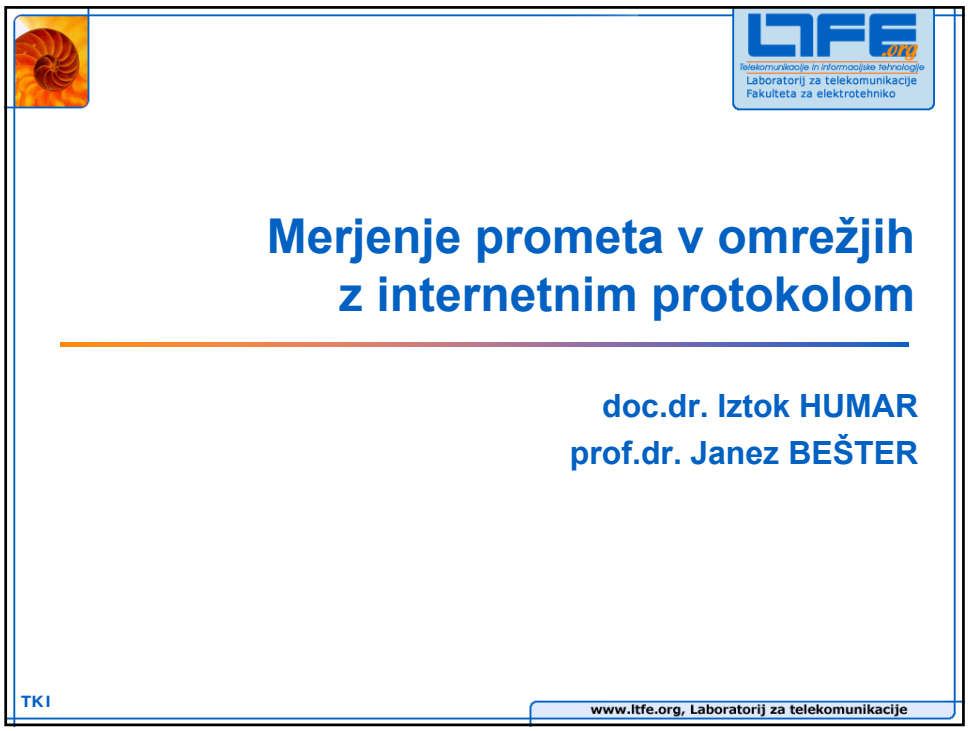
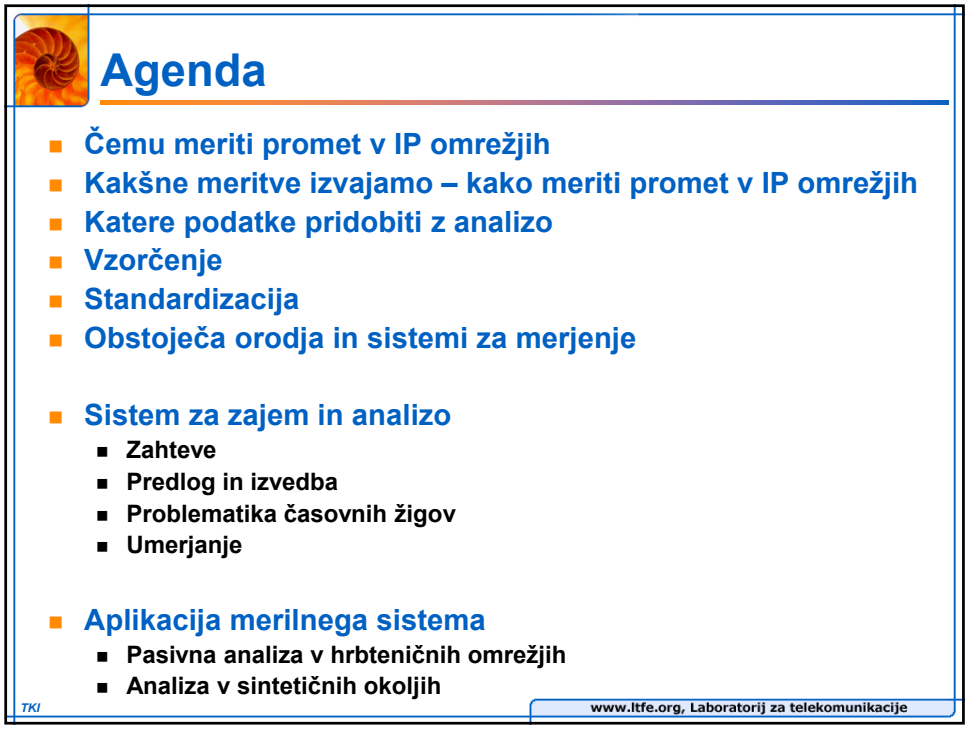
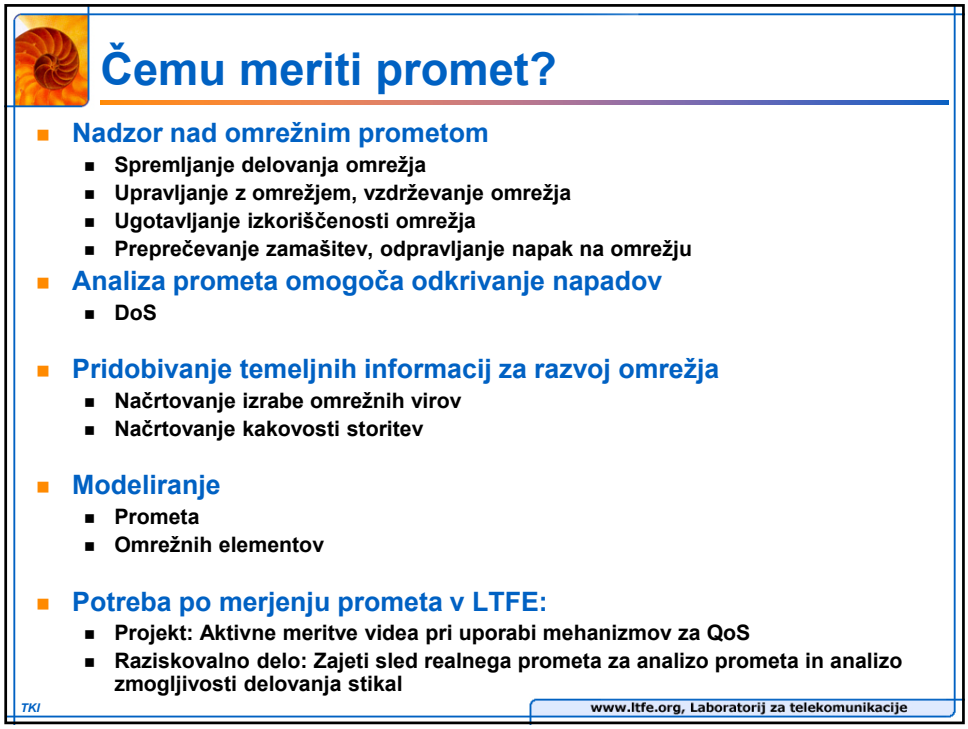
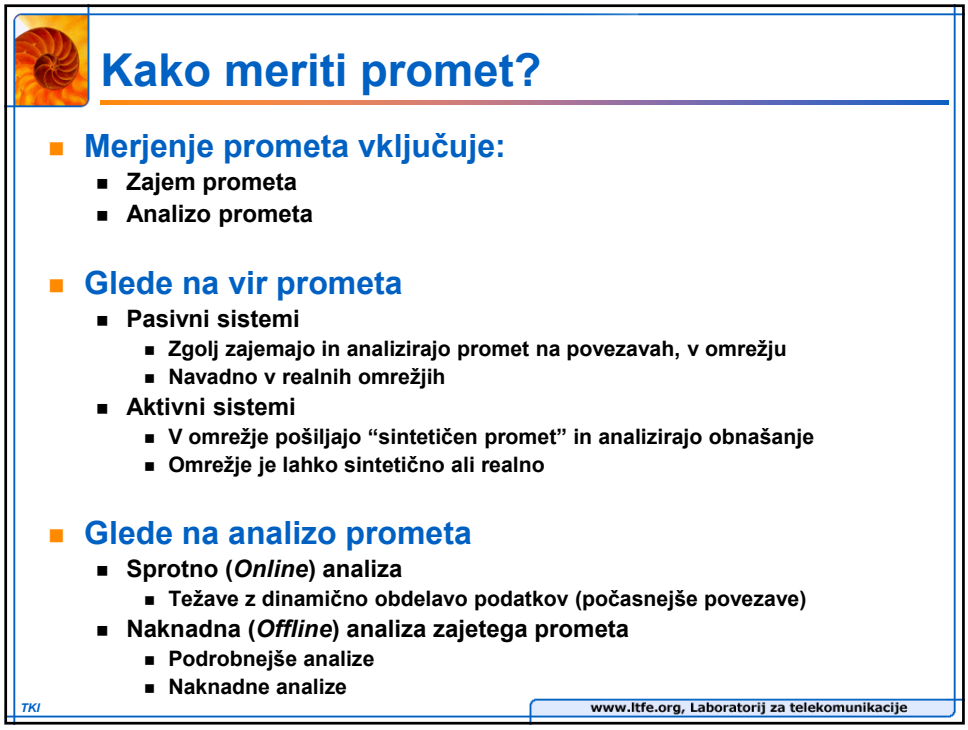

Laboratorij za telekomunikacije
Fakulteta za elektrotehniko
Merjenje prometa v omrežjih
z internetnim protokolom
doc.dr. Iztok HUMAR
prof.dr. Janez BEŠTER
TKI
www.ltfe.org, Laboratorij za telekomunikacije


Agenda
Čemu meriti promet v IP omrežjih
Kakšne meritve izvajamo – kako meriti promet v IP omrežjih
Katere podatke pridobiti z analizo
Vzorčenje
Standardizacija
Obstoječa orodja in sistemi za merjenje
Sistem za zajem in analizo
Zahteve
Predlog in izvedba
Problematika časovnih žigov
Umerjanje
Aplikacija merilnega sistema
Pasivna analiza v hrbteničnih omrežjih
Analiza v sintetičnih okoljih
TKI
www.ltfe.org, Laboratorij za telekomunikacije



Čemu meriti promet?

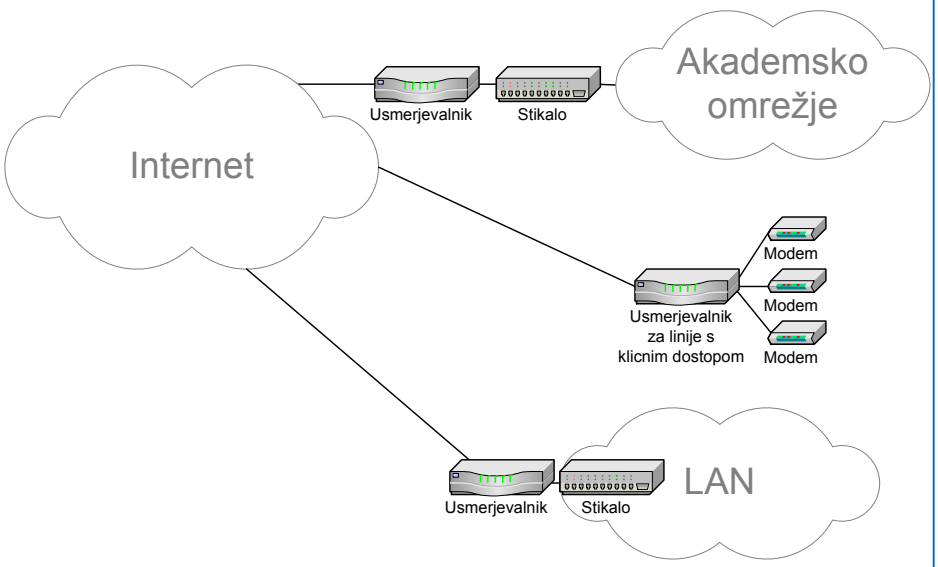
- **Nadzor nad omrežnim prometom**
  - Spremljanje delovanja omrežja
  - Upravljanje z omrežjem, vzdrževanje omrežja
  - Ugotavljanje izkoriščenosti omrežja
  - Preprečevanje zamašitev, odpravljanje napak na omrežju
- **Analiza prometa omogoča odkrivanje napadov**
  - DoS
- **Pridobivanje temeljnih informacij za razvoj omrežja**
  - Načrtovanje izrabe omrežnih virov
  - Načrtovanje kakovosti storitev
- **Modeliranje**
  - Prometa
  - Omrežnih elementov
- **Potreba po merjenju prometa v LTFE:**
  - Projekt: Aktivne meritve videa pri uporabi mehanizmov za QoS
  - Raziskovalno delo: Zajeti sled realnega prometa za analizo prometa in analizo zmogljivosti delovanja stikal



Kako meriti promet?

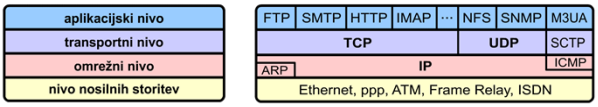
- **Merjenje prometa vključuje:**
  - Zajem prometa
  - Analizo prometa
- **Glede na vir prometa**
  - Pasivni sistemi
    - Zgolj zajemajo in analizirajo promet na povezavah, v omrežju
    - Navadno v realnih omrežjih
  - Aktivni sistemi
    - V omrežje pošiljajo “sintetičen promet” in analizirajo obnašanje
    - Omrežje je lahko sintetično ali realno
- **Glede na analizo prometa**
  - Sprotno (*Online*) analiza
    - Težave z dinamično obdelavo podatkov (počasnejše povezave)
  - Naknadna (*Offline*) analiza zajetega prometa
    - Podrobnejše analize
    - Naknadne analize

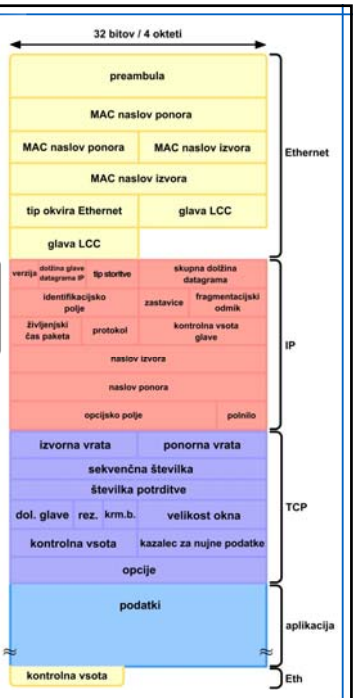
Topologija omrežja z internetnim protokolom



Zajemani podatki

- **Podatki iz glave:**
  - **mrežnega nivoja IP**
  - **transportnega nivoja**





- **Časovni žig:**

```
7.12.2012, 8:12:23.253845
```

Merjeni in analizirani podatki

- **Analiza časovnih žigov, štetje datagramov**
  - Določanje števila prenesenih datagramov v časovnem intervalu
  - Usmerjevalniki: število paketov na sekundo (10000 - 10^7)
- **Analiza časa med prihodi paketov (interarrival time)**
  - Obremenitev stikal, usmerjevalnikov
- **Merjenje obhodnega časa in enosm. zakasnitev v omrežju**
- **Merjenje avtokorelacijske funkcije**
  - Ugotavljanje *dolgoročne odvisnosti* (LRD): $r(k) \approx Ck^{-\beta}$, ko gre $k \to \infty, 0 < \beta < 1$
  - Ugotavljanje *kratkoročne odvisnosti* (SRD): $r(k) \sim \rho^k, 0 < \rho < 1 \quad \sum_k r(k) < \infty$
- **Analiza samopodobnosti (*Hurst* parameter)**
  - X ima samopodobne lastnosti s parametrom H, če velja, da ima za vsak pozitiven m enako porazdelitev kot X, le da je ta m-krat skalirana

$$X_n = m^{-H} \sum_{i=(n-1)m+1}^{nm} X_i = m^{-H} X^{(m)}; \quad 0{,}5 \le H \le 1$$

Merjeni in analizirani podatki

- **Analiza velikosti datagramov**
  - Določitev povprečne velikosti paketov
  - Določitev porazdelitve števila paketov glede na velikost paketa
  - Določitev bitne hitrosti na merjeni povezavi v posamezno smer
- **Analiza naslovov omrežnega nivoja**
  - Podatki o kdo komunicira s kom (vloge sistemov)
  - Koliko prometa izvira/konča na istem sistemu
  - Simetričnost prometa
- **Analiza življenskega časa paketa**
  - Preko koliko usmerjevalnikov je prepotoval datagram
  - Različne začetne vrednosti

OS	TTL
Windows 95	32
Digital OSF	60
Linux, Sun OS	64
Windows 98, NT, 2000	128

Merjeni in analizirani podatki

- **Analiza protokola**
  - Grobo sklepanje na tip aplikacij
    - TCP – potrjevanje
    - UDP – slepo nadgrajuje IP
  - Obnašanje prometa je povezano s protokolom
    - TCP – elastičen promet
    - UDP – pretočni promet
- **Analiza naslovov transportnega nivoja**
  - Podatki o aplikacijah
  - Potrebna analiza glav transportnega nivoja
    - večja količina zajetih podatkov
    - zamudnejša analiza
- **Analiza tokov**

  Tok (*flow*) = Zaporedje koreliranih paketov (denimov v TCP povezavi)
  - Analiza izvorov/ciljev
  - Analiza določine tokov (bitih), porazdelitev
  - Analiza trajanja tokov, porazdelitev

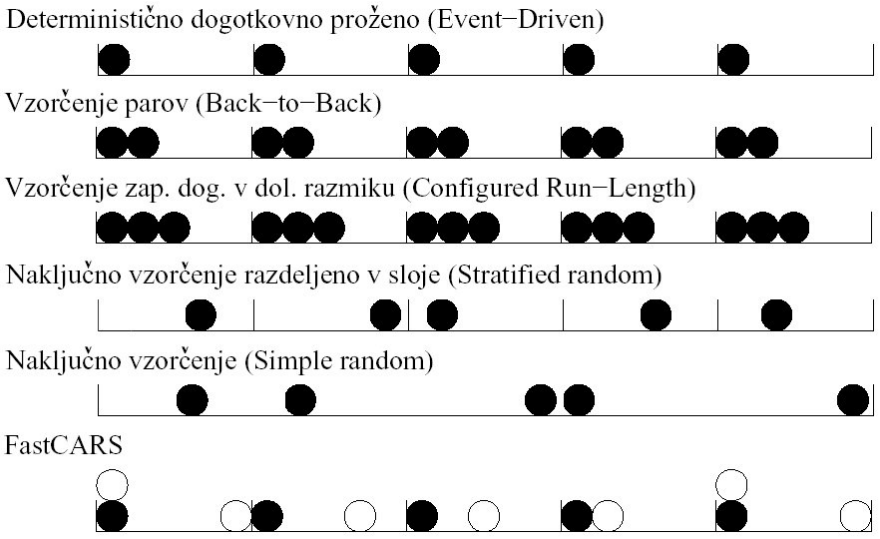
Merjenje z vzorčenjem

- **Omogoča izvajanje analize parametrov z uporabo bistveno krajših zajetih sledi.**
- **Zahteve:**
  - analiza vzorcev naj omogoča čimbolj točno merjenje statističnih parametrov celotne sledi
  - tehniko vzorčenja mora biti mogoče implementirati na čim bolj enostaven način
  - vzorci naj omogočajo določitev korelacije med zaporednimi datagrami in korelacijo med datagrami, ki so dlje narazen
- **Dogodki, ki prožijo zajem vzorca:**
  - časovnik (*timer-driven sampling*)
  - števec (*packet-driven sampling*)

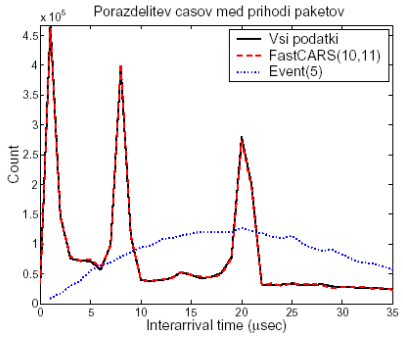
Tehnike vzorčenja

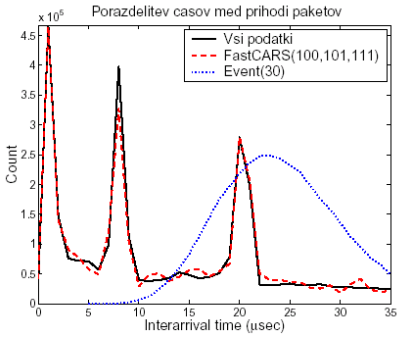
- **Deterministično dogodkovno proženo vzorčenje**
  - **event-driven sampling:** Event(p)
  - **Vzorce zajemamo v intervalih** $0, p, 2p$
- **Vzorčenje več zaporednih dogodkov v določenem razmiku**
  - **configured run-level sampling:** Conf(p, q)
  - **Vzorce zajemamo v intervalih** $kp, (kp + 1), ..., (kp + q - 1)$
- **Vzorčenje zaporednih parov**
  - **back-to-back sampling:**
    - back-to-back(p) = Conf(p, 2), **vzorce zajemamo v intervalih:** $0, 1, p, (p + 1), 2p$
    - back-to-back(p, s), **vzorce zajemamo v intervalih:** $0, s, p, (p + s), 2p, (2p + s)$
- **Naključno vzorčenje**
  - **razdeljeno v sloje (*stratified random sampling*)**
  - **enostavno naključno vzorčenje (*simple random sampling*)**
- **Hitra metoda vzorčenja, ki upošteva korelacijo: FastCARS**
  - **Fast, correlation-aware sampling method:** FastCARS(p_1, p_2, ..., p_n)
  - **Vzorce zajemamo v intervalih** $p_1, p_2, ... , p_n$; p_i **tuja števila ali praštevila**

Tehnike vzorčenja



Primerjava različnih tehnik vzorčenja





- Z vzorčenjem po metodi FastCARS izmerimo bistveno bolj točno oceno porazdelitve časov med prihodi datagramov, pri čemu ne gre spregledati dejstva, da je število vzorcev pri uporabi metode FastCARS(10,11) (713435) celo nekoliko manjše od števila vzorcev pri uporabi metode Event(5) (747407).

Standardi

- Internet Engineering Task Force
  - Internet Protocol Performance Metrics – IPPM
    - Internet Draft dokumenti (6)
    - RFC dokumenti (9)
- Cooperative Association for Internet Data Analysis
  - + Univerza v Michiganu + ponudnik internet dostopa Merit Network
  - Internet Performance Measurement and Analysis – IPMA
    - Merjenje internetne statistike za potrebe zagotavljanja stabilnosti pri usmerjanju, nadzora topologije in merjene ter vizualizacijo merjenih zmogljivosti.
    - Izdelali so priporočilo za izvajanje meritev in analizo statističnih podatkov, ter izdelali eksperimentalno študijo o stabilnosti interneta v primeru izpada hitrih hrbteničnih povezav za Ameriko.
- IP Network Management and Performance Deptartment, AT&T
  - AT&T Network Measurement Tools
    - Zajem: *PacketScope* + *Cisco NetFlow* oziroma *Traffic Aggregation Probe*
    - Analiza
    - Podatki za nadzor in upravljanje AT&T hrbtenice

Orodja

- **Pasivna orodja**
  - SNMP Agenti
  - tcpdump
  - NetFlow
- **Aktivna orodja**
  - ping
  - traceroute
- **Sistemi**
  - Dag merilna kartica
  - IPMON
  - Tstat

LTFE TestCenter

- **Test and verification lab**

  Critical mass of knowledge, experience and top-level equipment, R&D support
  Academic research – B.Sc. And Ph.D. students
  Industry partners and organizations

- **Test and verification services, R&D**

  Celovito testiranje in verifikacija

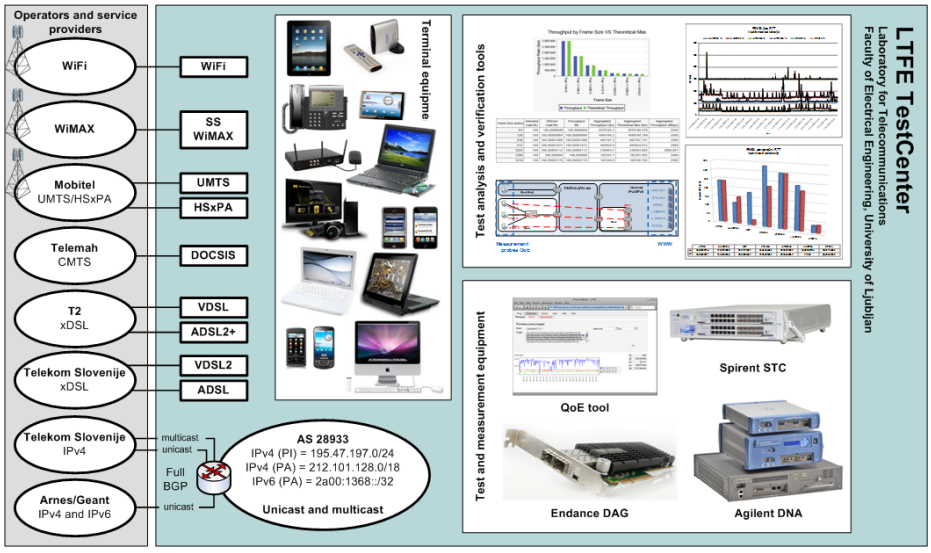
  1. Vzpostavitev in konfiguracija testnih sistemov in pilotnih implementacij
  2. Izvedba meritev, testiranj in verifikacije za telekomunikacijske sisteme, storitve in protokole
  3. Analiza rezultatov, diagnostika in verifikacija

TIPI TESTIRANJ: performančni, funkcionalnih interoperabilnostnih primerjalni in skladnostni testi
IZVEDBA: z vrhunsko opremo, ki je na voljo v TestCentru
Izvedba celotnega R&D cikla
Raziskave in analize
Načrtovanje, razvoj in implementacija sistemov, storitev in protokolov
Meritve, testiranje in verifikacija
Vzdrževanje

LTFE TestCenter – solutions&services

- **R&D**
  Entire R&D cycle – analysis, research, design, development, programming, testing and verification, maintenance&support
- **Pilot implementations**
  Networking solutions and services
  IP, IPv6, MPLS, MetroEthernet, VPN…
  Mobile&wireless architectures
  UMTS, WiFi, WiMAX, UMA…
  NGN/IMS and WEB 2.0 development (solutions, services)
  System tools
  QoS/QoE measurement tool, VPN security solution, Broadband network planning tool
- **Product development&implementations**
  Protocol development and integration into vendor equipment
  SS7, SIGTRAN, AAA (Diamater, Radius, …)
  Monitoring, SORM, DPI
  Media gateway signalling part, Call servers
  System integration and engineering
- **Professional equipment**
  Spirent STC, Agilent DNA, Endace DAG,Efficient IPv4/IPv6 networking infrastructure
  Broad range of BB SP connections

LTFE TestCenter infrastructure summ.

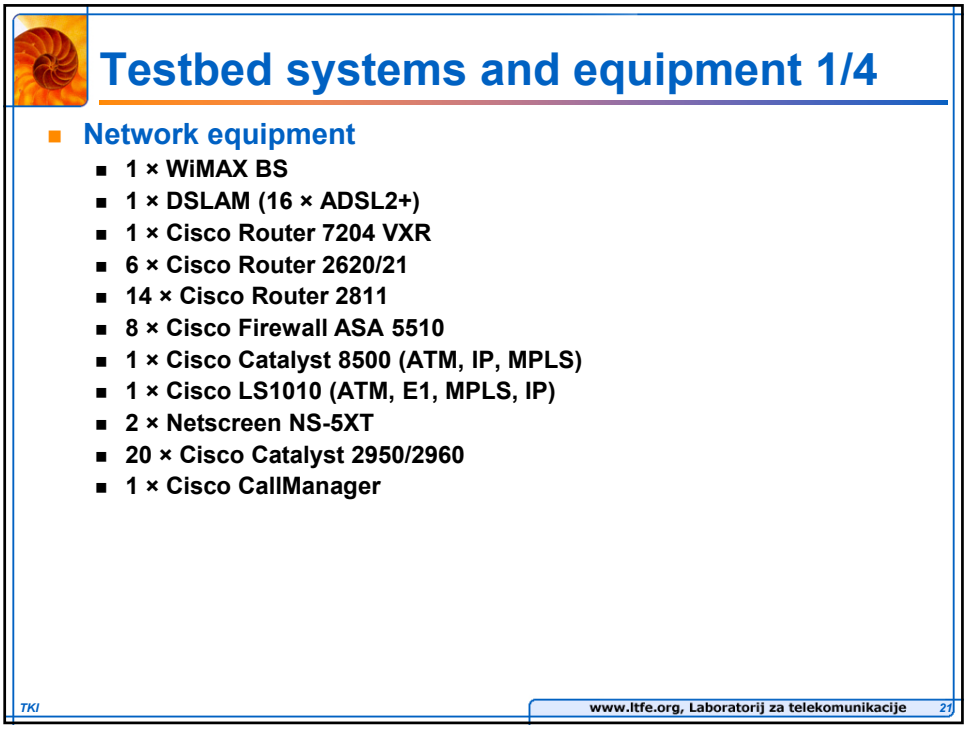


TestCenter infrastructure – details 1/2

- Dual stack IPv4/IPv6 network
  - Multicast enabeled
  - Structured wireing: cat6, fiber SM/MM
  - IPSec VPN, SSL VPN
  - Equipment
    - Cisco 7604, 11 × Cisco Catalyst 3560, Cisco ASA 5510, Juniper ISG 1000
- Connectivity
  - Full BGP connectivity, AS = 28933
  - 4 × native ISP connections
    - ARNES/GIANT, Telecom Slovenia
  - 10+ BB access connections (various slovenian providers)
    - Technolgies ADSL, ADSL2+, VDSL, VDSL2, FTTH, WiMAX 802.16D, WiMAX 802.16e, HSxPA, DOCSIS)
  - ALL Slovenian VoIP providers
    - Telekom, T2, AMIS, UPC Telemach, Detel, Planet9, Tuš …

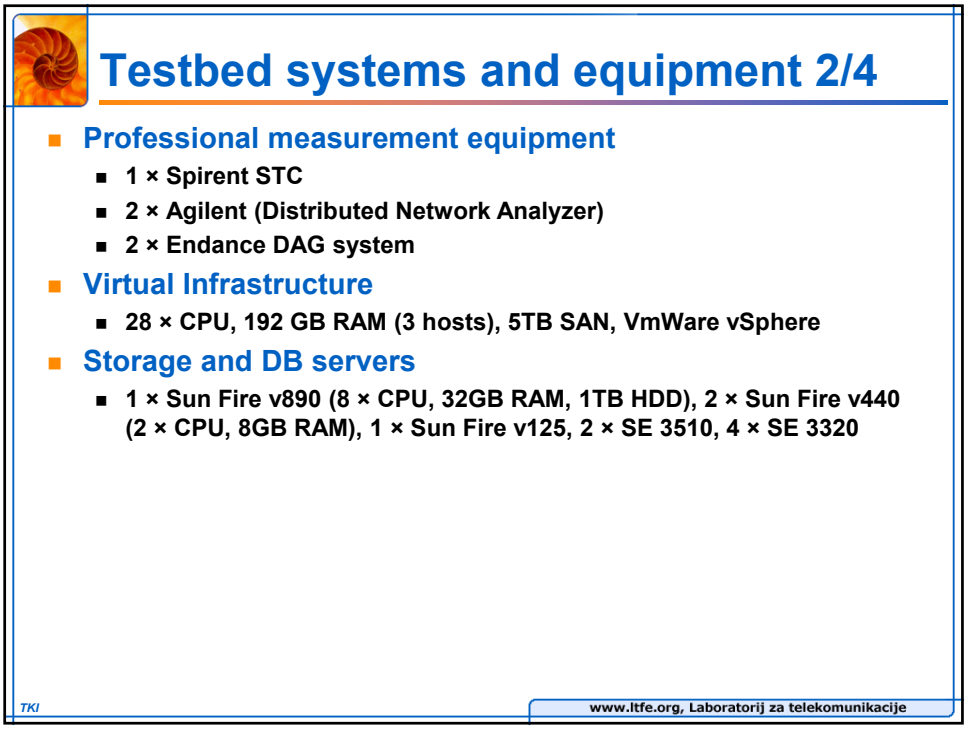
TestCenter infrastructure – details 2/2

- WiMAX test-bed (Telsima)
  - QoS implemetation for WiMAX BS/SS
  - beta testers for WiMAX 802.16D and 802.16e
- NATO – “TACOMS Phase 1” test-bed
  - Integratin: DNS, LDAP, CO BGP, H323 call control
  - Cisco CM, ISODE (M-Vault), OPEN LDAP,
- NGN/IMS test-bed
  - IMS – Fraunhofer FOKUS
  - 2 × Asterix VoIP system
  - 2 × SER VoIP system
  - Development Sigtran, Diameter, ParlayX GW, presence services
- IPTV test-bed
  - First commercial IPTV solution in Europe (coperation with Telecom Slo.)



Testbed systems and equipment 1/4

- Network equipment
  - 1 × WiMAX BS
  - 1 × DSLAM (16 × ADSL2+)
  - 1 × Cisco Router 7204 VXR
  - 6 × Cisco Router 2620/21
  - 14 × Cisco Router 2811
  - 8 × Cisco Firewall ASA 5510
  - 1 × Cisco Catalyst 8500 (ATM, IP, MPLS)
  - 1 × Cisco LS1010 (ATM, E1, MPLS, IP)
  - 2 × Netscreen NS-5XT
  - 20 × Cisco Catalyst 2950/2960
  - 1 × Cisco CallManager



Testbed systems and equipment 2/4

- Professional measurement equipment
  - 1 × Spirent STC
  - 2 × Agilent (Distributed Network Analyzer)
  - 2 × Endance DAG system
- Virtual Infrastructure
  - 28 × CPU, 192 GB RAM (3 hosts), 5TB SAN, VmWare vSphere
- Storage and DB servers
  - 1 × Sun Fire v890 (8 × CPU, 32GB RAM, 1TB HDD), 2 × Sun Fire v440 (2 × CPU, 8GB RAM), 1 × Sun Fire v125, 2 × SE 3510, 4 × SE 3320

Testbed systems and equipment 3/4

- **Audio – video infrastructure**
  - 4 × ProHD JVC, 2 × full HD JVC, 2 × ProHD Sony cameras
  - 5 × Sony BRC300 remote controled cameras
  - 4 × video mixer (with audio, graphics, title insertion, chroma keying,..)
  - 2 × audio mixers
  - 2 × audio-video matrix 16×16
  - Lightning and other audio equipment
- **Apple equipment (video production)**
  - 12 × iMac 27” i7 2,93 GHz, 8GB RAM,
  - 5 × MAC Pro (2×6 core 2,66 GHz, 16 GB RAM, 4TB disc, Cinema Display 27”, AJA kona 3)
  - 4 × MacBook PRO (15,4”, C2D 2,8 GHz, 4GB RAM)
  - 2 × Mac Mini
  - 1 × Xserve (2×4 core 2,66 GHz, 12GB RAM, 3TB HDD, Fiber channel)
  - ES_6216SX storage 32TB (Fiber Channel)

Testbed systems and equipment 4/4

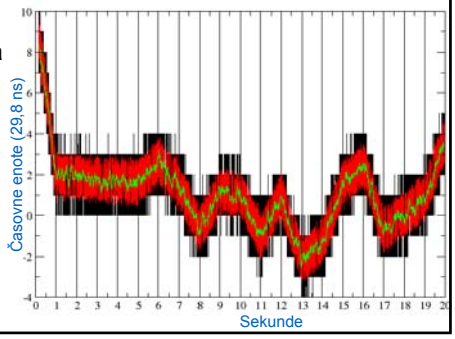
- **Broadcasting infrastructure (producting and measuring)**
  - DVB-T/H RF probe and Digital spectrum analyzer
  - DVB-T/H VHF and UHF modulators and demodulators
  - DVB Multiplexer
  - DVB-T reciver (redistributor, dual channel, diversity mode)
  - DVB Analayzer
  - Multipurpose ASI / IP Stream station with analyzing tools
  - ASI/SDI streamer
  - Harris VTM4100 video analyzer (Waveform, Vector, Gamut, Picture, and Timing screens with digital and analog module)
  - Reference monitors JVC and Sony with waveform and vectroscope
- **Production system**

  Video-audio system, Apple equipment and broadcasting infrastructure can be combined and conected in whole TV production system with Non-Linear editing and live channel production.

  Apple equipment is connected in cluster mode infrastructure to ensure efficient workflow.

Dag merilna kartica

- Točno časovno žigosanje datagramov
- Razvoj skupine The Waikato Applied Network Dynamics Group (WAND) od leta 1997 naprej
- Merjenje na OC-192 povezavah (10 Gbit/s)
- 64-bitni zapis časovnega žiga:
  - 32 bitov časovnega žiga je namenjeno štetju sekund (68 let)
  - 32 bitov pa predstavlja decimalni del (ločljivosti četrtinko ns)
- Urin impulz generira kristalni oscilator
  - frekvenca 33554432 Hz
  - pokriva 25 bitov decimalnega dela
  - časovno ločljivost okrog 30 ns
  - s stabilnostjo nekaj ppm
- Sinhronizacija; impulz vsako s
  - GPS
    - natančnost, boljšo od 100 ns
  - CDMA
    - nedoločljiva zakasnitev prehoda signala v celici



TKI

Sprint IP Monitoring System

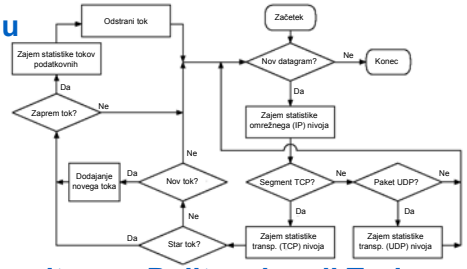
- Zelo zmogljiv sistem za naknadno analizo:
- Sistem za zajem podatkov: IPMON
  - Robne zmogljivosti današnjih osebnih računalnikov
- Oblika zapisa zajetih podatkov
  - Časovni žig
  - Prvih 44 oktetov datagrama IP: zajeta IP, navadno tudi glava transp. protokola
  - Skupaj – 64 oktetov
- Kapaciteta naprav za shranjevanje sledi in fizične zahteve sistema
  - Prenosne hitrosti na medijih:

	OC-3	OC-12	OC-48
podatkovna hitrost (Mb/s)	155	622	2480
velikost enourne sledi (GB)	11	42	176

  - Podpora merjenju velikim prenosnim hitrostim
    - Pisanje na disk (najslabši primer – OC48): 396,8 Mb/s = 50 MB/s
    - 5 SCSI diskov, RAID
    - 64 bitno vodilo PCI s 66 MHz uro 4224 Mb/s
  - Izvedba časovnega žigosanja paketov: Dag kartica;
  - Ocenjena napaka absolutne ure 5 µs
  - Časovna sinhronizacija (GPS), analiza zakasnitev

Tstat

- Sistem za tekočo pasivno analizo podatkov IP, UDP in TCP
- Razvit v letu 2001, predstavljen na GlobeCom-u 2002
- Podprtih več različnih zapisov sledi
- Problematiki časovnega žigosanja se ne posvečajo
  - Uporabljajo časovne žige osebnega računalnika
  - Uporabljajo časovne žige Dag katic
  - Promet zajemajo s `tcpdump`, `libpcab`
- Program napisan v C-ju, perlu



- Uporabili so ga za izvajanje meritev na Politecnico di Torino

Hvala za pozornost.

Vprašanja?