Синхронізація часу IT-мереж та їх безпека – нові виклики

як покращити синхронізацію часу (NTP або PTP) без погіршення безпеки IT мережі

IT-мережі у сучасному світі забезпечують функціонування практично всіх галузей діяльності суспільства через створення, зберігання та обмін інформацією. Кожен з цих етапів роботи з інформацією потребує її ретельного захисту.

Одним з чинників, що забезпечує такий захист, безперечно, є інформація про точний час (часова мітка). Використання неточних або спотворених даних про час в сучасних умовах є критичною проблемою практично для всіх галузей: від мобільного зв'язку, фінансів, аероруху, енергетики, урядових та військових структур до кабельного телебачення та медицини.

Стосовно потреб в забезпеченні точним часом вказаних галузей IT-індустрія перебуває в тренді стрімкого зростання – вимоги основних галузей зросли, як мінімум, в 1000 разів за останні 5 років: з 1 секунди до 1 мілісекунди в фінансах та енергетиці, з 1 мілісекунди до 1 мікросекунди в мобільному зв'язку і т.д.

Таке зростання значущості інформації про час призводить до потреби в перегляді засобів для її створення, отримання та відповідного захисту на кожному з етапів роботи з нею.

Відповідно, там, де ще можливо забезпечувати вказані потреби за рахунок протоколу NTP, необхідно оптимізувати його роботу, а інша частина вимог вже може бути реалізована лише при доповненні NTP засобами нового протоколу – PTP.

а) б) в)

Рис. 1

Таким чином, звичний, найбільш поширений і найбільш бюджетний спосіб забезпечення IT-мереж часом від зовнішнього джерела часу NTP (Рис. 1, а)) потребує кардинального перегляду (Рис. 1, б), в)) з таких причин:

1) різко зросли вимоги до точності та надійності забезпечення часу;
2) зростання в потребі використання зовнішнього каналу надходження критичної для IT-мережі інформації;
3) потреба у використанні в повному обсязі всіх програмно-апаратних засобів сервера часу у складі IT-мережі для забезпечення її мітками часу.

На наступній сторінці схематично представлені типові технічні рішення для синхронізації часу з різними ступенями кіберзахисту на основі сучасних серверів часу **Microsemi SyncServer S600/650**, застосованих для широкого спектру споживачів.

Ці рішення забезпечують широке коло як спеціальних апаратних **(Time Firewall**; **GPS Firewall**; **DoS Firewall (Reflector™))**, так і програмних засобів:

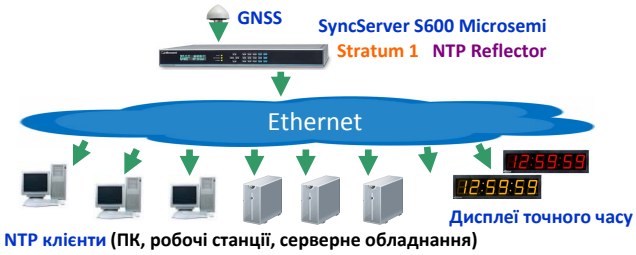
- NTP Autokey, TACACS, RADIUS і LDAP, X.509 HTTPS certificates
- NTP (SHA1 and MD5), SNTP (unicast)
- SNMP v2c, v3
- SNMP MIB II, Custom MIB, system status via SNMP
- DHCP/DHCPv6
- HTTPS/SSL (TLS 1.1/1.2)
- SMTP forwarding
- SSHv2
- Telnet
- IPv4/IPv6
- Syslog: 1 to 8 servers
- Key management protocols can be individually disabled
- Port 1: Management and Time protocols
- Port 2, 3, and 4 (optional 5 and 6): Time protocols only

WIRCOM
04070, м. Київ, вул. Волоська, 23, оф. 1
Тел. +38 044 467 63 64, 467 63 65
www.wircom.ua info@wircom.ua

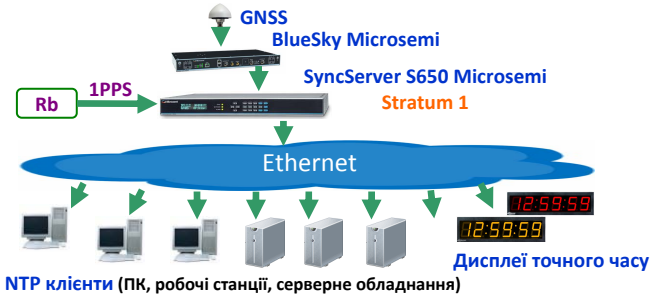
IT-мережі з внутрішнім джерелом часу (комерційні установи)

Time Firewall — Standard Solution

Time Firewall + DoS Firewall — Advanced Solution



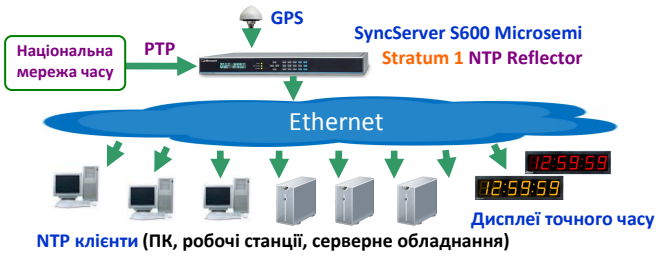
Time Firewall + DoS Firewall + GPS Firewall — Confident Solution



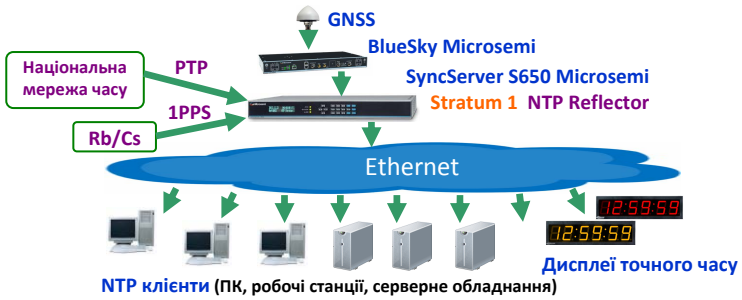
IT-мережі з внутрішнім джерелом часу (державні установи)

Time Firewall — Standard Solution

Time Firewall + DoS Firewall — Advanced Solution



Time Firewall + DoS Firewall + GPS Firewall — Confident Solution



Офіційний представник Microsemi (Symmetricom)

23 жовтня 2019, м. Київ

WIRCOM
04070, м. Київ, вул. Волоська, 23, оф. 1
Тел. +38 044 467 63 64, 467 63 65
www.wircom.ua info@wircom.ua

компанія WIRCOM проводить
XV Міжнародний семінар
"СИНХРОНІЗАЦІЯ ЧАСТОТИ ТА ЧАСУ В КОРПОРАТИВНИХ МЕРЕЖАХ"
Детальна інформація про семінар: www.wircom.ua

Sync 2019