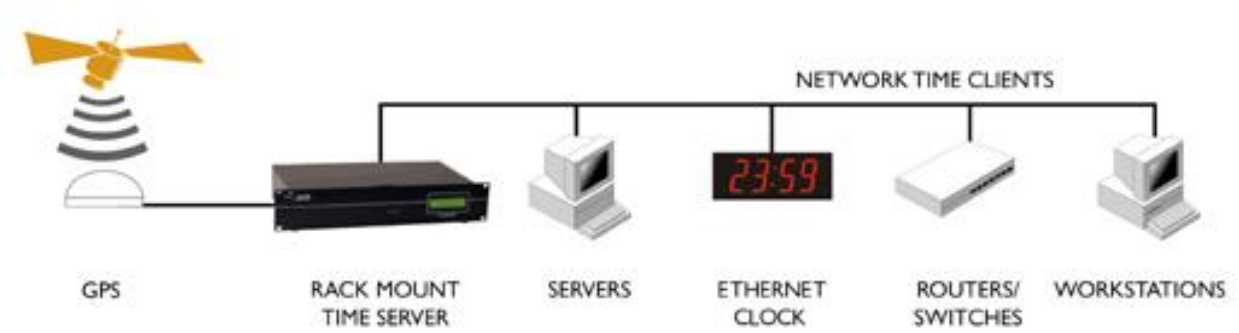
PREDMET:
MREŽNI SERVISI

NTP (NETWORK TIME PROTOCOL)

Dr Dušan Stefanović CCNA, CCNA Security,CCNP

NETWORK TIME PROTOCOL

- Network Time Protocol (NTP) je protokol koji je namenjen sinhronizaciji sistemskih satova računara preko mreže.
- Razvijen je 1985. i od tada se konstantno upotrebljava i usavršava.
- Protokol je opisan kao klijent-server model, ali se lako može koristiti kao peer-to-peer veza, gde oba čvora obezbeđuju izvor vremena.
- Šalje i prima vremenske oznake koristeći UDP (engl.User Datagram Protocol) protokol, preko porta 123.
- Može koristiti broadcast i multicast, gde klijenti osluškuju promene vremena nakon inicijalne povratne razmene podešavanja.



NETWORK TIME PROTOCOL

- Tačno vreme je važno podesiti na mrežnim uređajima i potrebno je da svi uređaji u mreži imaju konzistetno vreme
  - Log poruke koje sadrže informaciju o nekom događaju treba da sadrže i tačno vreme kreiranja takve poruke
  - Vremenske ACL liste
  - Servisi koji svoj rad zasnivaju na tačnom vremenu
- Većina Cisco rutera ima dva časovnika
  - Hardverski časovnik (napaja se iz baterije) a u CLI se vidi kao *calendar*
  - Softverski časovnik, CLI se vidi kao *clock*.
- Ova dva časovnika su odvojena, što znači da vreme na ovim časovnicima može da se razlikuje
- **Primarni časovnik** koji se koristi je **softverski časovnik**

NAČINI PODEŠAVANJA SISTEMSKOG SATA

- **NTP**
- **SNTP (Simple Network Time Protocol)**
- **Virtuelni mrežni vremenski servis (VINES)**
- **Ručno**

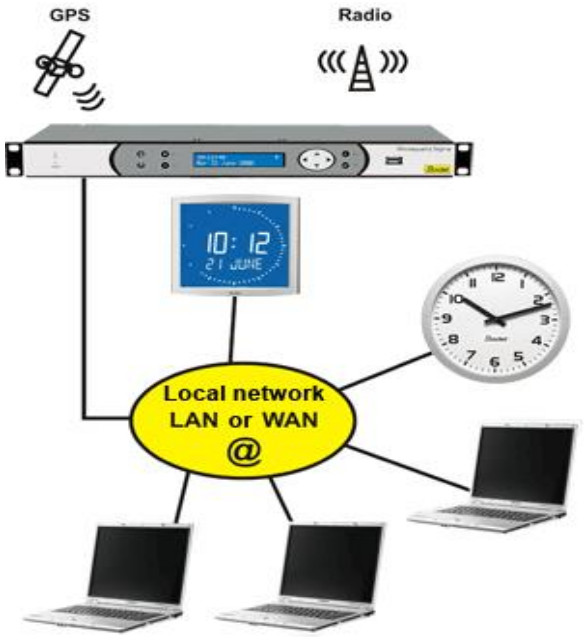
- Softverski časovnik može dinamički da se ažurira, može da bude precizniji od hardverskog časovnika
- Ukoliko se koristi više vremenskih izvora, NTP uvek ima prioritet
- Informaciju o softverskom časovniku gubimo uvek kada se uređaj restartuje, Cisco IOS prilikom podizanja sistema sihronizuje softverski časovnik sa hardverskim

NETWORK TIME PROTOCOL

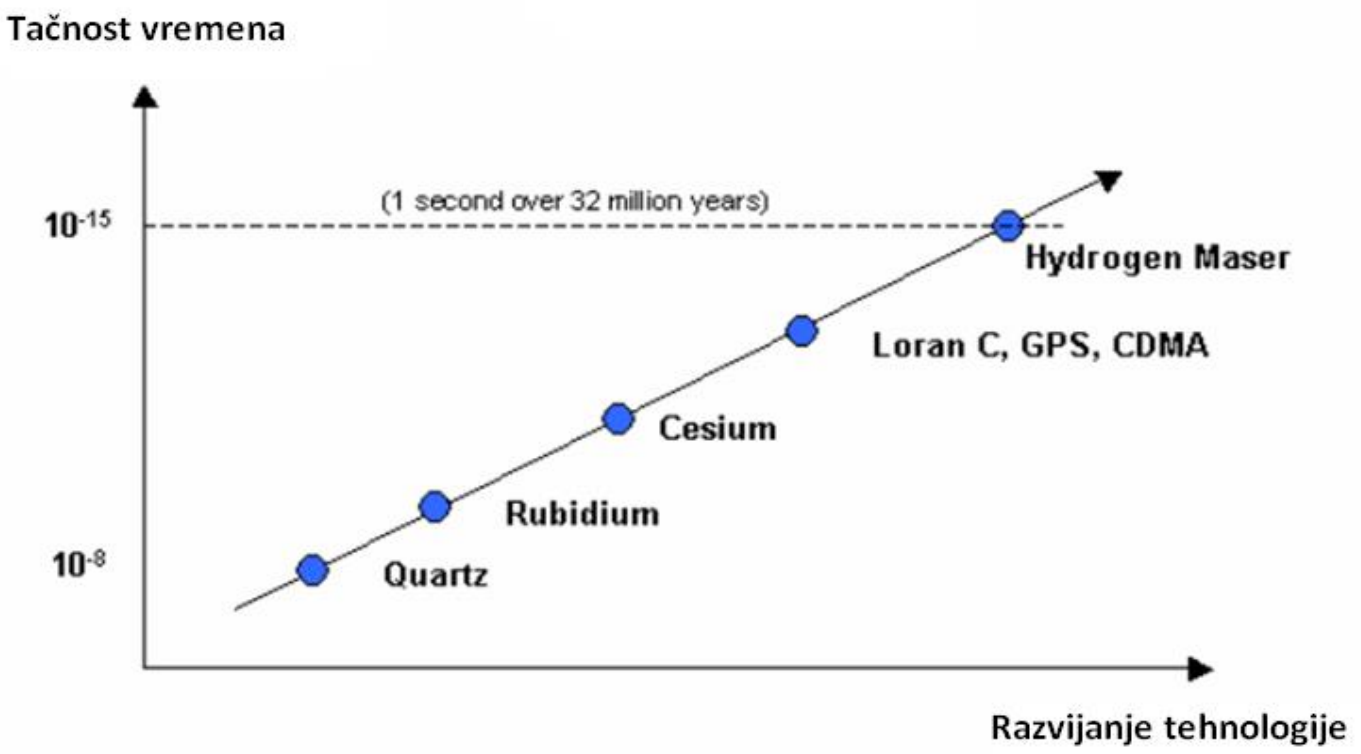
- NTP je protokol za sihronizaciju časovnika u računarskim mrežama, preko IP tehnologije prenosa (packet-switched) koja ima promenjivo kašnjenje prilikom prenosa podataka.
- Osnovni problem IP tehnologije prenosa je varijabilno kašnjenje
- Otpornost na promenjivo kašnjenje se postiže upotrebom *jitter* bafera.
- NTP koristi matematičke formule koje uključuju prisutno kašnjenje i prosleđuju nam super tačno vreme
- Verzija NTPv4 nam omogućava tačno vreme reda 10ms.
- NTP spada u grupu starijih protokola koji je razvijen davne 1985.
- **NTP** koristi **UDP** protokol **port 123**
- Trenutno je aktuelna **NTPv4**
- Cisco uređaji su podešeni da koriste NTPv3 (by default)
- NTPv4 ima bolje matematičke proračune, na Internetu tačnost je reda **10ms** a u lokalu reda **200us**.

NETWORK TIME PROTOCOL

- NTP serveri obično vreme dobijaju od autorativnih vremenskih izvora kao što su:
  - **radio časovnik**
  - **atomski časovnik**
- NTP serveri su fizički povezani na ove časovnike
- NTP koristi hijararhiju prilikom prosleđivanja tačnog vremena
- Što je uređaj udaljeniji od atomskog časovnika ima manje tačno vreme
- NTP je izuzetno efikasan, nije potrebno više od jednog paketa za sihronizaciju vremena između dva uređaja sa tačnošću ms.



TAČNOST SA RAZVOJEM TEHNOLOGIJE

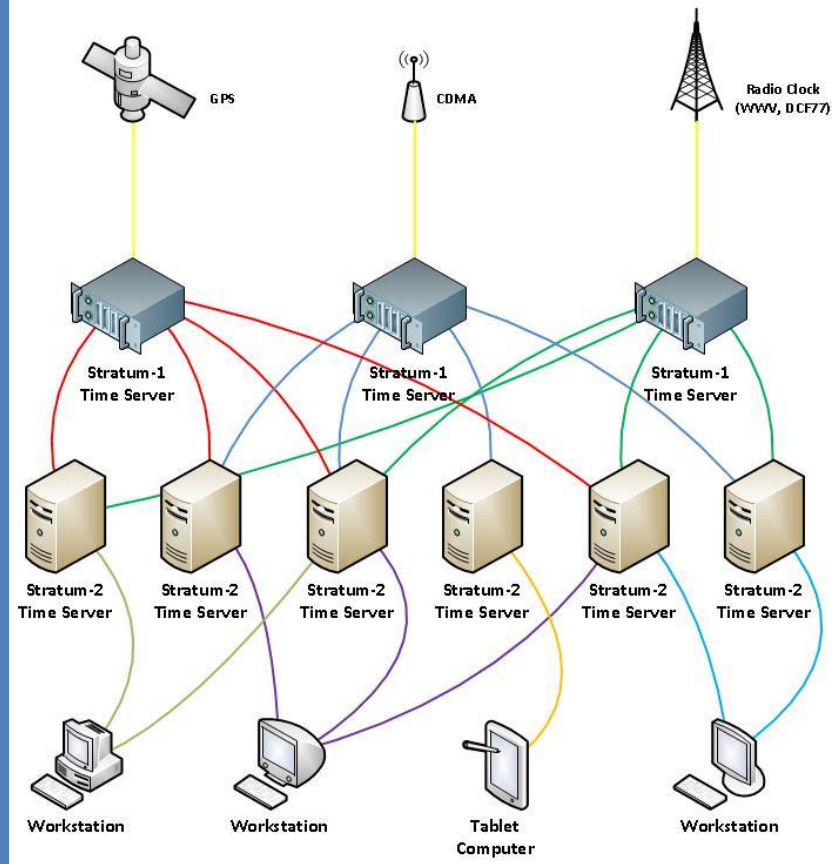


NTP VERZIJE

RFC dokumenat	Naziv
RFC 958	Network Time Protocol (NTP)
RFC 1059	Network Time Protocol (v1) Specifikacija i Implementacija
RFC 1119	Network Time Protocol (v2) Specifikacija i Implementacija
RFC 1305	Network Time Protocol (v3) Specifikacija, Implementacija, Analize
RFC 1361	Simple Network Time Protocol (SNTP)
RFC 1769	Simple Network Time Protocol (SNTP)
RFC 2030	Simple Network Time Protocol (SNTP) v4, IPv4, IPv6 i OSI
RFC 4330	Simple Network Time Protocol (SNTP) v4, IPv4, IPv6 i OSI
RFC 5905 *	Network Time Protocol (v4), Protokol i Algoritamska specifikacija
RFC 5906 *	Network Time Protocol (v4), Autokey specifikacija
RFC 5907 *	Definicije za upravljačke objekte za Network Time Protocol (v4)
RFC 5908 *	Network Time Protocol (NTP) Serverska opcija za DHCPv6

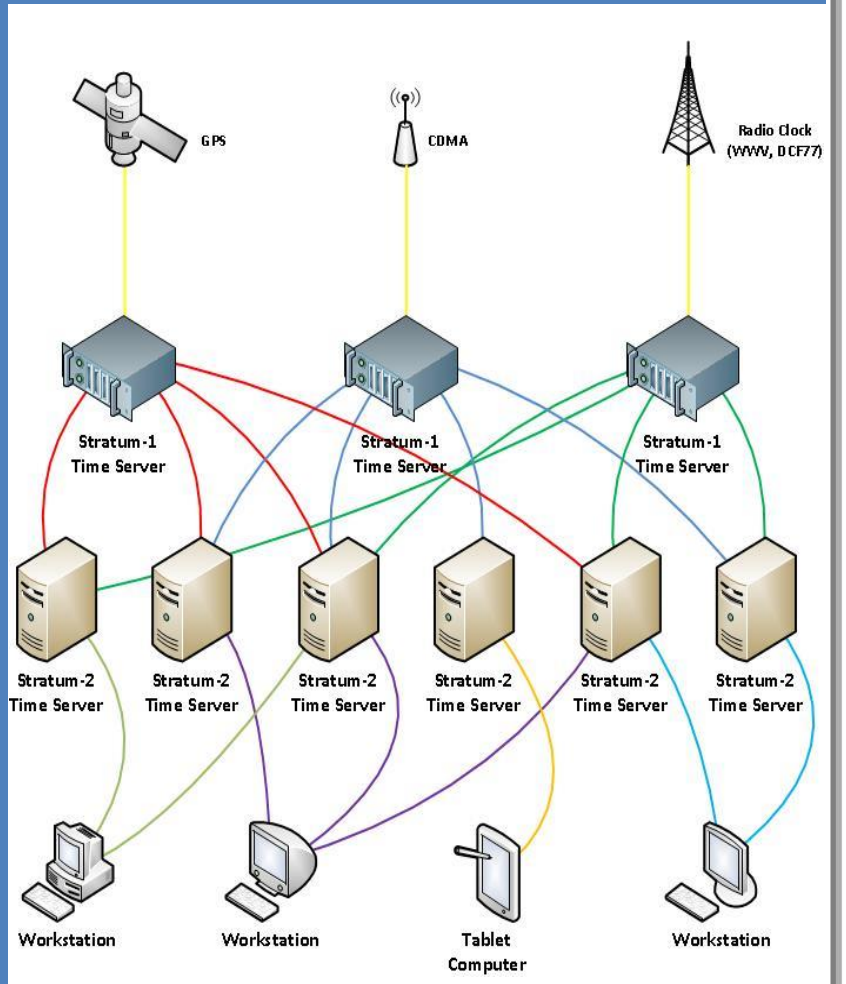
NETWORK TIME PROTOCOL

- Časovnik koji ima najpreciznije vreme je definisan kao STRATUM 0.
- Sledeći su NTP serveri koji su definisani kao STRATUM 1, STRATUM 2, ...
- NTP je hijararhijski organizovan u nivoe, tj. Stratume.
- Nivo koji je na samom vrhu je STRATUM 0
- Nivoi definišu logičko rastojanje od referetnog sata (super precizni sat)
- Broj Stratuma definiše koliko *skoka* je uređaj udaljen od autorativnog vremenskog izvora



NETWORK TIME PROTOCOL

- Stratum nije indikator kvaliteta ili pouzdanosti, može da se desi da je STRATUM 3 vremenski izvor pouzdaniji od STRATUM 2 vremenskog izvora.
- NTPv3 podržava do 16 nivoa za razliku od NTPv4 koja podržava 128 nivoa.
- Što je uređaj hijararhijski udaljeniji od atomskog časovnika ima manje precizno vreme.



STRATUM 0

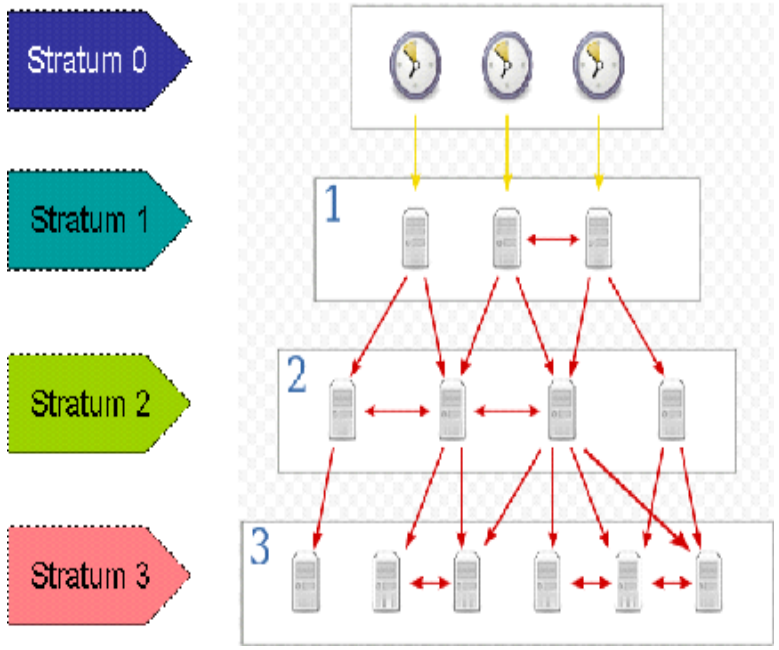
- Tu spadaju časovnici kao što su:
  - ***Atomski časovnik*** *(rubidijum),* rezonatna frekvencija atoma kao brojača
  - **GPS časovnik**
  - **Radio časovnik**
- Ovi uređaji nisu povezani na mrežu, oni su lokalno povezani na računar preko RS232 porta (Stratum 1)

STRATUM 1

- To je uređaj koji je direktno povezan na Stratum 0.
- Oni su izvori vremena sa Stratum 2 NTP servere
- Cisco implemetacija ne podržava Stratum 1 servis

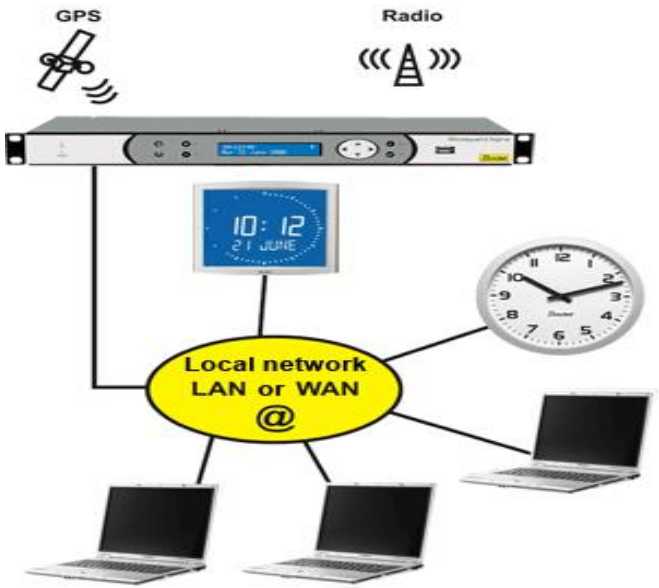
STRATUM 2

- To su računari koji šalju NTP zahteve ka Stratumu 1.
- Obično Stratum 2 računar može da se referencira na više Stratum 1 servera i da na osnovu NTP algoritma izabere precizniji
- Stratum 2 uređaji su izvori vremena za Stratum 3 uređaje.



NETWORK TIME PROTOCOL

- NTP nam uvek obezbeđuje vreme u UTC (*Cordinated Universal Time*) formatu.
- NTP poruka ne sadrži informacije o vremenskim zonama ili o letnjem računanju vremena (*daylight saving*).
- Naš zadatak je da vreme dobijeno od NTP servera prebacimo u lokalnu zonu.



SIMPLE NETWORK TIME PROTOCOL

- Manje kompleksna implementacija od NTP-a
- Koristi se u embeded uređajima i aplikacijama u kojima se ne zahteva veoma precizno vreme.
- SNTP uređaj može da primi vreme od NTP servera, ali se on ne može koristiti za dalju distribuciju vremena

NETWORK TIME PROTOCOL

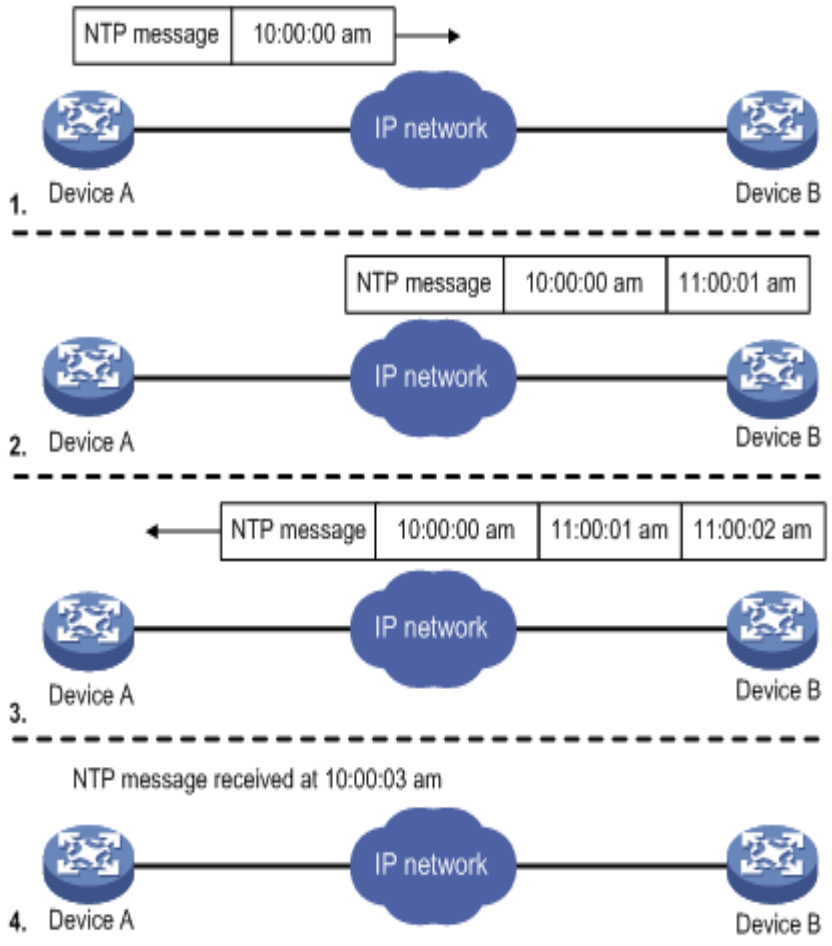
- Dozvoljeno je da se više NTP servera koriste kao izvori vremena
- U tom slučaju koristi se NTP server koji ima manji STRATUM
- Ukoliko oba izvora imaju isti STRATUM, konfigurisani server ima prioritet u odnosu na broadcast server.
- Ukoliko su oba konfigurisana bira se onaj kome je prvo poslata NTP poruka

CISCO NTP

- Snaga NTP-a je što ne zahteva ažuriranje često
- *Polling* interval je 1024 sekunde (17 minuta)
- NTP klijent na svakih 17 minuta kontaktira NTP server tj. sihronizuje svoje vreme.
- NTP ima pet operacionih modova
- Cisco implementacija NTP-a podržava 3 operaciona moda
- Cisco uređaj može preko IP mreže da se sihronizuje na sledeća dva načina:
  - *Polling,* šalje zahtev NTP serveru
  - *Slušajući NTP* broadcast *poruke*

PRINCIP SIHRONIZACIJE SA NTP SERVEROM

- Pre nego što su uređaji A i B sihronizovali svoje časovnike, Uređaj A je svoj časovnik podesio na 10:00:00 am dok je uređaj B svoj časovnik podesio na 11:00:00 am
- Uređaj B je NTP server, uređaj A želi da sihronizuje svoj časovnik sa uređajem B
- Potrebna je 1 sekunda da NTP poruka stigne od jednog uređaja do drugog



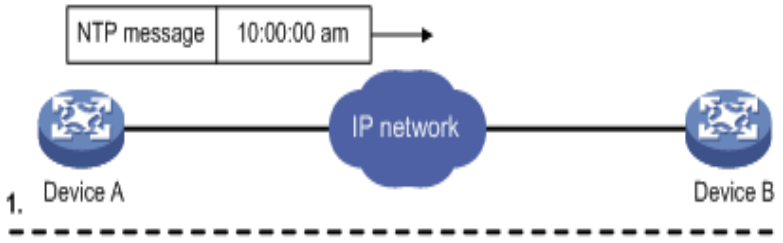
PRINCIP SIHRONIZACIJE SA NTP SERVEROM

1. Uređaj A šalje uređaju B NTP zahtev u kojem setuje svoj timestamp na 10:00:00 am (T1)

2. Kada NTP poruka stigne, uređaj B koristi svoje vreme (timestamp) 11:00:01 am (T2).

3. Kada NTP poruka napusti uređaj B, timestamp je 11:00:02 am (T3).

4. Kada uređaj A primi NTP poruku, lokalno vreme na uređaju A je 10:00:03 am (T4).



PRINCIP SIHRONIZACIJE SA NTP SERVEROM

U ovom trenutku uređaj A ima dovoljno informacija da izračuna dva najbitnija parametra:

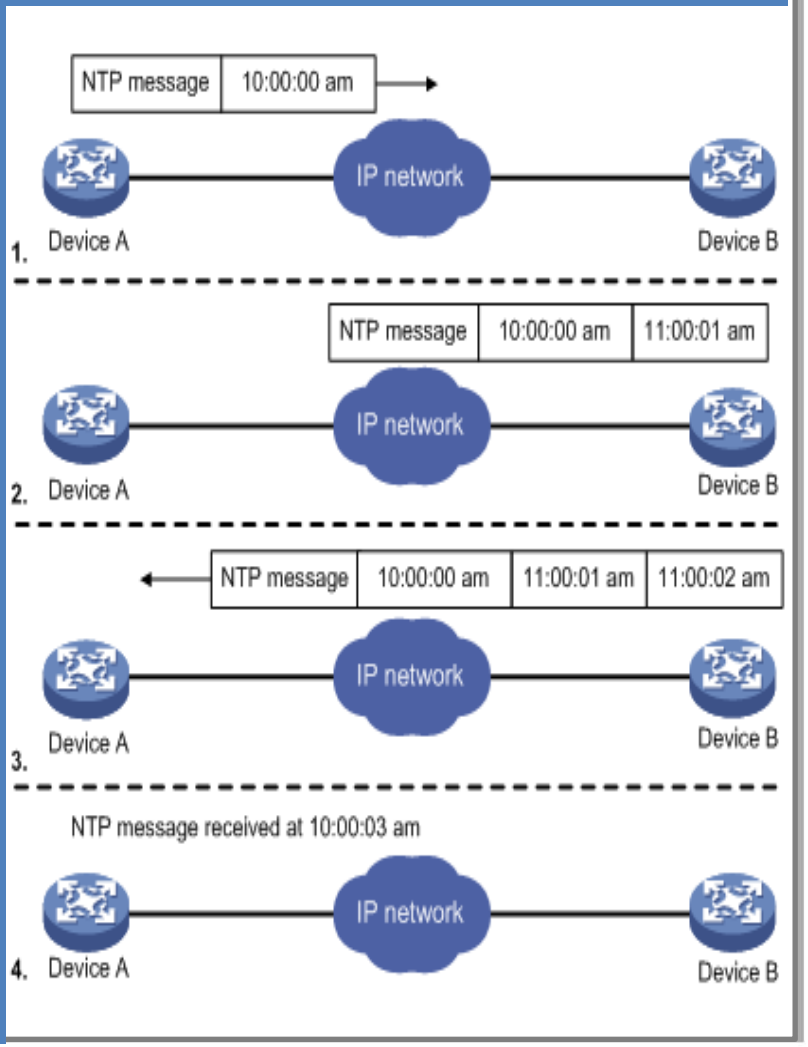
Ukupno kašnjenje (roundtrip delay) NTP poruke:

Kašnjenje = (T4–T1) – (T3-T2) = 2 sekunde

Vremenska razlika između uređaja A i uređaja B:

Offset = ((T2-T1) + (T3-T4))/2 = 1 sat.

Na osnovu ovih parametara uređaj A može da sihronizuje svoj časovnik sa časovnikom uređaja B



BEZBEDNOST NTP-a

Najznačajniji rizici za NTP usluge

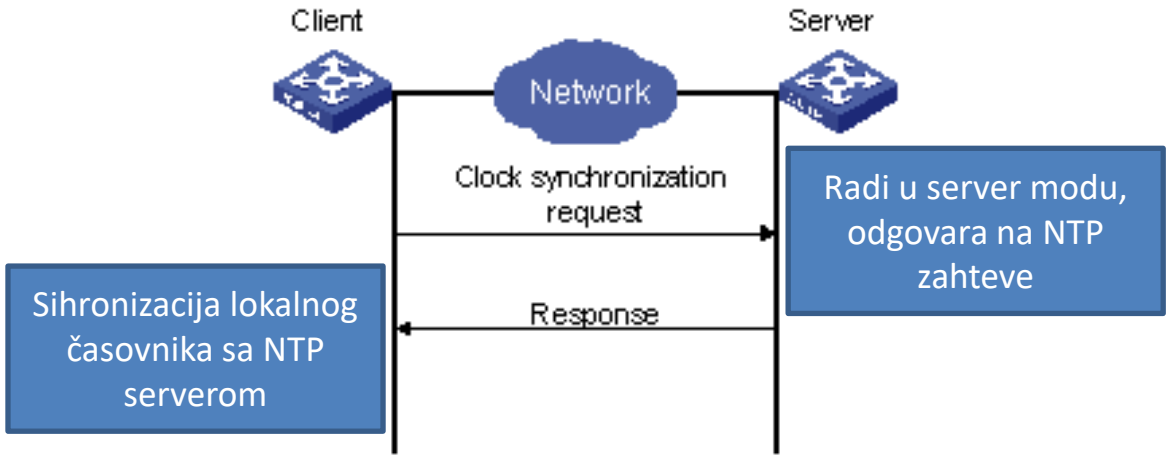
- Servis NTP je u stanju da se zaštiti protiv nekih od ovih pretnji koristeći konfiguraciona podešavanja kao što su:
  - **kontrola pristupa** – određuje kojim NTP funkcijama može da pristupi specifičan uređaj ili sa koje mreže
  - **autentifikacija** – je omogućena upotrebom simetričnih ključeva koji su instalirani na NTP serverima i klijentima

ZANIMLJIVOSTI O NTP-u

- Početak upotrebe sinhronizacije vremena na uređajima u mreži potiče od 1980-te.
- Početna odstupanja od nekoliko stotina milisekundi su danas smanjena na desetak nanosekundi.
- Prva NTP verzija 0 je napisana 1985. i sadržana je u RFC 958.
- Zadnja NTP verzija 4 je napisana 1996. sa RFC 2030.
- Preko 100 000 NTP servera postoje na Internetu.
- NTP servis zahteva 1.54% od raspoloživog CPU vremena i generiše 10.5, 608-bitnih paketa u sekundi.
- "Leap Seconds“ - kako se brzina rotacija Zemljine kugle smanjuje, da se početak dana ne bi pomerao s vremenom, ponekad se u UTC ubacuje leap sekunda pa se na taj način, taj dan produžava za jednu sekundu. Od 1972. godine do danas to se dogodilo 22 puta.

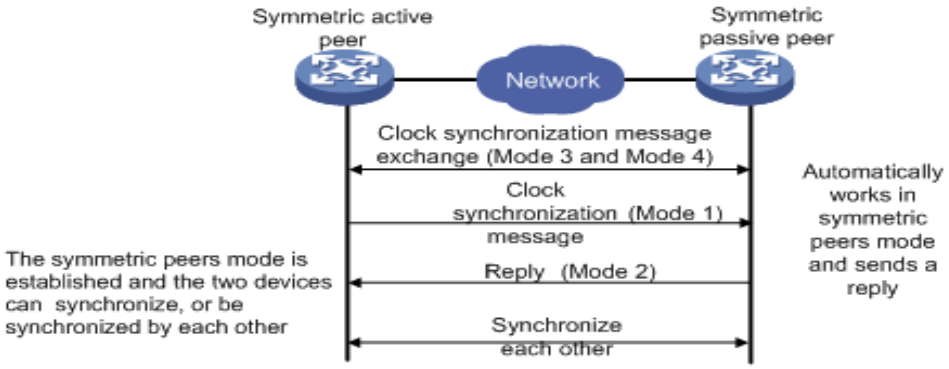
CLIENT MODE

- Najčešće se koristi.
- Princip rada je client-server arhitektura, klijent se veže za javni NTP server i sa njim sihronizuje svoje vreme.
- Komandom kojom uređaj radi u klijent modu je:
  - *ntp server*
- Uređaj na ovaj način periodično kontaktira NTP server kako bi sihronizovao svoj softverski časovnik.



SYMETRIC ACTIVE MODE

- U simetričnom peer modu, uređaji koji rade u simetričnom aktivnom modu i simetričnom pasivnom modu razmenjuju NTP poruke
- Koristi se u slučaju kada postoji više redudatnih NTP servera koji su povezani preko različitih mrežnih putanja
- Uređaj koji radi u simetričnom aktivnom modu periodično šalje poruke o sihronizaciji časovnika, dok uređaj koji prima ovakvu poruku automatski prelazi u simetrični pasivni mod i šalje odgovor.
- Uređaji se dogovaraju o zajedničkom vremenu
- **To su uređaji koji se nalaze u istom Stratumu ali imaju različite izvore vremena**
- Komandom kojom uređaj radi u ovom modu je:
  - *ntp peer*



BROADCAST CLIENT MODE

- Kada uređaj radi u ovom modu on ne kontaktira NTP server (pooling), umesto toga on sluša NTP broadcast pakete koje šalju NTP serveri
- Preciznost može biti smanjena jer je komunikacija samo u jednom smeru
- Ovaj mod se koristi u slučaju kada se ne zahteva izuzetna preciznost i kada lokalna mreža ima više od 20 klijenata, ograničen propusni opseg, memoriju ili CPU