cesnet

BEZPEČNÁ DISTRIBUCE PŘESNÉHO ČASU

Vladimír Smotlacha

CESNET

seminář 24. 5. 2018
Praha

BEZPEČNÁ DISTRIBUCE PŘESNÉHO ČASU

- Hodiny
- Přenos času
- TF Infrastruktura

cesnet

HODINY

- **frekvence – přirozená veličina**
  - periodicky se opakující děje v přírodě (mikrosvět i makrosvět)

- **čas – určeno konvencí, integrál frekvence**
  - jednotka určená periodou
  - nutnost zvolit počáteční bod – T_0

oscilátor

- určuje požadovanou periodu

  příklad: kyvadlo $\nu = \sqrt{(g/l)} / 2\pi$

  foton $\nu = E/h$

čítač (integrátor)

- počítá periody
- příklad: mechanický převod, elektronický čítač

PARAMETRY HODIN

- **stabilita**
  - maximální změna relativní frekvence v daném časovém úseku
    - vyjadřuje se často v jednotkách ppm (Part per Million) a ppb (Part per Billion)
- **přesnost**
  - absolutní odchylka od správného času
- **rozlišení**
  - granularita poskytované časové informace
- **„holdover“**
  - jak dlouho vydrží odchylka v daném rozmezí bez synchronizace

VÝSTUP HODIN

- **1-PPS (Pulse per Second)**
  - elektrický signál, 1 puls za sekund – začátek impulsu reprezentuje začátek sekundy
  - analogicky 100-PPS, 1000-PPS
- **textový údaj o čase (label sekundy)**
  - vztahuje se k právě probíhající sekundě
- **timestamp**
  - pro danou událost (elektrický impuls) poskytnou hodiny časový údaj, kdy k událost i došlo.

Hodiny v počítači

- **hodiny v počítači jsou virtuální objekt**
  - lze použít pro timestampování události v rámci operačního systému
- **implementovány v jádře operačního systému**
  - rozlišení minimálně 0.838 μs ~ 1.193 MHz (starší architektura od PC-XT)
  - typicky odpovídá frekvenci CPU (registr TSC počínaje řadou Intel Pentium)
- **funkce kernelu Linuxu**
  - gettimeofday() – relativní čas v mikrosekundách
  - getnstimeofday () – relativní čas v nanosekundách

cesnet

PŘENOS ČASU A FREKVENCE

Cíl přenosu času

- **synchronizace hodin**
  - nastavení časového údaje podle jiných hodin
  - nemusí zahrnovat úpravu „rychlosti hodin“ (frekvence)

- **syntonizace**
  - sjednocení frekvence dvou zařízení
  - nemusí zahrnovat sjednocení časového údaje

Příklad: nastavení rafiček x změna délky kyvadla u kyvadlových hodin

PŘENOS ČASU - HISTORIE

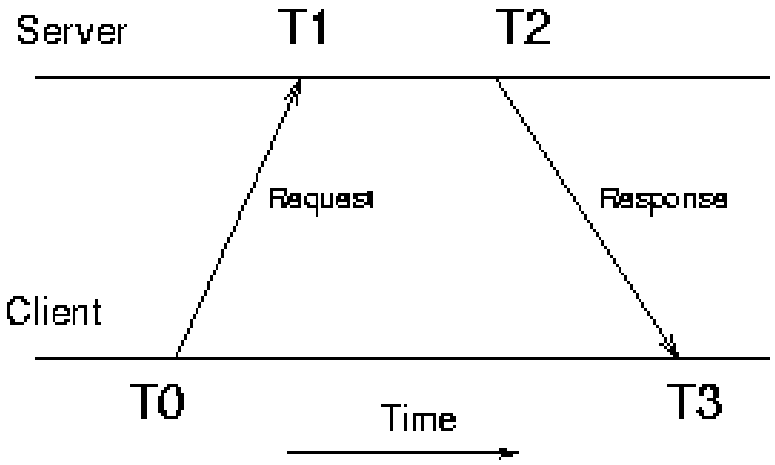
- **akusticky**
  - zvon
  - výstřel z děla
    - problém s malou rychlostí zvuku, při nastavení lodních hodin znamená odchylka 1s chybu určení zeměpisné délky 15 úhlových vteřin (1/4 námořní míle na rovníku)
- **vizuální symbol**
  - „Time ball“ – Greenwich Observatory (1833), USNO (1845)
- **telegraf**
  - USNO (1865)
- **rádiový signál**
  - 1905

PŘENOS ČASU - SOUČASNOST

- **kabel, optická linka**
  - kratší vzdálenost, neuplatní se vnější vlivy (teplotní dilatace)
- **radiové systémy**
  - DCF (77.5 kHz) – šum v řádu milisekund
- **satelitní navigační systémy (GPS, Galileo, GLONASS, Beidou)**
  - absolutní – šum v řádu desítek nanosekund
  - diferenciální – porovnání hodin, shodný vliv atmosféry v geograficky blízkých lokalitách, absolutní přesnost cca 1 ns (např. GTR50)
- **obousměrný satelitní přenos (TWSTFT)**
  - předpoklad stejné doby šíření v obou směrech
- **obousměrný přenos optickou linkou**

- **datetime - port 13, RFC 867**
  - řetězec ASCII bez pevného formátu
    - např. “Fri Apr 6 08:51:38 2012”
- **time - port 37, RFC 868**
  - binární, 32-bit unsigned integer
  - vyjadřuje počet sekund od 1.1.1900
- **NTP - port 123**
  - obousměrný přenos, binární
  - 64-bit časový údaj
    - 32-bit: počet sekund od 1.1.1900
    - 32-bit: “desetinná část”, rozlišení 2 -32 (~0.23 ns)

PRINCIP NTP



- **zpoždění** $\delta = (t3 - t0) - (t2 - t1)$
- **offset** $\theta_0 = ((t1 - t0) + (t2 - t3)) / 2$

$$\theta_0 - \delta/2 \leq \theta \leq \theta_0 + \delta/2$$

Další síťové protokoly

- **protokol IEEE 1588 (PTP)**
  - implementace v 2. vrstvě podle OSI (Ethernet) nebo ve 4. vrstvě (UDP)
  - follow-up paket (přenáší informaci o předchozím paketu)
  - přepokládá HW podporu ve switchi (měření zpoždění, aktualizace follow-up paketu)
- **White Rabbit**
  - vychází z PTP
  - přenos na 2. vrstvě
  - využívá synchronní Ethernet (přenos frekvence, syntonizace hodin)
  - dedikované switche
- **TSA (časová razítka)**

PŘESNOST SÍŤOVÝCH PROTOKOLŮ

- **přesnost synchronizace hodin pomocí síťových protokolů**
  - linková vrstva **x** transportní vrstva
  - standardní **x** dedikované síťové prvky
  - standardní PC **x** podpora v HW

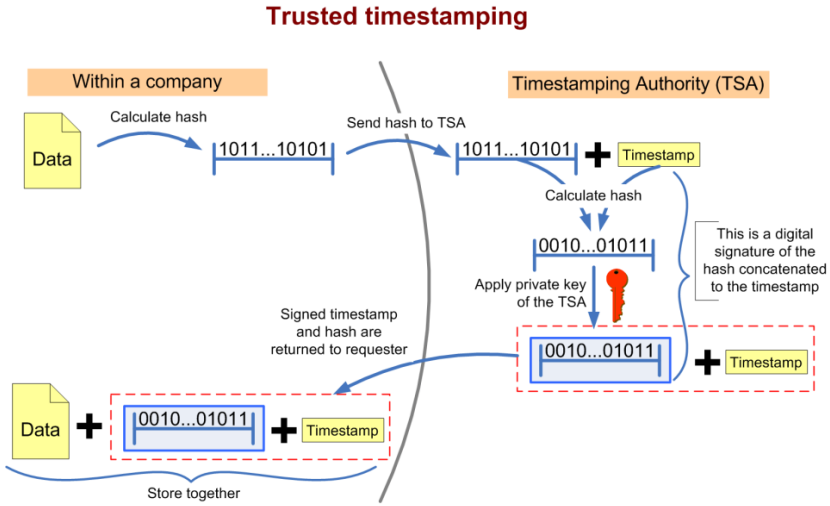
- **prakticky dosažitelná nejistota**
  - NTP: 1 ms (rozsáhlá síť, PC se standardním krystalem)
    10 µs (lokální síť, kvalitní oscilátor, HW podpora)
  - IEEE-1588: 1 µs (lokální síť, Ethernet)
  - White Rabbit : < 1 ns (synchronní Ethernet)

TSA – Time Stamp Authority

- RFC-3161
- kryptograficky podepsané certifikáty s časovou informací
- poskytuje důkaz, že daný objekt existoval (resp. událost nastala) nejpozději v určitém okamžiku v minulosti
- rozlišení 1 s – 1 μs

Princip

- uživatel odešle dotaz (TSQ)
  - obsahuje unikátní řetězec (nonce)
- server odpoví zprávou (TSR) obsahující
  - nonce
  - časový údaj
  - podpis privátním klíčem TSA



RUŠENÍ ČASOVÉHO PŘENOSU

- **jamming**
  - přijímaný signál je rušen (úmyslně i neúmyslně) natolik, že není dostupný časový údaj
    - lze ovlivnit vhodnou modulací
    - příklad: přijímače GPS ovlivněné „antiradarem“

- **spoofing**
  - podvržení nesprávného časového údaje
    - existují systémy, které dokáží vnutit nesprávný čas/polohu přijímači GPS
    - lze se bránit pomocí vysílání kryptovaného signálu

Závěr: kritické aplikace se v současné době nemohou spolehnout na čas poskytovaný GNSS (Galileo slibuje problém v budoucnu řešit).
Probíhají intenzivní práce na komerčním řešení.

Zabezpečení síťového signálu

- **NTP podporuje kryptování a autentizaci serveru**
  - symetrický klíč – funkční, ale nepraktické – každý uživatel musí mít svůj klíč
    - provozuje např. NIST
  - veřejný klíč (autokey) – implementováno, ale prakticky nepoužitelné
    - pracuje se na řešení (RFC 7384)

- **IEEE-1588**
  - problém méně kritický než u NTP – distribuce převážně v lokální síti
  - existují různé verze kryptovaného (secure) 1588
    - pravděpodobně se nevyužívá ve větším rozsahu

- **optický přenos**
  - v principu bezpečnější pokud neprochází veřejným Internetem
  - obtížné neautorizované „připojení“ na optický kabel

Požadavky na přesnost času

- **ITU-T (telekomunikace)**
  - kategorie hodin rozlišena podle stability a délky doby „holdover“
  - Stratum-1 (stabilita $1*10^{-11}$) až Stratum-4 (stabilita $3.2*10^{-5}$)

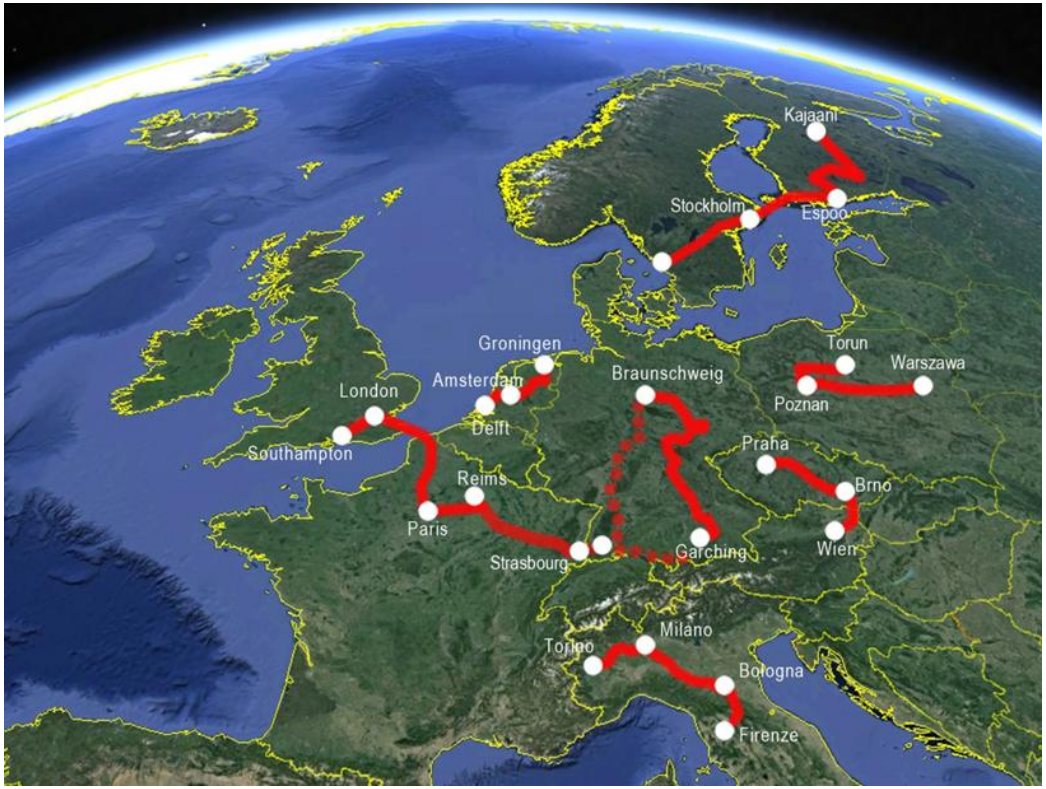
- **ESMA (European Securities and Markets Authority)**
  - MiFID-II RTS-25
  - požadavky na přesnost hodin využívaných v obchodě a jejich navázání na UTC
  - nejvyšší kategorie je
    - max. odchylka do 100 µs od UTC
    - rozlišení časového razítka 1 µs nebo lepší

cesnet

OPTICKÁ INFRASTRUKTURA PRO PŘENOS ČASU A FREKVENCE

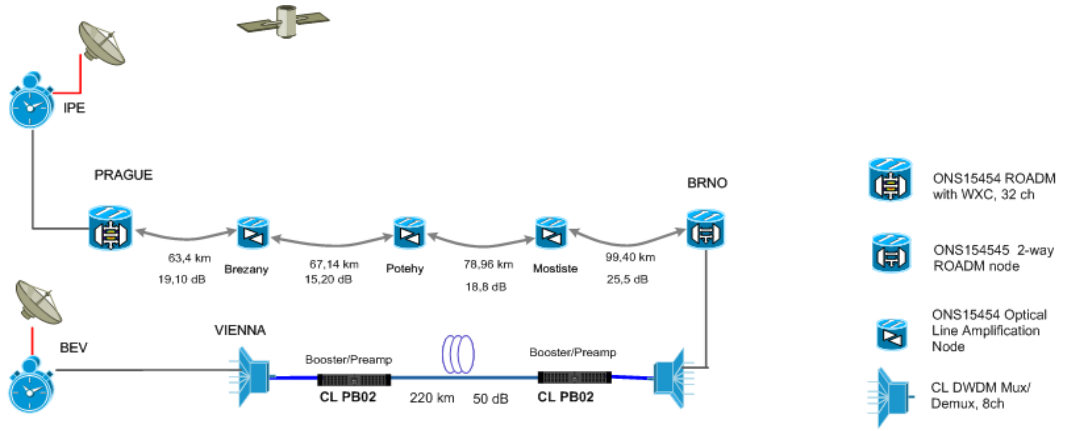
CÍLE TF-INFRASTRUKTURY

- Kontrola a porovnávání časových stupnic propojených atomových hodin
- Vylepšení národní časové stupnice UTC(TP) provozované v UFE AV ČR, porovnání UTC(TP) a rakouskou stupnicí UTC(BEV)
- Distribuce přesného času a stabilní frekvence
- Experimentální provoz koherentního přenosu optické frekvence
- Propojení s obdobnými infrastrukturami v Evropě

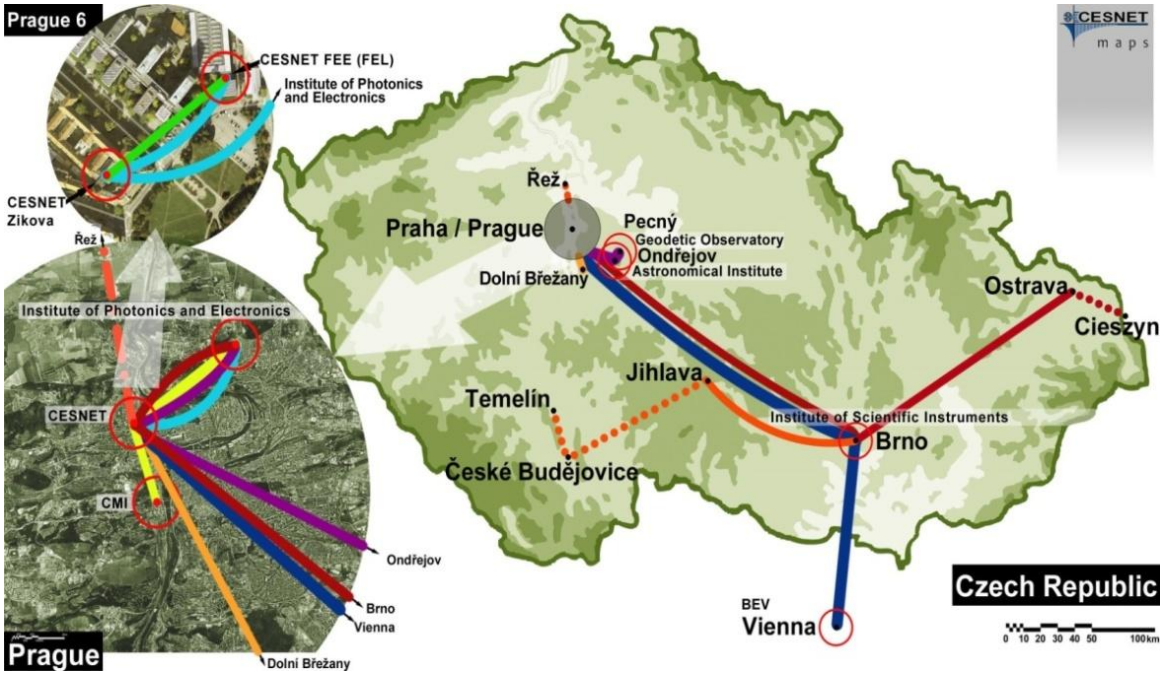


Přenos času UFE – BEV

- **optické porovnávání časových stupnic UTC(TP) a UTC(BEV)**
  - délka trasy Praha – Vídeň 550 km
  - v provozu od srpna 2011
  - první optické porovnávání stupnic dvou národních laboratoří na světě
  - spolupráce CESNET, UFE AV ČR, BEV a AcoNET



TF-INFRASTRUKTURA



Připojené organizace:

- CESNET
- UFE AV ČR
  - státní etalon času
  - UTC(TP)
- BEV (Vídeň)
  - rakouský státní etalon času
- UPT AV ČR
- VUGTK
- FEL ČVUT
- ČMI (laboratoř délky)

ATOMOVÁ ČASOVÁ STUPNICE CESNETU

- **CESNET provozuje cesiové hodiny typu 5071A → atomová časová stupnice**
  - 5071A jsou nejběžnější komerční cesiové hodiny
    - vyráběné přes 25 let
    - HP5071A (1991) -> Agilent -> Symmetricom -> Microsemi

Stabilita $1 \cdot 10^{-14}$ (ADEV, 5 dní)

Přesnost $5 \cdot 10^{-13}$

cesnet

DĚKUJI ZA POZORNOST

DOTAZY?