



Cisco Expo
2009

Omrežne storitve in infrastruktura



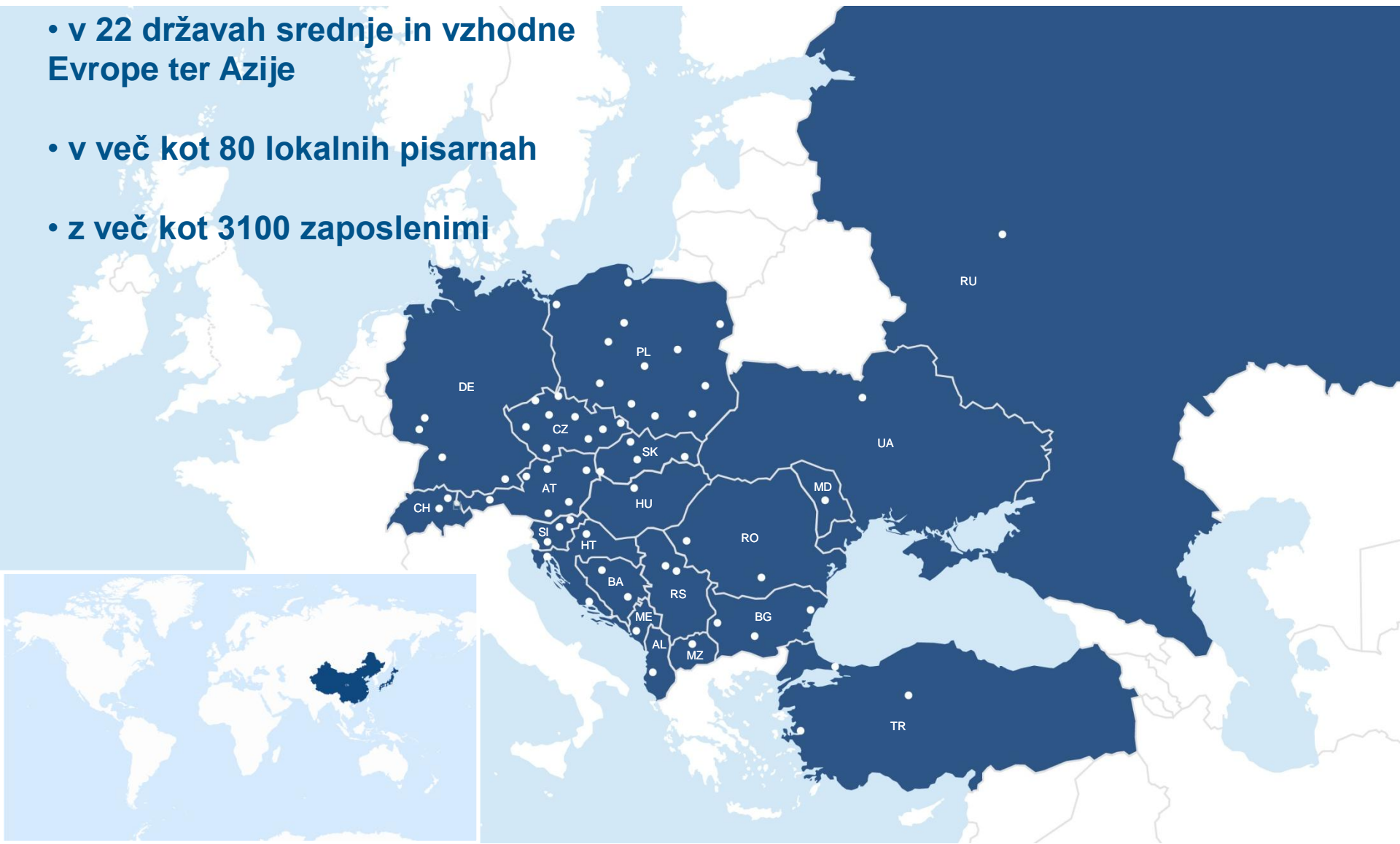
Marko Rahne, S&T Slovenija d.d.



- a. Predstavitev S&T
- b. Model Infrastruktura/Storitve/Aplikacije/Upravljanje
- c. Omrežna Infrastruktura
- d. Upravljanje in SLA

S&T je vodilni dobavitelj IT rešitev in storitev

- v 22 državah srednje in vzhodne Evrope ter Azije
- v več kot 80 lokalnih pisarnah
- z več kot 3100 zaposlenimi



Bosna in Hercegovina

podružnici: Sarajevo
Banja Luka

Slovenija

podružnice: Ljubljana
Celje
Koper
Maribor

Hrvaška

podružnice: Zagreb
Split
Rijeka

Črna gora

podružnica: Podgorica

Albanija

podružnica: Tirana

Srbija

podružnici: Beograd
Novi Sad

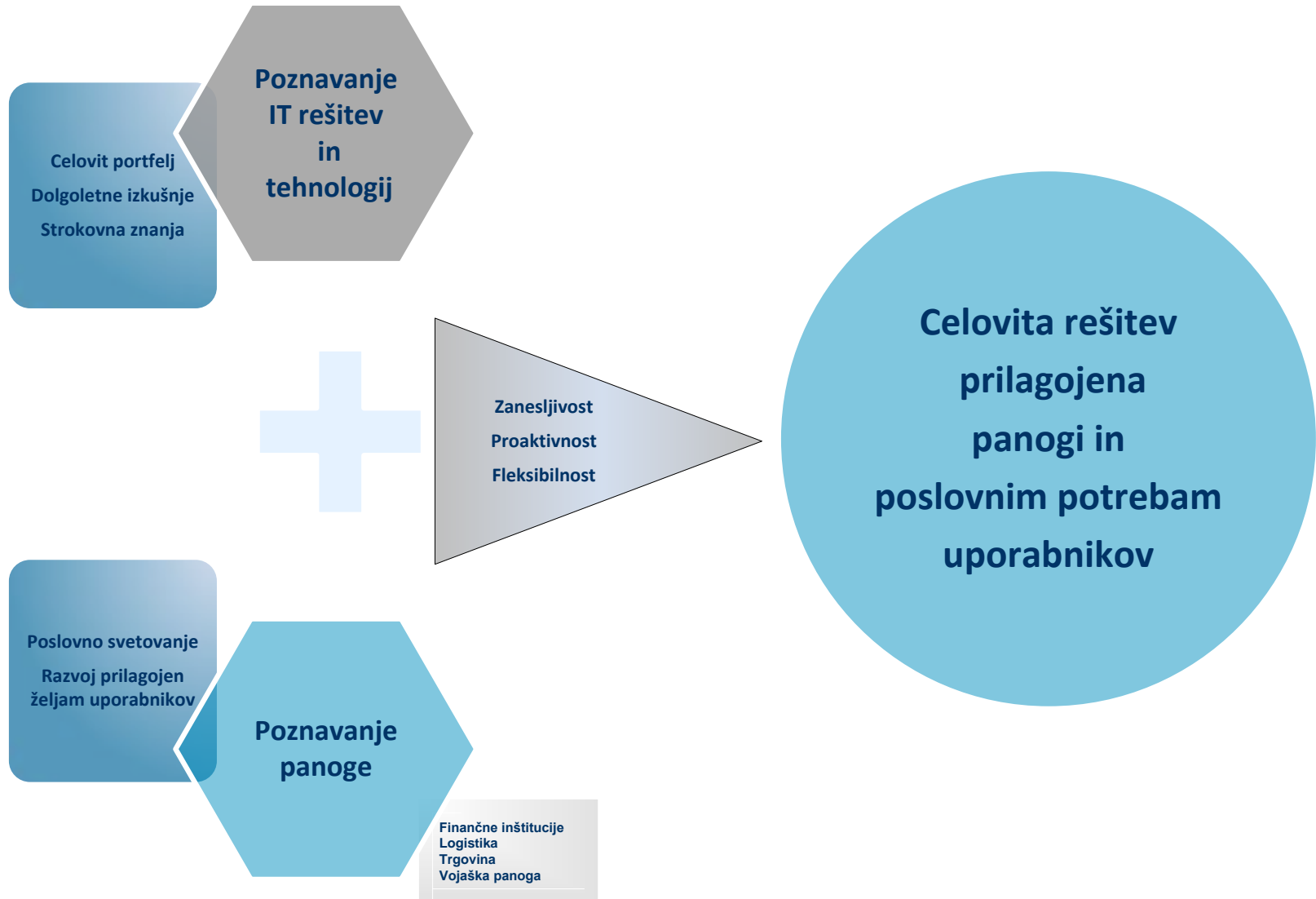
Makedonija

podružnica: Skopje

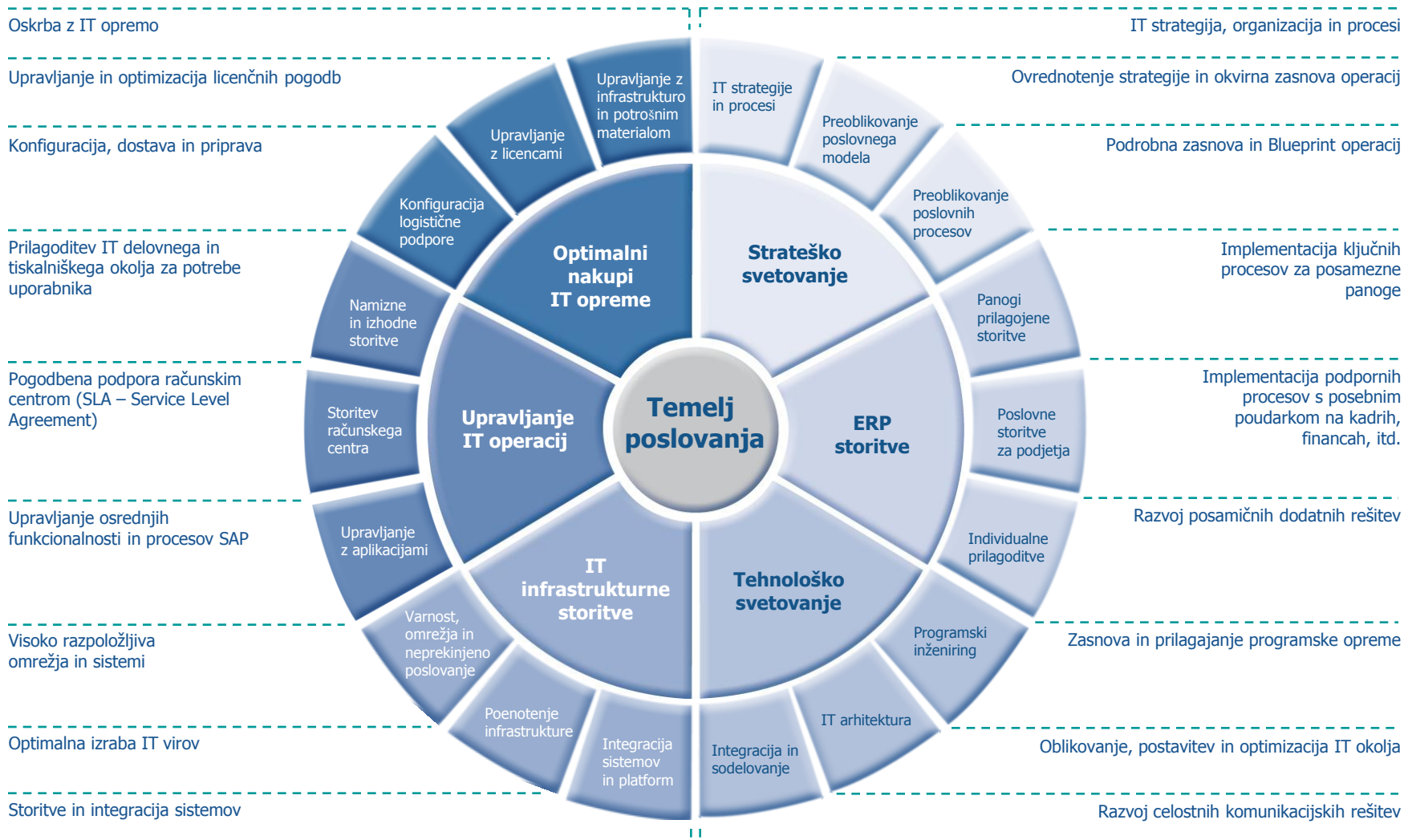
Turčija

podružnice: Istanbul
Ankara
Izmir





Ponujamo celosten nabor IT rešitev



Enterprise Computing

2008 Preferred Partner



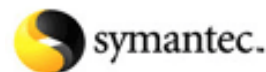
Enterprise Storage



2008 Preferred Partner



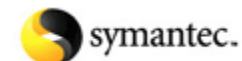
Information Management



2008 Preferred Partner



Networks & Security



Model Infrastruktura/Storitve/ Aplikacije/Upravljanje



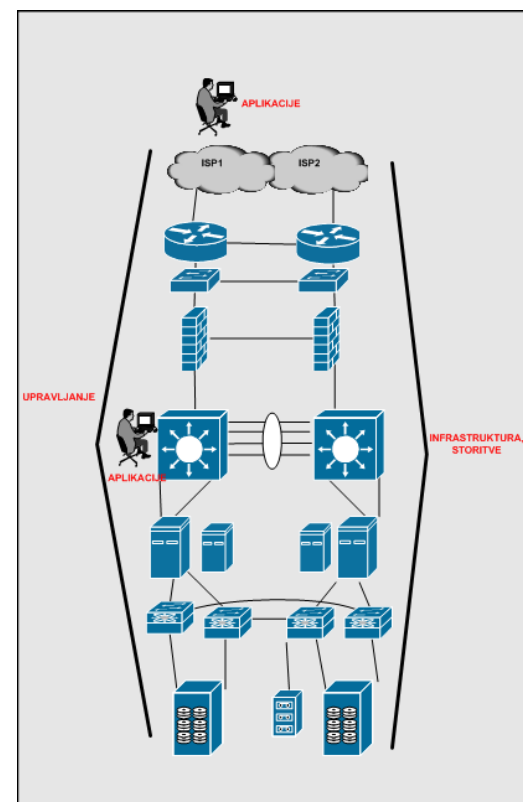
UPRAVLJANJE

APLIKACIJE

OMREŽNE STORITVE

OMREŽNA INFRASTRUKTURA

SLA



- **Omrežna infrastruktura (IT resursi)**

- Strežniki, klienti (PC, prenosniki, mobilne naprave), diskovje, stikala, usmerjevalniki, požarne pregrade..) glede na različne področja v omrežju (LAN, Data Center, SAN/NAS, WAN/MAN, ISP, Branch, SOHO)

- **Omrežne storitve (storitve na infrastrukturi)**

- Switching, VLAN, Routing, QoS, SLB, L2/L3 security

- IP Telefonija, Video

- WLAN, VoWLAN

- Oddaljeni dostopi (VPN, IPSEC, SSL, ..)

- FW, IPS, Anti-X, Content Security, Desktop/End-Point Security

- DNS, DHCP, AD, AAA

- Virtualizacija strežnikov

- Varnostno kopiranje, Replikacije/migracije, HA Clustering, DRC

- **Aplikacije**

- Poslovne aplikacije (ERP, CRM, HR, DB,)
- Aplikacije za sodelovanje (e-MAIL, IM,)

- **Upravljanje (FCAPS)**

- **Način**

- Upravljanje napak/okvar (Fault Management)
 - Upravljanje konfiguracij (Configuration Management)
 - Upravljanje s porabo resursov (Accounting Management)
 - Upravljanje zmogljivosti (Performance Management)
 - Uporabljanje varnosti (Security Management)

- **Področje**

- Upravljanje infrastrukture
 - Upravljanje storitev (MGMT za FW, IPS, WLAN, NAC, ..)
 - Upravljanje aplikacij

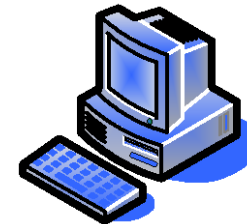
- **Zagotavljanje ravni storitve (SLA)**

Omrežna infrastruktura

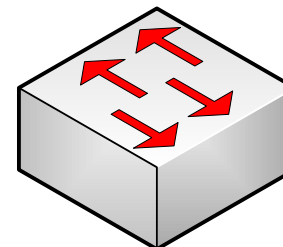


- Urejena omrežna infrastruktura je eden izmed pogojev za dobro integracijo dodatnih »**omrežnih storitev**«
- Topologija omrežja (L1; razdalje, vrsta kablov (UTP, FO),
lastnosti FO (SMF/MMF, “core size”, “modal bandwidth”))
- Design omrežja (VLANi, redundanca, IP shema, storitve, aplikacije ..)

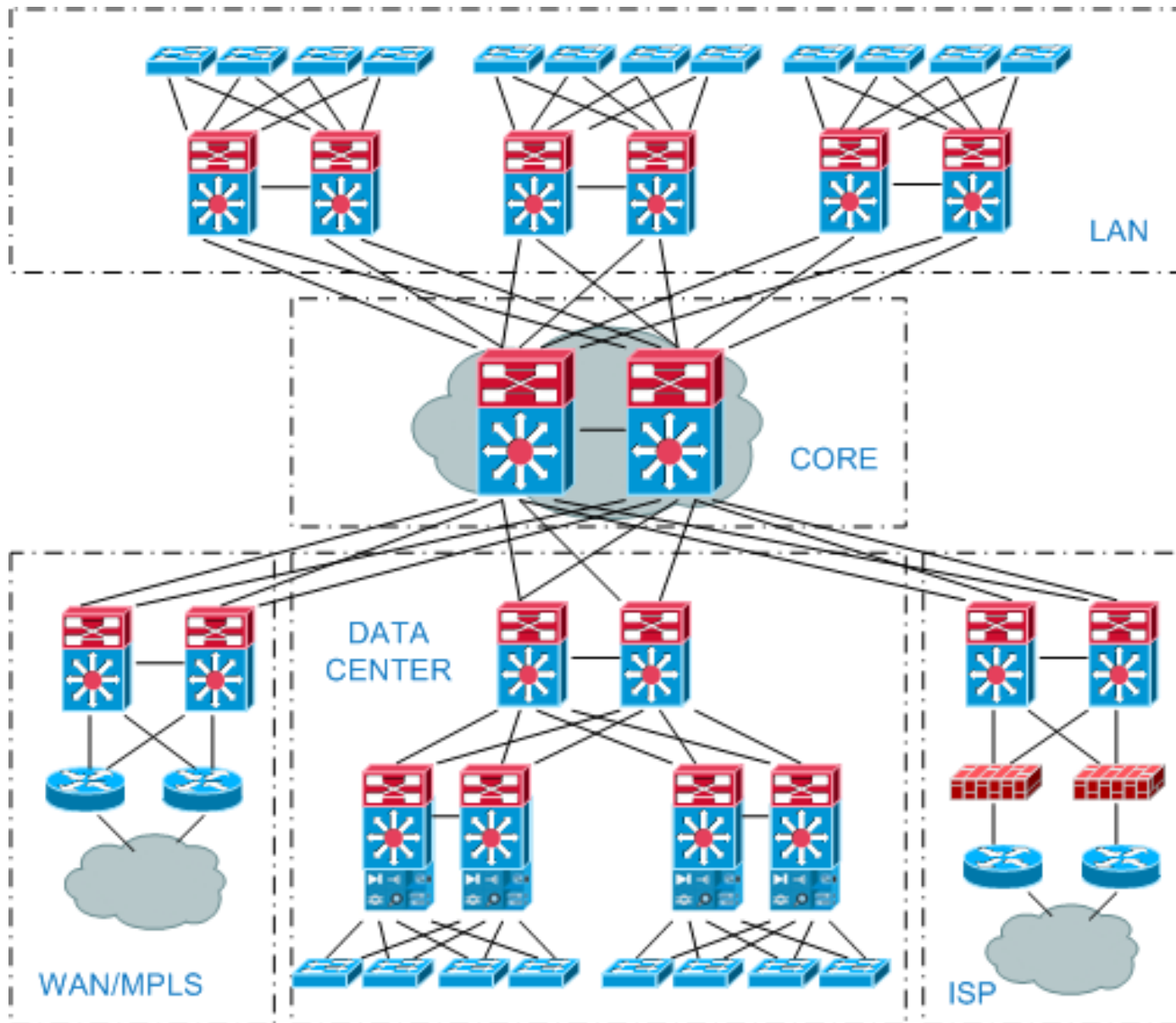
uporabniki



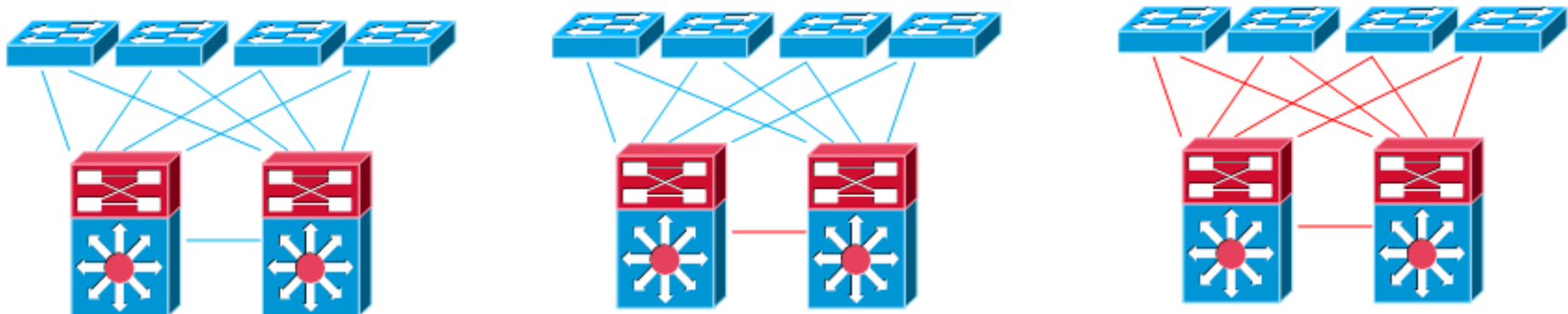
infrastruktura



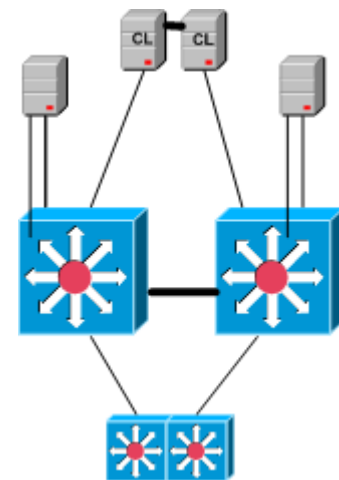
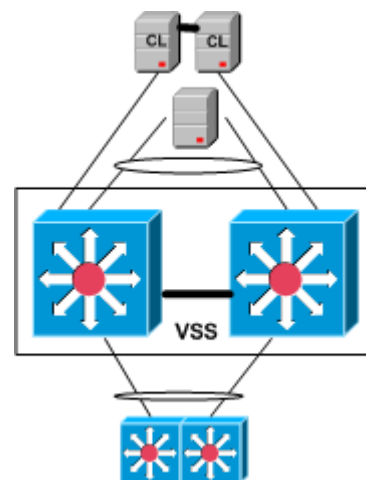
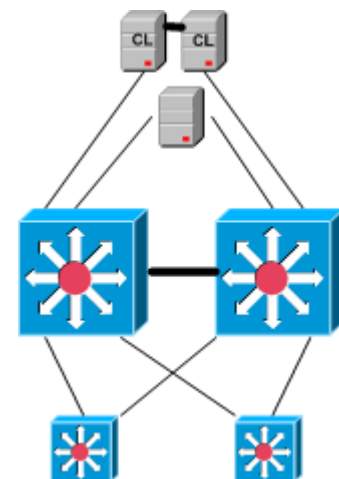
Cisco Enterprise Design



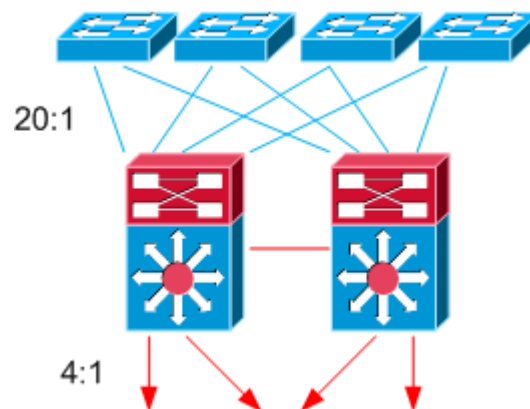
- 3 splošne arhitekture, vsaka s svojimi posebnostmi
 - L2 link (trunk) med stikaloma distribucijskega nivoja
VLAN “kjerkoli”, L2 zanke v omrežju (STP), FHRP,
L3 routing na distribucijskem nivoju
 - L3 link med stikaloma distribucijskega nivoja
VLAN “vozlišče”, ni L2 zank v omrežju, FHRP,
L3 routing na distribucijskem nivoju
 - L3 link do pristopnega nivoja
VLAN “vozlišče” (ni možen VLAN “kjerkoli”), ni potreben FHRP,
L3 routing (RIP, EIGRP, OSPF) na pristopnem nivoju



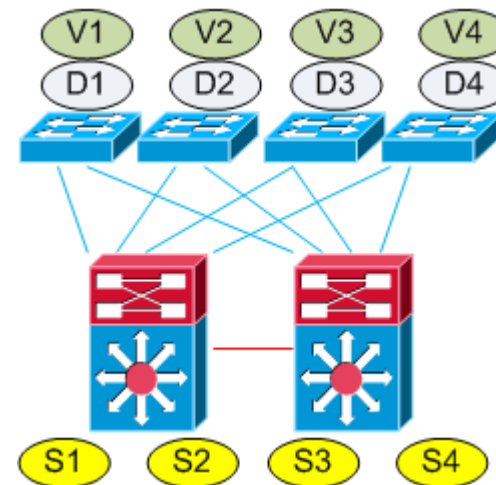
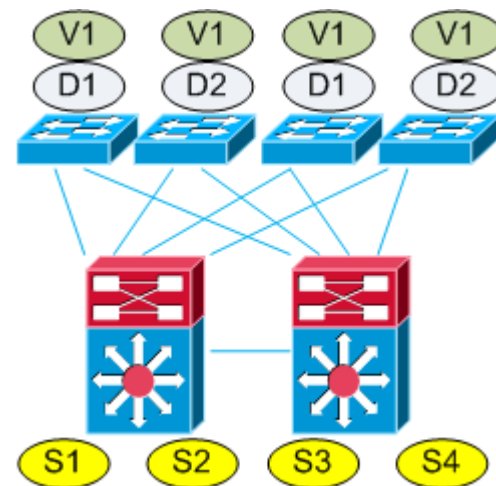
- Ustrezna arhitektura na nivoju opreme (A/A, A/S)
- STP
- FHRP
- L3 Keepalives, Link Tracking
- Routing
- Redundantno modularno stikalo
 - Supervisor modul
 - SSO (Stateful switchover), NSF (Nonstop Forwarding)
 - VSS (Virtual Switching System)
 - Podatkovni moduli (FO, UTP, ..)
- Stackwise/Stackwise+, CableStack
- EtherChannel/MultiChassis Etherchannel
- NIC Teaming
- HA Clusters



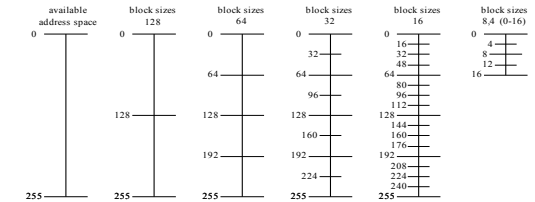
- UTP, FO
- Oversubscription (→ QoS)
 - access → distribution (tipično 20:1)
 - distribution → core (tipično 4:1)
- N x 1 Gbs (SX, LX; GBIC, SFP)
- N x 10 Gbps (SR, LX4, LR, ..; XENPAK, X2, SFP+, ..)
- Redundanca in uporaba vseh linkov (Load Balancing)
- Cena ena povezave (cca 800 € - 6400 €)



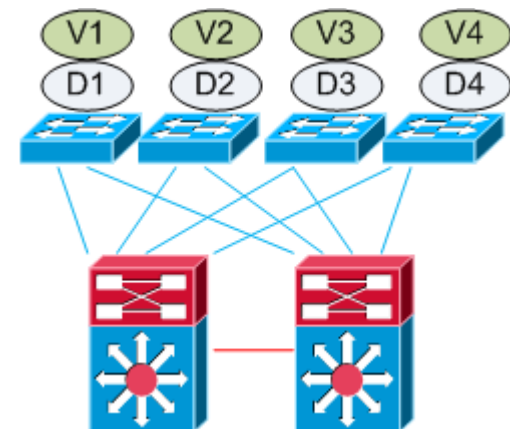
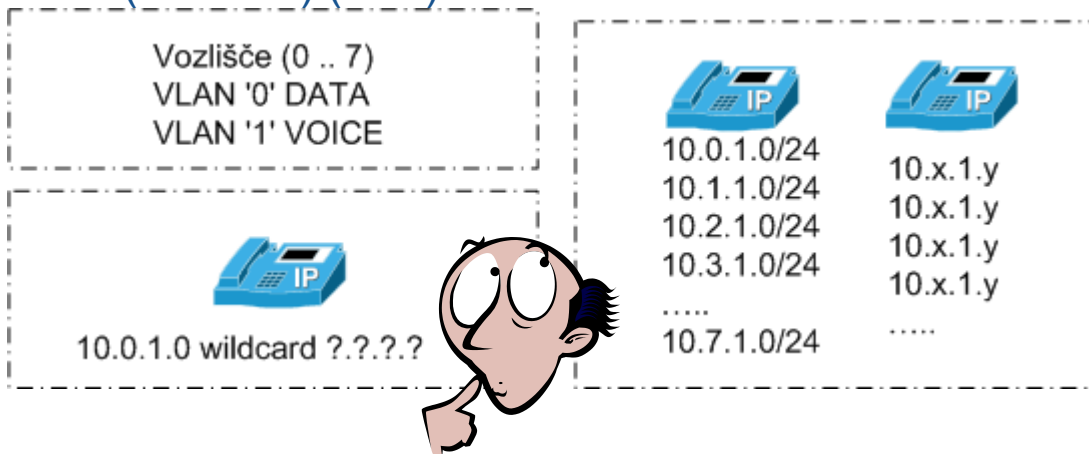
- VLAN-i glede na lokacijo (odvisno od dizajna)
 - VLAN “kjerkoli”
 - VLAN “vozlišče”
- Uporabniški VLAN-i glede na tip storitve (VLAN “storitve”)
 - DATA
 - VOICE
 - WLAN/VoWLAN
 - “ROLE-BASED” (801.x/NAC; guest, auth, quarantine, ..)
- Strežniški VLAN-i
 - L2 vidnost (NIC teaming, HA clustering, ..)
- DHCP za uporabniške VLAN-e



- pravilo 2^N , binarna aritmetika
- Ustrezna IP shema (sumarizacija)
 - sklicevanje na IP naslove (routing, ACL, QoS, SEC, IPT,..)
- VLAN \leftrightarrow IP naslovni prostor
- Povezovalni segmenti (L3, /30)
 - L3 link do pristopnega nivoja
- Menjava IP sheme
- Privatni naslovni prostor
 - 10.0.0.0/8
 - 172.16.0.0 do 172.31.0.0
 - 192.168.0.0 do 192.168.255.0
- 10.(vozlišče).(vlan).0 /24



- 192.168.0.0/24
 - 192.168.1.0/24
 - 192.168.2.0/24
 - 192.168.3.0/24
 - 192.168.4.0/24
 - 192.168.5.0/24
 - 192.168.6.0/24
 - 192.168.7.0/24
- 192.168.0.0/21



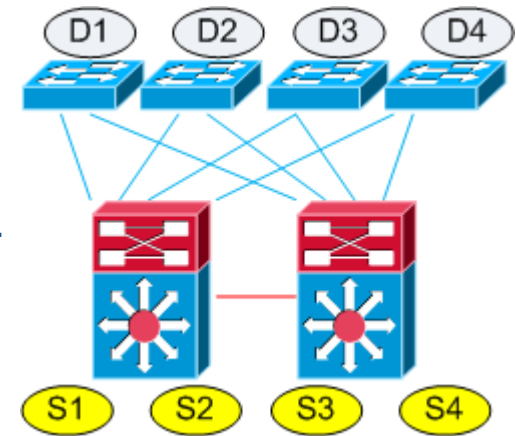
Omrežne storitve



- Osnovne omrežne storitve

Zagotavljajo redundanco in segmentacijo

Switching, VLAN, Routing, STP, FHRP, EtherChannel, DHCP ...



- Razširjene/dodatne omrežne storitve

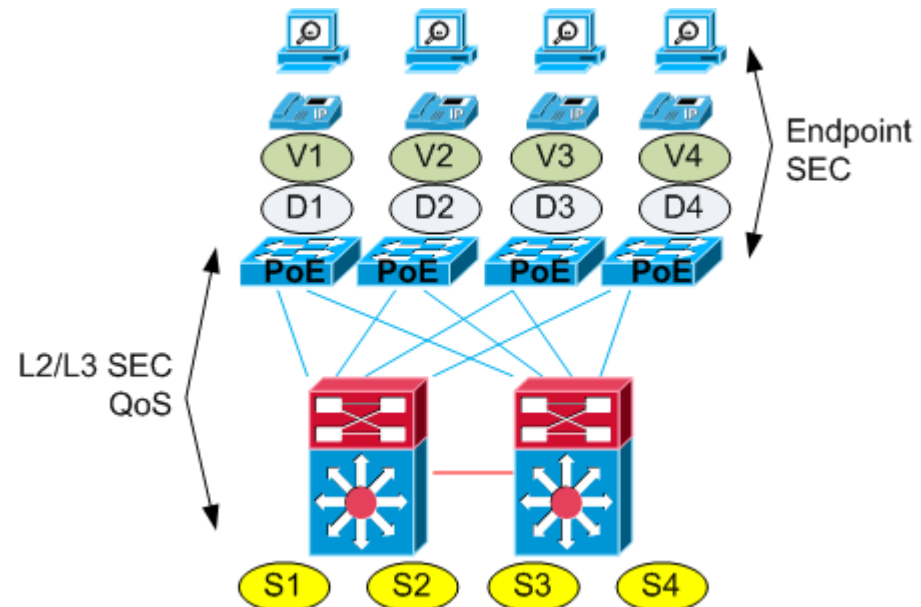
L2/L3 security

QoS

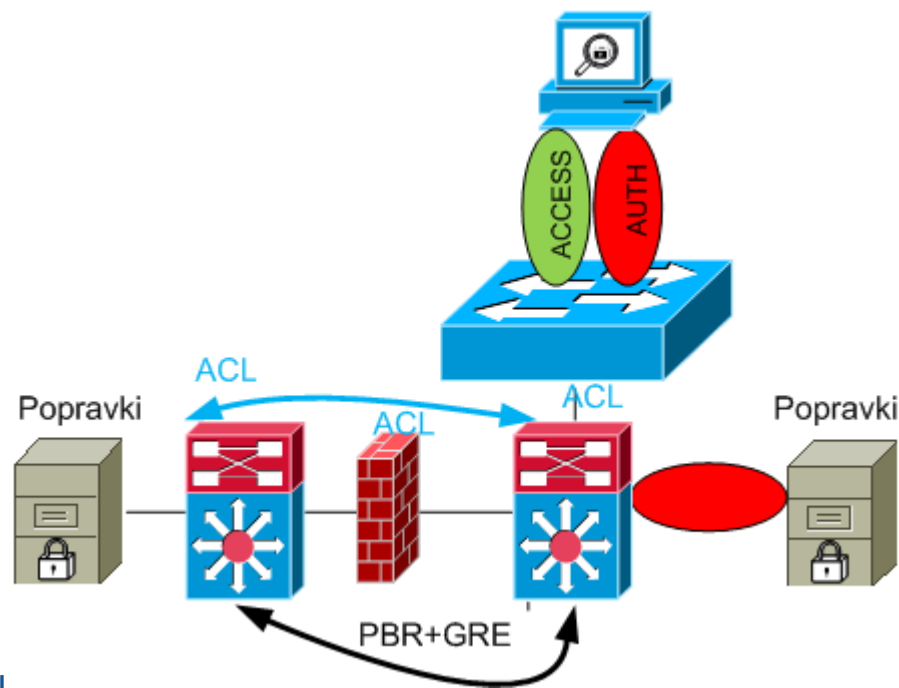
IP telefonija (VOICE VLAN, PoE, QoS, ...)

WLAN

Endpoint Security (SW agenti)



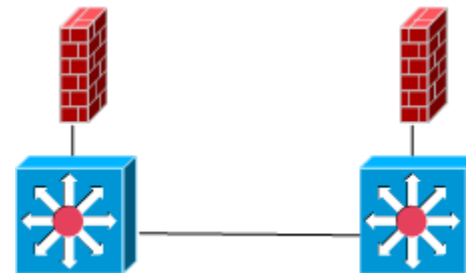
- VLAN, 802.1q trunk
- STP dodatki
- Port Security
- PVLAN
- ACL, VACL
- DHCP snooping
- ARP inspection
- IP Source Guard
- QoS
- 802.1x, NAC
 - Role-Based" VLAN-i
 - Uporabniški port pripada določenemu VLAN-u (access, auth, guest, quarantine, remediation, ...)
 - Uporabniku moramo omogočiti dostop samo do popravkov
 - ACL
 - PBR + GRE
 - NAC Appl. Inband način
- Servisni moduli za modularna stikala (6500)
 - FW, IDS, ACE, WiSM, CSS/SSL, ...
 - Strežniški segment



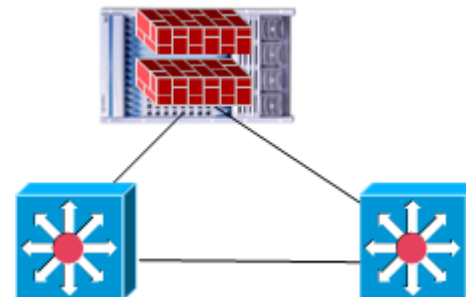
- FW modul za modularno stikalo (6500)



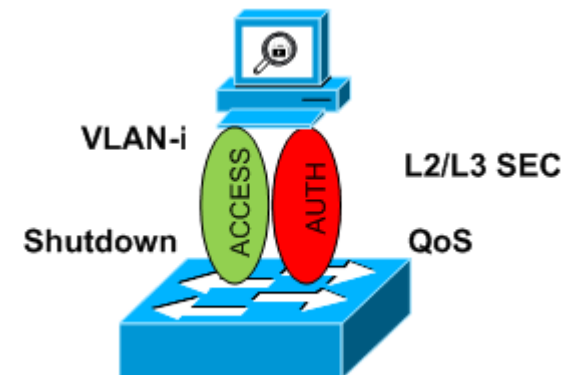
- Zunanji FW



- Zunanje modularno ohišje



- Nov pogled na switch
 - VČASIH (število/tip portov (10/100/1000; UTP/FO) + propustnost)
 - DANES (+ varnostne funkcije)
- Zle namene in napadalce je treba blokirati v prvi možni točki omrežja
 - Shutdown porta na switchu
 - Izoliran VLAN (omejene pravice)
 - QoS policing
 - DHCP snooping, ARP inspection,



- VLAN “kjerkoli”
- VLAN “vozlišče”
- VLAN “storitve”
 - Klasični podatki
 - DATA VLAN
 - IP telefonija
 - VOICE VLAN
 - WLAN;
 - Brez WLAN kontrolerjev; L2 roaming zahteva VLAN “kjerkoli”
 - Z WLAN kontrolerji; ni potrebe po VLAN “kjerkoli”, zaradi tuneliranja med AP in WLC
 - 802.1x, NAC Appliance;
 - Uporabniški “Role-based” VLAN-i
 - CAS v redundanci zahteva L2 vidnost (kluster način)
 - CAM v redundanci zahteva L2 vidnost (kluster način)

- SW agenti z različnimi funkcionalnostmi

- 802.1x, NAC
- SPI FW, Program control
- HIPS
- Anti-X (virus, spyware, malware, ..)
- Oddaljeni dostop (IPSec, SSL)
- Zaščita podatkov
 - Enkripcija diskovnih enot, izmenljivih medijev (FLASH ključi, CD/DVD, in datotečnih direktorijev
 - Kontrola uporabe perifernih naprav (WLAN, Bluetooth, USB, CD/DVD enote, ..)
 - Kontrola dostopa do datotek



- Nov pogled na končno točko v omrežju
 - VČASIH (popravki OS, AV)
 - DANES (+ Endpoint security)
- Nepooblašcene aktivnosti je zelo težko/nemogoče preprečevati na komunikacijski poti (enkripcija, SSL, mobilni uporabniki)
- Kontrola varnosti se seli na končno točko
 - Enkripcija podatkov na medijih, odtekanje informacij
 - IPv6 in IPSec
 - End-to-end enkripcija
- Številne mobilne naprave (OS: Windows Mobile, SmartPhone, Symbian, Palm, Pocket PC, ..)

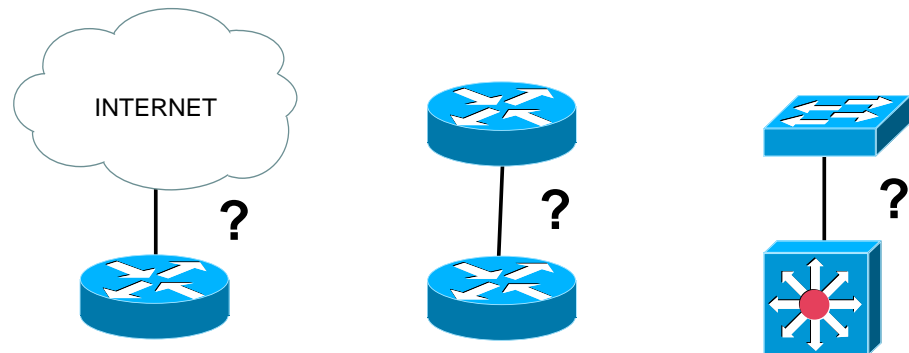


INFORMACIJSKA VARNOSTNA POLITIKA !!

Upravljanje in SLA

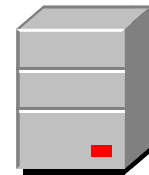


- Povezava do ponudnika internetnih storitev
- Povezava med partnerji (najeti vodi)
- Povezave med vozlišči LAN
- Kaj se dogaja na linkih (obremenjenost, vrsta prometa) ?
 - Ukazi na napravah (show interfaces, ifconfig)
 - Podatki za trenutek opazovanja
- Preverjanje kakovosti storitve/linka (SLA) ?
- Statistika za daljše obdobje
- Zbiranje podatkov
 - SMNP + orodja (MRTG, CACTI, ..)
 - NETFLOW
 - NBAR
 - IP SLA

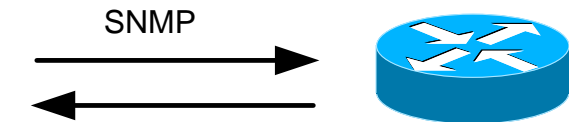


- Prikazuje koliko prometa gre preko omrežnega vmesnika
- Različna časovna obdobja (dnevni, tedenski, mesečni)
- Vhodni (in) in izhodni (out) promet
- Statistika prometa (Max, Average, Current)
- PERL, za UNIX/LINUX, WINDOWS
- Merjenje prometa na linkih med vozlišči

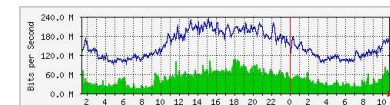
5 minute input rate 2000 bits/sec, 3 packets/sec
 5 minute output rate 1000 bits/sec, 2 packets/sec
 6675110 packets input, 2786553400 bytes, 0 no buffer
 4424267 packets output, 405059623 bytes, 0 underruns



MRTG

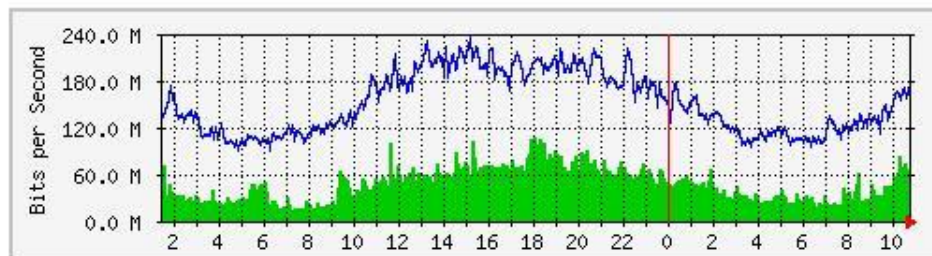


'Daily' Graph (5 Minute Average)



	Max	Average	Current
In	106.2 Mb/s (10.6%)	45.4 Mb/s (4.5%)	65.5 Mb/s (6.6%)
Out	233.2 Mb/s (23.3%)	149.9 Mb/s (15.0%)	180.0 Mb/s (18.0%)

'Daily' Graph (5 Minute Average)



	Max	Average	Current
In	106.2 Mb/s (10.6%)	45.4 Mb/s (4.5%)	65.5 Mb/s (6.6%)
Out	233.2 Mb/s (23.3%)	149.9 Mb/s (15.0%)	180.0 Mb/s (18.0%)

- Detektira aplikacije glede na port (L2-L4)
- Bazira na flow-u (Kdo? Kaj? Kdaj? Kam?)
- Možnost uporabe NETFLOW

analiza novih aplikacij v povezavi z obremenitvijo omrežja

analiza uporabe omrežja (TopTalkers, Accounting, Billing)

detekcija neavtorizirane uporabe WAN linkov, omrežnih virusov in anomalij

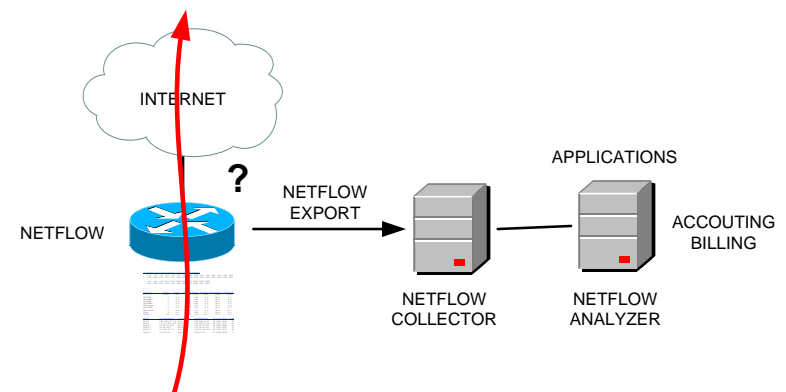
validacija QoS parametrov

- Flow

Source IP address, Destination IP address, Source port, Destination port,

L3 protocol type, TOS byte (DSCP), Input interface (Packets, Bytes, Time stamps)

- Več nadzornih aplikacij za grafični prikaz NETFLOW statistike
- Podpora na usmerjevalnikih in večjih stikalih



NETFLOW CLI in SNMP

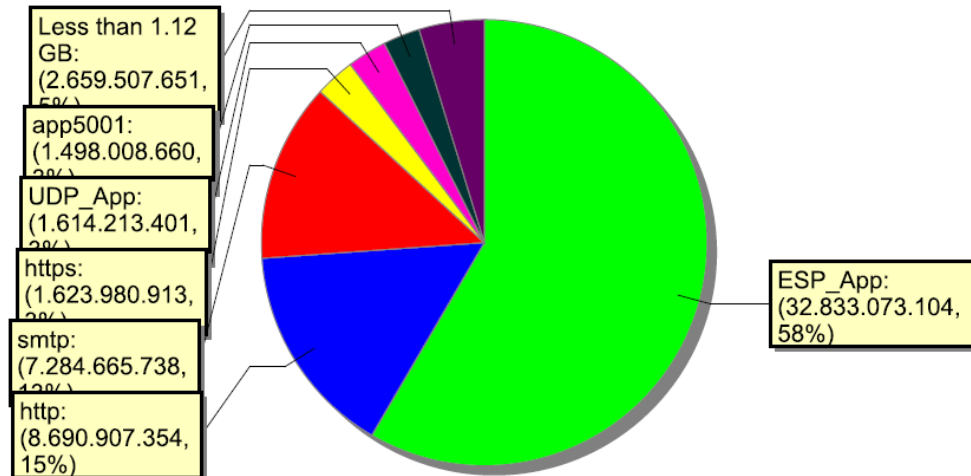
IP packet size distribution (2381 total packets):

1-32	64	96	128	160	192	224	256	288	320	352	384	416	448	480
.092	.000	.003	.000	.141	.048	.000	.000	.000	.093	.000	.000	.000	.000	.000
512	544	576	1024	1536	2048	2560	3072	3584	4096	4608				
.000	.000	.048	.189	.381	.000	.000	.000	.000	.000	.000				

.....

Protocol	Total Flows	Flows /Sec	Packets /Flow	Bytes /Pkt	Packets /Sec	Active (Sec) /Flow	Idle (Sec) /Flow
TCP-FTP	4	0.0	67	840	2.6	59.4	0.7
TCP-SMTP	1	0.0	67	168	0.6	59.4	0.5
TCP-BGP	1	0.0	68	1140	0.6	60.3	0.4
TCP-NNTP	1	0.0	68	1340	0.6	60.2	0.2
TCP-other	7	0.0	68	913	4.7	60.3	0.4
UDP-TFTP	1	0.0	68	156	0.6	60.2	0.1
UDP-other	4	0.0	36	151	1.4	45.6	14.7
ICMP	4	0.0	67	529	2.7	60.0	0.2
Total:	23	0.2	62	710	14.3	57.5	2.9

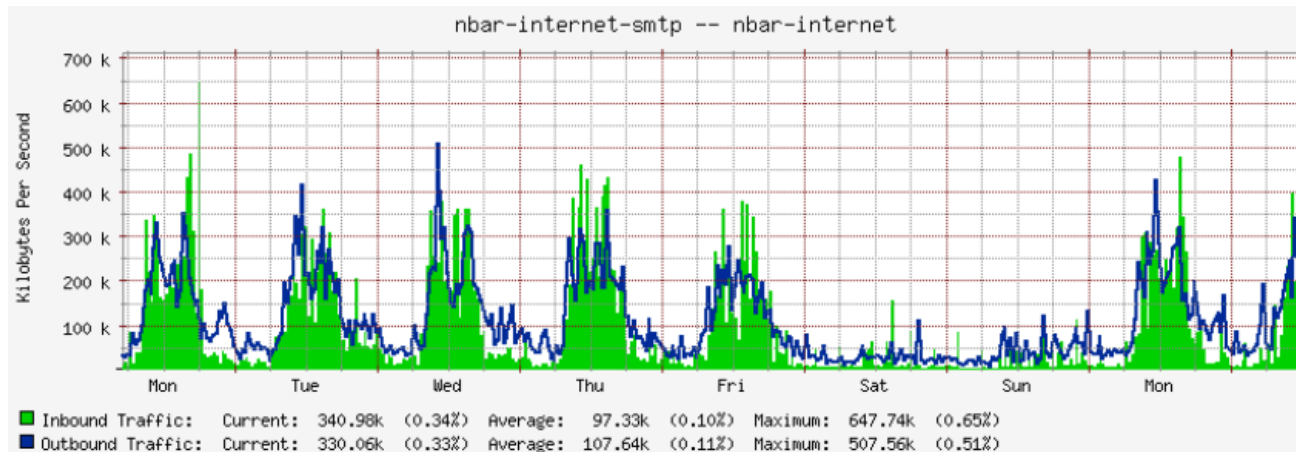
SrcIf	SrcIPaddress	DstIf	DstIPa
Et2/0	192.168.137.78	Et3/0*	192.16
Et2/0	172.19.216.196	Et3/0*	192.16
Et0/0.1	10.56.78.128	Et1/0.1	172.16
Et0/0.1	10.10.18.1	Et1/0.1	172.16
Et0/0.1	10.162.37.71	Et1/0.1	172.16
Et0/0.1	172.16.6.1	Null	224.0.



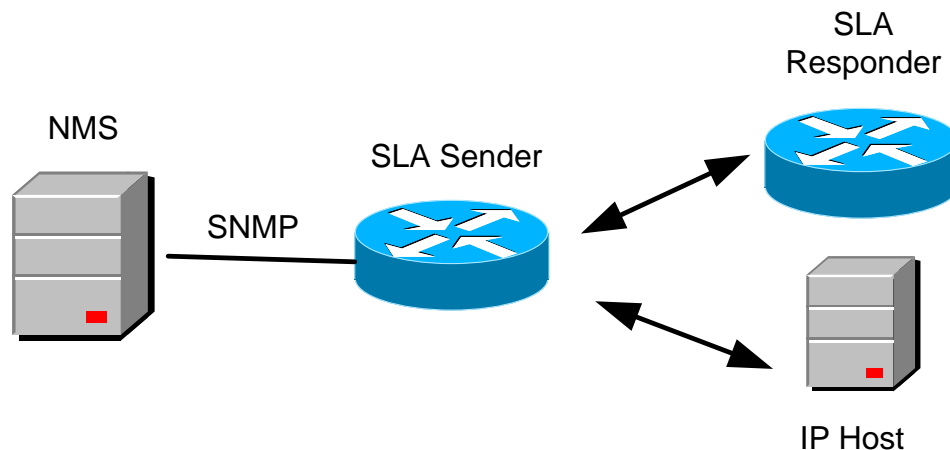
- Prepoznavanje aplikacij na OSI L3-L7 v realnem času
 - aplikacije, ki uporabljajo statične porte
 - aplikacije, ki uporabljajo dinamične porte (Stateful Inspection, Traffic Patterns)
- Možnost uporabe NBAR
 - QoS (classification, policing, marking, limiting, dropping)
 - Accounting
- Realtime statistika glede na vmesnik in servis (Bit rate (bps), Packet counts, Byte counts)
- Možnost definiranja vzorca za lastne aplikacije (npr. HTTP aplikacije)
- NBAR MIB, statistika za aplikacije na vmesnik preko SNMP
- Več nadzornih aplikacij za grafični prikaz NBAR statistike
- Podpora na usmerjevalnikih (Branch)

FastEthernet6/0

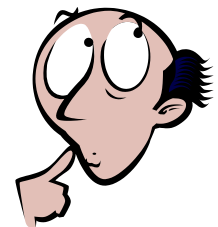
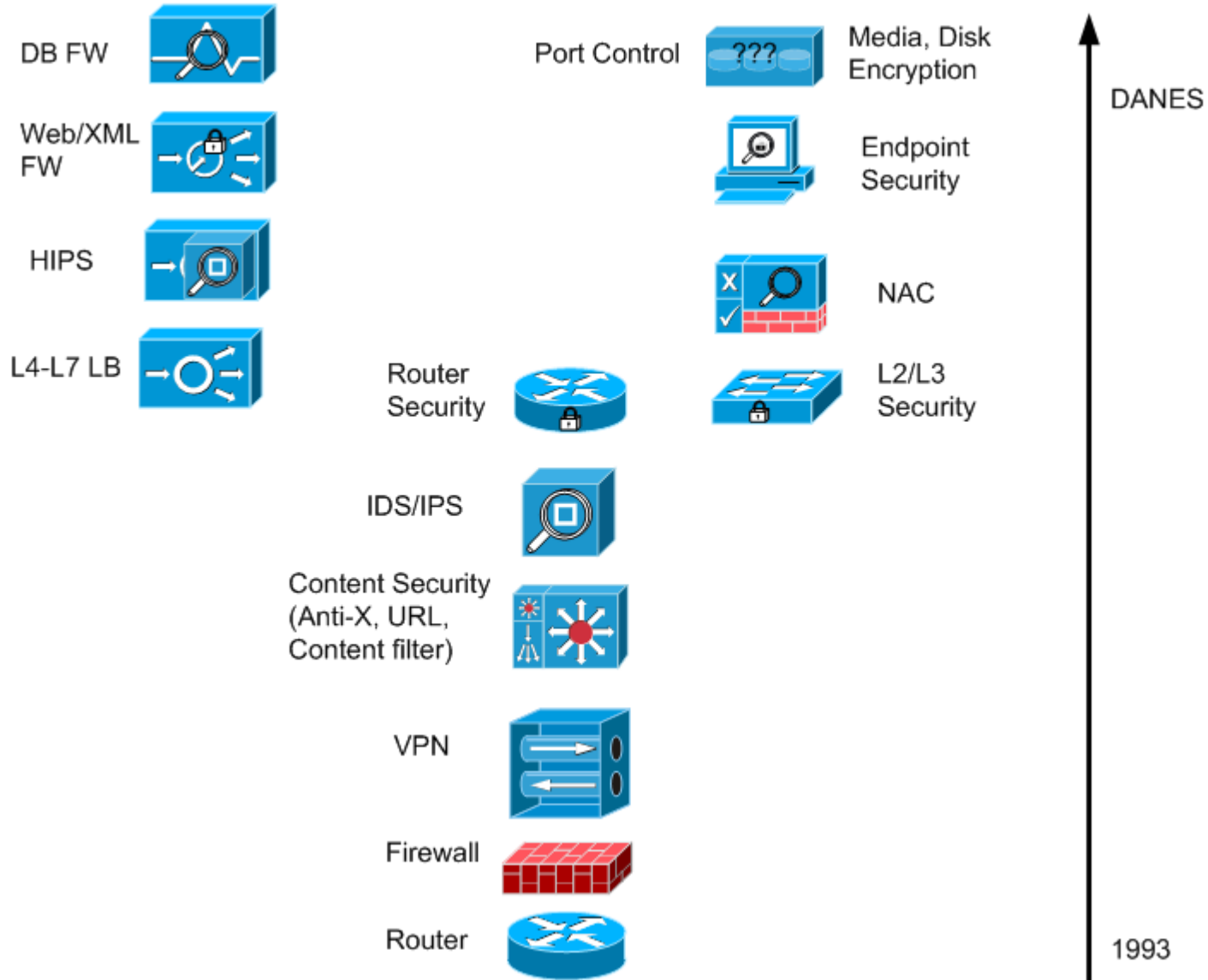
	Input	Output
<u>Protocol</u>	Packet Count Byte Count 5 minute bit rate (bps)	Packet Count Byte Count 5 minute bit rate (bps)
<u>http</u>	316773 26340105 3000	0 0 0
<u>Pop</u>	34437 2301891 3000	7367 339213 0
<u>Snmp</u>	279538 319106191 0	14644 673624 0
<u>ftp</u>	8979 906550 0	7714 694260 0
....		
....		
<u>Total</u>	17203819 19161397327 4179000	151684936 50967034611 6620000



- Zbiranje informacij
 - Delay (round-trip, one-way), Jitter (\rightarrow S2D, \leftarrow D2S)
 - Packet loss (directional), Packet sequencing/ordering
 - Path (per hop), Connectivity (directional)
 - Voice quality scoring, Application performance, Server response time
- Umeten promet, zbiranje informacij v realnem času
- Kontrola/verifikacija/merjenje SLA, preverjanje QoS
- SLA Sender (IOS naprava)
- SLA Responder (IOS naprava ali IP host)
- Nadzorna postaja (Cisco RTTMON MIB)



Nedokončana zgodba



Učinkovite IT rešitve za modre odločitve

Z vami in za vas v prihodnost ...

S&T Slovenija

Kontakti:

matija.brglez@snt.si

marko.rahne@snt.si

Informacijska varnostna politika:

matej.saksida@snt.si

**We
love
IT**