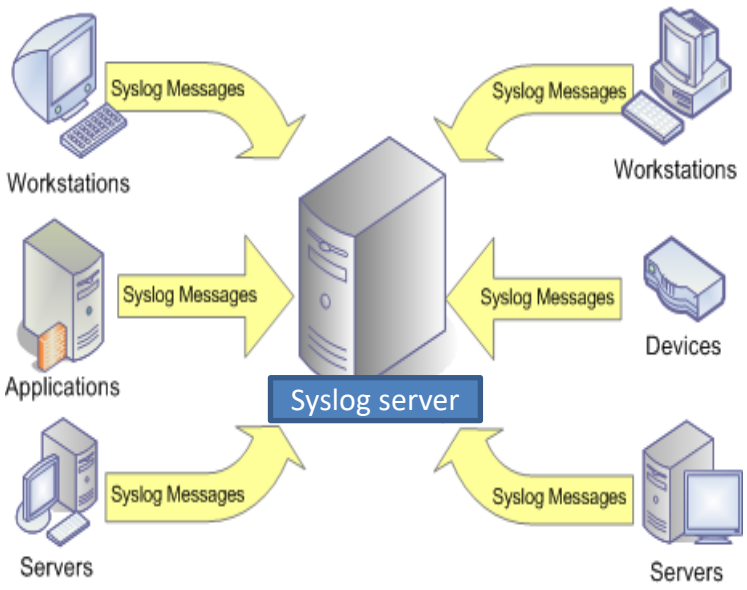
PREDMET:
MREŽNI SERVISI

Syslog servis

Dr Dušan Stefanović CCNA, CCNA Security,CCNP
Visoka Tehnička Škola - Niš

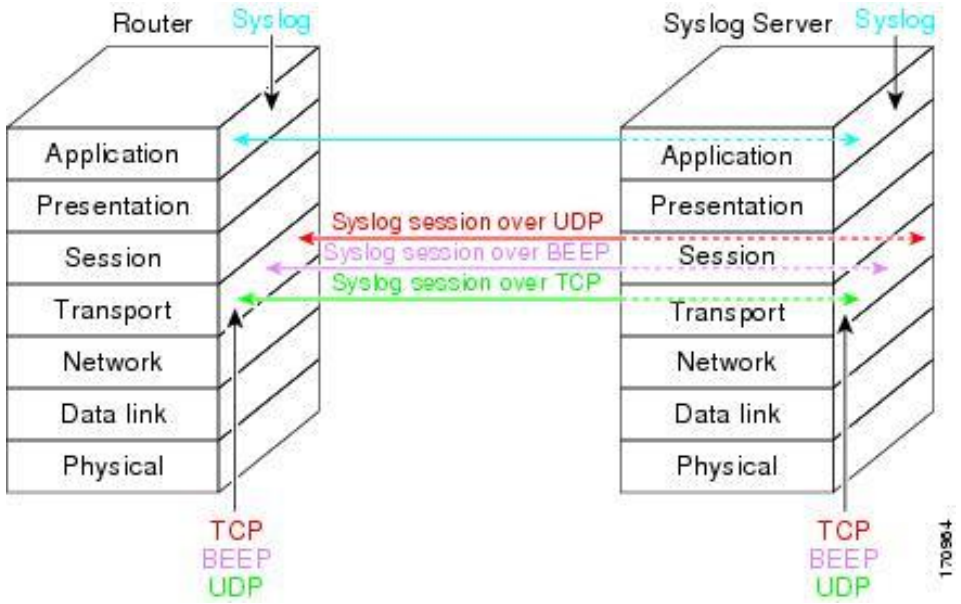
UVOD U SYSLOG SERVIS

- Syslog servis je industrijski standard za prosleđivanje log poruka preko IP mreže na centralnom serveru.
- Syslog je standardizovan 2009 od strane IETF.
- Syslog je klijent server protokol
- Na klijentskoj strani aplikacije izvršava se softver koji generiše poruku na osnovu događaja na uređaju
- Na serverskoj strani servisa izvršava se softver koji obrađuje, analizira i skladišti poruke pristigle sa različitih IP uređaja(ruteri, svičevi, štampači, serveri,...)
- Osnovna prednost syslog servisa je integracija log poruka sa različitih IP uređaja na jednom mestu.



KARAKTERISTIKE SYSLOG PROTOKOLA

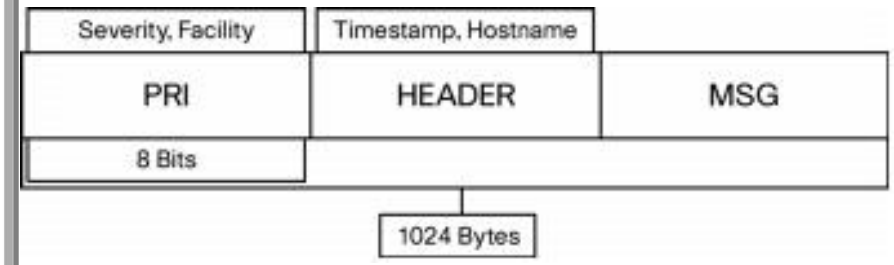
- Syslog protokol na transportnom sloju može se enkapsulirati u **TCP** ili **UDP** protokol
- Syslog port na transportnom sloju je **514**
- Poruke se šalju u čistom tekstu, nisu kriptovane.
- SSl može da se koristi kako bi se obezbedila kripcija podataka prilikom prenosa logova
- Syslog servis je podržan od velikog broja proizvođača mrežne opreme



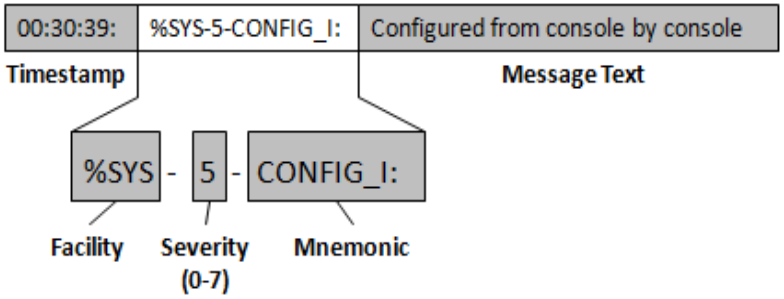
FORMAT SYSLOG PORUKE

- Syslog poruka sastoji se iz tri segmenta
  - 8-bitna priority vrednost (opisuje važnost poruke)
  - Zaglavlje (vreme kada je kreirana poruka i IP adresa uređaja koji je poslao poruku)
  - Poruka
- Klijentska strana aplikacije maksimalno može da pošalje 1024 Byte tekstualne poruke ka syslog serveru

Opis Strukture Syslog poruke



Primer Syslog poruke



Identifikacija servisa/uređaja (Facility levels)

- Log poruke su obeležene tzv. ***facility* kodom** (auth, authpriv, daemon, cron, ftp, lpr, kern, mail, news, syslog, user, uucp, local0 ... local7) koji ukazuje na vrstu softvera koji je kreirao log
- Syslog facility je softversko okruženje koje kreira log poruke, a predstavlja način da odredimo koji proces tj. mašina je kreirala poruku
- Mapiranje između Facility koda i softvera koji kreira log nije uniformna već zavisi od različitih syslog implementacija

Facility Number	Keyword	Facility Description
0	kern	kernel messages
1	user	user-level messages
2	mail	mail system
3	daemon	system daemons
4	auth	security/authorization messages
5	syslog	messages generated internally by syslogd
6	lpr	line printer subsystem
7	news	network news subsystem
8	uucp	UUCP subsystem
9		clock daemon
10	authpriv	security/authorization messages
11	ftp	FTP daemon
12	-	NTP subsystem
13	-	log audit
14	-	log alert
15	cron	clock daemon
16	local0	local use 0 (local0)
17	local1	local use 1 (local1)
18	local2	local use 2 (local2)
19	local3	local use 3 (local3)
20	local4	local use 4 (local4)
21	local5	local use 5 (local5)
22	local6	local use 6 (local6)
23	local7	local use 7 (local7)

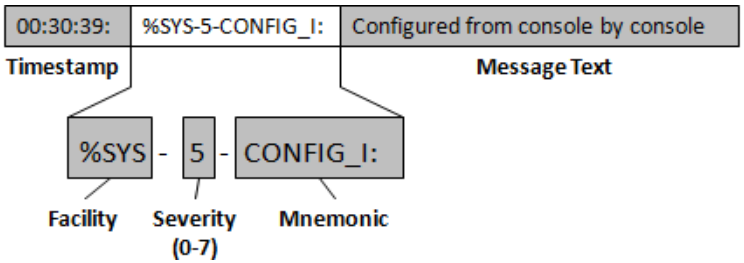
KATEGORIZACIJA SYSLOG PORUKA (Severity levels)

Log poruke se kategorišu na osnovu važnosti samog događaja.

Log poruke se svrstavaju u jedan od 8 nivoa.

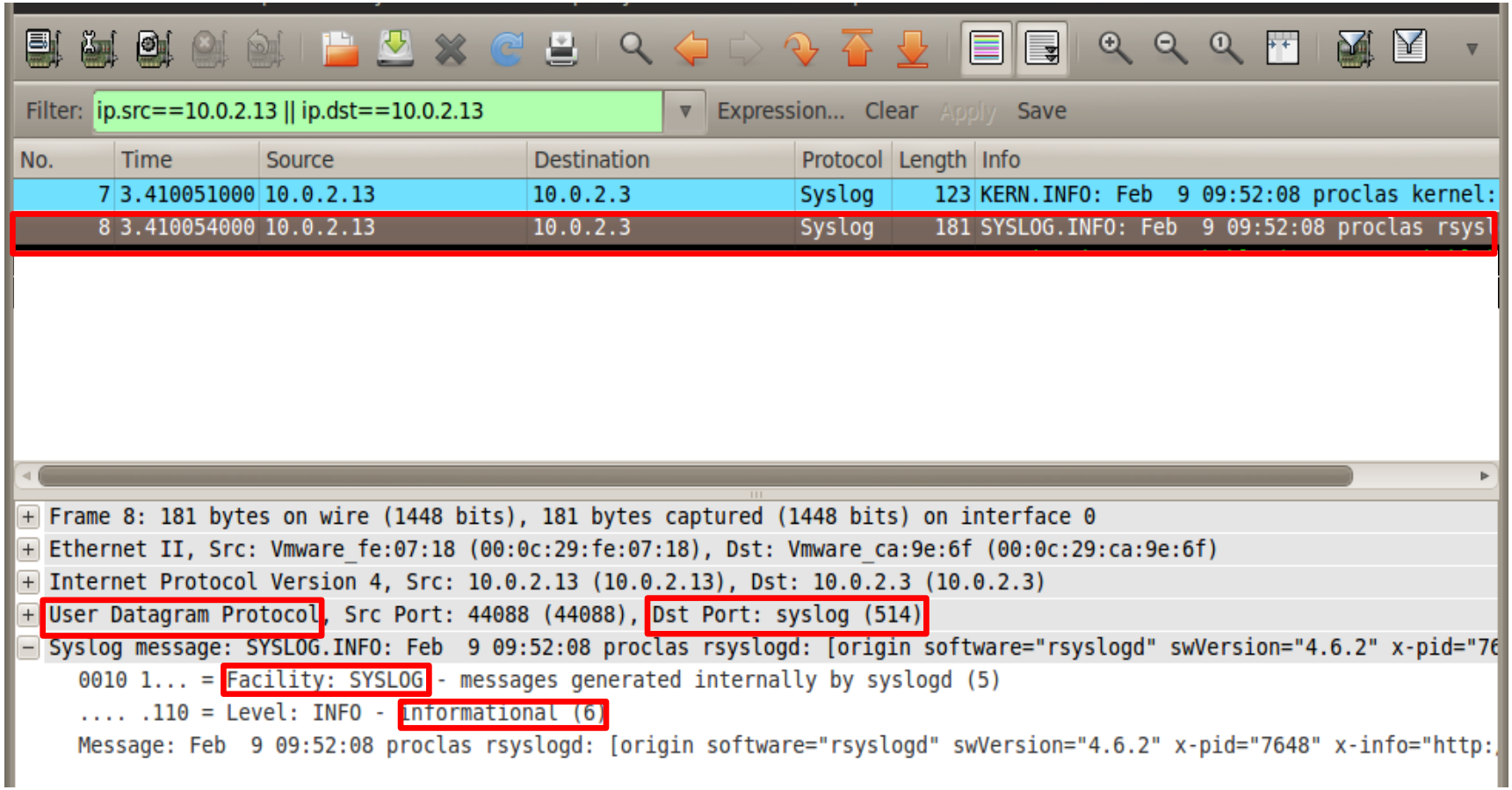
Code	Severity	Keyword	Description	General Description
0	Emergency	emerg (panic)	sistem je neupotrebljiv	Najozbiljniji nivo upozorenja, obično zahteva hitnu reakciju
1	Alert	alert	Hitno mora da se preduzme nešto	Primer je otkaz primarne konekcije ka provajderu
2	Critical	crit	Kritični događaj	Ukazuje obično na otkaz backup sistema, primer je otkaz backup konekcije ka ISP
3	Error	err (error)	Ukazuje na grešku u sistemu	Nije hitan problem, ali je potrebno rešiti u što kraćem roku
4	Warning	warning (warn)	Upozorenje	Nije greška već upozorenje koje može dovesti do otkaza ako se ne preduzme odgovarajuća akcija, primer hard disk je 85% pun
5	Notice	notice	Normalno ali bitno obaveštenje	Signalizira događaje koji nisu toliko česti, ne predstavljaju grešku
6	Informational	info	Informacione poruke	Uobičajne operacione poruke, zadavanje IP adrese, merenje propusnog opsega,...
7	Debug	debug	debug poruke	Ovu opciju koriste developeri prilikom testiranja aplikacije

Priority polje



- Svaka syslog poruka sadrži polje priority (prioritet)
- ***PRI*** je osmobitni broj koji je sastavni deo syslog poruke.
- Vrednost se kreće od 0 – 191 i formira se od facility koda i severity koda
- Prva tri bita najmanje težine identifikuju kategoriju (severity) poruke.
- Sa tri bita možemo da opišemo 8 različitih kategorija.
- Ostali biti (5) predstavljaju facility kod.
- Filtriranje određenih syslog poruka možemo da radimo ukoliko znamo ove vrednosti
- **Priority vrednost = Facility*8 + Severity Level**
- Primer: local use 4 (iz tabele je vrednost 20) sa Notice severity porukom 5 imaće priority vrednost 20*8 + 5 = 165

PRIKAZ SNIMLJENE SYSLOG PORUKE



BEZBEDNOST (1)

- Autentifikacija
  - Syslog nema mehanizam za autentifikaciju syslog klijenta
  - Napadač može da pošalje syslog poruku
- Nadgledanje poruke
  - Poruka se šalje nekriptovana(clear-text)
- Bombardovanje syslog servera
  - Napadač može da sprovede Denial of Service napad, na taj način što će beznačajnim porukama napuniti hard disk syslog servera.
- Integritet poruke
  - Napadač može da promeni log poruku koja je poslata syslog serveru.

CISCO RUTER (LOGGING PORUKE)

Sistemske poruke o greškama (System error messages) kontroliše logging proces koji ove poruke može da šalje na različite destinacije

-- **Logging buffer** (lokalni bafer) je interna memorija uređaja. Kod većine uređaja je isključeno slanje log poruka u bafer. Ne preporučuje se zbog korišćenja resursa samog uređaja

-- **Logging console,** prosleđuje syslog poruke preko terminalnih linija (tty)

-- **Logging monitor**, prosleđuje syslog poruke preko virtualne linije (vty)

-- **Logging host**, prosleđuje syslog poruke udaljenom serveru. Sistemske poruke kao i debug poruke prosleđuju se udaljenom hostu.

R(config)# logging host 10.10.10.10

ili

R(config)# logging 10.10.10.10

CISCO LOGGING KOMANDE

R(config)# logging trap <level>

R# show logging (samo ova komanda se koristi za proveru loggin konfiguracije)

Koristi se da ograničimo koju kategoriju poruka šaljemo syslog serveru

Syslog serveru se podrazumevano šalju kategorije poruka od 0(emergency) – 6 (informational)

Kada se konfiguriše nivo, sve poruke tog nivoa i ispod se šalju syslog serveru

Primer: logging trap 4, slaće log poruke 0 – 4(warrning)

CISCO LOGGING KOMANDE

R(config)# logging source interface loopback 0

Ovom komandom želimo da syslog klijent log poruke šalje sa definisanom izvorišnom adresom

Na ovaj način lakše možemo da utvrdimo sa kog uređaja je primljena log poruka

Ruter će izabrati izvorišnu IP adresu koja je najbliža syslog serveru ukoliko ne koristimo gornju komandu

R(config)# logging origin-id <hostname|IP|string>

Koristi se kao dodatni identifikator log poruke koja se šalje syslog serveru

Dodaje se na početku log poruke (ne u hederu syslog poruke)

Identifikator može biti hostname, IPv4 adresa, bilo koji text

PREDNOST UPOTREBE SYSLOG SERVEREA

- Prednost upotrebe syslog servera u odnosu na lokalno čuvanje log poruka je višestruko
  - Reboot uređaja briše sve poruke
  - Kada se bafer napuni, svaka nova poruka briše najstariju iz bafera (duplex mismatch poruka) može da obriše sve bitne log poruke
- Syslog server nam omogućava čuvanje log poruka na duži period, čak i trajno.
- Syslog server ima svoj Timestamp ali prikazuje i timestamp uređaja koji je poslao log poruku. To je dobro za uređaje koji nemaju sihronizovano vreme.
- Syslog server nam obezbeđuje alate za sortiranje i pretragu log poruka
- Rešavanje problema je znatno lakše ukoliko se koristi syslog server

- Obaranje interfejsa (shutdown), generisaće level 3 (error) poruku
- Podizanje interfejsa (no shutdown), generisaće level 5 (notofication) poruku
- Promena časovnika (clock set), generisaće level 6 (informational) poruku
- Brisanje brojača sa interfejsa (clear counters), generisaće level 5 poruku

Code	Severity	Keyword	Description	General Description
0	Emergency	emerg (panic)	sistem je neupotrebljiv	Najozbiljniji nivo upozorenja, obično zahteva hitnu reakciju
1	Alert	alert	Hitno mora da se preduzme nešto	Primer je otkaz primarne konekcije ka provajderu
2	Critical	crit	Kritični događaj	Ukazuje obično na otkaz backup sistema, primer je otkaz backup konekcije ka ISP
3	Error	err (error)	Ukazuje na grešku u sistemu	Nije hitan problem, ali je potrebno rešiti u što kraćem roku
4	Warning	warning (warn)	Upozorenje	Nije greška već upozorenje koje može dovesti do otkaza ako se ne preduzme odgovarajuća akcija, primer hard disk je 85% pun
5	Notice	notice	Normalno ali bitno obaveštenje	Signalizira događaje koji nisu toliko česti, ne predstavljaju grešku
6	Informational	info	Informacione poruke	Uobičajne operacione poruke, zadavanje IP adrese, merenje propusnog opsega,...
7	Debug	debug	debug poruke	Ovu opciju koriste developeri prilikom testiranja aplikacije