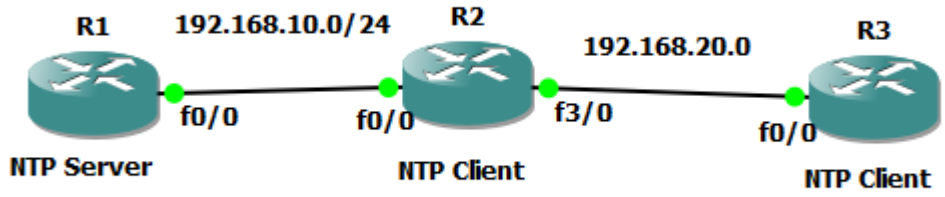
Configuring NTP Server and Client on Cisco Devices

NTP এর পূর্ণরূপ হলো Network Time Protocol । ইহা এমন এক ধরণের Service যার মাধ্যমে একটি নেটওয়ার্কের বিভিন্ন Device সমূহের সময় ও তারিখ Identical রাখা যায়। ধরি, আমাদের নেটওয়ার্কে দশটি Device (সার্ভার, রাউটার ইত্যাদি) রয়েছে। এখন এই Device সমূহের সময় ও তারিখ যদি আমরা manually Configure করি তাহলে সবগুলো ডিভাইসের সময় একেবারে Identical হবে না, কোন না কোন ভাবে সেকেন্ড পরিমাণ বা তার বেশি সময়ের পাথর্ক্য থেকেই যাবে। যদি নেটওয়ার্কটিতে ডিভাইসের সংখ্যা আরো বেশি হয় তাহলে সবগুলো ডিভাইসে সময় ও তারিখ ম্যানুয়ালভাবে কনফিগার করা যথেষ্ঠ সময় সাপেক্ষ ও পরিশ্রমলব্ধ ব্যাপার। এই সমস্যা থেকে মুক্তি পাওয়ার জন্য আমরা নেটওয়ার্কে একটি NTP সার্ভার ব্যবহার করতে পারি। NTP সার্ভার হলো এমন একটি সার্ভার যার সময়ের সাথে NTP ক্লায়েন্টসমূহ তাদের সময়কে স্বয়ংক্রীয়ভাবে সিনক্রোনাইজ করে নেয়। নেটওয়ার্ক নিরাপত্তার ক্ষেত্রেও একটি NTP সার্ভার গুরুত্বপূর্ণ ভূমিকা পালন করে। একটি নেটওয়ার্কের বিভিন্ন ডিভাইসসমূহ RSYSLOG সার্ভারের কাছে নিজেদের Log পাঠায়। এই Log দেখে নেটওয়ার্কের বিভিন্ন পরিবর্তন বা অস্বাভাবিক গতি-প্রকৃতি পর্যবেক্ষন, বিশ্লেষণ ও প্রয়োজনীয় ব্যবস্থা গ্রহণ করা যায়। নেটওয়ার্ক এ্যাটাক আইডেন্টিফাই করার সময় ডিভাইসসমূহের Log এর সময়ের (Timestamp) সঠিক ধারাবাহিকতা থাকা অত্যন্ত গুরূত্বপূর্ণ।



একটি NTP নেটওয়ার্কের NTP ক্লায়েন্ট ডিভাইসসমূহ ঐ নেটওয়ার্কের একটি Private NTP সার্ভারের কাছ থেকে অথবা ইন্টারনেটের যেকোন একটি Public NTP সার্ভারের কাছ থেকে NTP আপডেট গ্রহণ করে সংশ্লিষ্ট সার্ভারের সাথে নিজেদের সময় সিনক্রোনাইজ করতে পারে। NTP প্রটোকল UDP 123 নম্বর পোর্ট ব্যবহার করে।

কনফিগারেশন: NTP Server

প্রথমে আমরা নিচের কমান্ডের মাধ্যমে NTP_SRV এর সময় ও তারিখ দেখে নেব।

```
NTP_SVR#show clock
17:56:23.562 UTC Thu Feb 19 2002
```

অতঃপর নিচের কমান্ডের মাধ্যমে NTP_SVR এর সময় ও তারিখ ম্যানুয়ালভাবে সেট করবো এবং পরিবর্তিত সময়টি দেখে নেব।

```
NTP_SVR#clock set 10:28:00 SEP 25 2014
NTP_SVR#show clock
10:28:09.923 UTC Thu Sep 25 2014
```

NTP_SVR এ ম্যানুয়ালভাবে সময় ও তারিখ সেট করার পর আমরা এটিকে NTP Server হিসেবে কনফিগার করবো। এজন্য নিচের কমান্ডটি দিতে হবে।

```
NTP_SVR#configure terminal
NTP_SVR(config)#ntp master 1
```

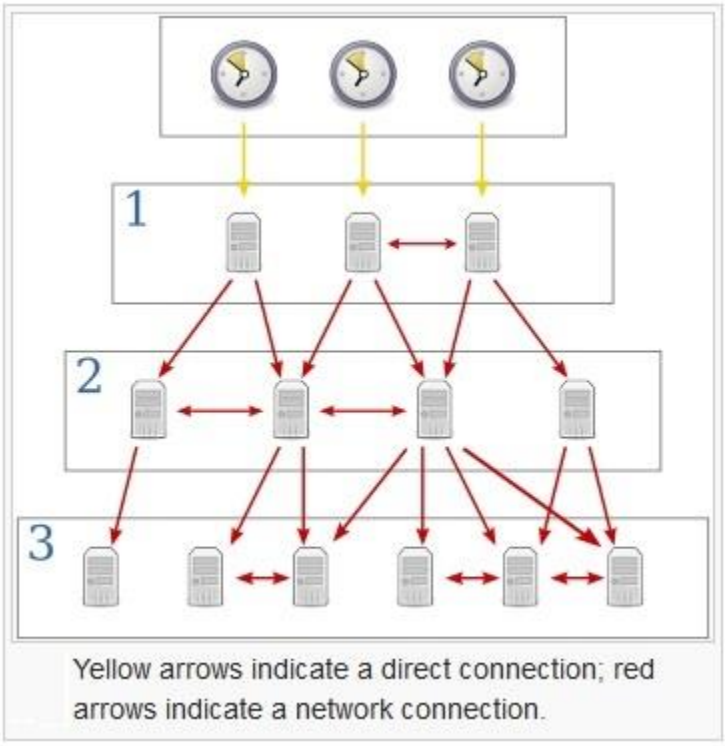
NTP_SVR টি এখন একটি Private NTP সার্ভার হিসেবে কাজ করবে। এখানে 1 হলো Stratum Number ।

Stratum Level

Stratum লেভেল দ্বারা বুঝায় একটি NTP সার্ভার কোন একটি Reference Clock থেকে কত Hop দূরে আছে। Reference Clock হলো এমন একটি Clock যা Coordinated Universal Time (UTC) এর ব্যবস্থাপনার সাথে সরাসরি জড়িত। ইহা একেবারে Accurate সময় প্রদান করে। এই Reference Clock কে আবার Master Clock বা Stratum-0 সার্ভারও বলা হয়। এই Stratum-0 সার্ভারসমূহ সাধারণ নেটওয়ার্কে ব্যবহার করা যায় না।

Stratum-1 হলো এমন এক ধরণের NTP সার্ভার যা Stratum-0 সার্ভারের সাথে সরাসরি ফিজিক্যাল কানেকশন দ্বারা সংযুক্ত থাকে এবং এর সাথে নিজের সময় সিনক্রোনাইজ করে। Stratum-1 সার্ভারসমূহকে Primary NTP সার্ভারও বলা হয়। এক্ষেত্রে Stratum-0 এর সাথে ইহার কয়েকে মাইক্রো সেকেন্ডের ব্যবধান থাকে।

অনুরূপভাবে Stratum-2 সার্ভারসমূহ Stratum-1 এর সাথে, Stratum-3 সার্ভারসমূহ Stratum-2 এর সাথে নিজেদের সময় সিনক্রোনাইজ করে। এক্ষেত্রে সার্ভারসমূহ সরাসরি ফিজিক্যাল কানেকশন দ্বারা সংযুক্ত থাকে না, Network Reachable থাকলেই চলে। NTP এর ক্ষেত্রে 0 থেকে 15 পর্যন্ত লেভেলগুলো হলো Valid লেভেল। Stratum-16 দ্বারা বুঝায় ডিভাইসটি একটি Unsynchronized ডিভাইস।



Yellow arrows indicate a direct connection; red arrows indicate a network connection.

কনফিগারেশন: NTP Client

এখন আমরা অন্য আরেকটি রাউটার Router2 কে NTP ক্লায়েন্ট হিসেবে কনফিগার করবো। এতে Router2 রাউটারটি NTP ক্লায়েন্ট হিসেবে কাজ করবে এবং NTP_SVR এর সাথে নিজের সময় ও তারিখ সিনক্রোনাইজ করবে।

```
Router2#show clock
*00:21:51.791 UTC Fri Mar 1 2002
Router2#configure terminal
Router2(config)#ntp server 192.168.10.1
Router2(config)#end
```

```
Router2#show clock
10:28:11.145 UTC Thu Sep 25 2014
```

একটি NTP ক্লায়েন্ট NTP আপডেটের জন্য একটি NTP সার্ভারের সাথে নিজে থেকে যোগাযোগ করতে পারে অথবা NTP সার্ভারের কাছ থেকে ম্যাসেজ পাওয়ার জন্য অপেক্ষা করে। আমরা যদি চাই একটি NTP ক্লায়েন্ট NTP সার্ভারের কাছ থেকে অটোমেটিকভাবে Broadcast ম্যাসেজ গ্রহন করার মাধ্যমে সময় সিনক্রোনাইজ করবে তাহলে নিচের কমান্ড দিতে হবে। এজন্য ক্লায়েন্ট ডিভাইসের ইন্টারফেস নির্দিষ্ট করে দিতে হবে।

```
Router2#configure terminal
Router2(config)#interface fa0/0
Router2(config-if)#ntp broadcast client
```

NTP Client Configuration on Router3

```
Router3#show clock
*00:21:51.791 UTC Fri Mar 1 2002
Router2#configure terminal
Router3(config)#ntp server 192.168.10.1
Router3(config)#ntp peer 192.168.10.2


Router3#configure terminal
Router3(config)#interface fa0/0
Router3(config-if)#ntp broadcast client
```

আমরা show ntp status কমান্ডের মাধ্যমে সার্ভার ও ক্লায়েন্টের NTP স্ট্যাটাস দেখতে পারি।

```
NTP_SVR#show ntp status
Clock is synchronized, stratum 1, reference is .LOCL.
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**18
reference time is D7CE70F8.D2EE8BE6 (10:46:16.823 UTC Thu Sep 25 2014)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 0.02 msec, peer dispersion is 0.02 msec

Router2#show ntp status
Clock is synchronized, stratum 2, reference is 192.168.10.5
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**18
reference time is D7CE7111.BFF56099 (10:46:41.749 UTC Thu Sep 25 2014)
clock offset is -9.9029 msec, root delay is 16.07 msec
root dispersion is 19.53 msec, peer dispersion is 9.60 msec
```

NTP Authentication

যদি একটি Private NTP সার্ভারকে ইন্টারনেটের কোন NTP সার্ভারের সাথে সিনক্রোনাইজ করানো হয় তাহলে আমাদের লক্ষ্য রাখতে হবে ইন্টারনেটের NTP সার্ভারটি যেন একটি Valid ও Secured সার্ভার হয়। অন্যথায় তা নেটওয়ার্কের নিরাপত্তার জন্য হুমকি হয়ে দাড়াবে। যেমনঃ কোন এ্যাটাকার ভূয়া NTP ট্রাফিক পাঠানোর মাধ্যমে আমাদের নেটওয়ার্কে DoS এ্যাটাক করতে পারে।

NTP এমন একটি সার্ভিস যা নেটওয়ার্কের নিরাপত্তাজনিত কাজে ব্যবহৃত হয় কিন্তু প্রটোকল হিসেবে ইহা খুব একটা নিরাপদ নয়। সঠিকভাবে NTP অথেনটিকেশন মেকানিজম কনফিগার না করলে NTP ক্লায়েন্টসমূহ

বিভিন্ন অননুমোদিত NTP সার্ভার থেকে NTP আপডেটের সাথে সাথে Malicious ট্রাফিকও গ্রহন করতে পারে। এজন্য দুই ধরণের সিকিউরিটি মেকানিজম গ্রহণ করা যেতে পারে।

i. ACL Based Restriction Scheme
ii. Encrypted Authentication Mechanism with NTP version 3 or Later

NTP version 3 (NTPv3) ও এর পরবর্তী ভার্সনগুলোতে NTP ট্রাফিকসমূহ নিরাপদ রাখার জন্য সার্ভার ও ক্লায়েন্টসমূহের মধ্যে Cryptographic Authentication মেকানিজম যুক্ত করা হয়েছে। ইহা এনাবল করার জন্য সার্ভার ও ক্লায়েন্ট উভয় ডিভাইসেই নিচের কমান্ড দিতে হবে।

```
NTP_SVR#configure terminal
NTP_SVR(config)#ntp authenticate
NTP_SVR(config)#ntp authenticate-key 1 md5 c!$co234
NTP_SVR(config)#ntp trusted-key 1

Router2#configure terminal
Router2(config)#ntp authenticate
Router2(config)#ntp authenticate-key 1 md5 c!$co234
Router2(config)#ntp trusted-key 1
```

ক্লায়েন্টসমূহে NTP অথেনটিকেশন এনাবল করার একটি সুবিধা হলো যে, এতে ক্লায়েন্টসমূহ কোন Invalid সার্ভারের নিকট থেকে NTP আডেট গ্রহণ করবে না। সার্ভার ও ক্লায়েন্ট ডিভাইসে উপরিউক্ত কমান্ডগুলো দেওয়ার পর উভয়ের মধ্যে অথেনটিকেশন সম্পন্ন হতে বেশ কয়েক মনিট লেগে যায়। কোন একটি NTP সার্ভার অথেনটিকেটেড কি না তা আমরা ক্লায়েন্ট ডিভাইসে নিচের কমান্ডের মাধ্যমে দেখতে পারি।

```
Router2#show ntp associations detail | i 192.168.10.5
192.168.10.5 configured, our_master, sane, valid, stratum 1
```

কয়েক মিনিট পর.....

```
Router2#show ntp associations detail | i 192.168.10.5
192.168.10.5 configured, authenticated, our_master, sane, valid, stratum 1
```