentifikaciu
username someuser1 password ciscopppoe
username someuser1 autocommand logout

! Pool adries 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 158.193.152.2

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

! Nastav template na INPUT rozhranie smerom k zakaznik.
interface g0/1
  pppoe enable group global
```

- PPPoE Dialer (klient)

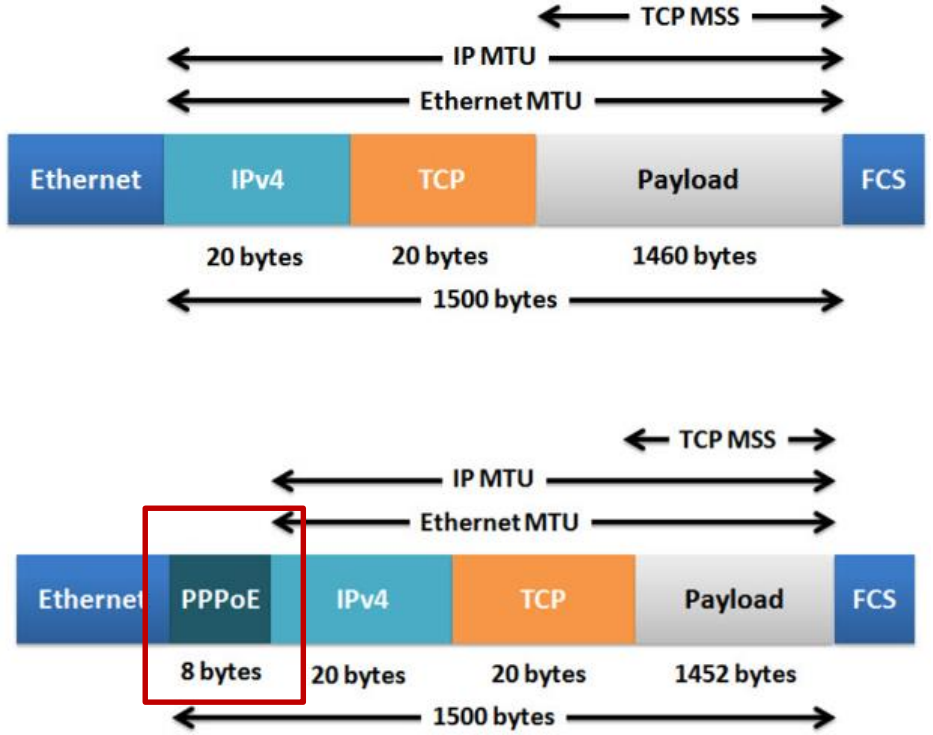
```
!Klient (customer 1):
!---
interface dialer 1
   encapsulation ppp
   ip address negotiated
   mtu 1492
   dialer pool 1

   ppp chap hostname someuser1
   ppp chap password ciscopppoe

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

! 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 g0/1
   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 …?

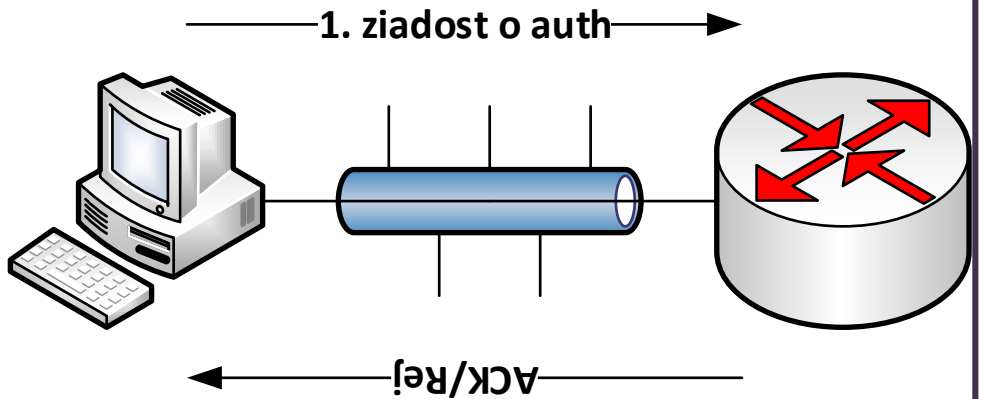
  Fragmentáciu!



- **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 pppoe server
! Tzv. Broadband aggregator
bba-group pppoe 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 autentifikaciu
! 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 h3sl0
username someuser1 autocommand logout
username someuser2 privilege 0 password 0 in3h3sl0
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

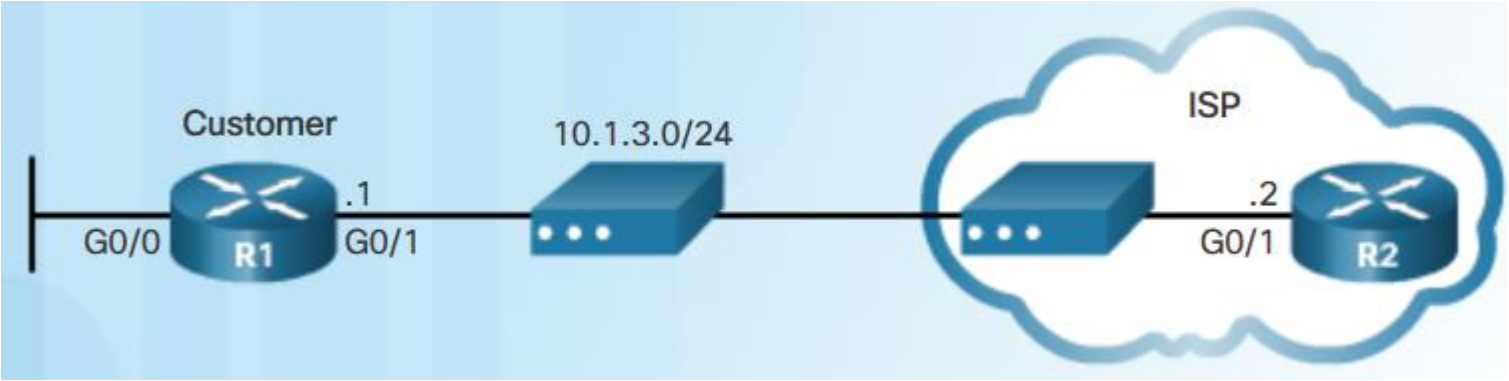
- PPPoE overenie
  - **show ip interface brief**
    - či sme dostali správnu IP adresu
  - **show interface dialer**
    - zobrazí, či je MTU a PPP enkapsulácia konfigurovaná na dialer rozhraní
  - **show pppoe session**
    - Zobrazí info o aktívnych PPPoE reláciach

```
Router# sh pppoe session
     1 session  in LOCALLY_TERMINATED (PTA) State
     1 session  total

Uniq ID  PPPoE  RemMAC          Port                 Source   VA          State
           SID  LocMAC                                        VA-st
      1      1  c002.1c7c.0001  Fa0/1                Vt1      Vi1.1       PTA
                c001.22ec.0001                                UP
```

PPPoE diagnostika

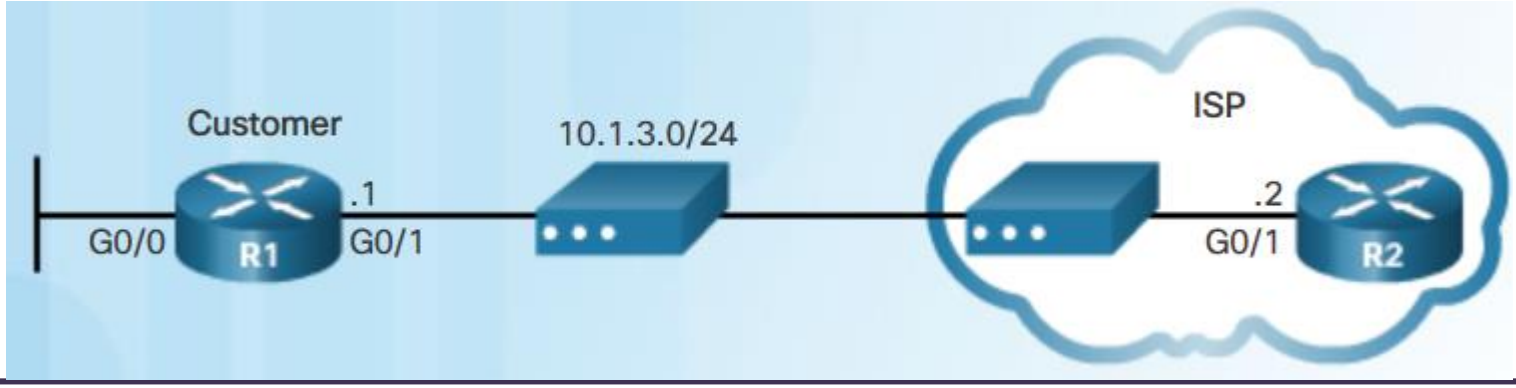
- Chyba pri PPPoE môže byť v:
  - Chyba v PPP negociácii (spomínate na LCP/NCP??)
    - Možné chyby
      - Nie je odpoveď od ISP
      - LCP neprebehol
      - Chyba autentifikácie
      - Chyba IPCP
    - **`debug ppp negotiation`**
  - Chyba v PPP autentifikácii
    - Možné chyby
      - Nenakonfigurovanie,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

Chyba v PPP negociácii či autentifikácii




```
R1# debug ppp negotiation
*Sep 20 19:05:05.239: Vi2 PPP: Phase is AUTHENTICATING, by the peer
*Sep 20 19:05:05.239: Vi2 LCP: State is Open
 <output omitted>
*Sep 20 19:05:05.247: Vi2 CHAP: Using hostname from interface CHAP
*Sep 20 19:05:05.247: Vi2 CHAP: Using password from interface CHAP
*Sep 20 19:05:05.247: Vi2 CHAP: O RESPONSE id 1 len 26 from "Fred"
*Sep 20 19:05:05.255: Vi2 CHAP: I SUCCESS id 1 len 4

*Sep 20 19:05:05.259: Vi2 IPCP:    Address 10.1.3.2 (0x03060A010302)
*Sep 20 19:05:05.259: Vi2 IPCP: Event[Receive ConfAck] State[ACKsent to Open]
*Sep 20 19:05:05.271: Vi2 IPCP: State is Open
*Sep 20 19:05:05.271: Di2 IPCP: Install negotiated IP interface address 10.1.3.2
*Sep 20 19:05:05.271: Di2 Added to neighbor route AVL tree: topoid 0, address 10.1.3.2
*Sep 20 19:05:05.271: Di2 IPCP: Install route to 10.1.3.2
R1# undebug all
```

Chyba v PPP autentifikácii



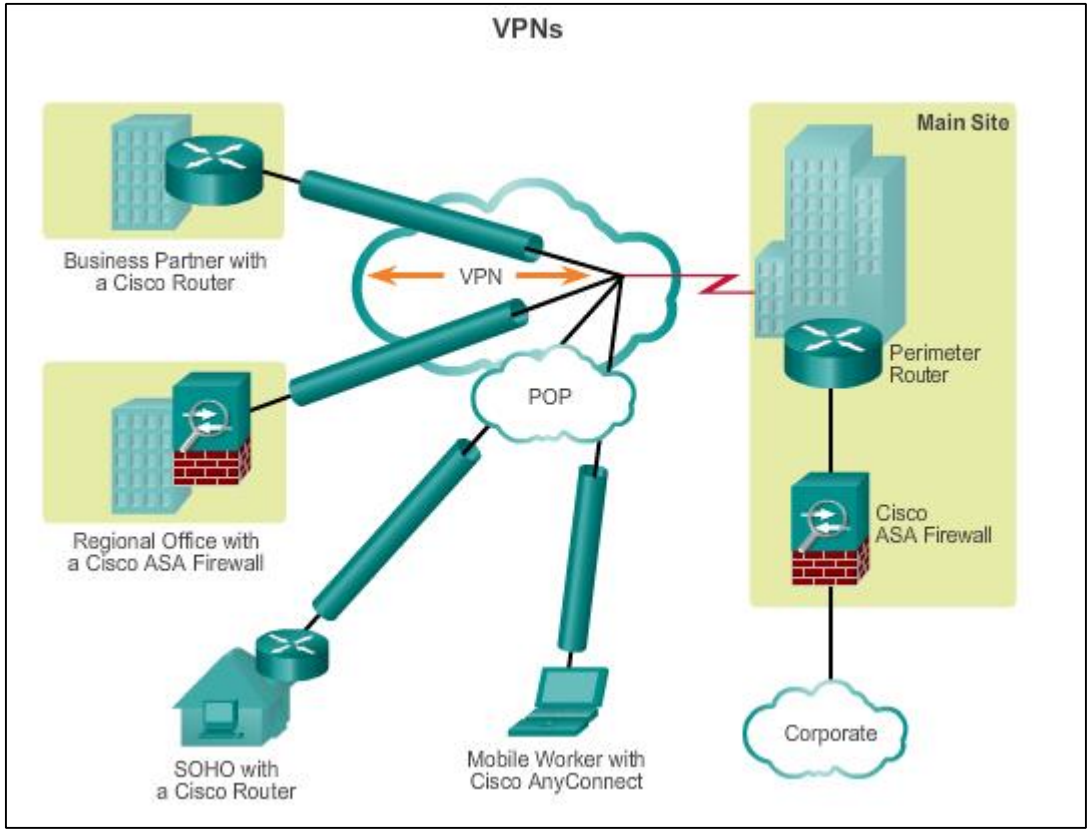

```
R2# debug ppp authentication
*Mar  1 00:23:04.059: ppp3 PPP: Using vpn set call direction
*Mar  1 00:23:04.059: ppp3 PPP: Treating connection as a callin
*Mar  1 00:23:04.059: ppp3 PPP: Session handle[59000005] Session id[3]
*Mar  1 00:23:04.071: ppp3 PPP: Authorization required
*Mar  1 00:23:04.091: ppp3 MS-CHAP-V2: O CHALLENGE id 1 len 23 from "R2"
*Mar  1 00:23:04.111: ppp3 MS-CHAP-V2: I RESPONSE id 1 len 63 from „R1"
*Mar  1 00:23:04.115: ppp3 PPP: Sent MSCHAP_V2 LOGIN Request
*Mar  1 00:23:04.119: ppp3 PPP: Received LOGIN Response PASS
*Mar  1 00:23:04.163: Vi1.1 PPP: Sent LCP AUTHOR Request
*Mar  1 00:23:04.167: Vi1.1 PPP: Sent IPCP AUTHOR Request
*Mar  1 00:23:04.171: Vi1.1 LCP: Received AAA AUTHOR Response PASS
*Mar  1 00:23:04.175: Vi1.1 IPCP: Received AAA AUTHOR Response PASS
*Mar  1 00:23:04.175: Vi1.1 MS-CHAP-V2: O SUCCESS id 1 len 46 msg is
"S=8FD9BE1E26DE2F8575ABFE9FE60A9396A8F3FBC"
```

VPNs - Virtual Private Networks

VPN základy

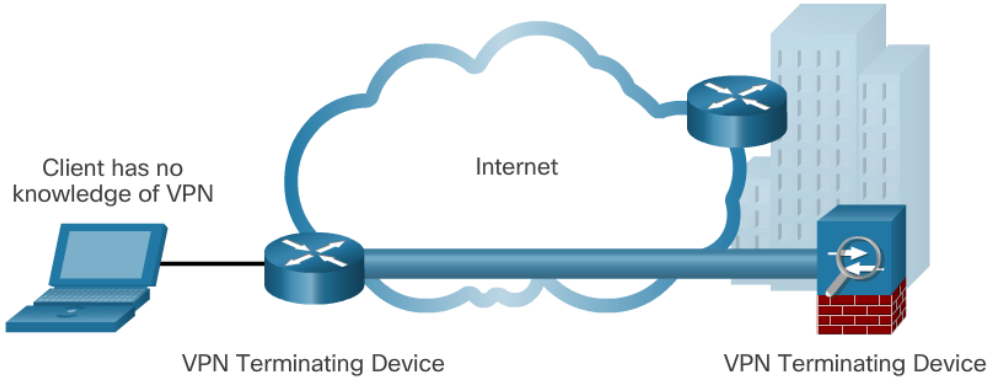
- Virtual Private Networks
  - Privátna end-to-end sieť, ktorou si organizácie prepájajú svoje časti
    - Typicky cez siete iných poskytovateľov (third-party networks), ako je napr. Internet.
  - V súčasností hlavne chápaná ako zabezpečená (šifrovaná) sieť vytvorená cez IPSec
- Na ich implementáciu typicky treba
  - VPN brána/brány
    - router, firewall, or Cisco Adaptive Security Appliance (ASA)
  - IPSec klienta (IPsec softvér)

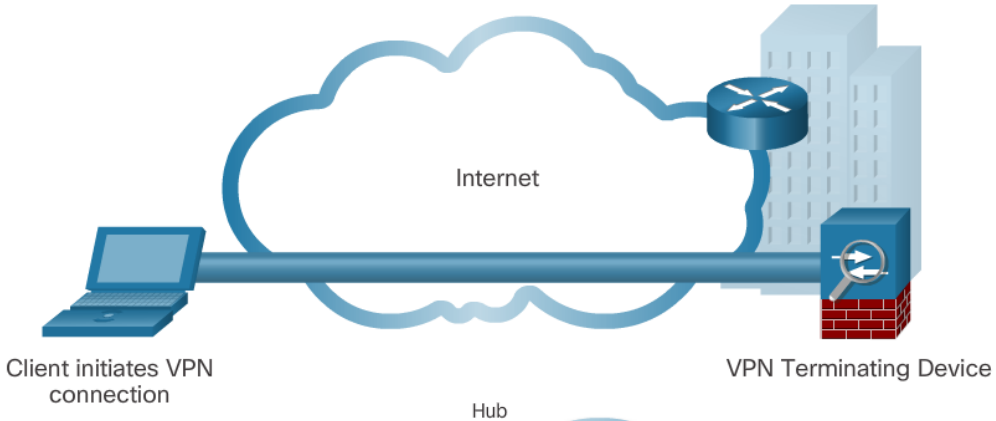
- Výhody VPN
  - Šetrenie nákladov
    - Teleworking, mobilita, využitie Internetu na bezpečný prístup do korporátnej siete
  - Škálovateľnosť
    - Jednoduché riadenie pridávania používateľov, sietí
  - Kompatibilita so širokopásmovými technológiami
  - Bezpečnosť
    - Vysoká úroveň zabezpečenia komunikácie

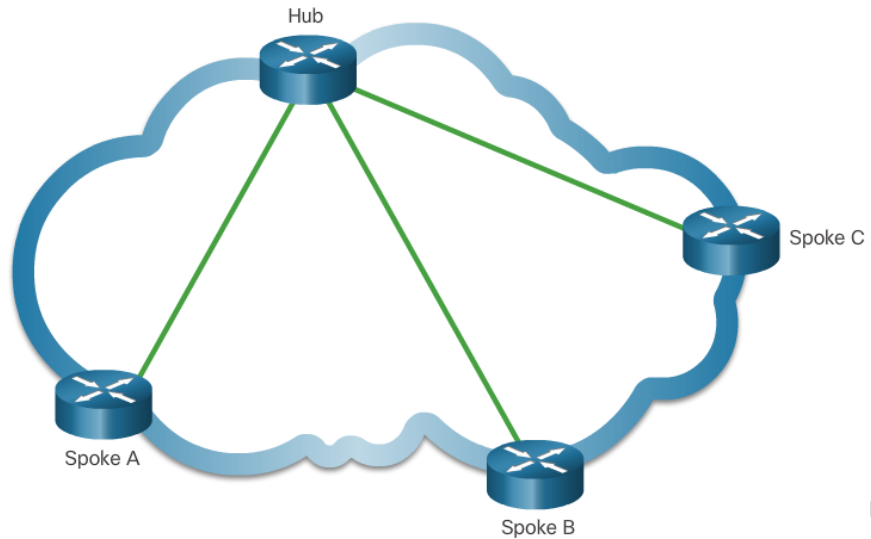


Typy VPN-niek

- Site-to-Site VPN
  - prepája navzájom celé siete, napr. pobočky s centrálou
  - Všetky činnosti implementované na VPN bránach
    - Na koncových PC nie je požadovaný žiaden softvér, nemajú zdanie o nejakej VPNke
- Remote Access VPN
  - Použitá na pripájanie individuálnych PC k VPN bráne, napr. pre prístup do centrály
  - Pre pripojenie k VPN bráne je požadovaný Ipsec softvér
- DMVPN
  - Dynamic Multipoint VPN (DMVPN) je Cisco riešenie pre zjednodušené a dynamické budovanie VPN-niek v prostredí, kde je potreba prepojiť veľa sieti navzájom







GRE -
Generic Routing Encapsulation

Site-to-site GRE tunnely

Čo je to tunelovanie?

- Mnohokrát je potrebné nad existujúcou sieťou vytvoriť ilúziu novej siete
  - Existujúca sieť nepozná protokol, ktorý cez ňu potrebujeme preniesť, alebo službu, ktorú chceme využiť
  - Existujúcu sieť chceme využívať iba ako transport, avšak z pohľadu našej internej siete má byť takmer neviditeľná
  - Potrebujeme prepojiť viaceré lokality, potenciálne s privátnym adresovým rozsahom
  - Existujúcej sieti nedôverujeme a chceme cez ňu preniesť dáta zabezpečeným spôsobom
- Tunelovanie je technika, pri ktorej sa hotové pakety opätovne obalia do nových paketov
  - Z pôvodných paketov sa stáva payload, do ktorého sa existujúca sieť nepozerá

Protokoly pri tunelovaní

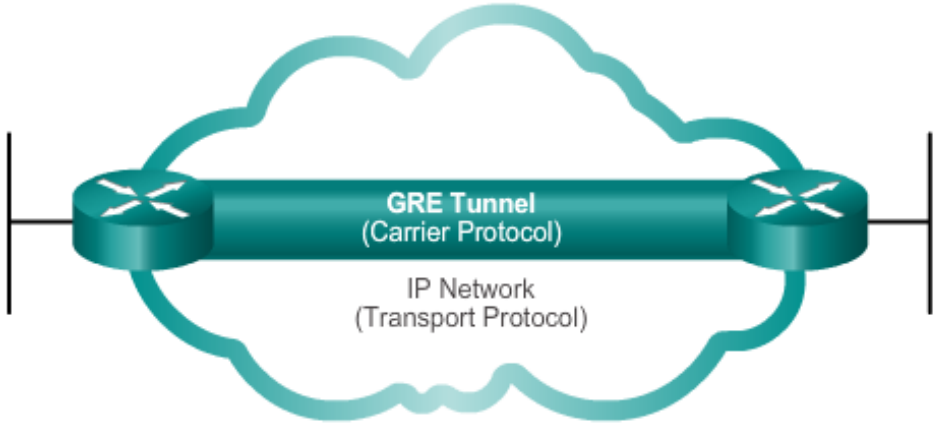
- Prenášaný protokol (passenger protocol)
  - Protokol, ktorého datagramy potrebujeme tunelovaním preniesť cez existujúcu sieť
- Pomocný tunelovací protokol (encapsulating protocol)
  - Protokol, ktorého hlavička sa prikladá k datagramom prenášaného protokolu
  - Umožňuje identifikovať prenášaný protokol, realizovať zabezpečenie, autentifikáciu a ďalšie funkcie
- Nosný protokol (carrier/transport protocol)
  - Protokol, na ktorom pracuje existujúca sieť a vo vnútri ktorého transportujeme datagramy prenášaného protokolu obalené pomocným tunelovacím protokolom

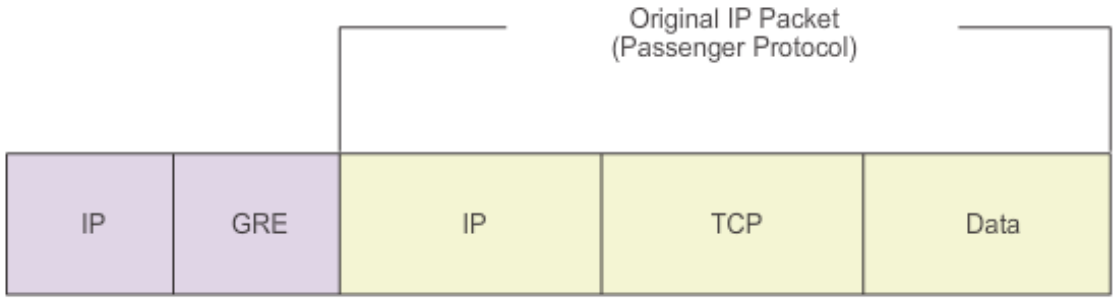
Tunelovacie protokoly

- Tunelovanie je možné realizovať s pomocným tunelovacím protokolom alebo bez neho
- Tunelovanie s pomocným tunelovacím protokolom
  - Tunelované (passenger) pakety sa obalia hlavičkou pomocného tunelovacieho protokolu, až potom sa opätovne vkladajú do nových paketov
  - Možnosti pre autentifikáciu, viacnásobné tunely medzi rovnakými zariadeniami, rôzne typy tunelovaných protokolov, šifrovanie
  - Potenciálne vyššia réžia
  - Napríklad: GRE, L2TP, PPTP
- Tunelovanie bez pomocného tunelovacieho protokolu
  - Tunelované pakety sa priamo vkladajú do nových paketov
  - Minimálna réžia
  - Obmedzené možnosti
  - Napríklad: IP-in-IP, IPv6-in-IPv4

Generic Routing Encapsulation – GRE

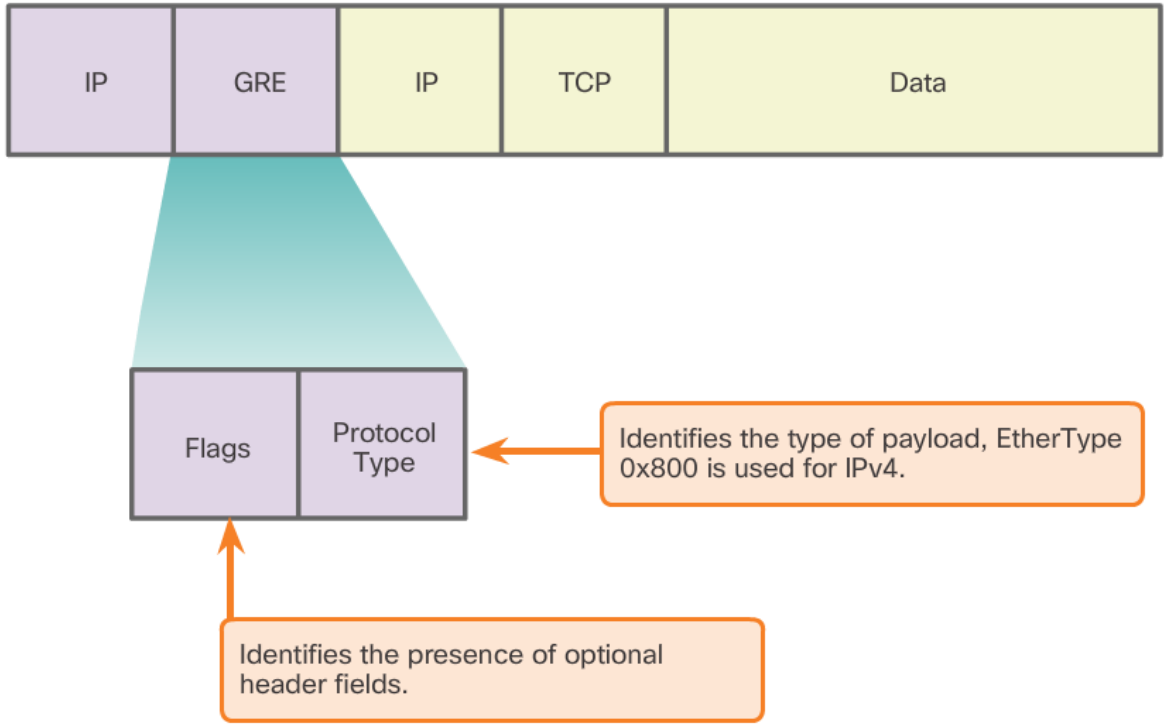
- GRE je pomocný tunelovací protokol na 3. vrstve
  - Podporuje rôzne typy tunelovaných paketov
    - Napr. IPv4, IPv6, IPX...
  - Vytvára virtuálny point-to-point prepoj medzi dvojicou smerovačov
  - Vkladá sa do IP paketov
  - Umožňuje prenášať aj multicastovú prevádzku (NBMA povaha)
- Autorom protokolu je spoločnosť Cisco
  - no protokol je v súčasnosti otvorený a dokumentovaný v RFC 2784





GRE - úvod

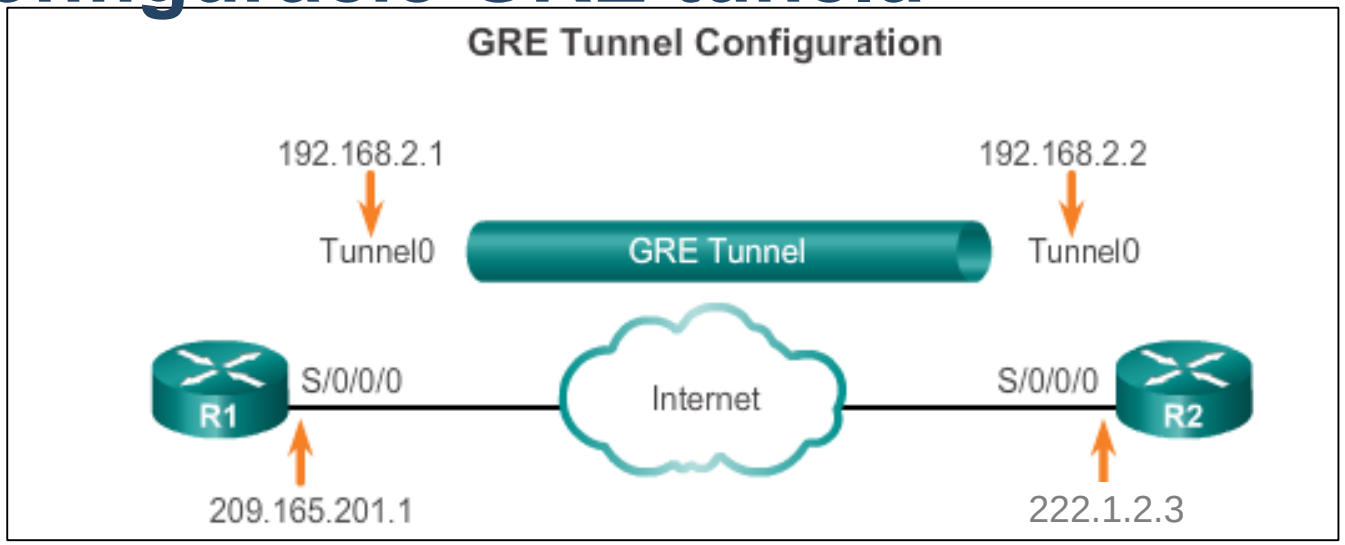
- GRE charakteristiky
  - je bezstavový, bez riadenia toku dát
  - IP protocol = 47
    - Identifikácia GRE v IP paket
  - GRE neposkytuje zabezpečenie
    - žiadna dôvernosť, autentifikácia alebo kontrola integrity
  - Overhead GRE tunelov je 24B
    - 20B na novú IP hlavičku a 4B na GRE hlavičku



Konfigurácia GRE tunelov

- GRE tunely sú na smerovači reprezentované virtuálnym rozhraním Tunnel
- Rozhranie Tunnel musí mať definované
  - Vlastnú IP adresu (ako každé iné rozhranie)
  - IP adresu odosielateľa
    - Odosielajúce rozhranie or IP adresa odosielajúceho rozhrania
  - IP adresu príjemcu nosných (carrier) paketov
  - Režim tunelovania
- Dvojica rozhraní Tunnel na rôznych smerovačoch, ktoré komunikujú, musí spĺňať tieto kritériá:
  - Vlastné IP adresy rozhraní Tunnel musia byť v tej istej sieti (rovnako ako na dvojici vzájomne prepojených rozhraní)
  - IP adresy odosielateľa a príjemcu musia navzájom korešpondovať (IP odosielateľa na jednom routeri musí zodpovedať IP príjemcu na druhom routeri a obrátene)
- Predvolený bandwidth rozhrania Tunnel je 9 Kbps
  - Mysli na EIGRP či OSPF metriku
  - Odporúča sa zvýšiť ho na realistickú hodnotu

Príklad konfigurácie GRE tunela




```
hostname Bratislava
!
interface Serial0/0/0
 ip address 209.165.201.1 255.255.255.0
 no shut
!
interface Tunnel0
 bandwidth 1000
 tunnel source s0/0/0
 ! Or
 ! tunnel source 209.165.201.1
 tunnel destination 223.1.2.3
 tunnel mode gre ip ! NEPOVINNÉ
 ip address 192.168.2.1 255.255.255.0
!
router ospf 1
 network 192.168.2.0 0.0.0.255 area 0
```

```
hostname Kosice
!
interface Serial0/0/0
 ip address 222.1.2.3 255.255.255.0
 no shut
!
interface Tunnel7
 bandwidth 1000
 tunnel source s0/0/0
 ! Or
 ! tunnel source 222.1.2.3
 tunnel destination 209.165.201.1
 tunnel mode gre ip ! NEPOVINNÉ
 ip address 192.168.2.2 255.255.255.0
!
router ospf 1
 network 192.168.2.0 0.0.0.255 area 0
```

Stav rozhraní Tunnel

- Rozhrania Tunnel pri GRE budú „up, protocol up“, ak sú splnené súčasne všetky nasledujúce podmienky
  - Rozhranie má definovaný zdroj a cieľ príkazmi **tunnel source**, **tunnel destination**
    - Tunel má definovanú platnú zdrojovú a cieľovú IP
  - Skutočné rozhranie, z ktorého si požičiavame zdrojovú IP v príkaze **tunnel source**, je v stave „up, protocol up“
    - Zdrojová IP adresa musí byť živá
  - V smerovacej tabuľke vieme vyhľadať cestu k náprotivnému koncu tunela definovanému príkazom **tunnel destination**
    - Cieľová IP adresa musí byť podľa našej RT dosiahnuteľná
  - Ak je zapnuté použitie GRE Keepalive, druhá strana odpovedá na naše Keepalive pakety
    - Vnútro transportnej siete musí byť schopné doručovať pakety medzi koncami tunela

Overenie

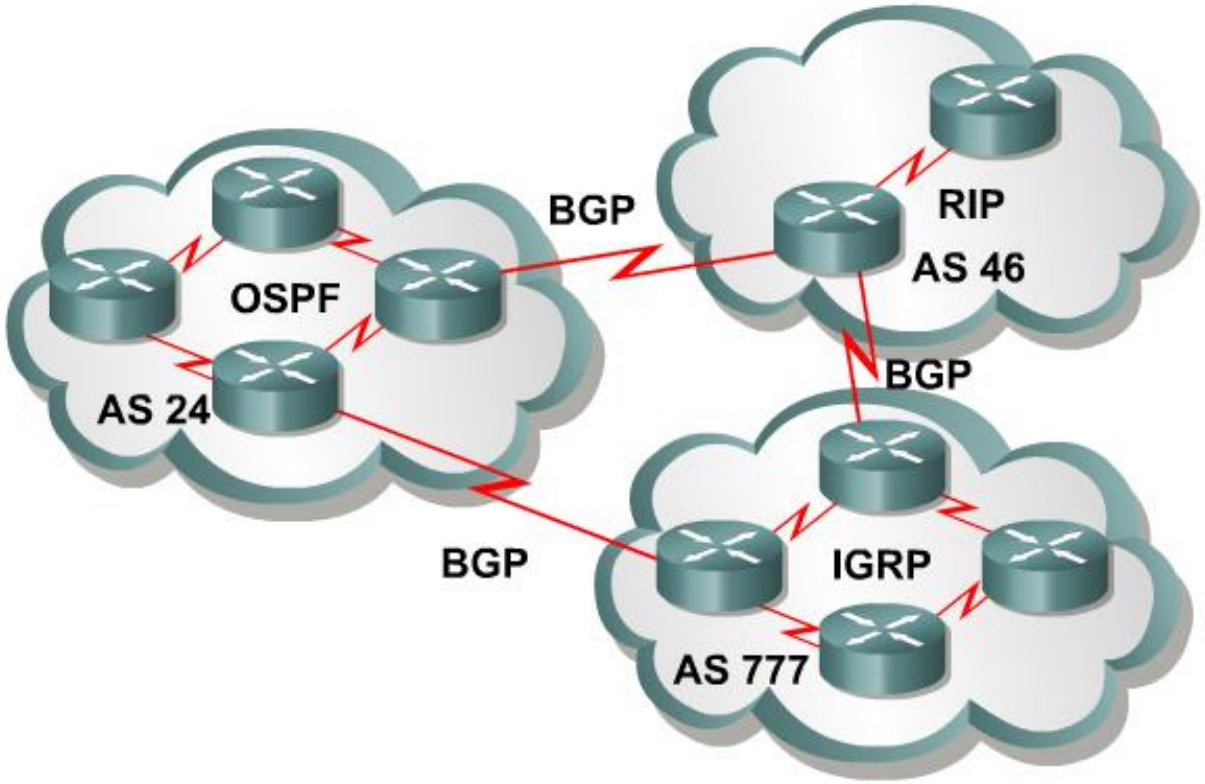
```
Branch# show interfaces tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 192.168.2.1/24
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 209.165.201.1, destination 223.1.2.3
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
  Tunnel transmit bandwidth 1000 (kbps)
  Tunnel receive bandwidth 1000 (kbps)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec

<output omitted>
```

Overenie a diagnostika - koncept

- Over že tunnel rozhranie je UP
  - **show ip interface brief**
    - Stav rozhraní
  - **show interface tunnel**
    - Stav GRE tunnel rozhrania
- Overenie smerovacieho protokolu
  - Overenie smerovacieho protokolu nad ním
    - Napr. OSPF susedstvo
    - **show ip ospf neighbor**
- Overenie smerovania
  - **show ip route**
    - Dostali sme čo sme mali?

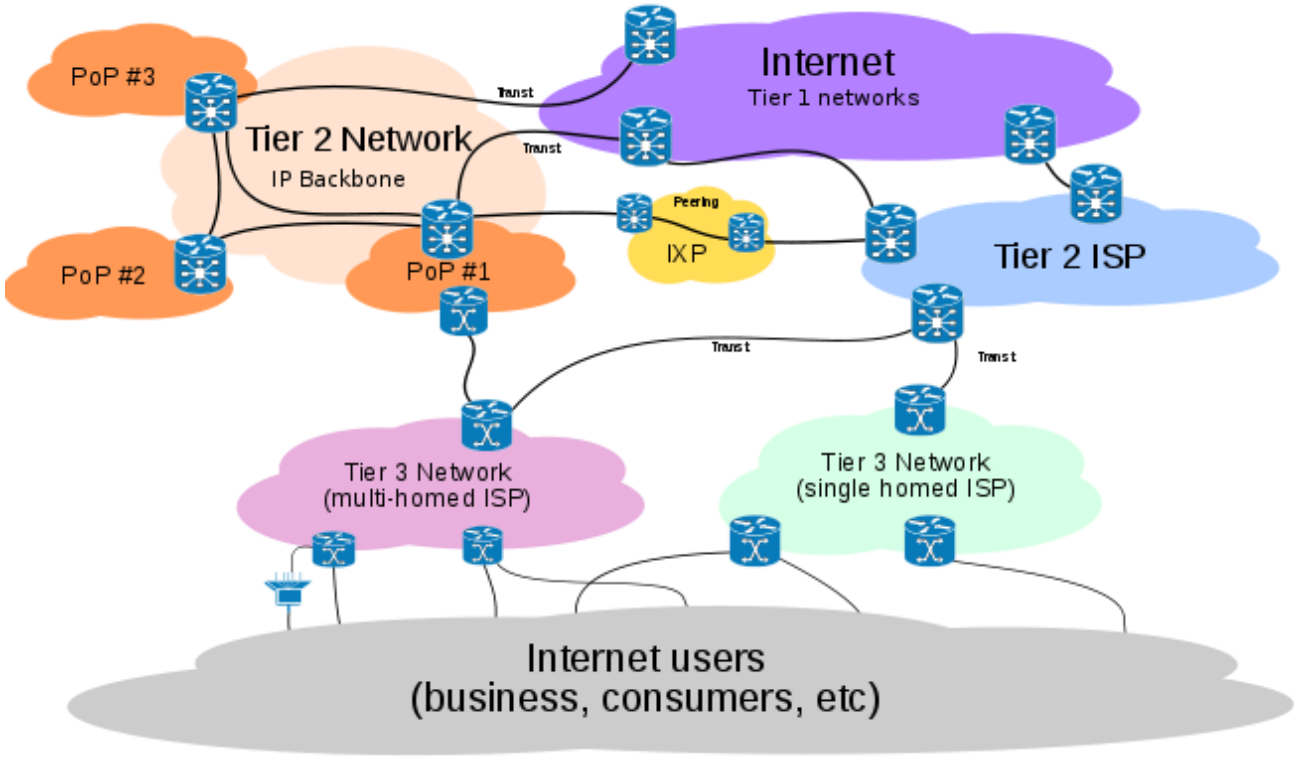
eBGP – external BGP

Logický pohľad na Internet



- Internet je skupina navzájom poprepájaných Autonómnych systémov (AS)
- Každý AS = 2B/4B identifikátor (public or private)

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 posielať cez svojich *tranzitných* providerov
    - Peering:
      - dobrovoľný prepoj AS za účelom vzájomnej výmeny dát („*ak prepošleš moje ja prepošlem tvoje*“)

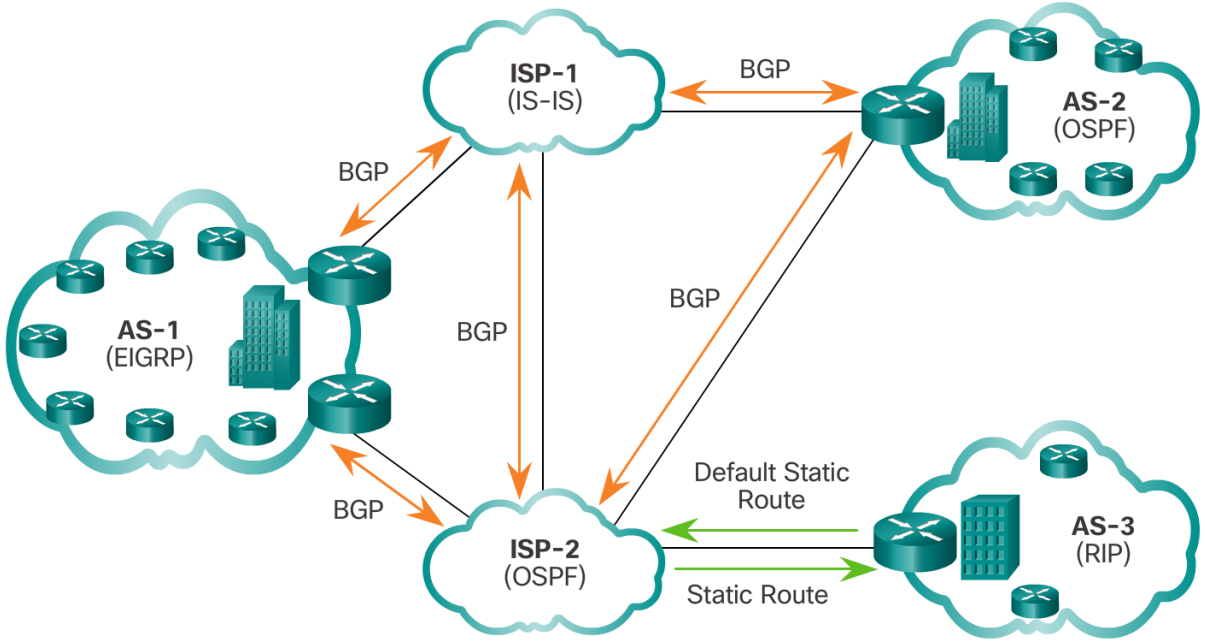
Európske IXP

IXP na Slovensku

- Slovensko má dva IXP body
  - BA a KE
- Slovak IXP (SIX) – www.six.sk
  - Špičková prevádzka – 212 Gbps
  - Priemer: okolo 50 Gbps
  - 60peerov

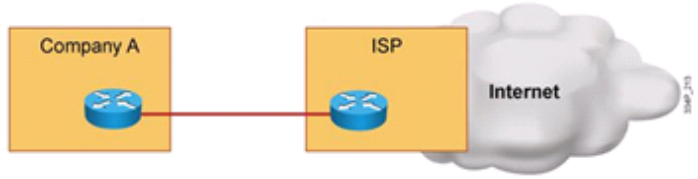
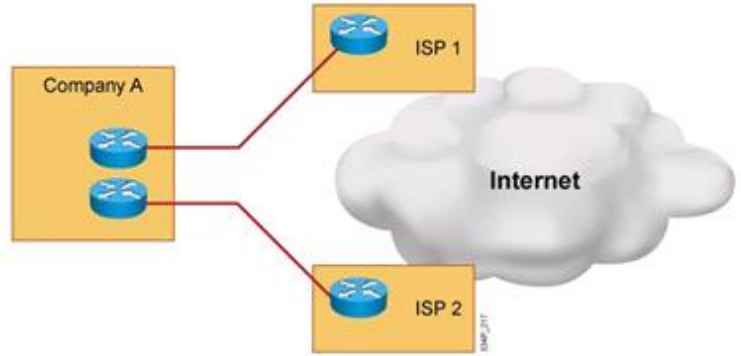
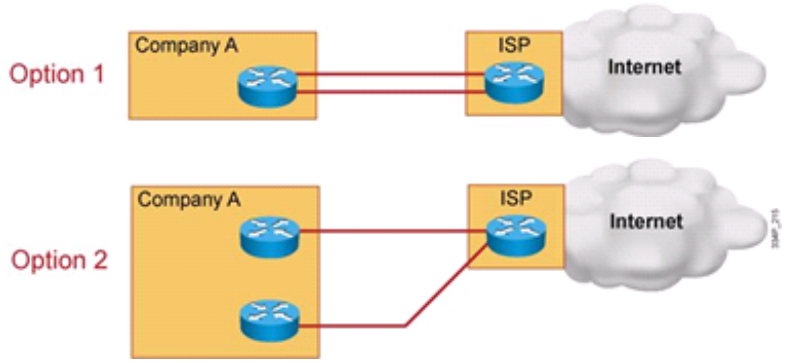
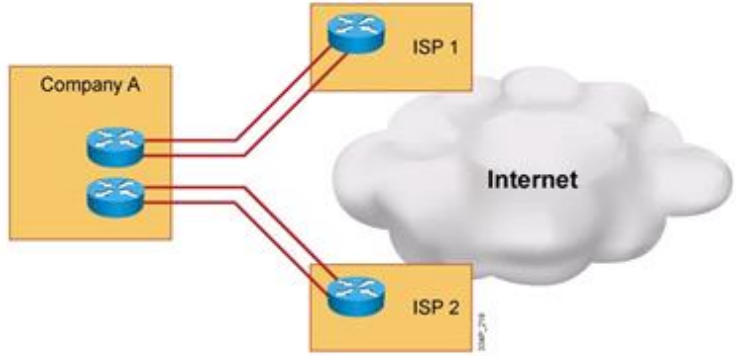
IGP vz EGP

- 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 rovný BGP**
    - Smerovací protokol pracujúci medzi rôznymi AS



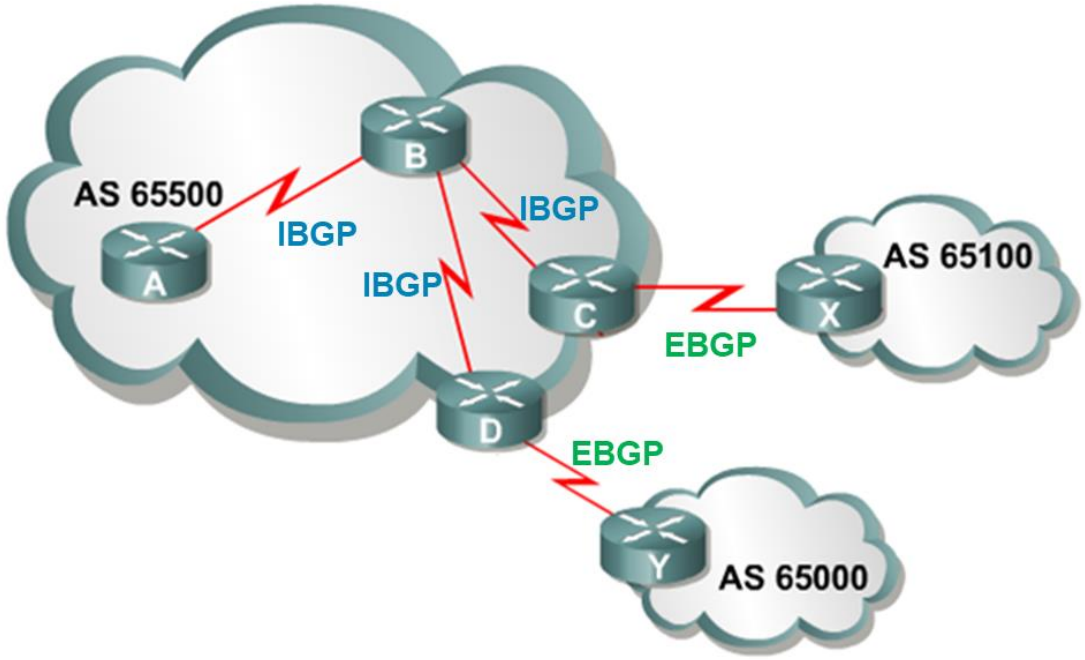
- BGP je v súčasnosti prakticky jediný používaný smerovací protokol pre inter-AS smerovanie
  - T.j. výmenu sieťových prefixov v daných AS a optimalizáciu smerovania cez tzv. atribúty cesty
  - Je typu Path vector (zoznam AS a atribútov)
  - Garantuje bezslučkovú výmenu smerovacích informácii
  - Dve AD
    - eBGP AD=20
    - iBGP AD = 200
- 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 zameriava len na eBGP

Prepojenie firmy s ISP

Connecting to One ISP	Connecting to Two or more ISPs
Single-homed 	**Multihomed** 
Dual-homed 	**Dual-multihomed** 

Možnosti prepojenie 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

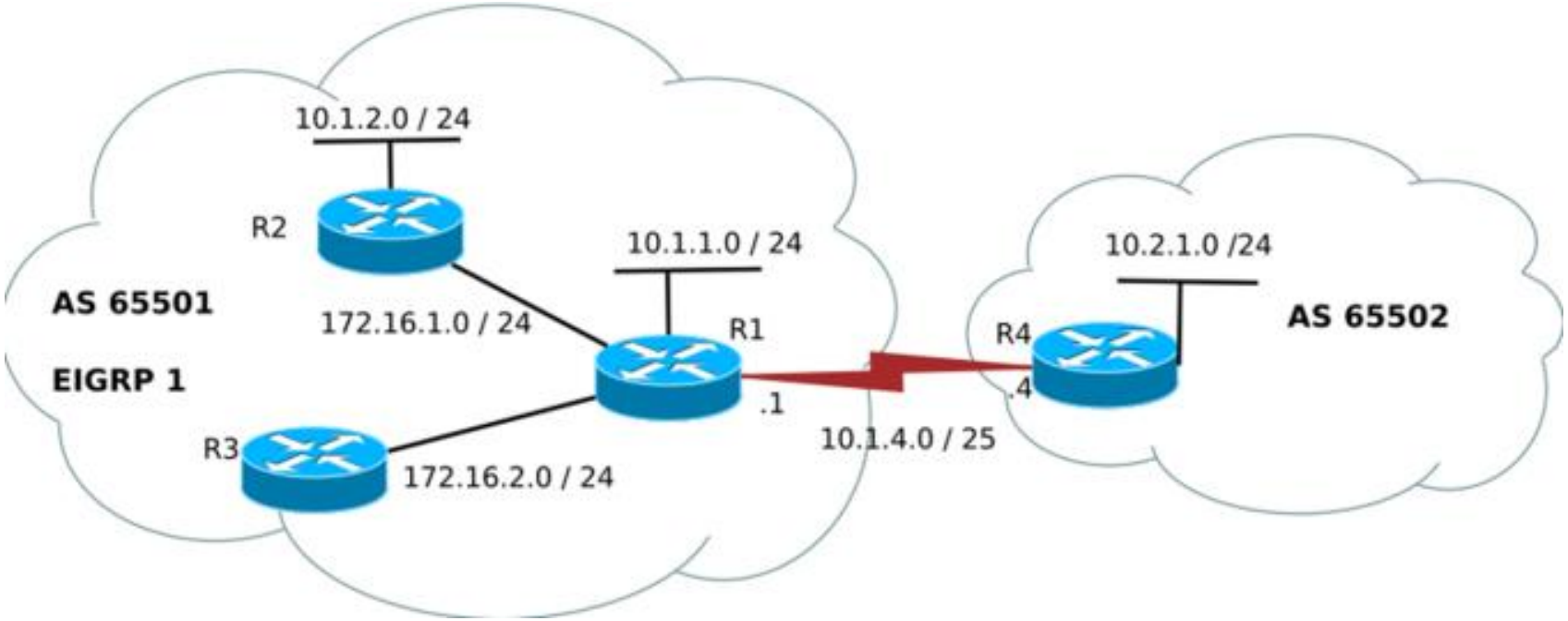
- Tri jednoduché kroky:
  - **Step 1**: spusti BGP proces
  - **Step 2**: konfiguruj BGP neighbor(s) (peering)
    - Susedia musia byť explicitne nakonfigurovaný, neexistuje auto objavovanie ako v IGP
  - **Step 3**: ohlás svoje siete (tie, ktoré pochádzajú z tvojho AS a sú v tvojej smerovacej tabuľke,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

Command	Description
`Router(config)# router bgp as-number`	Enables a BGP routing process, and places the router in router configuration mode.
`Router(config-router)# neighbor ip-address remote-as as-number`	Specifies a BGP neighbor. The as-number is the neighbor's AS number.
`Router(config-router)# network network-address [mask network-mask]`	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
  - **`Sh ip bgp`**
- Over smerovaciu tabuľku
  - **`Show ip route bgp`**

eBGP – Príklad jednoduchej konfigurácie

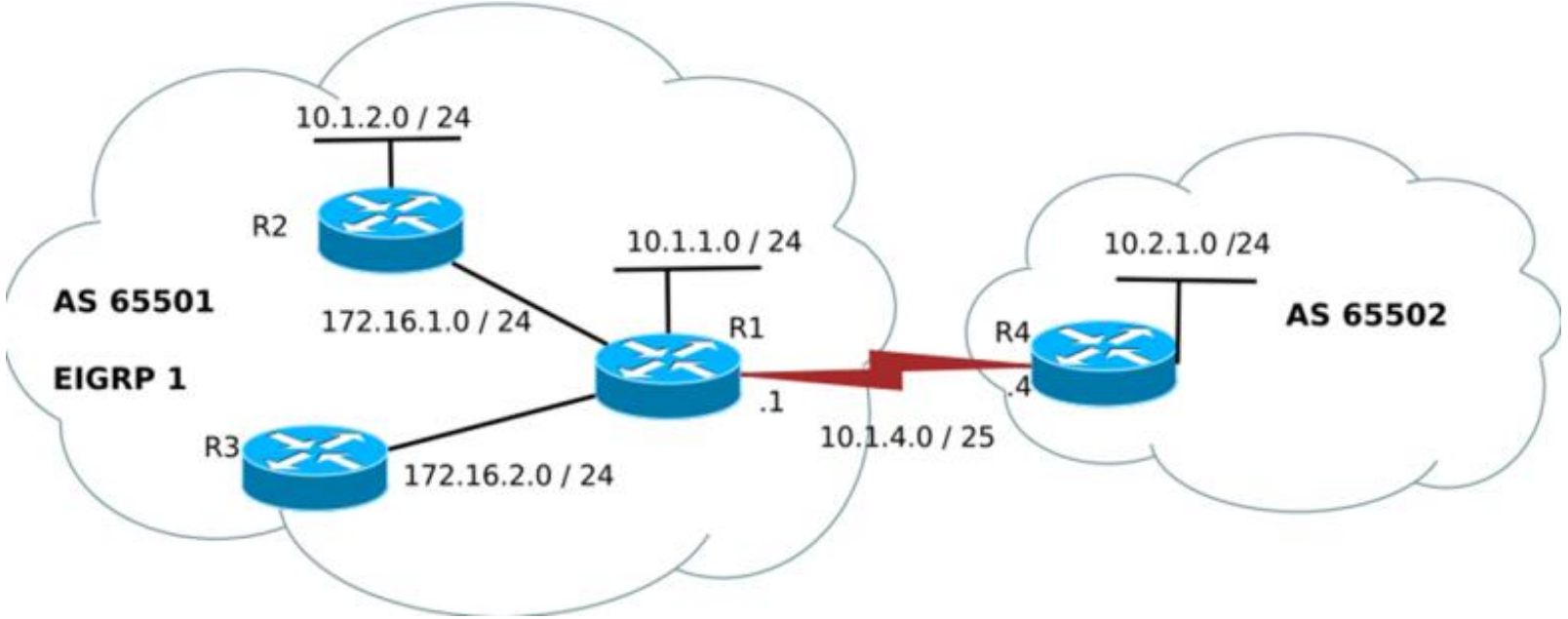


- Scenár:
  - Považuj 10.0.0.0 adresy ako Public – budú ohlásené mimo AS cez BGP
  - Považuj 172.16.0.0 adresy ako Private – nebudú ohlasované mimo AS

- 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:

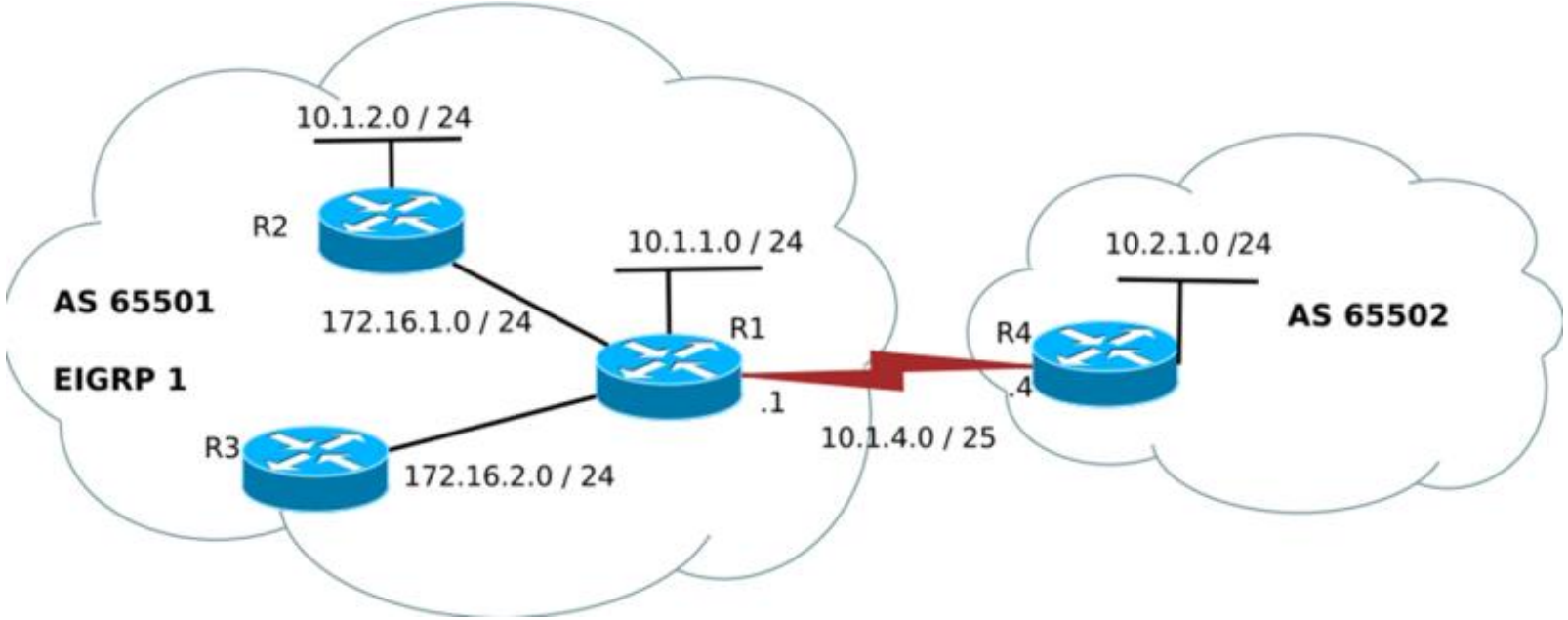
eBGP – Príklad jednoduchej konfigurácie




```
!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
```

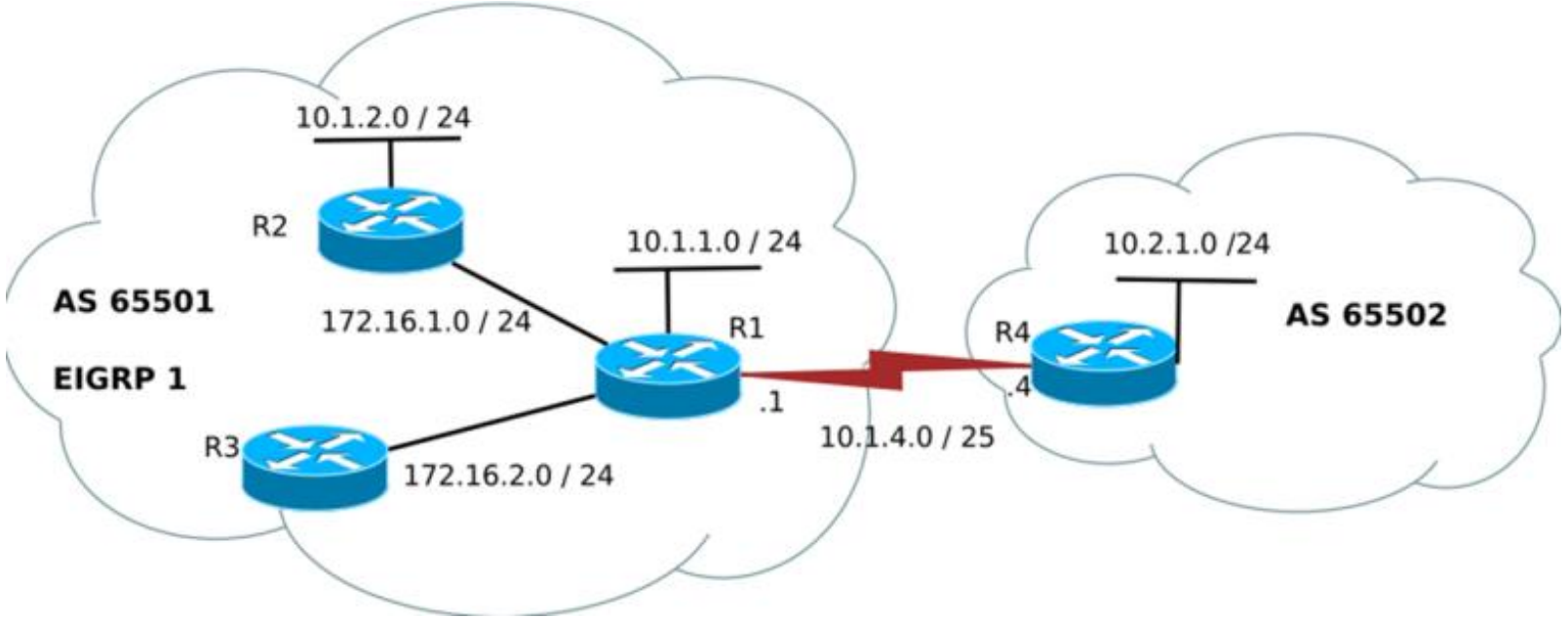
eBGP – Overenie susedov




```
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)
```

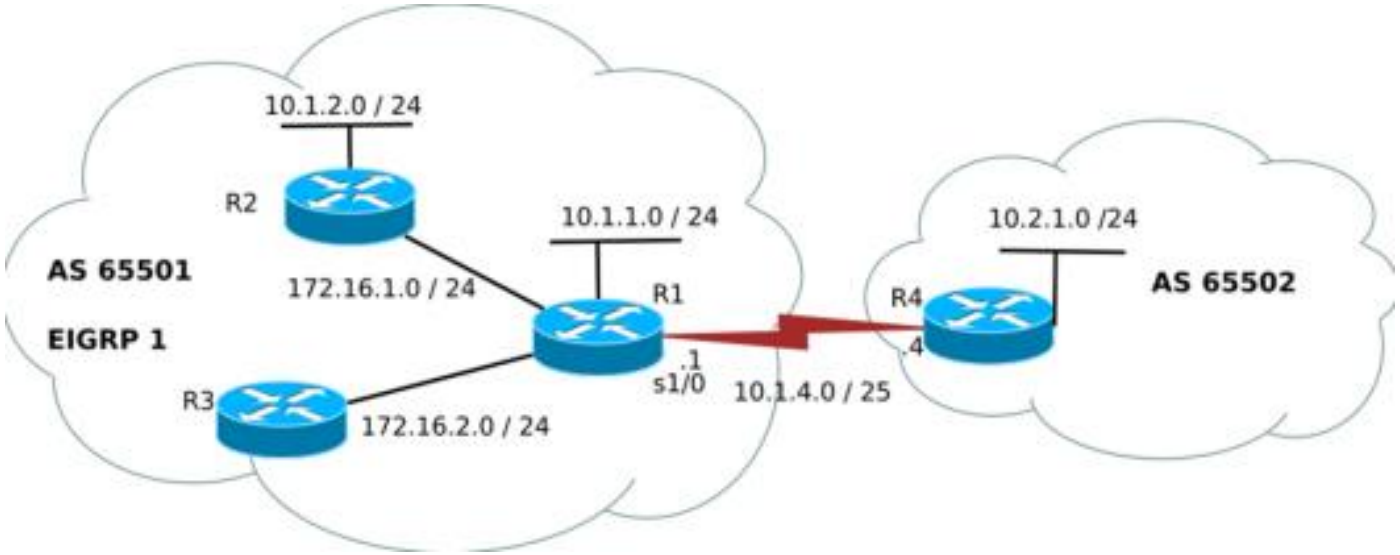
eBGP – ohlásenie sieti a overenie




```
! Siete musia byt v smerovacej tabulke
!
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



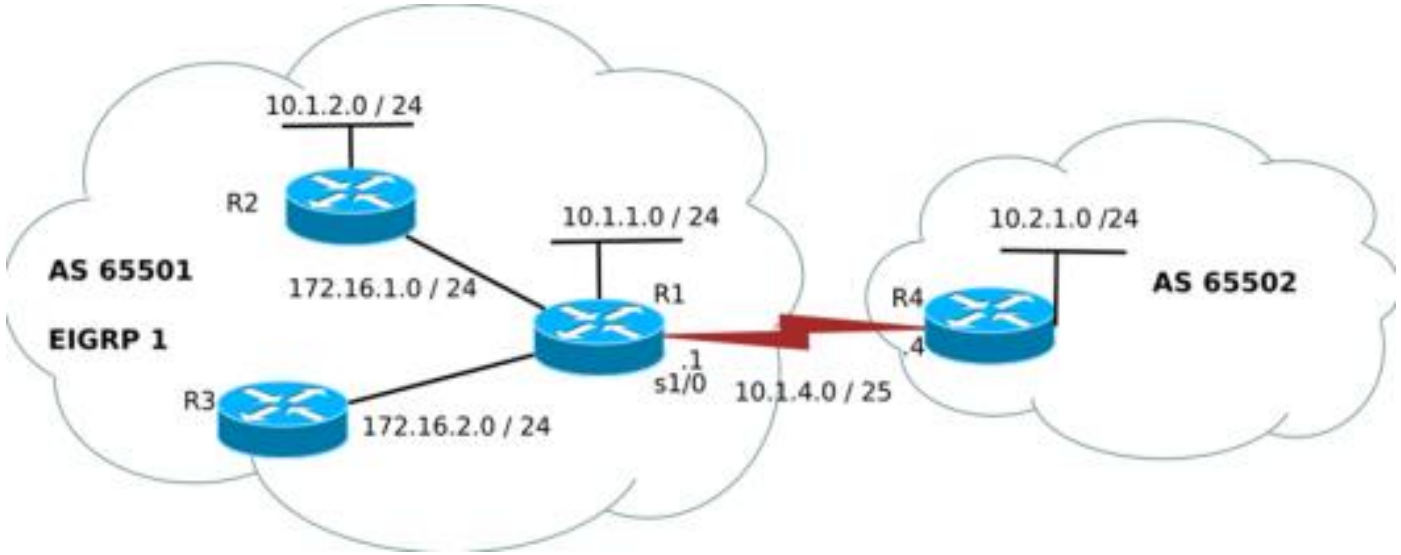
Kód/symbol

- * Dostupná cesta, BGP je nevybral na použitie
- ***>** naj cesta vybratá BGP. Bude ponúknutá do smerovacej tabuľky

- **Next Hop** – nasledujúci smerovač
  - = 0.0.0.0 som ním ja

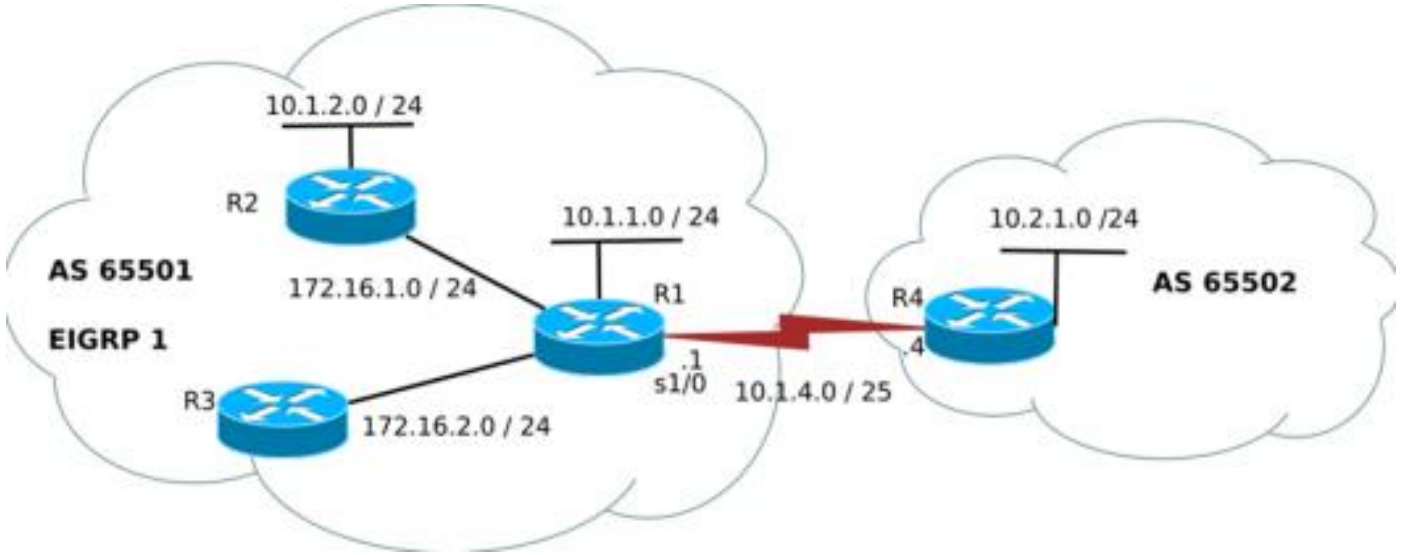
```
! R1 - vidi siet z R4 + dve svoje
R1# show ip bgp
BGP table version is 8, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, 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 65501 i
 *>  10.1.2.0/24      10.1.4.1            156160                    0 65501 i
 *>  10.2.1.0/24      0.0.0.0                  0                32768 i
```

Ako zabezpečiť smerovanie z R3 a R2?



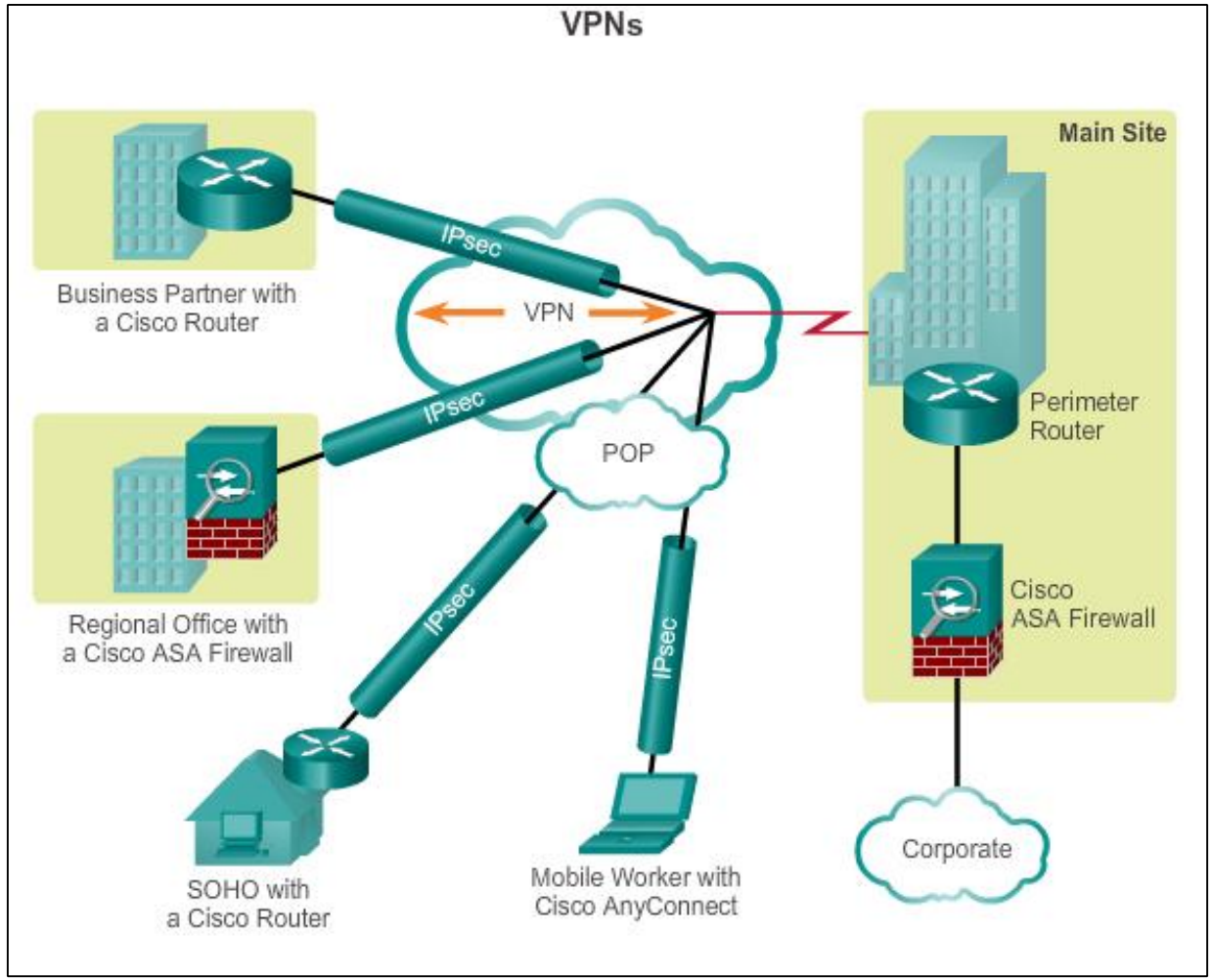
- V reále sú dve možnosti
  - R1 bude default router, ktorý sa ohlási cez EIGRP
  - Redistribúcia BGP ciest do EIGRP
    - Závisí od množstva ciest prijatých od ISP AS
      - Spomeň na možnosti BGP prepojenia zákazníka a ISP
        - Posledná možnosť – všetky cesty - je vražda EIGRP

Ďakujem za pozornosť, nasledujú snímky len pre „sieťo znalosti chtivých“

--

Introducing IPsec

IPsec VPNs



- Information from a private network is securely transported over a public network.
- Forms a virtual network instead of using a dedicated Layer 2 connection.
- To remain private, the traffic is encrypted to keep the data confidential.

IPsec Functions

- Defines how a VPN can be configured in a secure manner using IP.
- Framework of open standards that spells out the rules for secure communications.
- Not bound to any specific encryption, authentication, security algorithms, or keying technology.
- Relies on existing algorithms to implement secure communications.
- Works at the network layer, protecting and authenticating IP packets between participating IPsec devices.
- Secures a path between a pair of gateways, a pair of hosts, or a gateway and host.
- All implementations of IPsec have a plaintext Layer 3 header, so there are no issues with routing.
- Functions over all Layer 2 protocols, such as Ethernet, ATM, or Frame Relay.

IPsec Characteristics

IPsec characteristics can be summarized as follows:

- IPsec is a framework of open standards that is algorithm-independent.
- IPsec provides data confidentiality, data integrity, and origin authentication.
- IPsec acts at the network layer, protecting and authenticating IP packets.

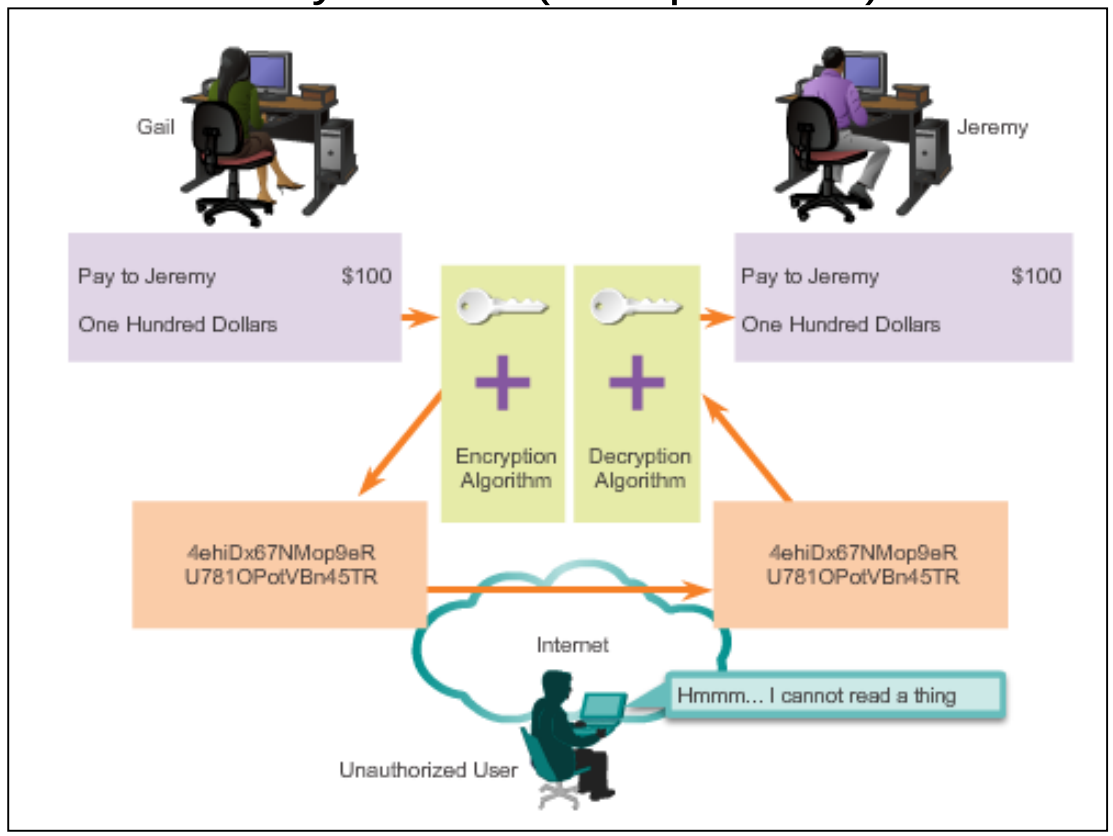
IPsec Security Services

- **Confidentiality (encryption)** – encrypt the data before transmitting across the network
- **Integrity (data)** – verify that data has not been changed while in transit, if tampering is detected, the packet is dropped
- **Authentication** – verify the identity of the source of the data that is sent, ensures that the connection is made with the desired communication partner, IPsec uses Internet Key Exchange (IKE) to authenticate users and devices that can carry out communication independently.
- **Anti-Replay Protection** – detect and reject replayed packets and helps prevent spoofing

CIA: confidentiality, integrity, and authentication

Confidentiality with Encryption

- For encryption to work, both the sender and the receiver must know the rules used to transform the original message into its coded form.
- Rules are based on algorithms and associated keys.
- Decryption is extremely difficult (or impossible) without the correct key.

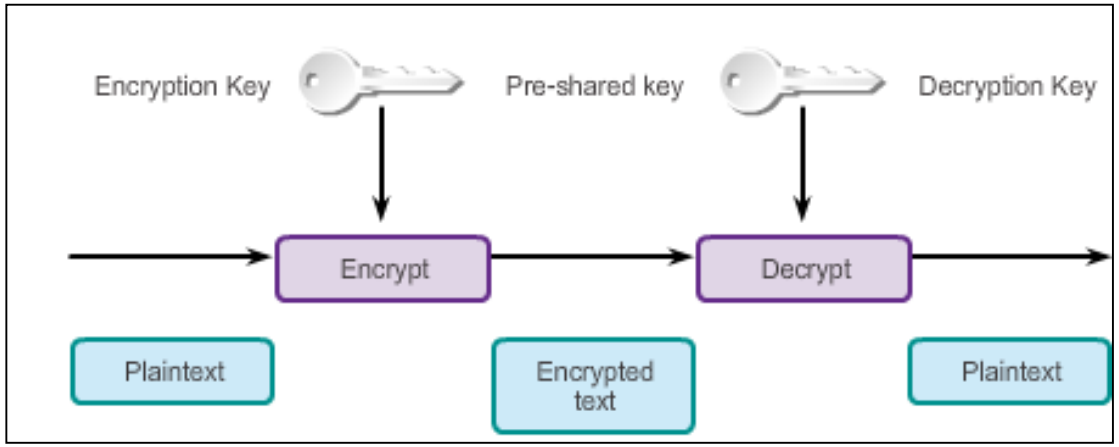


Encryption Algorithms

- As key length increases, it becomes more difficult to break the encryption. However, a longer key requires more processor resources when encrypting and decrypting data.
- Two main types of encryption are:
  - Symmetric Encryption
  - Asymmetric Encryption

Symmetric Encryption

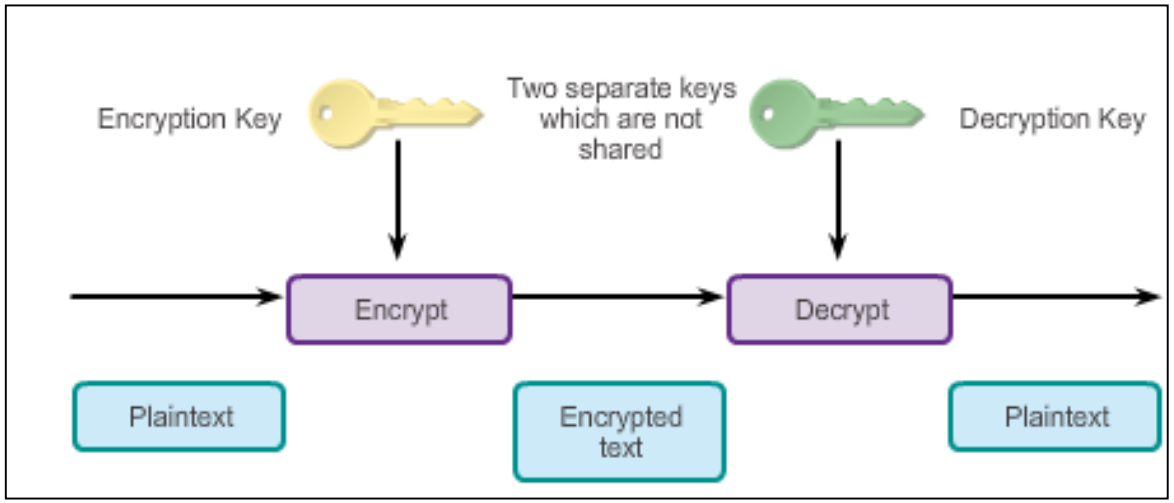
- Encryption and decryption **use the same key**.
- Each of the two networking devices must know the key to decode the information.
- Each device encrypts the information before sending it over the network to the other device.
- Typically used to encrypt the content of the message.
- Examples: DES and 3DES (no longer considered secure) and AES (256-bit recommended for IPsec encryption).



Algorithm	Key size
DES	56 bits
3DES	168 bits
AES	128 bits
AES192	192 bits
AES256	256 bits

Asymmetric Encryption

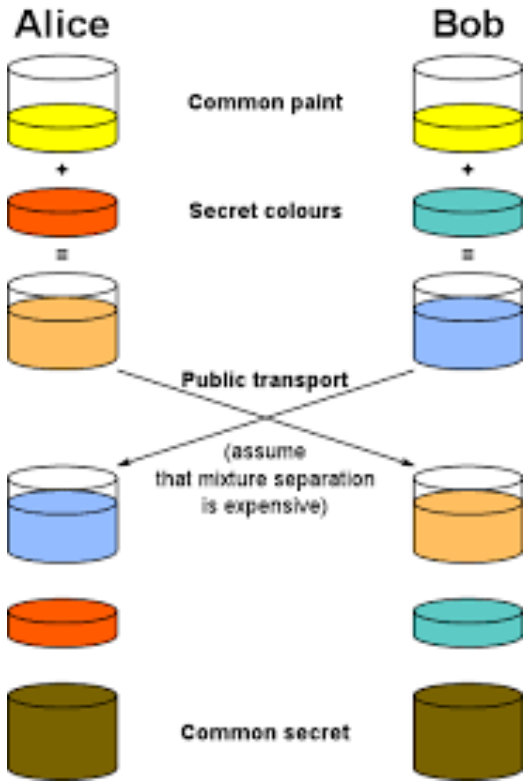
- Uses **different keys** for encryption and decryption.
  - Used also for authentication (signing)
- Knowing one of the keys does not allow a hacker to deduce the second key and decode the information.
- One key encrypts the message, while a second key decrypts the message.
- Public key encryption is a variant of asymmetric encryption that uses a combination of a **private** key and a **public** key.
- Typically used in digital certification and key management
- Example: RSA

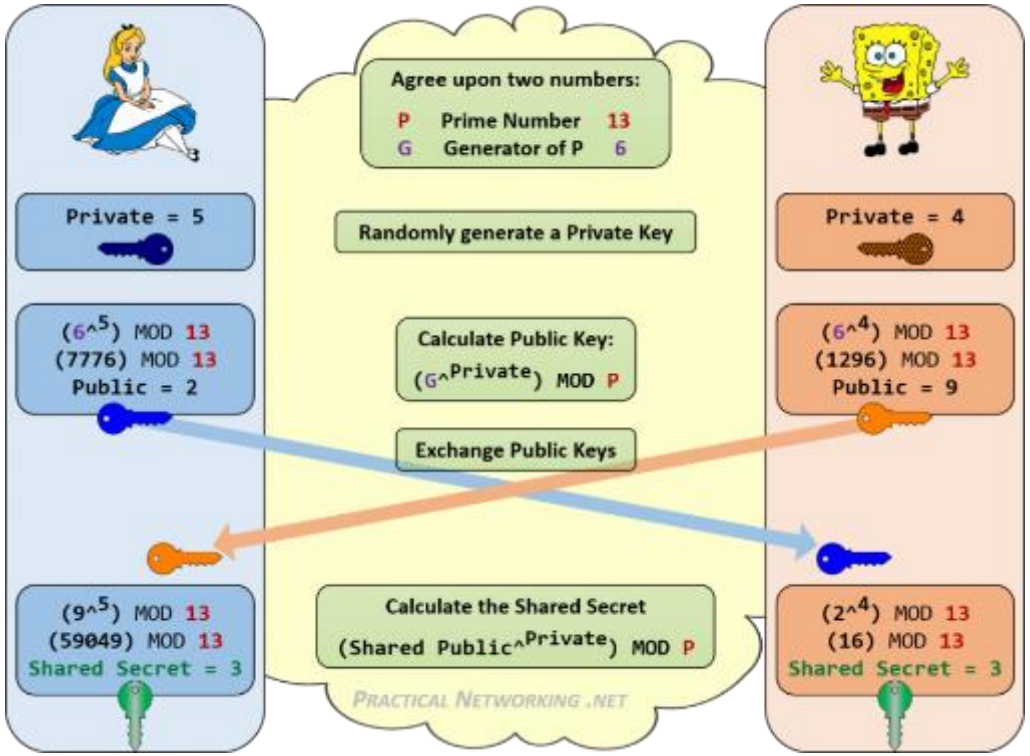


Diffie-Hellman Key Exchange

- Diffie-Hellman (DH) is not an encryption mechanism and is not typically used to encrypt data.
- DH is a method to securely exchange the keys that encrypt data.
- DH algorithms allow two parties to establish a shared secret key **used by encryption** and **hash algorithms** between parties which never meet before.
- DH is part of the IPsec standard.
- Encryption algorithms, such as DES, 3DES, and AES, as well as the MD5 and SHA-1 hashing algorithms, require a **symmetric, shared secret key t**o perform encryption and decryption.
- DH algorithm specifies a public key exchange method that provides a way for two peers to **establish a shared secret** key that only they know, although they are communicating over an insecure channel.

Diffie-Hellman Key Exchange

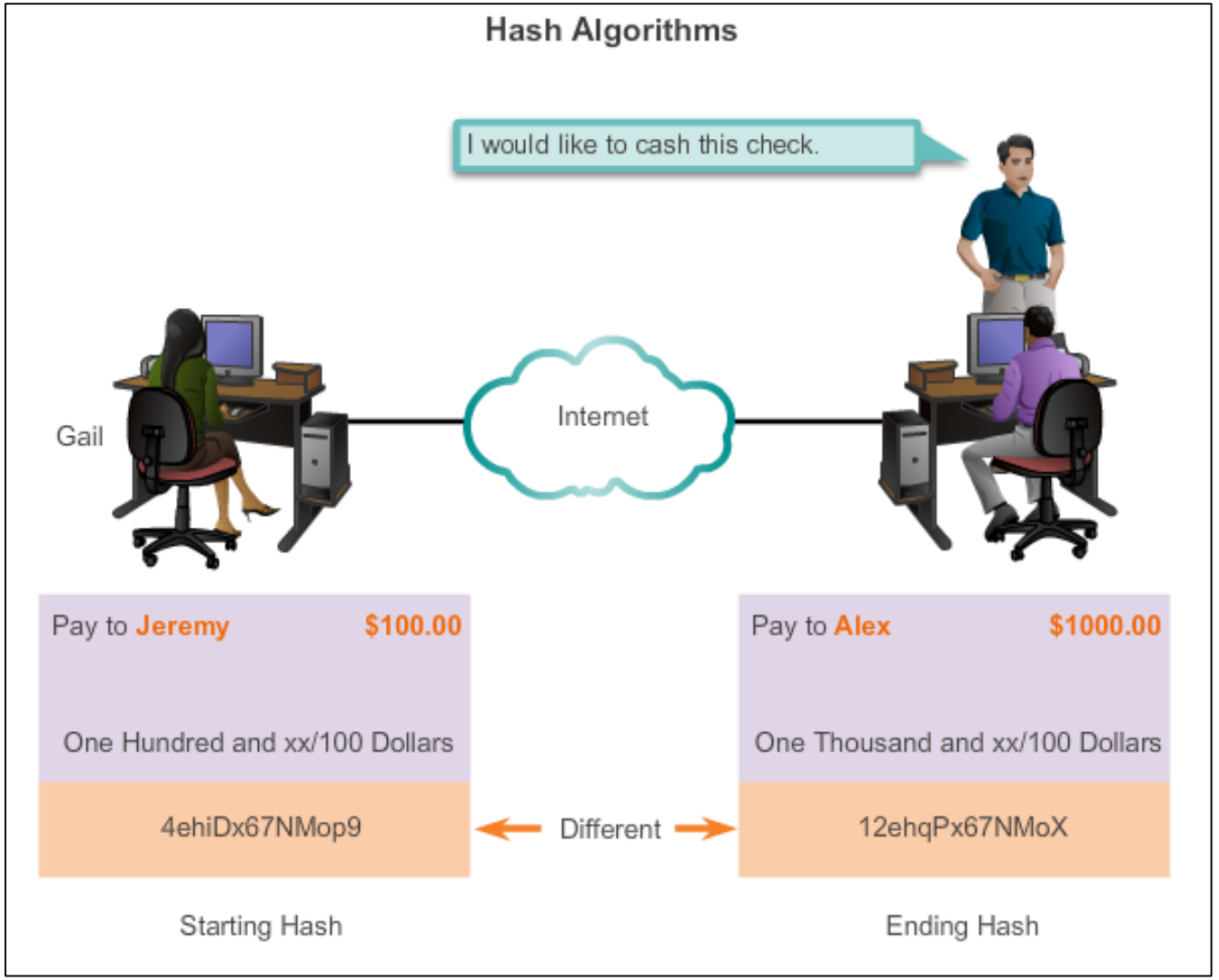




Integrity with Hash Algorithms

- The original sender generates a hash of the message and sends it with the message itself.
- The recipient parses the message and the hash, produces another hash from the received message, and **compares the two hashes**.
- If they are the same, the recipient can be reasonably sure of the integrity of the original message.

Integrity with Hash Algorithms (cont.)



Integrity with Hash Algorithms (cont.)

Hash-based Message Authentication Code (HMAC) is a mechanism for message authentication using hash functions.

- HMAC has two parameters:
  - A **message input** and a **secret key** known only to the message originator and intended receivers.
- Message sender uses an HMAC function to produce a value (the message authentication code) formed by condensing the secret key and the message input.
- Message authentication code is sent along with the message.
- Receiver computes the message authentication code on the received message using the same key and HMAC function as the sender used.
- Receiver compares the result that is computed with the received message authentication code.
- If the two values match, the message has been correctly received and the receiver is assured that the sender is a user community member who share the key.

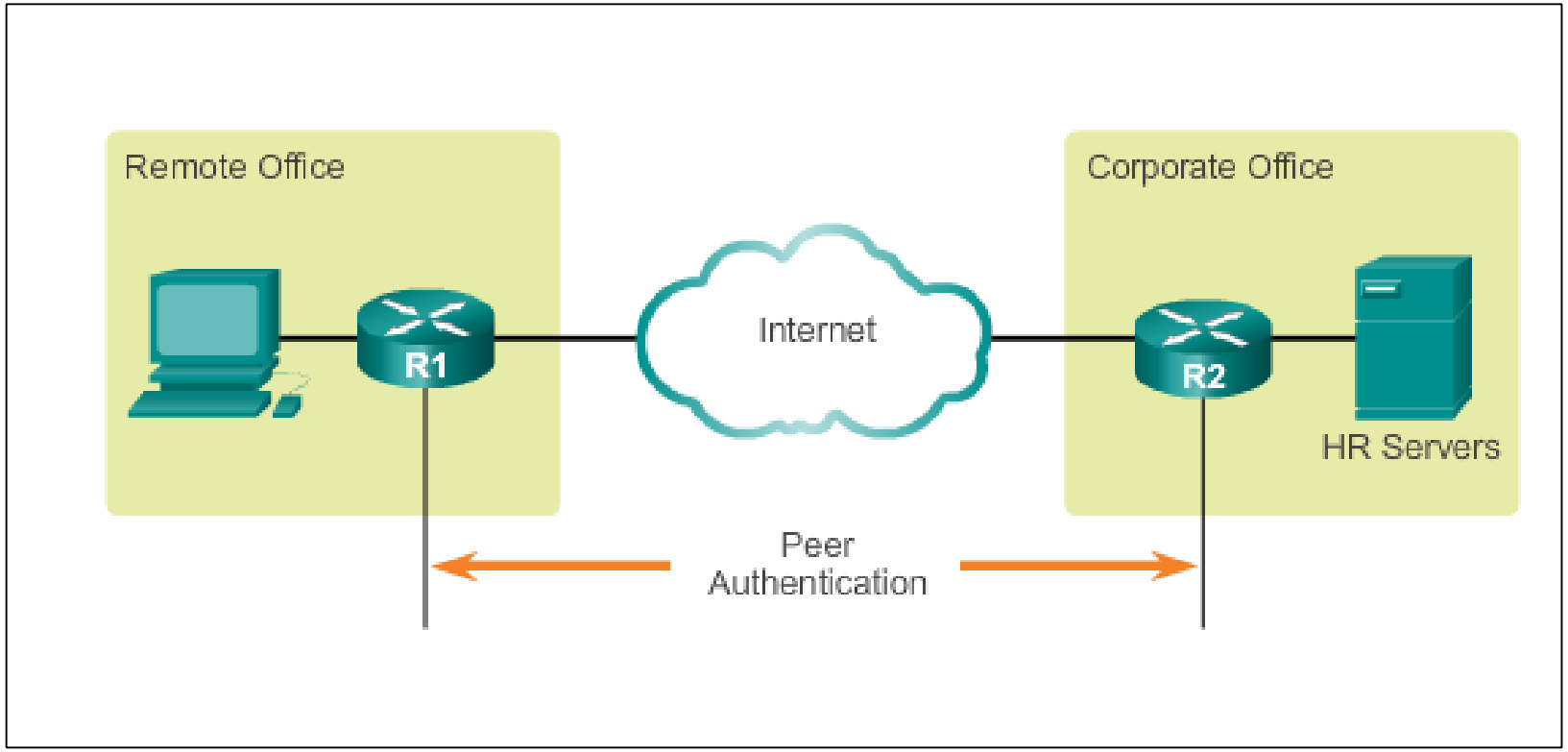
Integrity with Hash Algorithms (cont.)

There are two common HMAC algorithms:

- **MD5** – Uses a 128-bit shared secret key. The variable-length message and 128-bit shared secret key are combined and run through the HMAC-MD5 hash algorithm. The output is a 128-bit hash. The hash is appended to the original message and forwarded to the remote end.
- **SHA** – SHA-1 uses a 160-bit secret key. The variable-length message and the 160-bit shared secret key are combined and run through the HMAC-SHA1 hash algorithm. The output is a 160-bit hash. The hash is appended to the original message and forwarded to the remote end.

IPsec Authentication

- IPsec VPNs support authentication.
- Device on the other end of the VPN tunnel must be authenticated before the communication path is considered secure.



IPsec Authentication (cont.)

There are two peer authentication methods, PSK and RSA signatures:

- **PSK** (Pre Shared Key)
  - A secret key shared between the two parties using a secure channel before it needs to be used.
  - Use symmetric key cryptographic algorithms.
  - A PSK is entered into each peer manually and is used to authenticate the peer.

IPsec Authentication (cont.)

- **RSA (**Rivest, Shamir, Adleman**) signatures**
  - Digital certificates are exchanged to authenticate peers.
  - Local device derives a hash and encrypts it with **its private key**.
  - Encrypted hash, or digital signature, is attached to the message and forwarded to the remote end.
  - At the remote end, the encrypted hash is decrypted using the public key of the local end.
  - If the decrypted hash matches the recomputed hash, the signature is genuine.

IPsec Protocol Framework

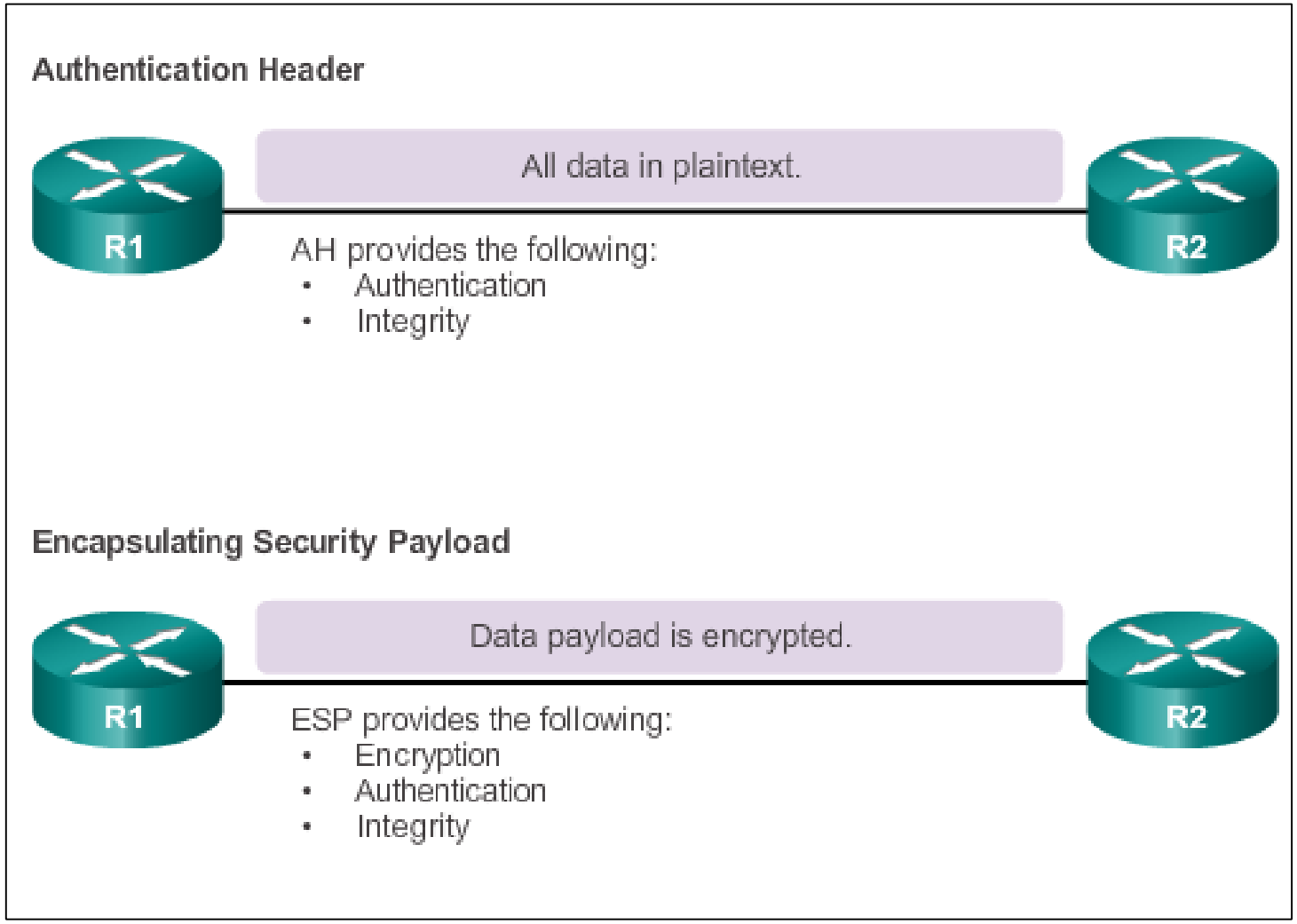
Authentication Header (AH)

- Appropriate protocol to use when confidentiality is not required or permitted.
- Provides data authentication and integrity for IP packets that are passed between two systems.
- Does not provide data confidentiality (encryption) of packets.

Encapsulating Security Payload (ESP)

- A security protocol that provides confidentiality and authentication by encrypting the IP packet.
- Authenticates the inner IP packet and ESP header.
- Both encryption and authentication are optional in ESP, at a minimum, one of them must be selected.

IPsec Protocol Framework (cont.)

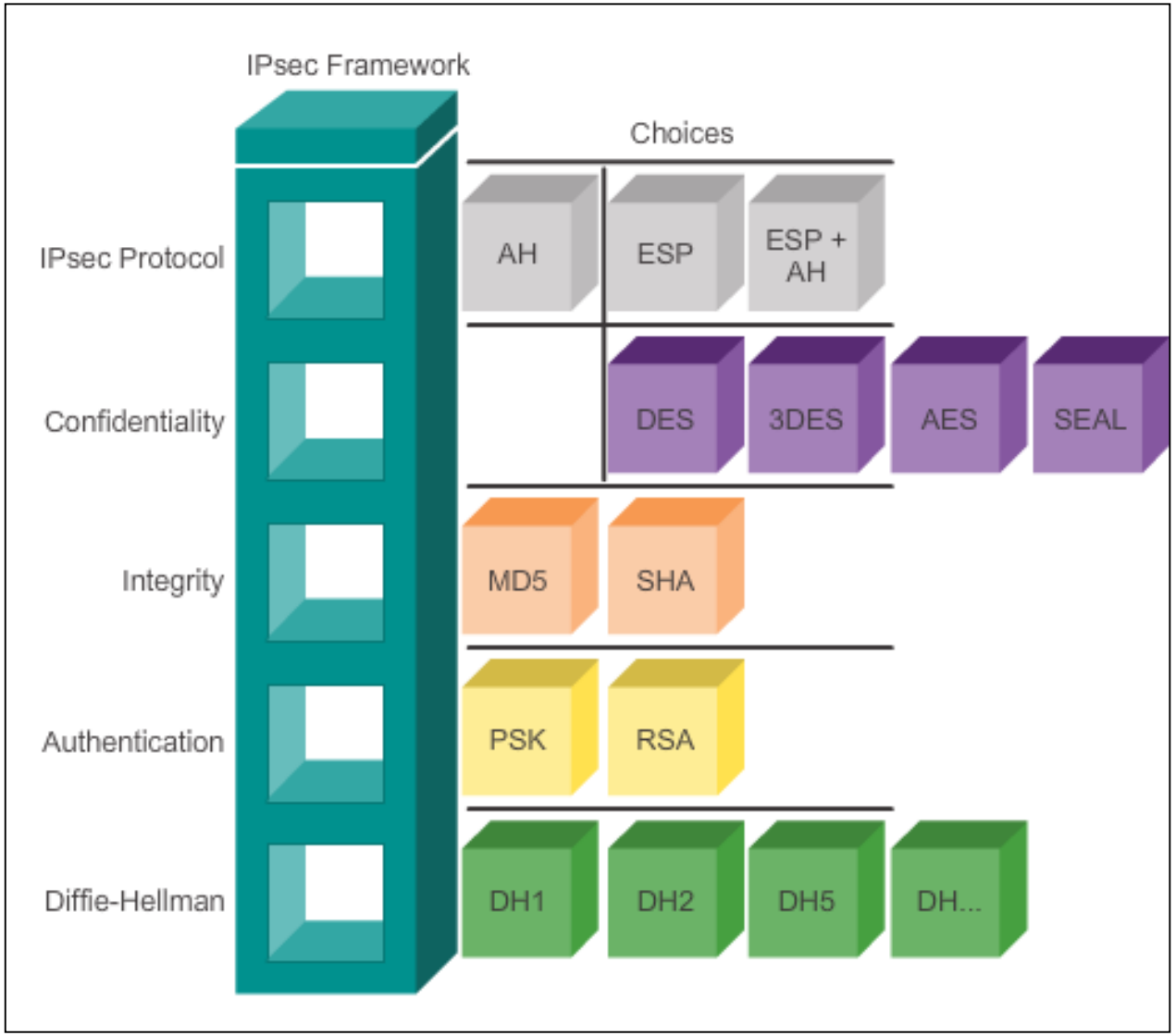


IPsec Protocol Framework (cont.)

Four basic building block of the IPsec framework that must be selected:

- **IPsec framework protocol** – A combination of ESP and AH, ESP or ESP+AH options are almost always selected because AH itself does not provide encryption.
- **Confidentiality** (if IPsec is implemented with ESP) – DES, 3DES, or AES, AES is strongly recommended since provides the greatest security.
- **Integrity** – Guarantees that the content has not been altered in transit using hash algorithms (MD5 or SHA).
- **Authentication** – Represents how devices on either end of the VPN tunnel are authenticated (PSK or RSA).
- **DH algorithm group** – Represents how a shared secret key is established between peers, DH24 provides the greatest security.

IPsec Protocol Framework (cont.)



Vytv

1. Host A sends interesting traffic to Host B.

2. Routers A and B negotiate an IKE Phase 1 session.

3. Routers A and B negotiate an IKE Phase 2 session.

4. Information is exchanged via the IPsec tunnel.

5. The IPsec tunnel is terminated.

Vytvorenie spojenia: IKE fáza 1 (IKE SA)

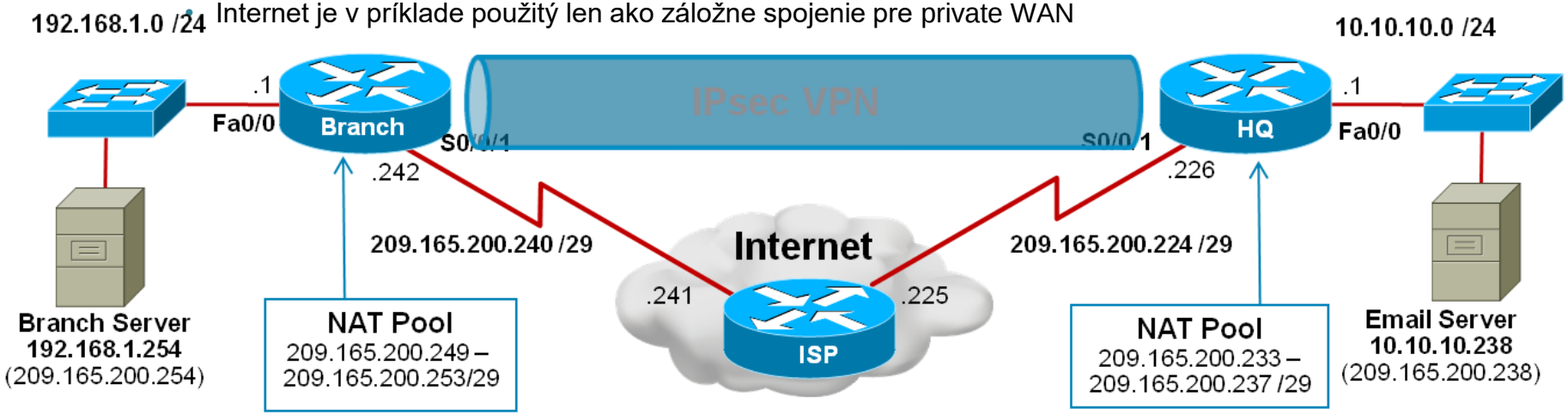
- IKE fáza 1 má tri kroky:
  - Dohodnutie ISAKMP politík
  - Výmenu šifrov./hash kľúčov pomocou Diffie-Hellmanovho algoritmu
  - Overenie **totožnosti susedov**
- Dohodnutie ISAKMP politík
  - Aký šifrovací algoritmus? (confident.)
  - Aký hashovací algoritmus? (integr.)
  - Aká Diffie-Hellmanova grupa?
  - Aký spôsob overenia totožnosti? (auth.)
- Overenie totožnosti
  - Podľa spôsobu dohodnutého v prvom kroku
- IKE fáza 1 si vytvára zabezpečený kanál pre overenie totožnosti IPsec susedov a prípadne používateľov
  - Nedohaduje samotné vlastnosti pre činnosť IPsec
  - Tie sa dohodnú až vo fáze 2 pomocou tohto zabezpečeného kanála

Vytvorenie spojenia: IKE fáza 2

- IKE fáza 2 zodpovedá za dojednanie spôsobu použitia IPsec medzi susedmi
  - Aký protokol – AH, ESP, AH+ESP?
  - Aký režim – tunelový alebo transportný?
  - Aký šifrovací algoritmus?
  - Aký hashovací mechanizmus?
  - Aké šifrovacie kľúče?
  - Aká životnosť dohodnutých informácií?
- Prvé štyri vlastnosti sa nazývajú aj *transformačná sada*

Kroky pri konfigurácii IPsec

- Postup pri konfigurácii IPsec
  - Vytvoriť aspoň jednu ISAKMP politiku pre fázu 1
  - Vytvoriť aspoň jednu transformačnú sadu pre fázu 2
  - Vytvoriť kryptovaciu mapu a ACL, ktoré popisujú, čo sa má zabezpečiť pomocou IPsec a ako
  - Aplikovať kryptovaciu mapu na výstupné rozhranie
- Poznámka:
  - Internet je v príklade použitý len ako záložne spojenie pre private WAN



Kompletná konfigurácia Branch Router IPsec VPN

```
Branch# conf t
Branch(config)# crypto isakmp policy 1
Branch(config-isakmp)# encryption aes
Branch(config-isakmp)# authentication pre-share
Branch(config-isakmp)# group 2
Branch(config-isakmp)# exit
Branch(config)# crypto isakmp key cisco123 address 209.165.200.226
Branch(config)#
Branch(config)# crypto ipsec transform-set MOJA_TR_SADA esp-sha-hmac esp-3des
Branch(cfg-crypto-trans)# exit
Branch(config)#
Branch(config)# access-list 110 permit ip 192.168.1.0 0.0.0.255 10.10.10.0 0.0.0.255
Branch(config)#
Branch(config)#
Branch(config)# crypto map MOJA_MAPA 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
Branch(config-crypto-map)# set transform-set MOJA_TR_SADA
Branch(config-crypto-map)# set peer 209.165.200.226
Branch(config-crypto-map)# match address 110
Branch(config-crypto-map)# exit
Branch(config)# int s0/0/1
Branch(config-if)# crypto map MOJA_MAPA
Branch(config-if)# ^Z
Branch#
```

❶ **ISAKMP Policy**
Specifies the initial VPN security details

❷ **IPsec Details**
Specifies how the IPsec packet will be encapsulated

❸ **Crypto ACL**
Specifies the traffic that will trigger the VPN to activate

❹ **VPN Tunnel Information**
Creates the crypto map that combines the ISAKMP policy, IPsec transform set, VPN peer address, and crypto ACL

❺ **Apply the Crypto Map**
Identifies which interface is actively looking to create a VPN

IPsec: Záverečné poznámky

- Pre NAT-T musia byť na firewalloch otvorené porty
  - UDP/500
  - UDP/4500
- Vzhľadom na pomerne vysokú technickú náročnosť IPsec sa pre mobilných klientov odporúča nová technológia SSLVPN, ktorá má nižšie technické nároky

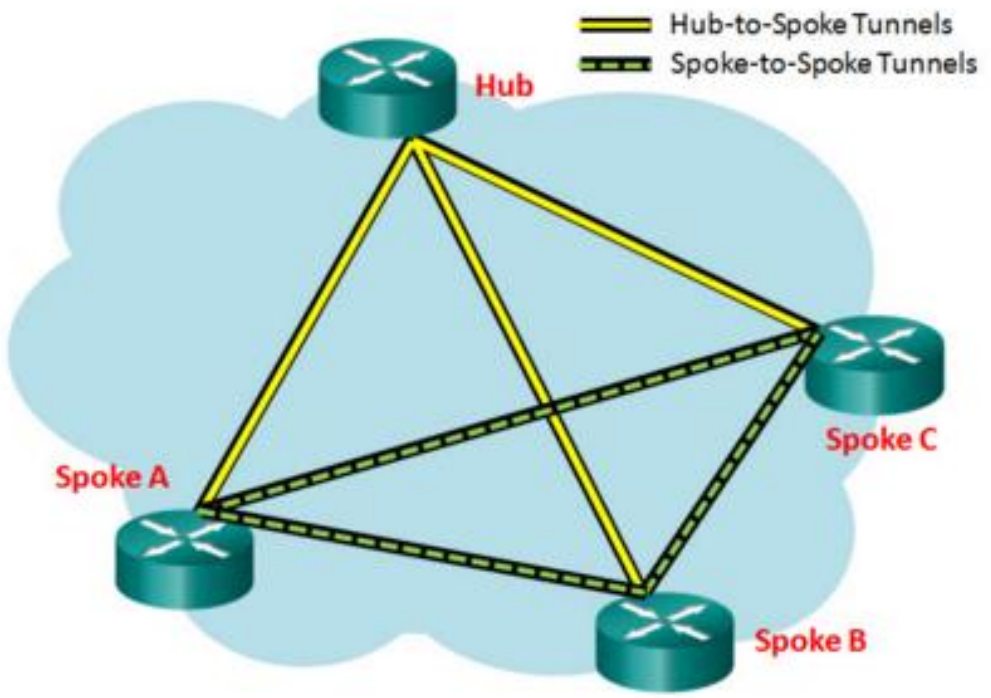
MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY

Dynamic Multipoint VPN (DMVPN)

MarMarc Khayat, CCIE #41288
Technical Manager, Cisco Networking Academy
ch 2016

Why DMVPN?

- To have efficient spoke-to-spoke communication in a hub-and-spoke topology.
- Dynamic tunneling
  - No more static configuration of separated p-t-p tunnels is required
  - Spoke-spoke
  - Hub-spoke

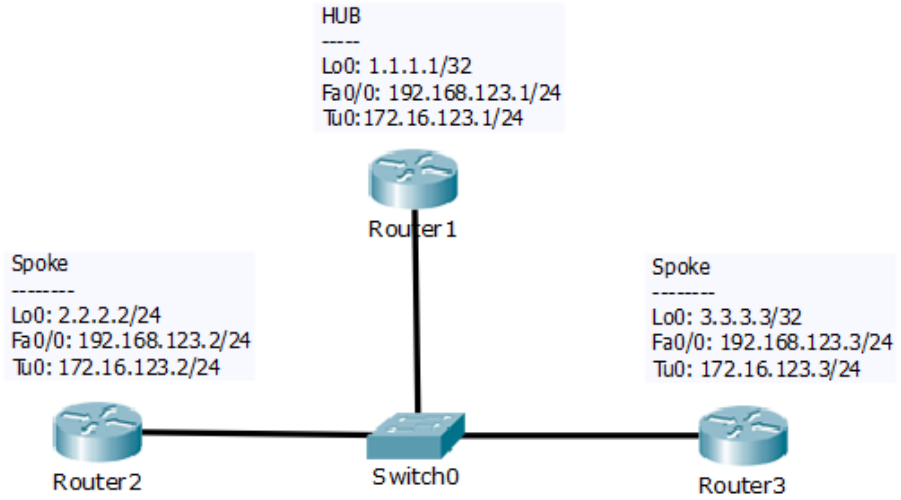


How are these tunnels built?

- Next Hop Resolution Protocol (NHRP)
- Multipoint Generic Routing Encapsulation (mGRE) tunnels
- IP Security (IPsec) encryption

Config Tasks

1. NHRP: set the hub as the server, allow multicast to flow to it.
2. mGRE tunnel config.
3. Enable IPSec encryption on the tunnels.



Príklad konfigurácie Hub and Spoke

```
!  Spoke config
crypto isakmp policy 1
 encr aes
 hash md5
 authentication pre-share
 group 2
crypto isakmp key MYKEY address 0.0.0.0
!
crypto ipsec transform-set MYSET esp-aes esp-md5-hmac
!
crypto ipsec profile MGRE
 set security-association lifetime seconds 86400
 set transform-set MYSET
!
interface Tunnel0
 ip address 172.16.123.1 255.255.255.0
 no ip split-horizon eigrp 10
 ip nhrp authentication CISCO
 ip nhrp map multicast dynamic
! Identifiy DMVPN net
! Have to be same on hub and spookes
 ip nhrp network-id 1
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile MGRE
! No explicit tunnel destination required
!
router eigrp 10
 network 1.0.0.0
 network 172.16.0.0
```

```
! Hub konfig
crypto isakmp policy 1
 encr aes
 hash md5
 authentication pre-share
 group 2
crypto isakmp key MYKEY address 0.0.0.0
!
crypto ipsec transform-set MYSET esp-aes esp-md5-hmac
!
crypto ipsec profile MGRE
 set security-association lifetime seconds 86400
 set transform-set MYSET
!
interface Tunnel0
 ip address 172.16.123.2 255.255.255.0
 ip nhrp authentication CISCO
 ip nhrp map multicast dynamic
! the HUB tunnel address
 ip nhrp nhs 172.16.123.1

! Map tunnel address of Hub to its real and globally
! reachable IP address
 ip nhrp map 172.16.123.1 192.168.123.1
 ip nhrp map multicast 192.168.123.1
 ip nhrp network-id 1
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile MGRE
!
router eigrp 10
 network 2.0.0.0
 network 172.16.0.0
```

Verification

```
Show dmvpn
! Not from the topology above
! Just an example

R1# show dmvpn
...

Tunnel0, Type:Hub, NHRP Peers:3,
 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
 1     172.16.25.2     192.168.0.2    UP 00:02:28 D
 1     172.16.35.2     192.168.0.3    UP 00:02:26 D
 1     172.16.45.2     192.168.0.4    UP 00:02:25 D
```