

MDS®

INFORMATIČKI INŽENJERING

B · E · O · G · R · A · D

Primena DMVPN tehnologije u zaštiti komunikacije kroz javnu MPLS VPN mrežu

Marko Tanasković – MDS Informatički inženjering

mtanaskovic@mds.rs

www.mds.rs

- **MDS Informatički Inženjering**
- **Uvod**
- **MPLS tehnologija**
- **DMVPN tehnologija**
- **Primena DMVPN tehnologije u tipičnoj korporativnoj mreži**

- **Kompanija je osnovana 1970 godine kao kompanija za informacione tehnologije**
- **Prvi Cisco uređaj je prodat 1993. godine**
- **Cisco Premier Partner od 1997. godine**
- **Cisco Silver Partner od 2006. godine**
- **Cisco Gold Partner od 2008. godine**

- **Tipovi VPN tehnologija**
 - **Secure VPN** (IPsec, L2TP preko IPsec-a, SSL enkripcija)
 - **Trusted VPN** (Layer 2 VPN, Layer 3 VPN)
 - **Hybrid VPN** (kombinacija prethodna dva tipa VPN-a)

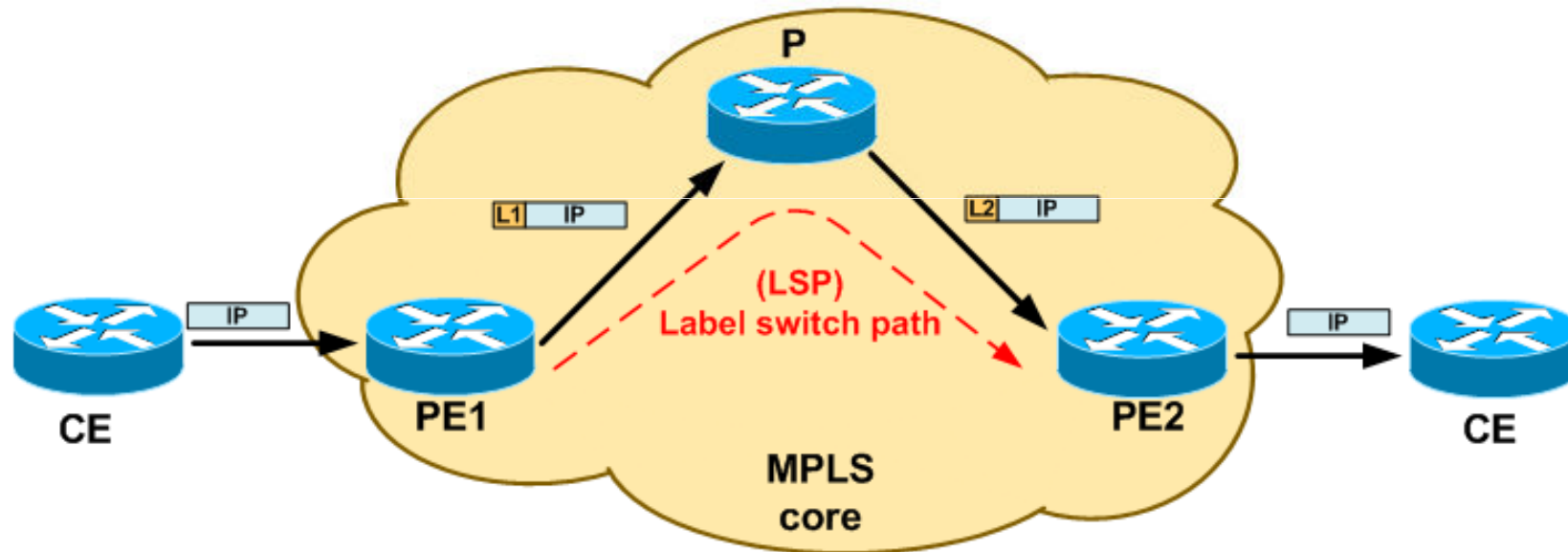
- MDS Informatički Inženjering
- Uvod
- **MPLS tehnologija**
 - **MPLS L3VPN**
 - **MPLS topologija**
- DMVPN tehnologija
- Primena DMVPN tehnologije u tipičnoj korporativnoj mreži

MPLS - L3 VPN



- **MPLS tehnologija kombinuje prednosti prosleđivanja paketa na OSI nivou 2 sa prednostima koje pruža rutiranje na OSI nivou 3.**
- **L3VPN tehnologija koristi MP-BGP i VRF instance u cilju kreiranja virtuelne privatne mreže nad IP/MPLS mrežom.**
- **L3VPN obezbeđuje servis provajderima mogućnost da implementiraju usluge QoS, Traffic Engineering, kao i brzo prerutiranje u slučaju otkaza mreže.**
- **L3VPN omogućava povezivanje svake dve krajnje tačke u mreži korisnika.**

MPLS - Topologija mreže



CE – (*Customer Edge*) ruter, povezuje opermu na strani korisnika sa PE (*Provider Edge*) ruterom. CE ruter je, logički gledano, deo korisničke mreže.

P – (*Provider*) ruter, se ne povezuje direktno na korisničku opremu.

- MDS Informatički Inženjering
- Uvod
- MPLS tehnologija
- **DMVPN tehnologija**
 - **Prednosti DMVPN tehnologije**
 - **Komponente koje čine DMVPN rešenje**
 - **Topologije DMVPN rešenja**
 - **Redundansa u DMVPN mrežama**
- **Primena DMVPN tehnologije u tipičnoj korporativnoj mreži**

Dynamic Multipoint VPN (DMVPN)



- **Zaštita podataka korišćenjem VPN tehnologija se pokazala kao bezbedan i siguran način komunikacije**
 - **Tradicionalne implementacije IPsec VPN mreža su tipa *hub-and-spoke point-to-point*.**
 - **Loša skalabilnost.**
 - **Loše iskorišćenje zakupljnog propusnog opsega.**
 - **Podrška samo za *unicast* saobraćaj.**
 - **Obimna konfiguracija i komplikovano održavanje.**
 - **DMVPN tehnologija je razvijena u cilju realizacije IPsec VPN WAN mreža velikih razmera.**

DMVPN – prednosti



- **Dinamičko podizanje hub-to-spoke i spoke-to-spoke IPsec tunela.**
- **Optimizovano funkcionisanje mreže.**
- **Smanjena latencija za aplikacije u realnom vremenu.**
- **Smanjena veličina konfiguracije centralnih rutera.**
- **Automatizovano dodavanje novih krajnjih tačaka mreže.**
- **Podrška za dinamičke ruting protokole u okviru DMVPN tunela.**
- **Podrška za *multicast* saobraćaj između centralne i udaljenih lokacija.**
- **Podrška za dinamičko adresiranje udaljenih rutera.**
- **Podrška za kvalitet servisa (QoS).**

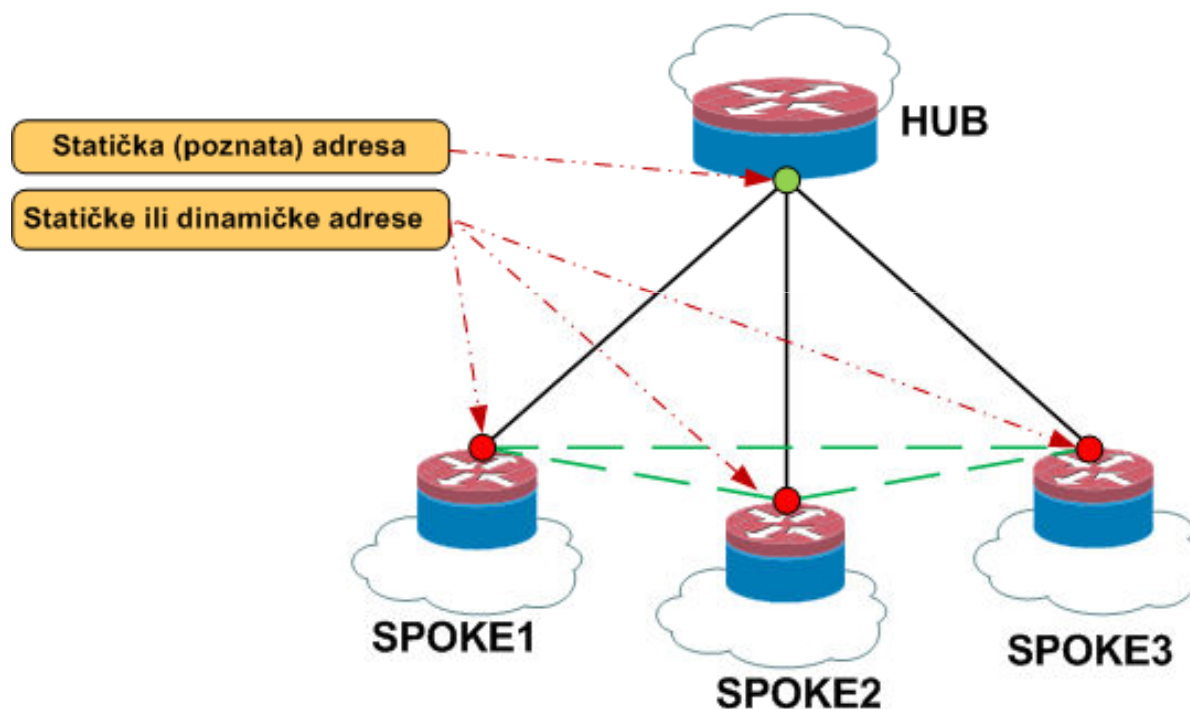
DMVPN – poređenje



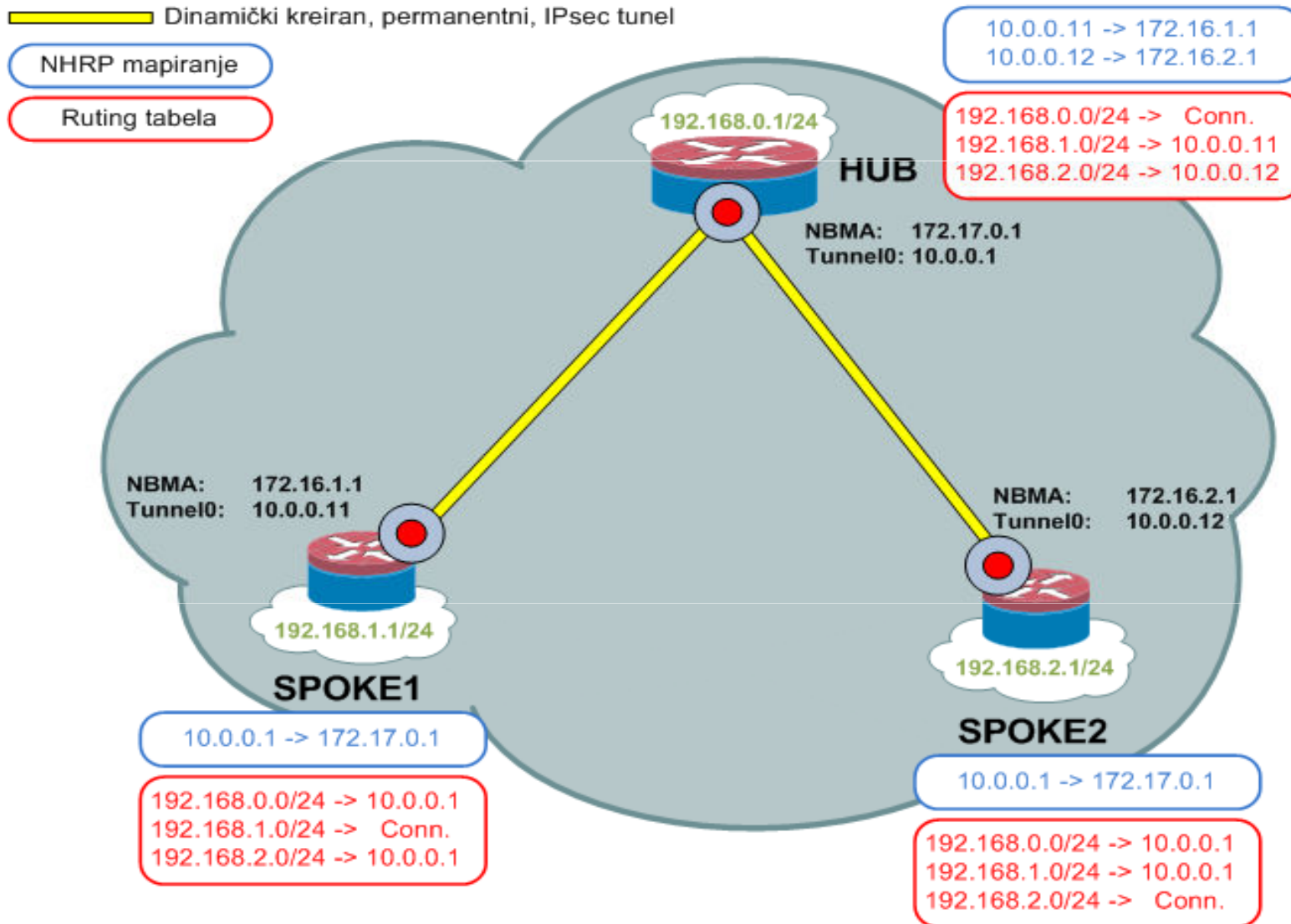
Pre DMVPN-a : p-pGRE + IPsec	Sa DMVPN-om : mGRE + IPsec
Jedan GRE interfejs za svaku udaljenu lokaciju	Jedan mGRE interfejs podržava SVE udaljene lokacije
Svi tuneli moraju biti unapred konfigurisani	Višestruki mGRE interfejsi mogu da postoje: svaki predstavlja odvojenu DMVPN mrežu
Koristi se statička adresa destinacije tunela	Dinamičko utvrđivanje adrese destinacije tunela
Udaljene lokacije moraju imati statičko adresiranje	NHRP registracija i dinamički ruting protokoli ukidaju ovo ograničenje
Podržava dinamičke ruting protokole	Podržava dinamičke ruting protokole
<i>Ogromna konfiguracija centralnog (hub) rutera</i> 1 tunel interfejs/u. lokaciji za 250 u.l. = 250 interfejsa 7 linija/u.lokaciji za 250 u.l = 1750 linija konfiguracije 4 IP adrese/u.lokaciji za 250 u.l = 1000 adresa	<i>Smanjena konfiguracija centralnog (hub) rutera</i> 1 tunel interfejs za sve udaljene u. lokacije Konfiguracija , uključujući NHRP za 250 u.l. je veličine 15 linija Sve udaljene lokacije su u istom opsegu adresa. 250 u.l. Zahteva 250 IP adresa
Dodavanje krajnjih tačaka zahteva intervenciju na centralnom ruteru	Nikakva intervencija nije potrebna
Saobraćaj između udaljenih lokacija prolazi kroz centralni ruter	Potpuno konfigurabilno, u zavisnosti od izabrane arhitekture

DMVPN – komponente

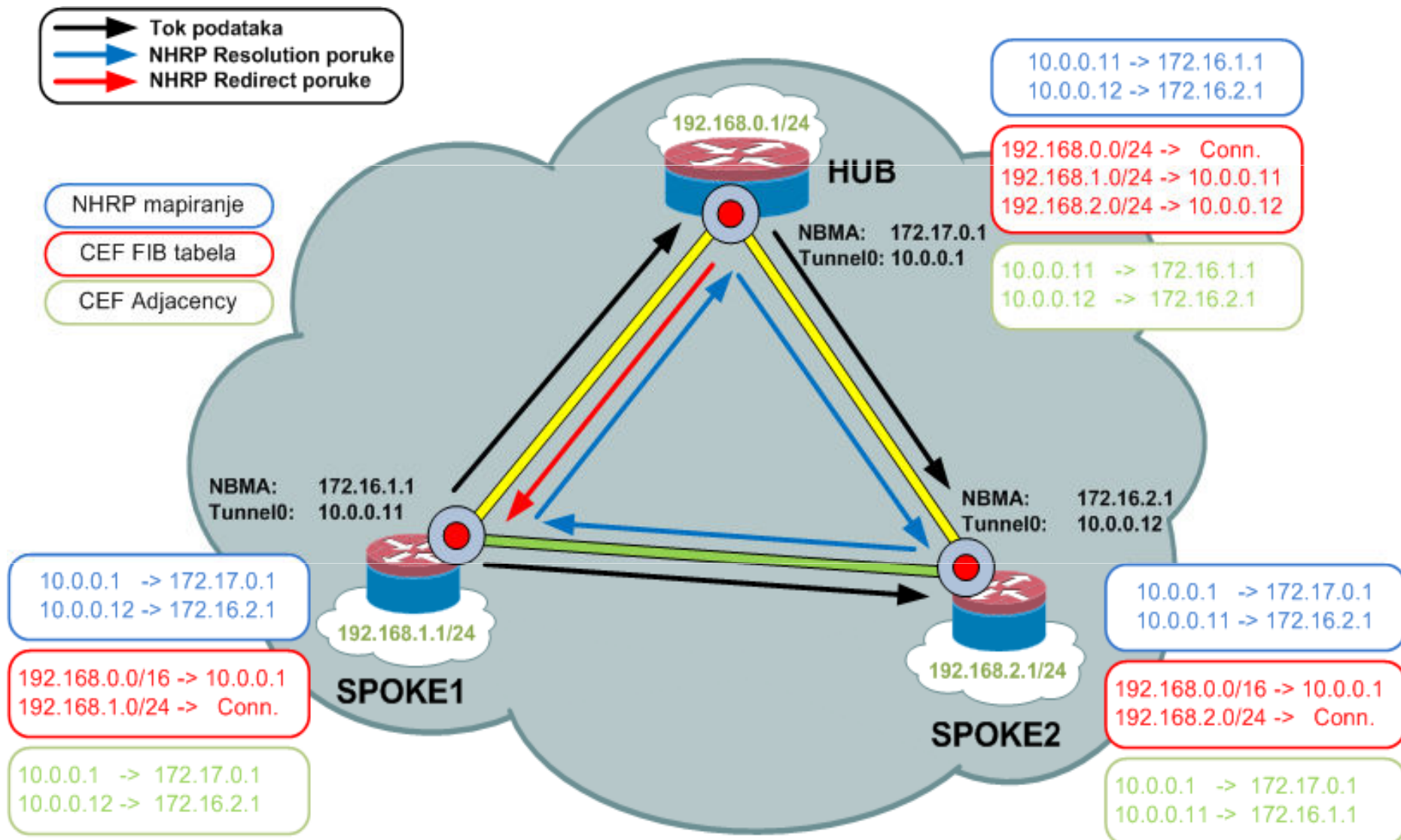
- DMVPN tehnologija se oslanja na nekoliko standardnih protokola:
 - GRE (Generic Routing Encapsulation) protokol
 - NHRP (Next Hop Resolution Protocol) protokol
 - Dinamički rutinški protokol (EIGRP, OSPF, RIPv2, BGP)
 - IPsec skup protokola za enkripciju



DMVPN – NHRP

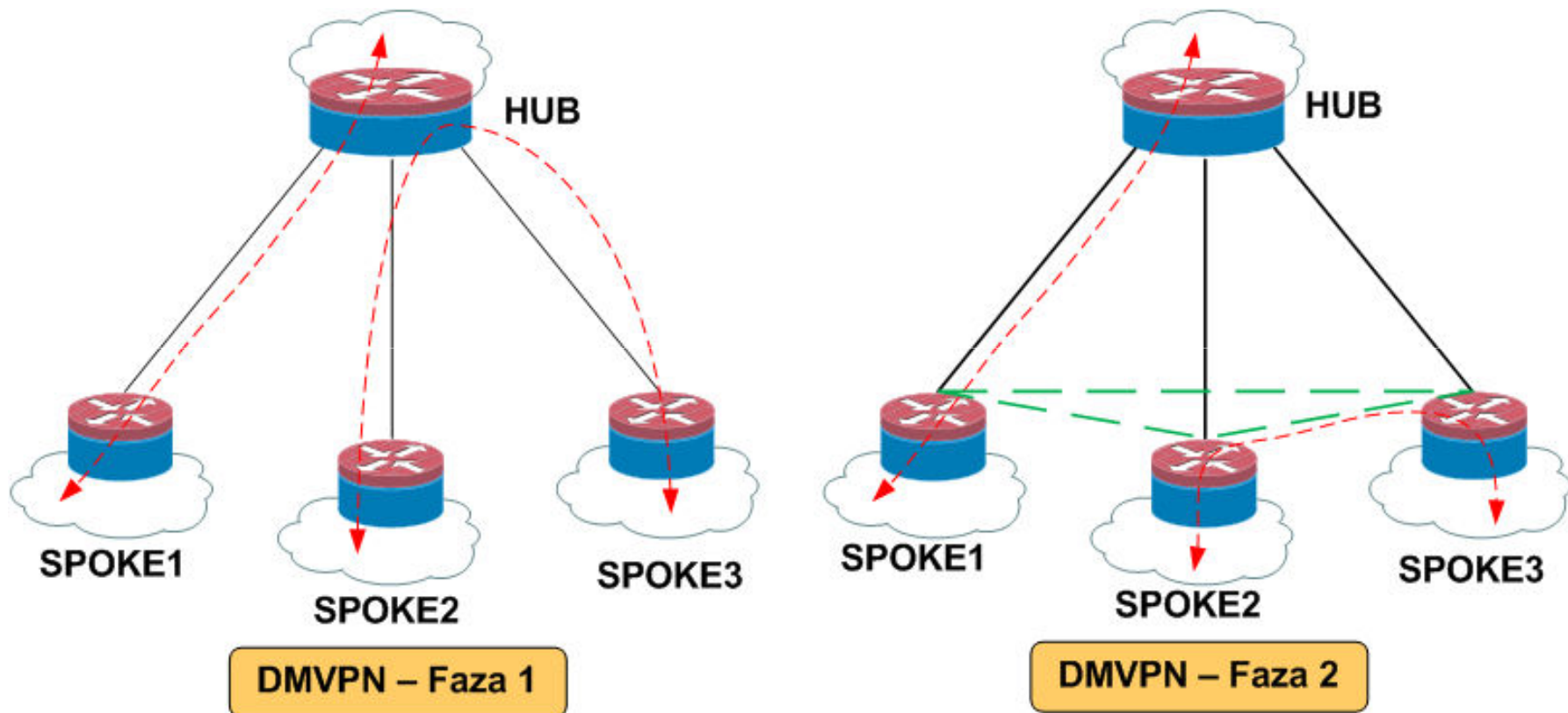


DMVPN – NHRP (nastavak)



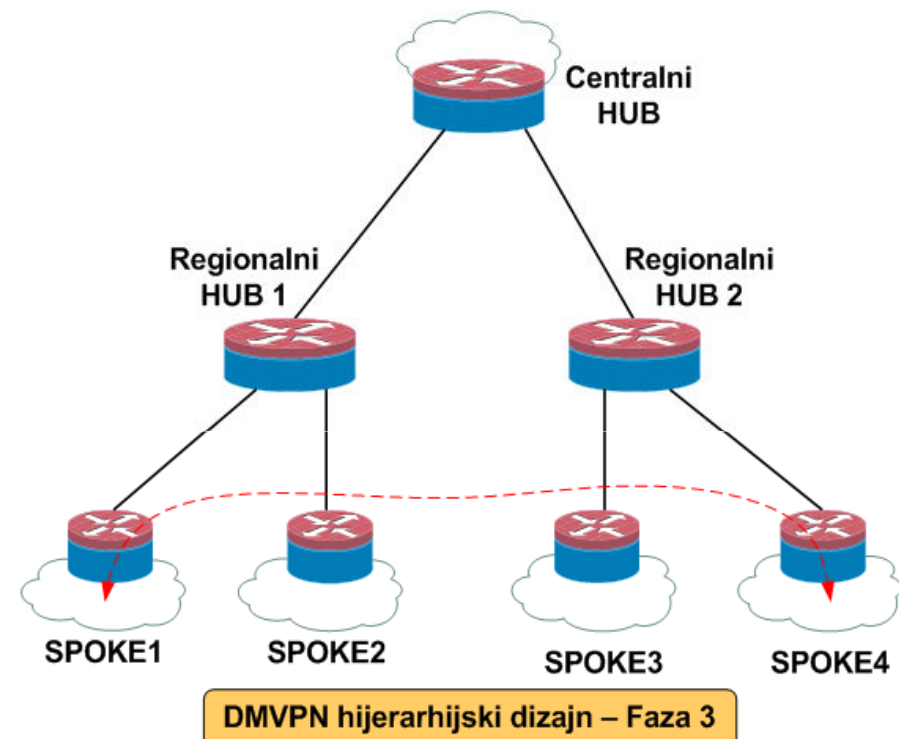
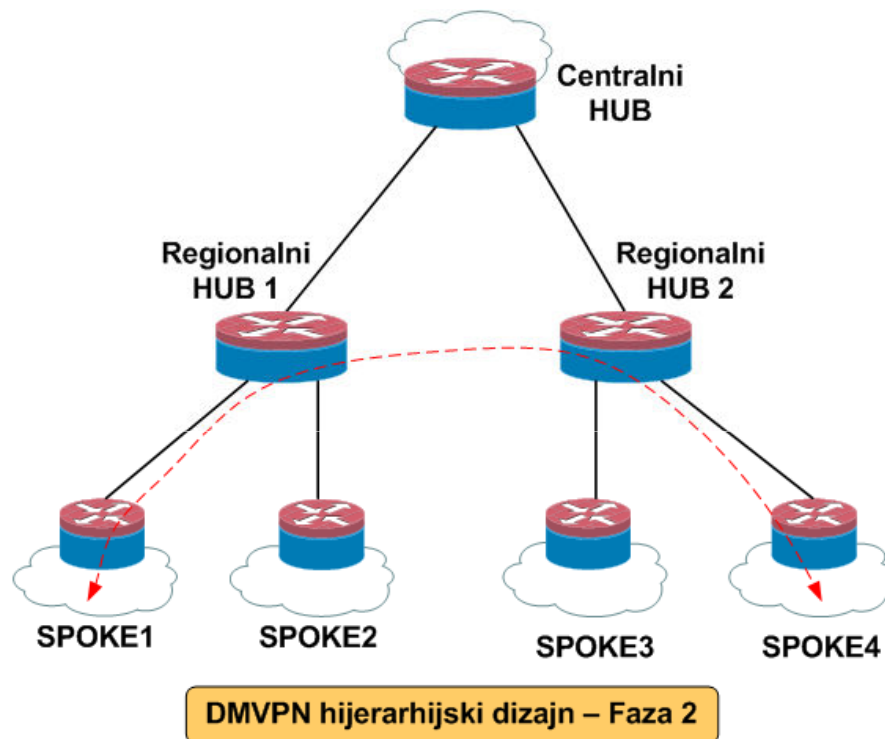
DMVPN – Topologije

- DMVPN se može implementirati po fazama, zavisno od zahtevanih topologija.
- Trenutno postoje Faze 1, 2 i 3



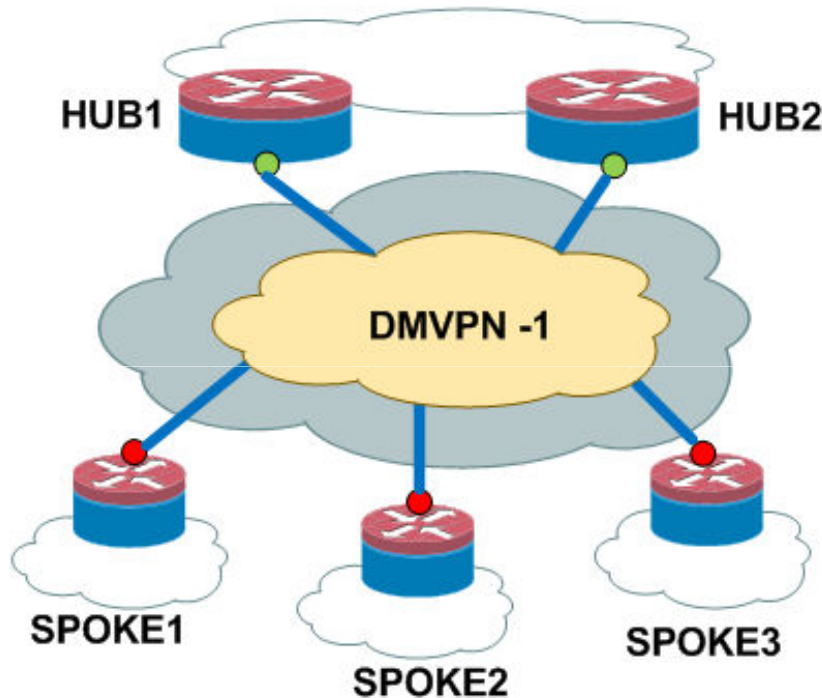
DMVPN – Topologije (nastavak)

- U DMVPN Fazi 3 se formiraju hijerarhijske topologije pri čemu je omogućena direktna komunikacija između krajnjih rutera u različitim regionima.

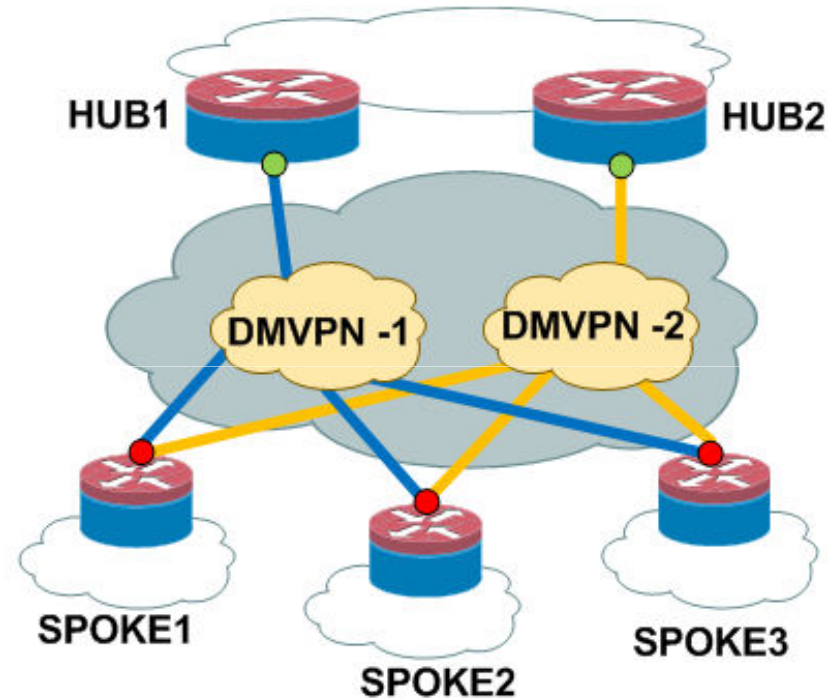


DMVPN – Redundansa

- Pri dizajniranju redundantne DMVPN topologije, mogu se primeniti dva dizajna:
 - Jedinstavna DMVPN mreža sa dva centralna rutera.
 - Dvostruka DMVPN mreža sa dva centralna rutera.



Dual HUB, single DMVPN cloud

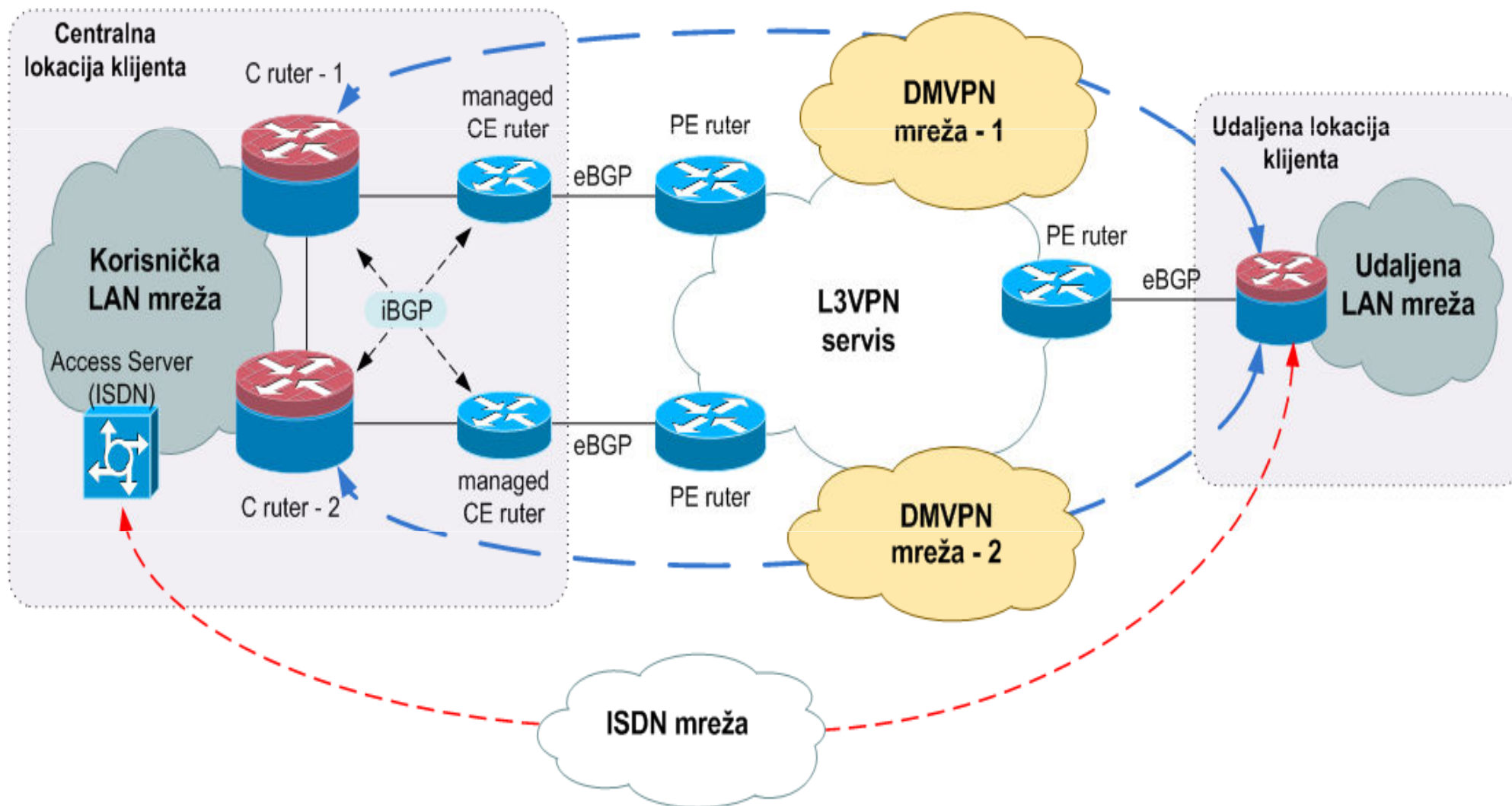


Dual HUB, dual DMVPN cloud

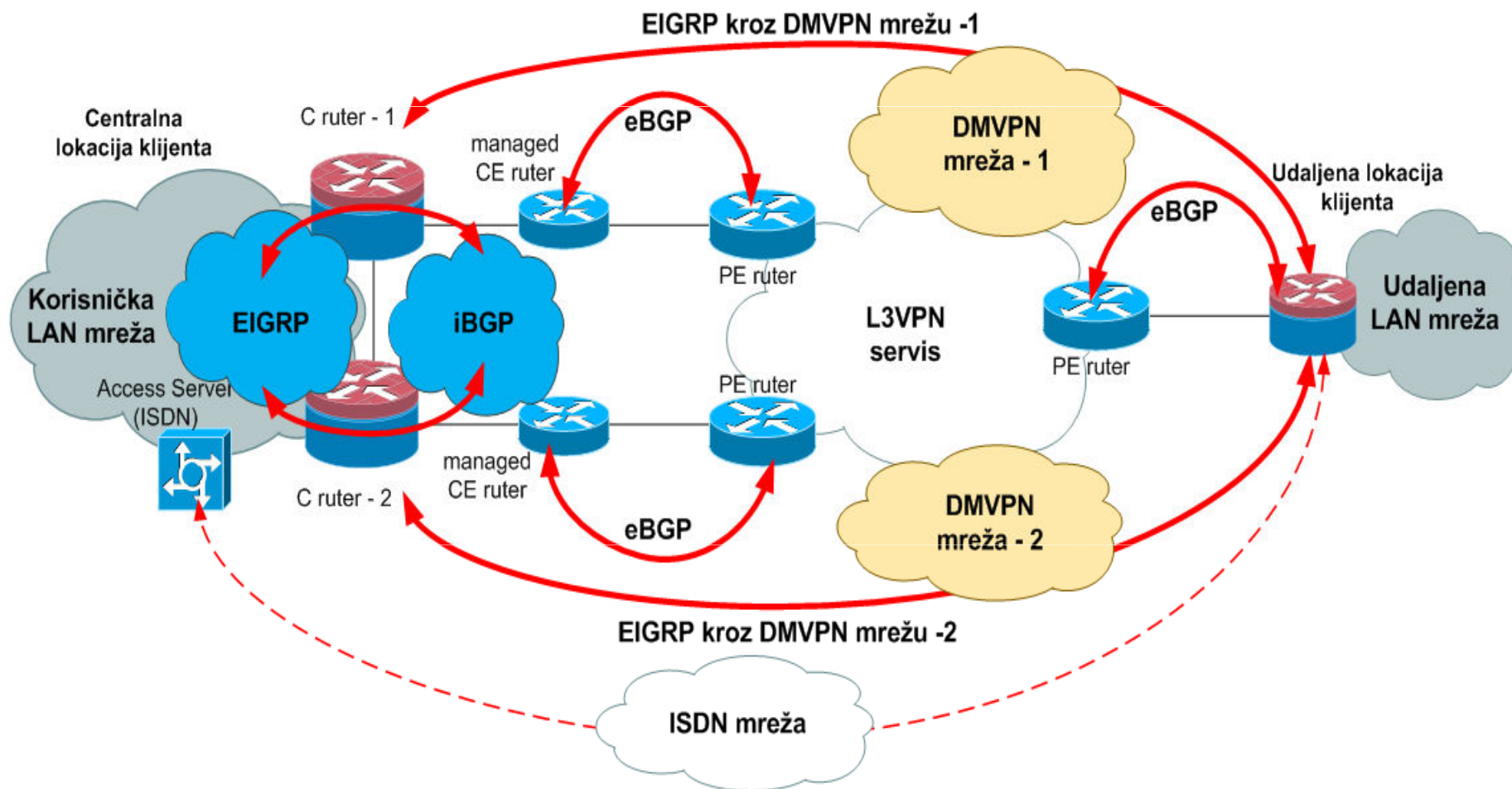
- MDS Informatički Inženjering
- Uvod
- MPLS tehnologija
- DMVPN tehnologija
- **Primena DMVPN tehnologije u tipičnoj korporativnoj mreži**
 - **Pregled rešenja**
 - **Pregled komponenti**
 - **Kvalitet servisa (QoS)**

- **Tipični korporativni zahtevi podrazumevaju:**
 - **Enkripciju podataka koji prolaze kroz L3VPN mrežu.**
 - **Otpornost mreže na ispade pojedinih komponenti u transportnoj mreži.**
 - **Prenos različitih tipova saobraćaja, sa različitim stepenom osetljivosti na kašnjenja i varijacije kašnjenja.**
 - **Topologiju sa direktnim povezivanjem svih udaljenih lokacija.**
 - **Dinamički ruting protokol.**
 - **Jednostavan mehanizam za prelazak sa postojećih WAN tehnologija na DMVPN.**

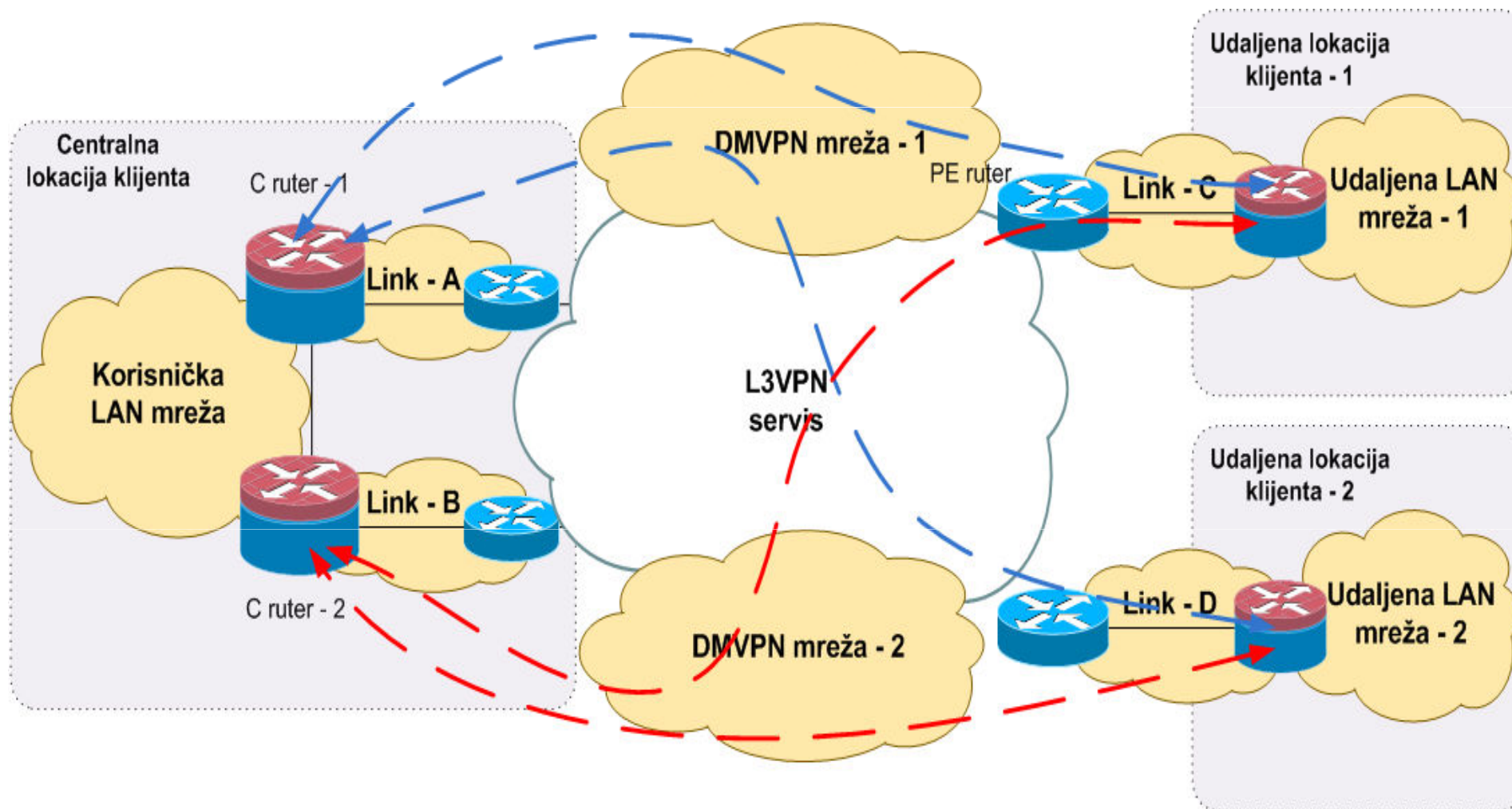
DMVPN – pregled rešenja



DMVPN – dinamički rutinski protokoli



DMVPN – Adresni plan



DMVPN – parametri mGRE interfejsa



- **Centralni (HUB) ruteri → po jedan mGRE interfejs**
- **Udaljeni (SPOKE) ruteri → po dva mGRE interfejsa**
- **Adresiranje početka i kraja tunela**
- **Autentifikacija → GRE tunnel key**

```
interface Tunnel0
! IP adresa u DMVPN 1 mreži
ip address < IP adresa iz DMVPN oblaka>
no ip redirects
ip mtu 1400
ip nhrp authentication PROBA
ip nhrp map multicast 10.19.123.6
ip nhrp map 10.19.126.1 10.19.123.6
ip nhrp network-id 12345
ip nhrp holdtime 300
ip nhrp nhs <NBMA adresa HUB ruteru >
ip route-cache flow
no ip split-horizon eigrp 111
delay 1000
qos pre-classify
tunnel source FastEthernet0/1
tunnel mode gre multipoint
tunnel key 54321
tunnel protection ipsec profile KriptoPRF shared
```

```
interface Tunnel111
description HUB-tunnel
ip address <IP adresa iz DMVPN oblaka>
no ip redirects
ip mtu 1400
ip nhrp authentication cisco
ip nhrp map multicast dynamic
ip nhrp network-id 12345
ip nhrp holdtime 600
ip tcp adjust-mss 1350
no ip split-horizon eigrp 111
delay 1000
qos pre-classify
tunnel source FastEthernet0/0
tunnel mode gre multipoint
tunnel key 54321
tunnel protection ipsec profile KriptoPRF
```

DMVPN – paramteri NHRP protokola



- **Postoje dva NHRP domena**
- **Centralni (HUB) ruteri → NHRP serveri**
- **Udaljeni (SPOKE) ruteri → NHRP klijenti**
- **Autentifikacija → NHRP network-id**

```
interface Tunnel0
! IP adresa u DMVPN 1 mreži
ip address <IP adresa iz DMVPN oblaka>
ip mtu 1400
ip nhrp authentication PROBA
ip nhrp map multicast < NBMA adresa >
ip nhrp map <IP adr Tunela-HUB> <NBMA adresa>
ip nhrp network-id 12345
ip nhrp holdtime 300
ip nhrp nhs < IP adr Tunela-HUB >
ip route-cache flow
no ip split-horizon eigrp 111
delay 1000
qos pre-classify
tunnel source FastEthernet0/1
tunnel mode gre multipoint
tunnel key 54321
tunnel protection ipsec profile KriptoPRF shared
```

```
interface Tunnel111
description HUB-tunnel
ip address <IP adresa iz DMVPN oblaka>
no ip redirects
ip mtu 1400
ip nhrp authentication PROBA
ip nhrp map multicast dynamic
ip nhrp network-id 12345
ip nhrp holdtime 600
ip tcp adjust-mss 1350
no ip split-horizon eigrp 111
delay 1000
qos pre-classify
tunnel source FastEthernet0/0
tunnel mode gre multipoint
tunnel key 54321
tunnel protection ipsec profile KriptoPRF
```

DMVPN – IPsec protokoli



- Definicija ISAKMP polisa
- Definicija kripto – profila
- Primena profila na tunel interfejsu

```
crypto isakmp policy 1
authentication pre-share
group 2
crypto isakmp key *** address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 10
```

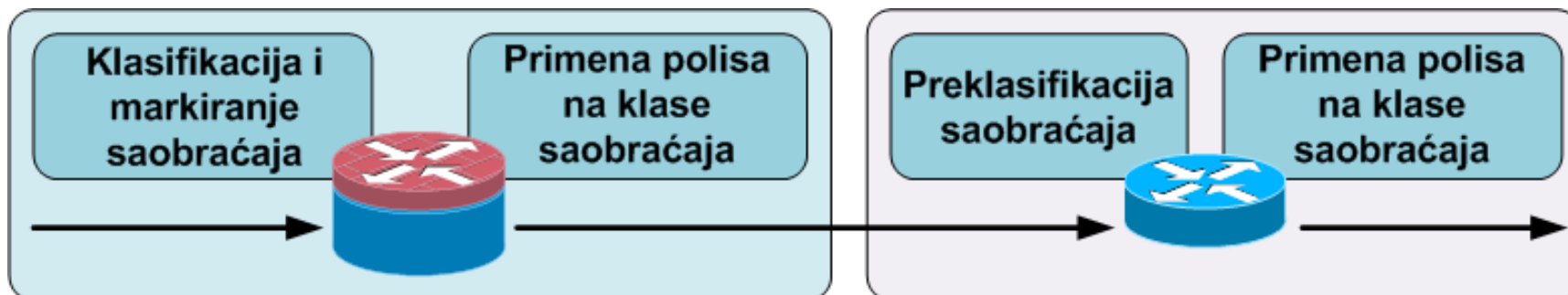
```
crypto ipsec transform-set <set-name> <enc.parameters>
```

```
crypto ipsec profile <profile-name>
set transform-set <transform-name>
```

```
interface tunnel<number>
...
tunnel protection ipsec profile <profile-name>
```

DMVPN – QoS

- U korporativnim mrežama je veoma bitno obezbediti konzistentnu QoS politiku sa kraja na kraj mreže.
- Problem sa transportom kroz mrežu servis provajdera.
- Problem sa definisanjem QoS politika u okruženju gde postoji potpuna konektivnost između udaljenih lokacija.
- Primena QoS polisa na centralnoj i na udaljenim lokacijama.



DMVPN – QoS (nastavak)



Klasa saobraćaja	Garancija za link 1 Mbps	Garancija za link 2 Mbps	Garancija za link 50 Mbps	Raspodela preostalog opsega
Upravljanje mrežom	-	-	-	9%
Prenos glasa	256 Kbps	1024 Kbps	11520 Kbps	-
Kontrola poziva	-	-	-	9%
Produkcione aplikacije	-	-	-	42%
Pomoćne aplikacije	-	-	-	16%
IP video nadzor	-	-	-	16%
Ostali saobraćaj	-	-	-	8%

- **DMVPN tehnologija pruža sledeće prednosti:**
 - **Veoma skalabilno rešenje za izgradnju IPsec VPN mreže sa potpunom konektivnošću (full mash).**
 - **Podrška za dinamički adresirane krajnje tačke.**
 - **Krajnje pojednostavljeno dodavanje novih udaljenih rutera.**
 - **Drastično smanjenje veličine konfiguracije centralnog rutera.**
 - **DMVPN koristi GRE protokol, čime je podržan IP multikast saobraćaj, kao i dinamički ruting protokoli.**
 - **Veoma jednostavna selekcija saobraćaja koji se štiti enkripcijom.**

Pitanja ?



mtanaskovic@mds.rs