



Cisco Expo
2008

CISCO SP technologies as an END-to-END IP solution in COSMOFON



(2G/3G, WIMAX, PDH/SDH converged networks from COSMOFON) –

Goran Rumenovski

Vladimir Josifovski

Stefan Ivanovski

CISCO SP technologies as an END-to-END IP solution in COSMOFON

(2G/3G, WIMAX, PDH/SDH converged networks from COSMOFON)



НОВИ ТЕХНОЛОГИИ

- Подготовка
- Имплементација
- Практична примена
- Систем за мониторирање

МОТИВИ

1. Интегрирање на новите технологии и целосно прилагодување на постојната мрежна инфраструктура кон истите
2. Обезбедување квалитетен END-to-END SLA за крајните корисници

ПРЕДИЗВИЦИ

1. Потреба за целосна диференцијација на постоечката корпоративна инфраструктура од продукциската целина и создавање на два автономни системи:
 - Корпоративен дел (Corporate Data Network - CDN)
 - Продукциски дел (Production Data Network - PDN)
2. Создавање простор за прифаќање на нови технологии и развој на нови сервиси
3. Флексибилност и отвореност на системот за понатамошна надградба
4. Константно подобрување на квалитетот на услугите

ГЕНЕРАЛНИ ПРАВЦИ

1. IP конвергенција во скоро секој сегмент на компанијата
 - Корпоративен дел
 - Продукциски дел
2. Обрнување посебен акцент на IP безбедноста и нејзино постојано подобрување
3. Избор на **CISCO** како стратешки партнер

ЗОШТО “CISCO”?

- Производител кој стриктно ќе ги почитува стандардите, заради непречена интероперабилност со останатите производители
- IP решенија кои не смеат да бидат лимитирани од технологијата
- Имплементација на софистицирани решенија кои навистина функционираат
- Логичен избор **CISCO** technologies

ОГРАНИЧУВАЊА

Технолошки

- Инфраструктура на класичен мобилен оператор – nonIP
- Комплексност на новите технологии (3G/WIMAX)
- Multivendor опкружување
- Осетливост на процесот на миграција (комерцијални системи)

Човечки

- Истовремен ангажман во тековното одржување на постојната инфраструктура
- Поделени сервисни потреби

РЕАЛИЗАЦИЈА (фаза 1-2) 1.

- Мигрирање на системи кои можат да ја променат IP адресата
- Мигрирање на системи кои не можат да ја променат сопствената IP адреса
- Маскирање кон јавна IP мрежа (ИНТЕРНЕТ)
- Маскирање кон приватните мрежи
- Физичко и безбедносно одвојување на корпоративната мрежа

РЕАЛИЗАЦИЈА (фаза 1-4) 2.

Phase 4
Phase 3
Phase 2
Phase 1

РЕАЛИЗАЦИЈА (фаза 3-5) 3.

- Креирање нова административна целина за 2G/3G
- Креирање нова административна целина за WIMAX
- Подобрување на ИНТЕРНЕТ периферијата
- Создавање MPLS core
- Развој на MPLS

РЕАЛИЗАЦИЈА (фаза 5) 4.

MPLS јадро во COSMOFON

- Зошто MPLS?

- Придобивка од MPLS апликациите (logical VPN, automated redundancy, Traffic engineering, etc)

РЕАЛИЗАЦИЈА (фаза 5) 5.

MPLS јадро во COSMOFON

- Како да се воведе?

- MPLS како јадро во прва фаза

- * Понуда на ИНТЕРНЕТ сервисите како менаџирани сервиси

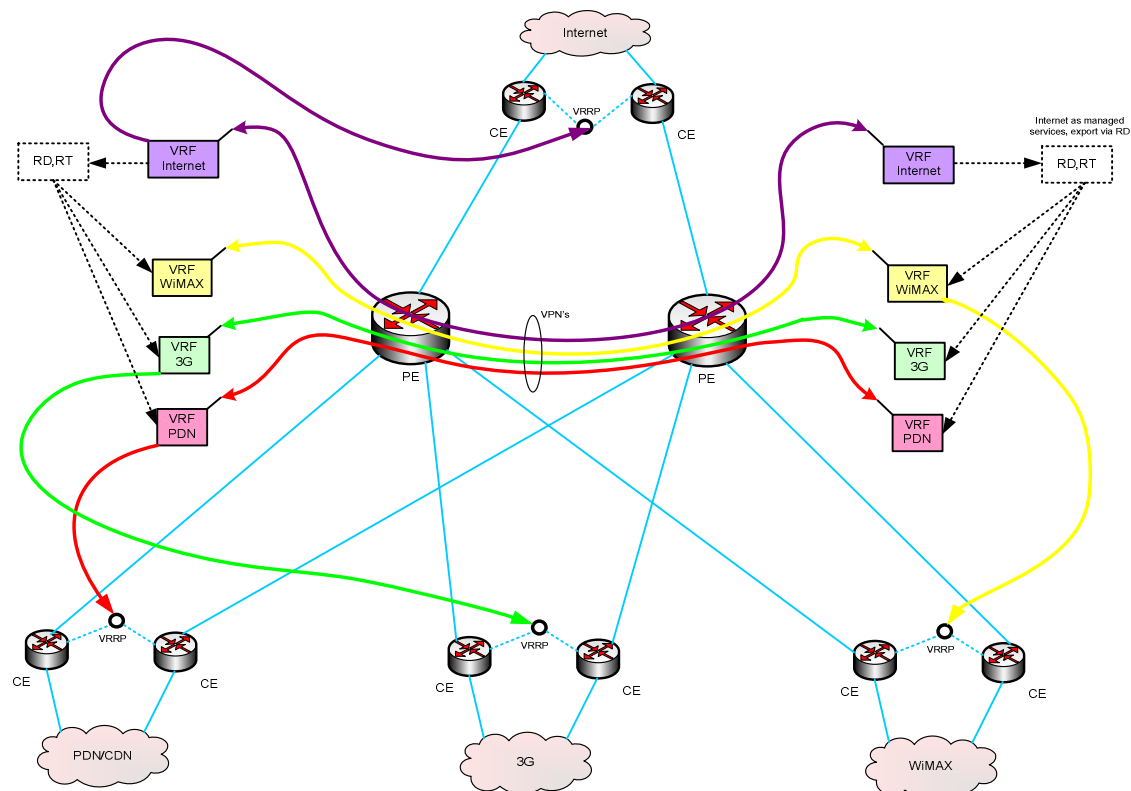
- * 4 корисници во пилот фазата (WIMAX, 2G/3G, PDN (продукциска мрежа), CDN (корпоративна мрежа)

- * Моделиран ТЕ и активно балансирање на излезниот сообраќај

РЕАЛИЗАЦИЈА (фаза 5)

6.

MPLS overview



РЕАЛИЗАЦИЈА (фаза 5) 7.

MPLS јадро во COSMOFON

- * 4x7606 во јадрото, colapsed PE сценарио, 2 со 2 редундантни машини
- * 2 машини за front BGP со виртуелни L3-gateways по целна група
- * 2 машини носители на MPLS апликациите

РЕАЛИЗАЦИЈА (фаза 5) 8.

Развој на MPLS во COSMOFON

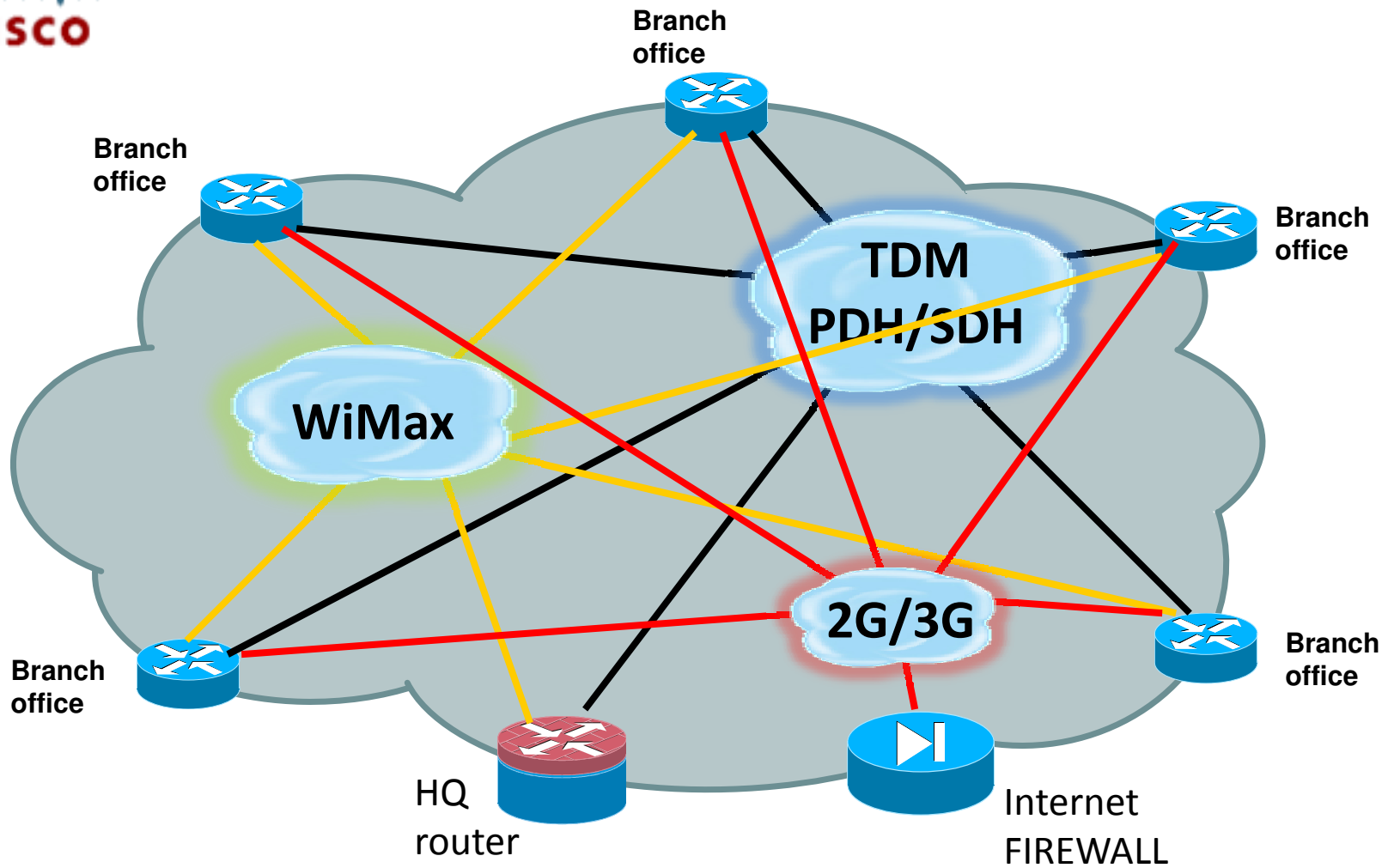
- Како да се прошири и развие?

- * Проширување ва пристапниот дел, во главните POP центри
- * Децентрализација на PE структурите, јадрото да се базира само на P структура
- * Проширување на MPLS апликациите (сервис базирани)
- * Понуда на висок и управуван SLA на крајните корисници

РЕАЛИЗАЦИЈА (фаза 5) 9.

Спецификација на опрема

- L2/L3 core
 - 2 x 7606S, 6-slot, RSP720-3CXL, PS, BGP IOS
 - 2 x 4503, 3slot, SE-IV, 48 port 10/100/1000
- MPLS core
 - 2 x 7606S, 6-slot, RSP720-3CXL, PS, BGP IOS
 - 2 x 7606S, 6-slot, RSP720-3CXL, PS, 10 x 1Gbps, MPLS IOS



РЕАЛИЗАЦИЈА (примена во корпоративен дел) 11.

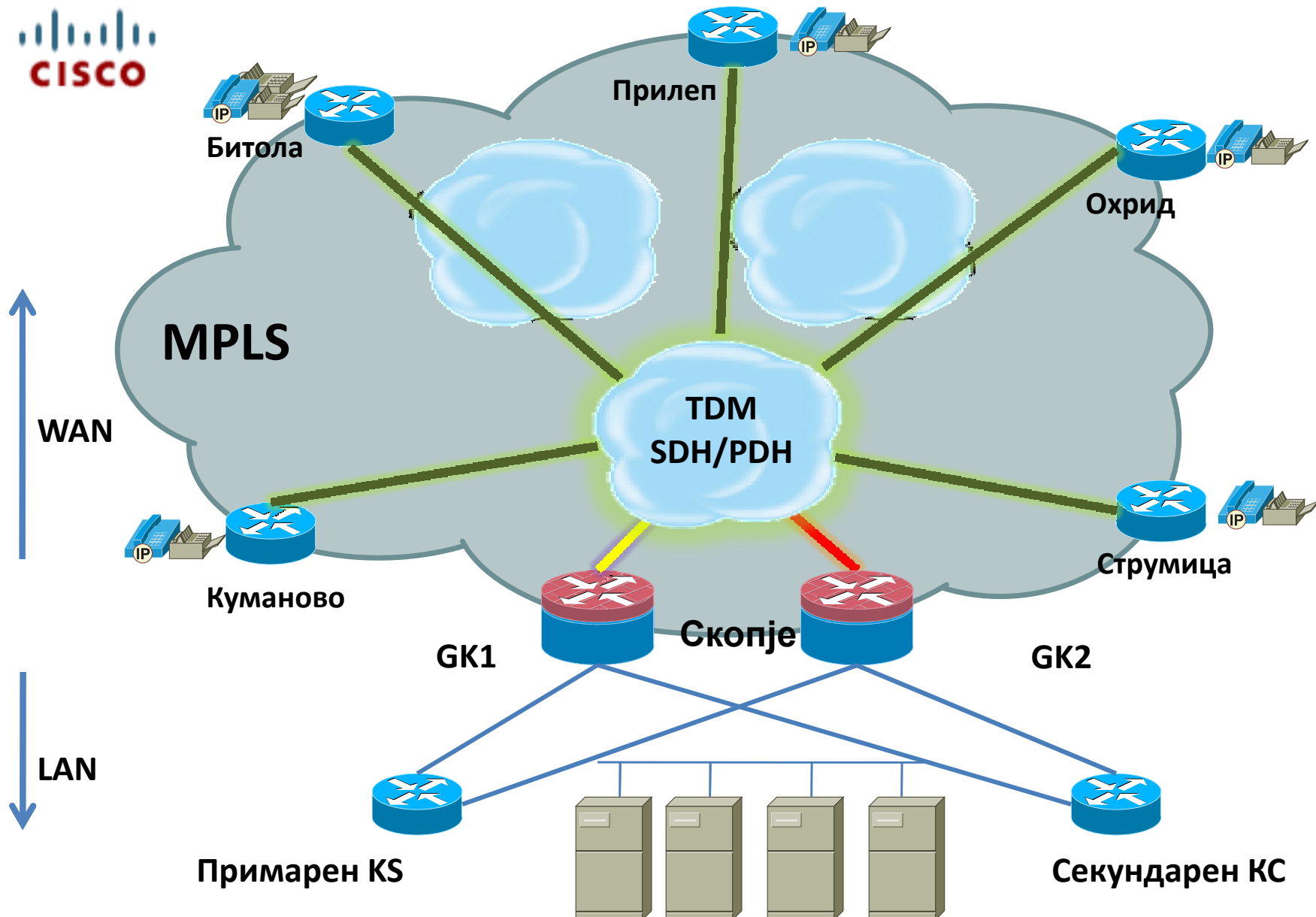
3G интеграција – корпоративна мрежа

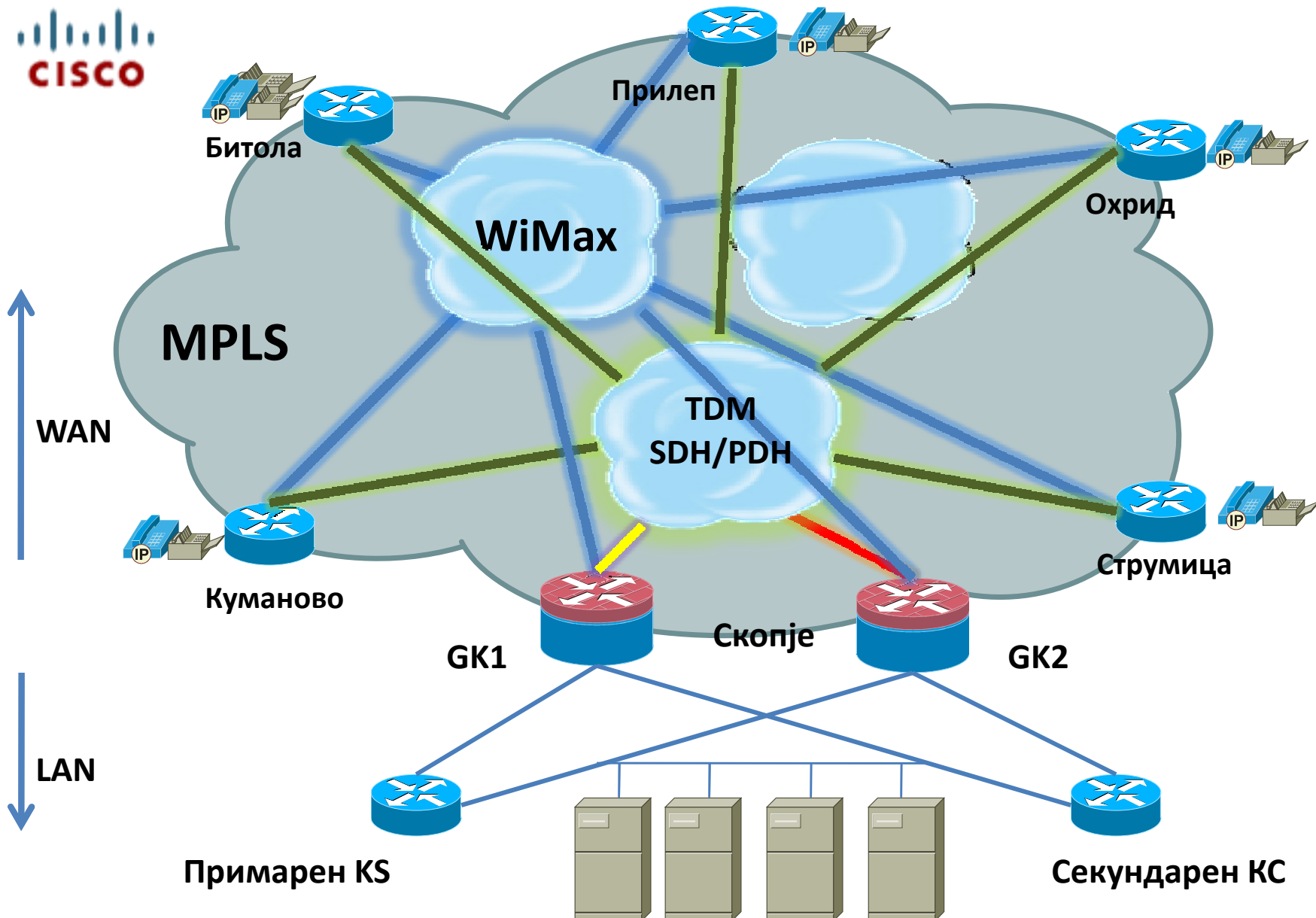
- Креирање посебен APN-corporate
- Креирање IPSEC tunnel помеѓу корисничката мрежа на крајникот корисник и продукциската мрежа
- Креирање GRE tunnel помеѓу GGSN и соодветна терминациска точка во корпоративната мрежа
- Тестирање и контрола на функционалноста на системот

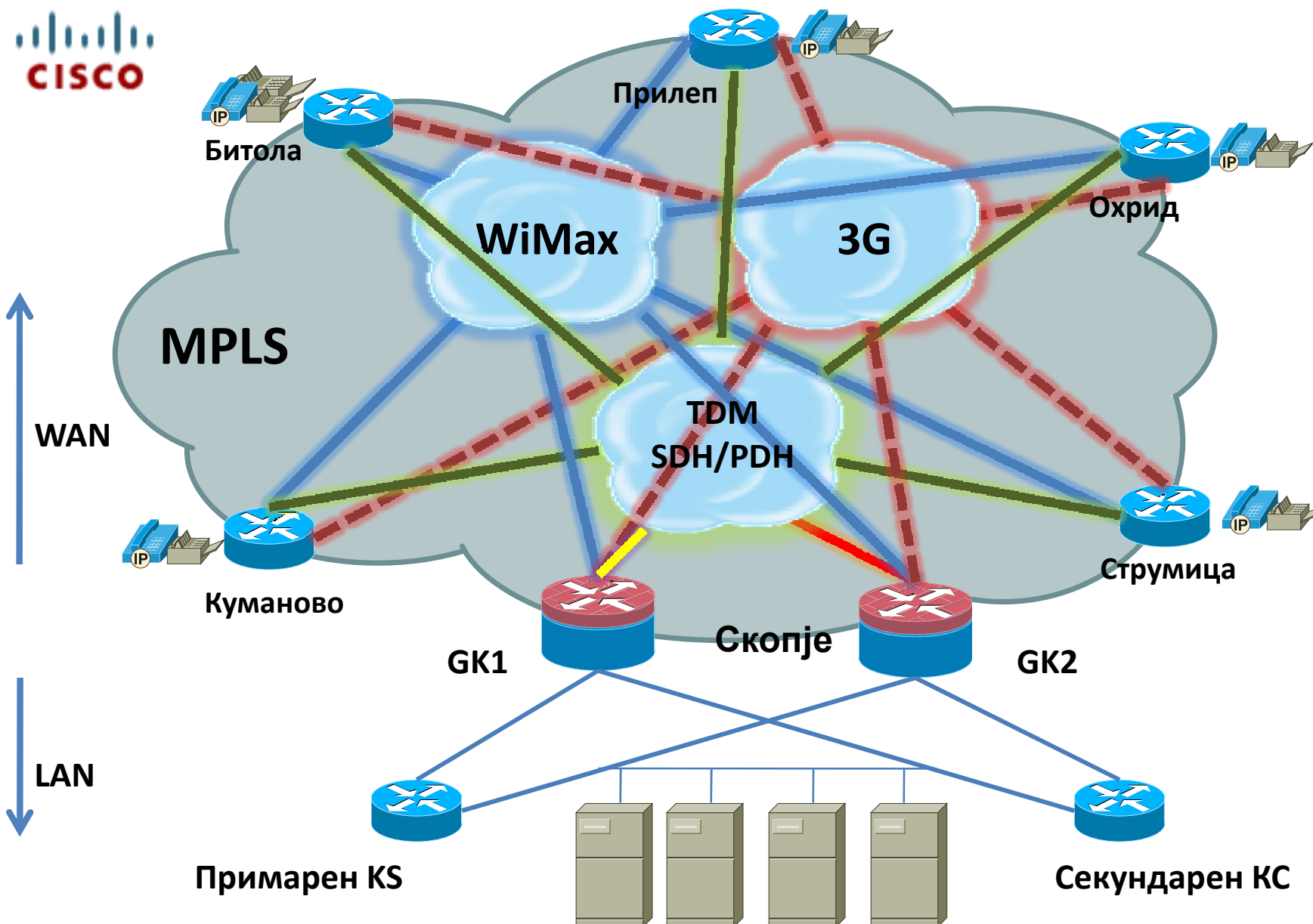
РЕАЛИЗАЦИЈА (примена во корпоративен дел) 12.

WIMAX интеграција – корпоративна мрежа

- Креирање посебен L2VPN
- Поставување CPE во далечни локации
- Креирање параметри за обезбедување QoS низ целокупната инфраструктура
- Креирање виртуелен пат низ MPLS
- Поврзување на централниор рутер во корпоративната мрежа
- Тестирање и контрола на функционалноста на системот







Cisco Advanced Site-to-Site VPNs

1. Hub-and-Spoke VPNs

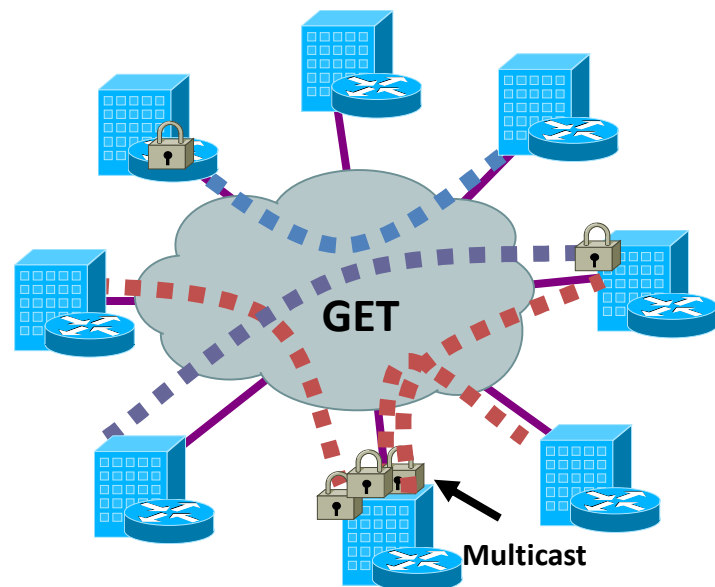
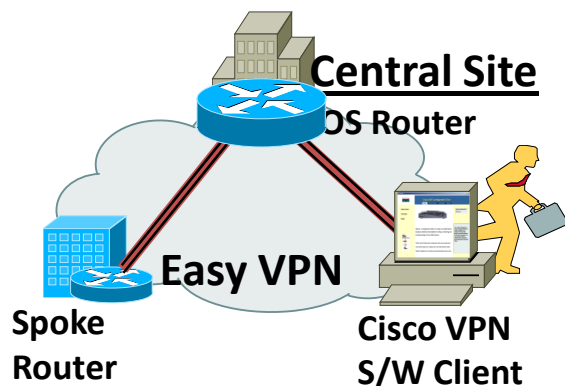
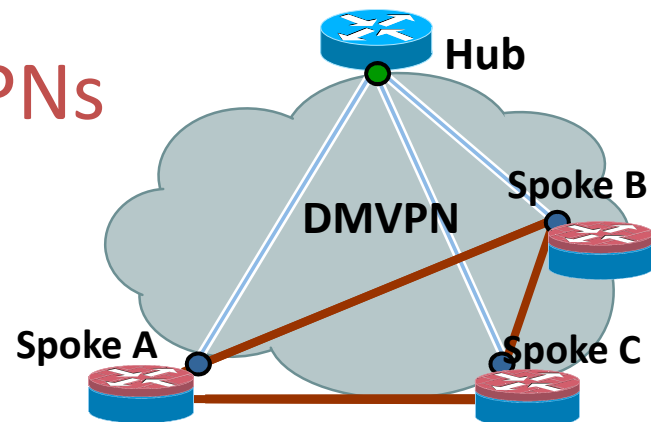
- IPSec+GRE: (Static Tunnels with Routing)
- Easy VPN (Dynamic Policy/Config Push)
- DMVPN (Zero Touch with Dynamic Routing)

2. Dynamic Spoke-to-Spoke VPNs

- DMVPN (On-Demand Partial-Mesh)

3. Tunnel-Less Any-to-Any VPNs

- Group Encrypted Transport (GET) VPN

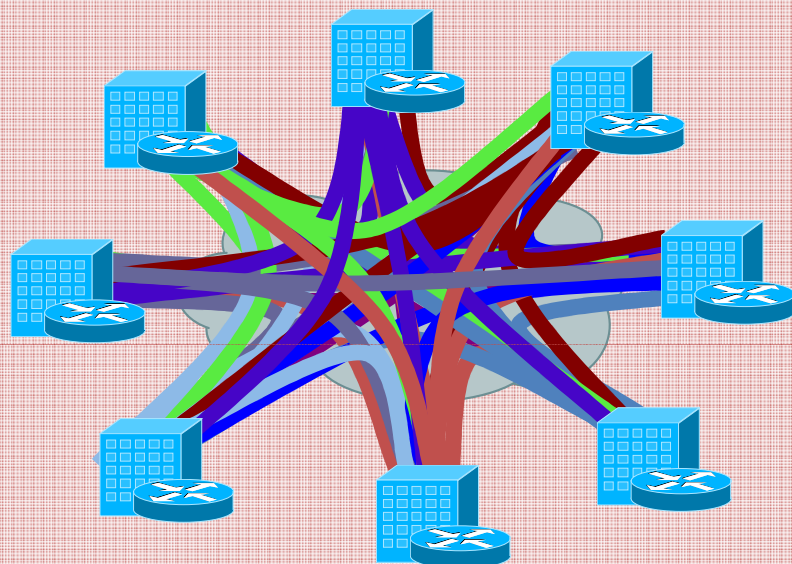


Tunnel-less VPN – Нов Безбедносен модел

Any-to-Any енкрипција: Пред и После GET VPN

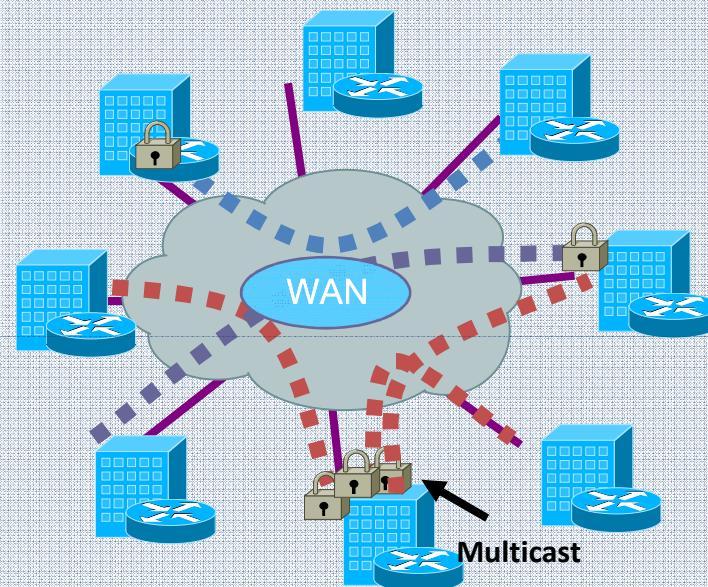


Пред: IPsec P2P Тунели



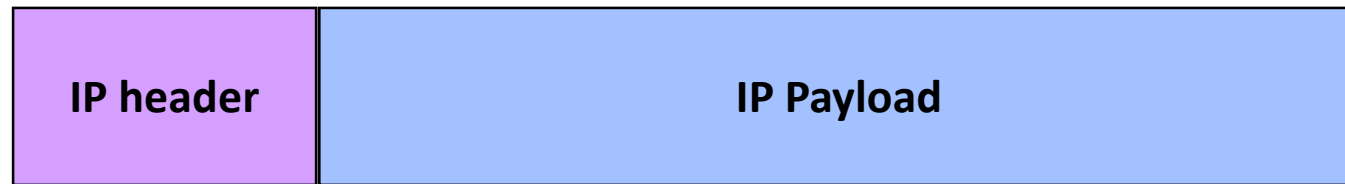
- Scalability—an issue (N^2 problem)
- Overlay routing
- Any-to-any instant connectivity can't be done to scale
- Limited advanced QoS
- Multicast replication inefficient

После: Tunnel-less VPN



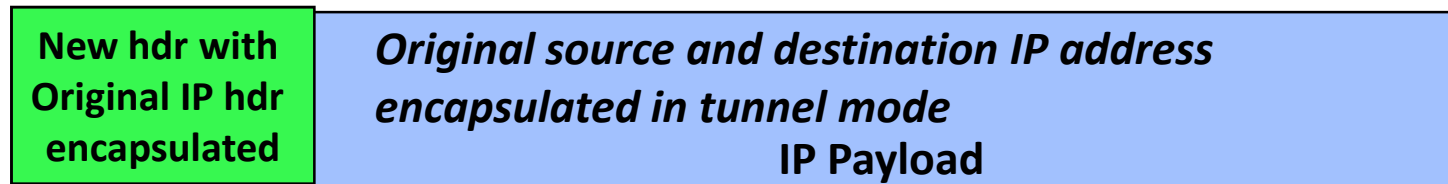
- Scalable architecture for any-to-any connectivity and encryption
- No overlays – native routing
- Any-to-any instant connectivity
- Advanced QoS
- Efficient Multicast replication

IPsec Tunnel Mode with IP Header Preservation

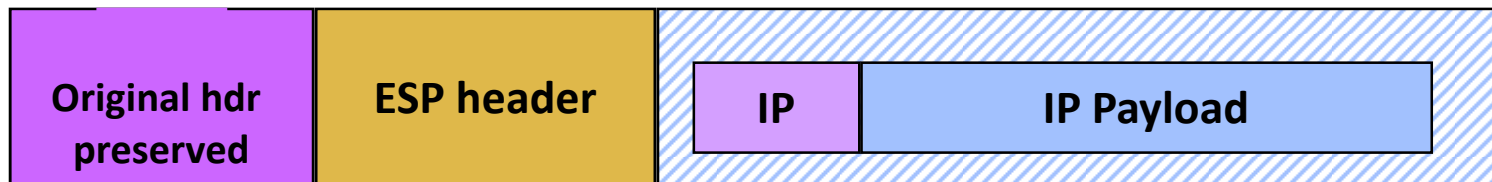


Original IP Packet

IPSec Tunnel Mode

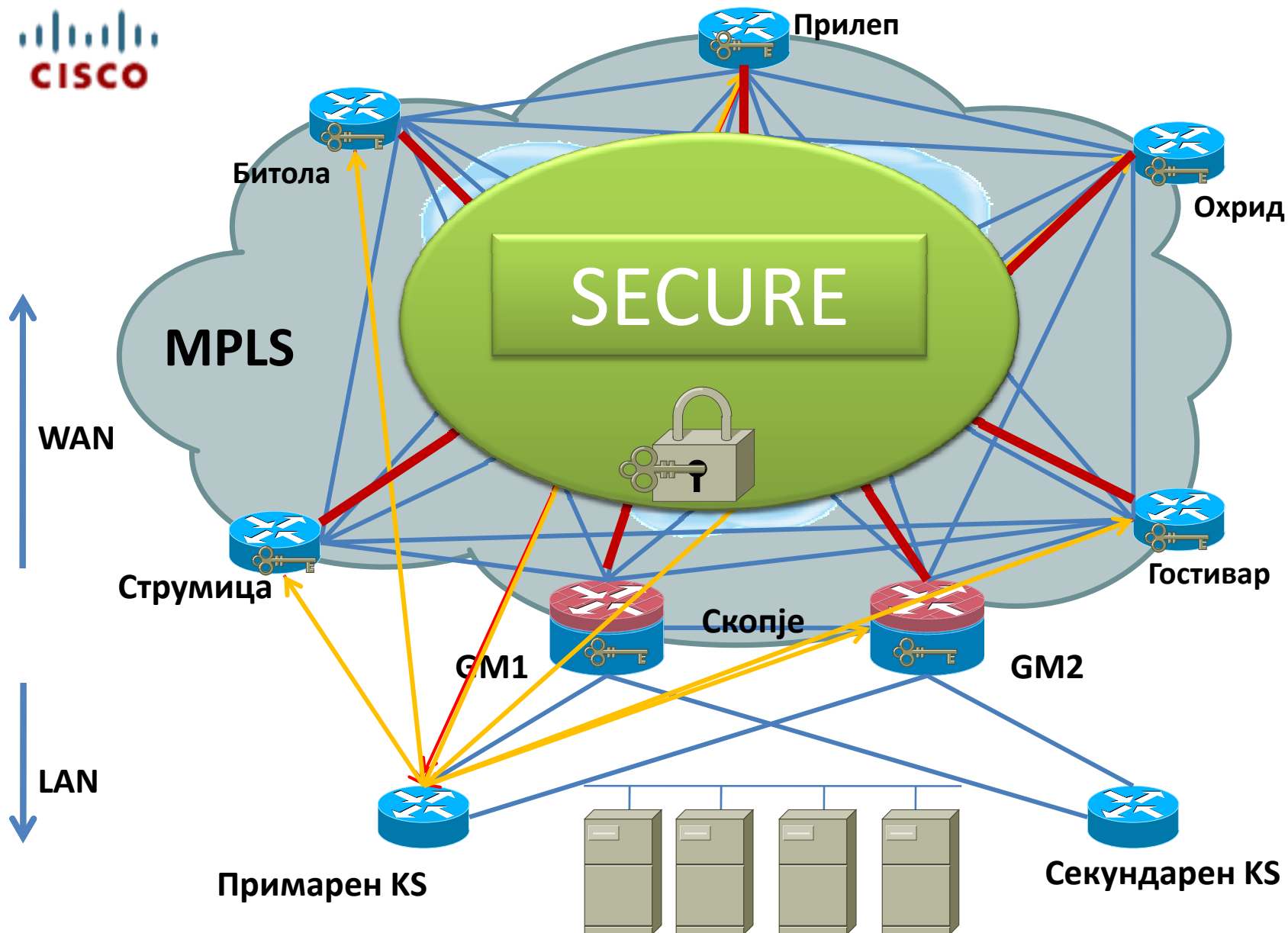


IP Header Preservation



IPSec packet

1. **Циско Рутер (1800, 2800, 3800, 7200, 7301)**
 1. Branch-offices **C2811-3G-G-SEC/K9**
Cisco 2811, HWIC-3G-GSM, 64MB FL /256MB DRAM, Adv Security
 1. Wan Aggregation **CISCO3845-HSEC/K9**
3845 Bund. w/AIM-VPN/SSL-3,Adv. IP Serv,25 SSL lic,128F/512D
 2. Key Server **C2811-3G-G-SEC/K9**
Cisco 2811, HWIC-3G-GSM, 64MB FL /256MB DRAM, Adv Security
2. **Циско IOS > 12.4.11-T2 Advanced Security**
3. **Космофон - WiMax L2 VPN**
4. **Космофон 3G Private APN **HSDPA (3,6 MBps)** Dialer бекан**





```
hostname Primary_Key_Server
!
crypto isakmp policy 10
encr aes
group 2
authentication pre-share
crypto isakmp key cisco address 100.1.1.9
crypto isakmp key cisco address 100.1.1.13
!
crypto ipsec transform-set mygdoi-trans esp-aes esp-sha-hmac
!
crypto ipsec profile gdoi-profile-getvpn
set security-association lifetime seconds 900
set transform-set mygdoi-trans
!
crypto gdoi group getvpn
identity number 1234
server local
rekey retransmit 10 number 2
rekey authentication mypubkey rsa getvpn-
export-general
rekey transport unicast
sa ipsec 1
profile gdoi-profile-getvpn
match address ipv4 199
address ipv4 100.1.1.1
redundancy
local priority 100
peer address ipv4 100.1.1.5

access-list 199 permit ip 10.1.0.0 0.0.255.255
10.1.0.0 0.0.255.255
```



```
hostname GroupMember-1 (BranchOffice1)
!
crypto isakmp policy 10
encr aes
group 2
authentication pre-share
crypto isakmp key cisco address 100.1.1.1
crypto isakmp key cisco address 100.1.1.5
!
crypto gdoi group getvpn
identity number 1234
server address ipv4 100.1.1.1
server address ipv4 100.1.1.5
crypto map getvpn-map 10 gdoi set group getvpn
```

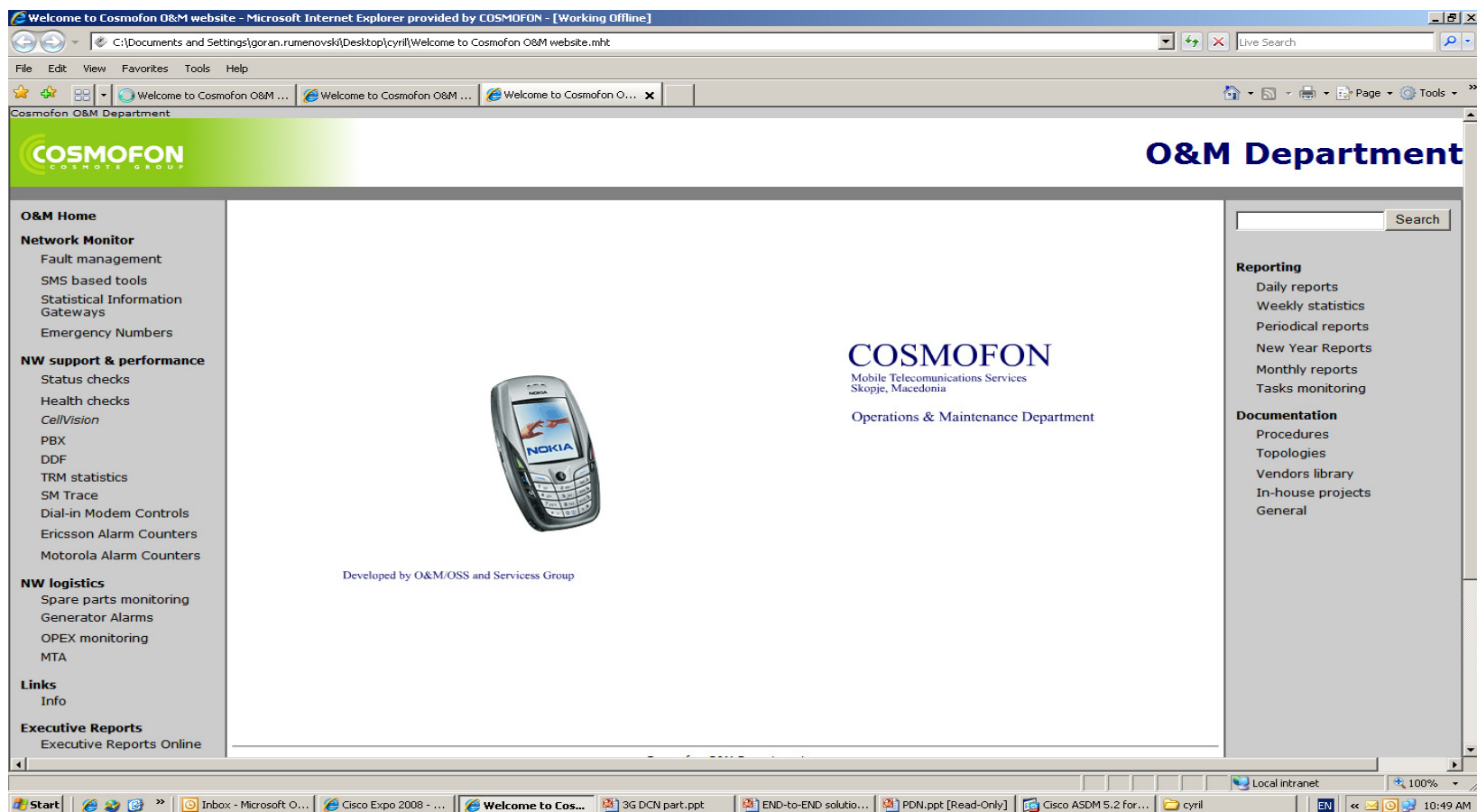
```
!
interface FastEthernet0/0
description Inside interface
ip address 10.1.11.1 255.255.255.0
!
interface FastEthernet0/1
description WiMax-UPLINK
ip address 100.1.1.9 255.255.255.252
crypto map getvpn-map
!
Interface Serial 0/1
Description To PDH
ip address 100.1.1.19 255.255.255.252
crypto map getvpn-map
```

Network Management system (NMS)

- Имплементација на целосно решение за NMS како продолжение на тековната мултивендор инфраструктура
- Комплетно решение во согласност со тековните сигурносни стандарди за:
 - CM – configuration management / provisioning
 - FM – Fault managment
 - PM – Performance mangment



NMS web portal



NMS – CM дел

- Configuration manager/provisioning како контролен процес преку централизиран TACACS сервис
- Посебни привилегии за оперативниот дел (admin привилегии) и развој и планирање (оператор привилегии)
- Интегриран тикетинг сервис за секоја измена на конфигурациите на било кој уред

NMS – FM дел

- Fault management – реализиран како продолжување на тековниот систем за аларми и испади, со комплетна архива
- Базиран на централизиран HPOV со дистрибуирани агенти за терминација на SNMP trap-ови за секоја логичка групација, DNS интегрирани
- Комплетна интеграција со NMC (Network Management Center)

NMS – FM дел

Пример од работата во NMC

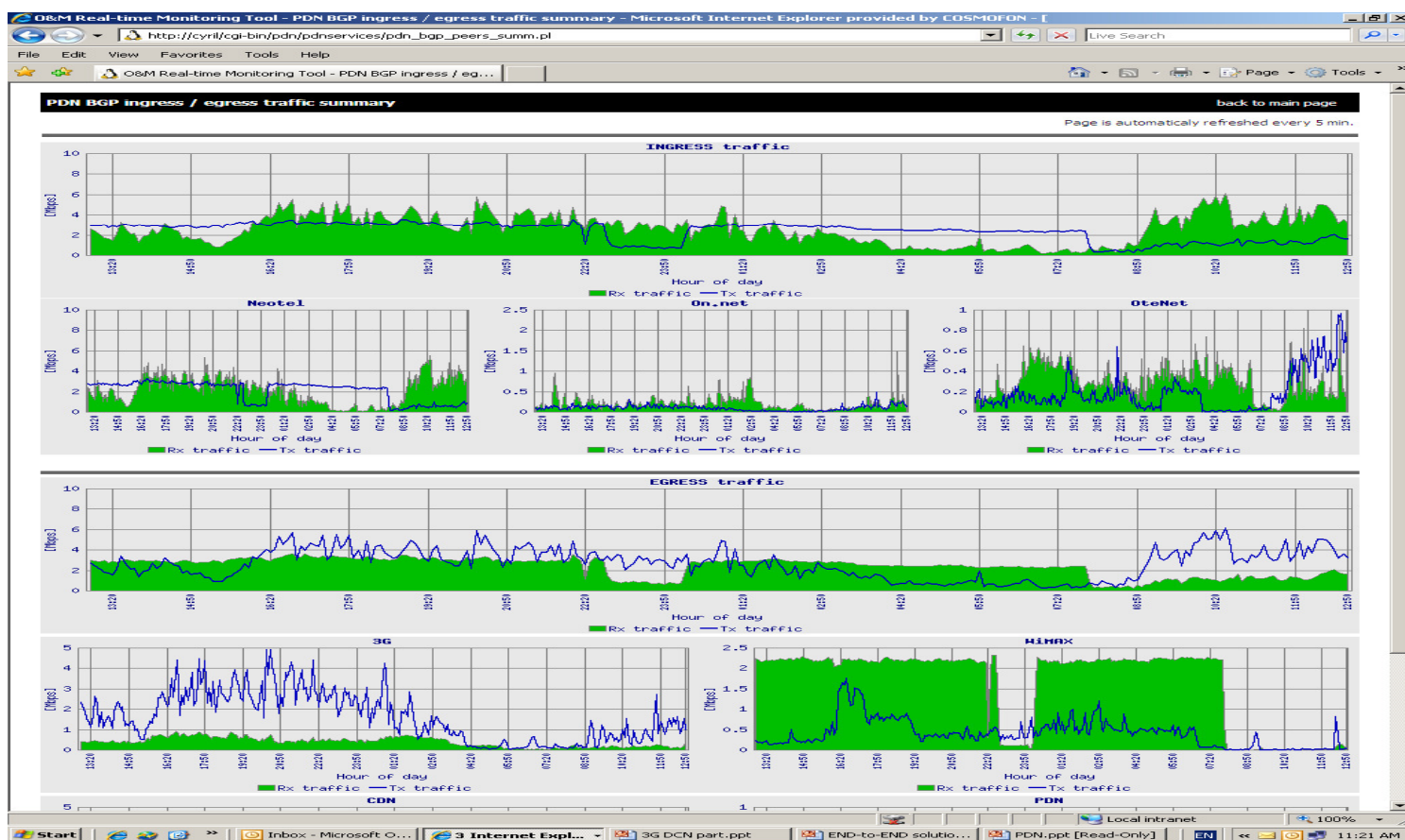
DCN Browser					
File Actions View Help					
Ack	Corr	Severity	Date/Time	Source	Message
	3	Normal	Wed Nov 19 08:00:57	13_bts_gorenci-1	Port 12 on E1 0/2/0 is UP.
	1	Normal	Wed Nov 19 15:18:12	10.144.30.13	Port 6 on Serial0/1/0:0 is UP.
	1	Normal	Wed Nov 19 15:22:15	mms-router2	Port 6 on Serial0/1/1:0 is UP.
	3	Normal	Wed Nov 19 16:48:32	mms-router1	Port 6 on Serial0/1/0:0 is UP.
	1	Normal	Wed Nov 19 23:04:37	13_bts_pozar	Port 12 on E1 0/2/0 is UP.
	1	Normal	Wed Nov 19 23:36:45	mms-router2	Port 5 on E1 0/1/1 is UP.
		CRITICAL	Thu Nov 20 03:01:17	mms-router2	Port 5 on E1 0/1/1 is DOWN.
		CRITICAL	Thu Nov 20 03:01:20	mms-router2	Port 6 on Serial0/1/1:0 is DOWN.
		CRITICAL	Thu Nov 20 03:03:02	gre-gprs-2	Port 6 on Serial0/0/1:0 is DOWN.
		CRITICAL	Thu Nov 20 03:26:38	gre-gprs-2	Port 6 on Serial0/0/1:0 is DOWN.
		CRITICAL	Thu Nov 20 03:45:52	gre-gprs-2	Port 6 on Serial0/0/1:0 is DOWN.
	9	Normal	Thu Nov 20 04:10:18	gre-gprs-2	Port 6 on Serial0/0/1:0 is UP.
	3	Normal	Thu Nov 20 05:00:20	mms-router2	Port 5 on E1 0/1/1 is UP.
	3	Normal	Thu Nov 20 05:00:22	mms-router2	Port 6 on Serial0/1/1:0 is UP.
	1	Normal	Thu Nov 20 10:19:41	mms-router1	Port 6 on Serial0/1/0:0 is UP.
		Normal	Thu Nov 20 14:13:27	12_bts_borula	synReceived
16 Alarms - Critical:5 Major:0 Minor:0 Warning:0 Normal:11 (5 acknowledged)					

Alarm Categories	
☒	Error Alarms
☐	Threshold Alarms
☐	Status Alarms
☐	Configuration Alarms
☐	Application Alert Alarms
☐	PrePaid Excel Switch
☒	PrePaid Application Alarms
☐	PrePaid Performance Alarms
☐	PrePaid Cluster Switchover
☐	GPRS
☒	Converse SMSC
☒	PBX
☒	VASGW
☒	LTS
☒	PrePaid Hardware Alarms
☒	Fun Dial
☐	DXX
☒	PrePaid JAction Alarms
☐	Telecontrol Alarms
☐	EMMA
☒	DCN
☐	SMS Welcome & Bon Voyage
☐	CB clock
☒	NMS
☒	EIR
☒	COW
☒	USSD
☒	All Alarms

NMS – PM

- Performance management – реализиран како продолжување на тековниот систем на перформанси, статистика и репортинг
- Базиран на 4 node cluster со дистрибуирани агенти за креирање на SNMP trap-ови кон секоја логичка групација, DNS интегрирани
- Автоматско откривање на нови сервиси, нови интерфејси и нови L2/L3 нодови
- Собирање статистики на секои 5 минути од сите главни интерфејси, CPU/Memory utilization преку SNMP traps
- Online мониторинг
- Автоматска агрегација и ретензија на податоците
- Предефинирани извештаи за комплетниот систем, како за оперативниот дел, така и за планерскиот долгорочен развој

NMS – PM дел



КАКО ЗАКЛУЧОК

- Употребата на CISCO IP базирани решенија овозможува надминување на многу технолошки лимити со кои COSMOFON се соочуваше во минатото.
- Професионалноста на локалната канцеларија на CISCO во сугестиите за имплементација на дел од решенијата беа фактор плус кој овозможи брз премин без никаква загуба во сервисите.

БЛАГОДАРАМ НА ВНИМАНИЕТО

