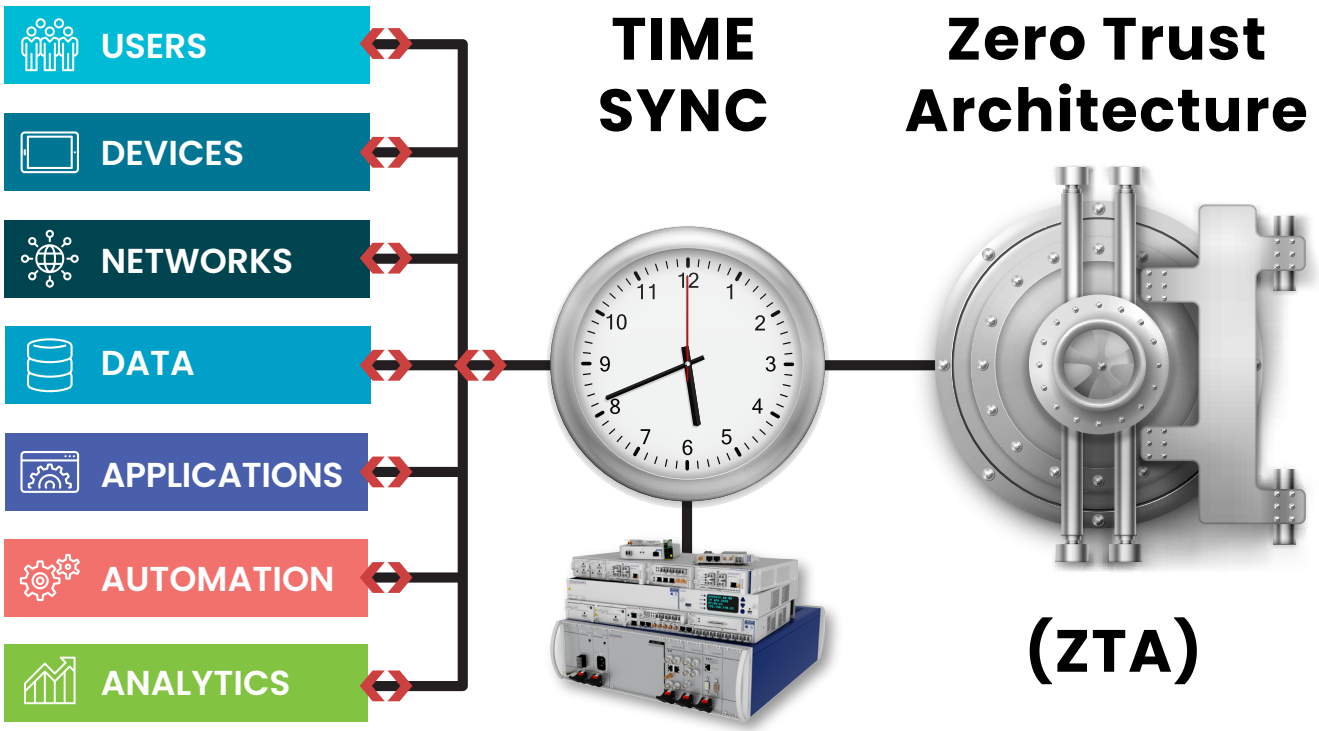
OSCILLOQUARTZ
A division of Adtran

Solution Brief



Precise time synchronization for ZTA

Why modern networks need Oscilloquartz time synchronization

Highlights

- **Zero Trust Architecture (ZTA) is becoming the base standard to guarantee the highest degree of security to modern computer networks. That makes precise and assured network synchronization vital to ensuring the proper operation of ZTA.**
- **Highly accurate and assured time synchronization also provides solid operational advantages in fields as diverse as finance, manufacturing, telecom, energy, metrology, academia, astronomy, defense systems and aerospace.**

Network time synchronization is an essential building block in IT operations and security for countless industries. It serves as the critical backbone in establishing a zero-trust architecture (ZTA) network. But what exactly is network time synchronization?

The process of network time synchronization (or time convergence) occurs throughout a network as each connected device accesses time from an accurate time server or primary clock. Automatic processes can trigger time synchronization. One example is directory synchronization and archiving. Jobs executing chronologically can also serve as a trigger.

We might assume that time on networked devices is correct or at least close enough. This mindset can be problematic. Computer and device clocks are notorious for time drift - the gradual speeding up or slowing down that skews the accuracy of devices by a few seconds per day. Time drift is a cumulative effect that creates significant errors over time.

The dramatic increase in distributed computing and interdependence of network infrastructures means a lot more elements need synchronization. And the issue of having device time continuously drifting apart puts the network, its security, infrastructure and applications running on it at risk for errors, failures and attacks. Time drift also makes impossible the proper implementation and realization of the many benefits of ZTA.

Precise time synchronization for ZTA

How aPNT+ provides trusted and precise time for ZTA networks

How ZTA works

Traditionally IT networks implemented defined safety perimeters. Inside the perimeter, all users, equipment and applications were thought secure. All security measures concentrated on protecting access to this perimeter. With cloud computing and remote access, this approach is no longer practical. That's because networks are now accessible anywhere across the globe.

With ZTA, each connected user, application and hardware device is continuously authenticated and authorized, with only necessary resources and data allowed network access. Access must therefore be granted individually in relation to the data and application instead of relying on a predefined perimeter. Never trust, always verify.

This approach helps ZTA reduce the risk of breaches and reduces the risk of cyberattacks by limiting access to sensitive data and equipment.

The need for reliable timing in ZTA

ZTA requires reliable time to enforce the safety of the network architecture. Precise time is a requirement for accurate timestamping and logging of relevant events, including:

- Connections and disconnections of every device
- Anomalous events that could be attacks
- Traffic bursts or lulls
- Fault diagnosis and recovery
- Event and application execution, critical in finance, trading, manufacturing (SCADA, automation, etc.), defense, aerospace and other time-sensitive applications
- Digital forensics
- Globally distributed computing and telemetry
- Regulatory/industry compliance standard behaviors

PTP versus GNSS versus NTP: Exact > Accurate > Close enough

The first step for proper ZTA is to establish a trusted and accurate primary time source, along with a protocol for delivering the time. The most common time synchronization protocols used in IT networks are Network Time Protocol (NTP), Global Navigation Satellite System (GNSS) and Precision Time Protocol (PTP).

NTP

NTP, currently in its fourth generation, is the oldest and most well-known protocol. Developed to mainly achieve accuracy in the sub-millisecond range, NTP has seen common adoption for network timekeeping. NTP, based on software timestamping, is where several factors including network latency, physical infrastructure (switches, routers, etc.), and power fluctuations can all negatively impact its accuracy. Therefore, NTP is not recommended for applications requiring critically accurate time synchronization.

GNSS

GNSS is a term that broadly encompasses all global satellite navigation systems. Global Positioning Satellite (GPS) is the most popular GNSS system globally. Developed by the US military in the 1970s, GNSS has been available to civilians since 1983.

Other GNSS systems include:

- GLONASS – Russia's global navigation satellite system
- Galileo – the European Union's global navigation system
- BeiDou – China's global satellite navigation system
- QZSS – Japan's regional satellite navigation system
- IRNSS – India's satellite navigation system

GNSS systems comprise a fixed constellation of dedicated orbiting satellites, each carrying:

- Stabilized Stratum 0 atomic clocks
- Transmitters continuously broadcasting their clock time and location coordinates
- Advanced location tracking hardware

GNSS satellites are specifically synchronized to the same time and locations because of their geosynchronous orbits. This results in receivers listening to multiple broadcast sources and using trilateration, similar to triangulation, to help determine their position and time deviation.

Nevertheless, the accuracy of GNSS has its limitations. Its accuracy is subject to fluctuations in atmospheric currents, solar eruptions, sky obstruction, harsh environmental conditions, etc. And the strength of the GNSS signal is very low, making signal jamming and spoofing relatively easy. This could be intentional attacks by hostile agents including criminal organizations or by accidental interference from anybody using inappropriate devices near the GNSS antenna.

PTP

Precision Time Protocol (PTP), also referred to as IEEE 1588 Version 2, is a network-based time synchronization standard created for distributing precise time and frequency from a clock source over packet-based networks. PTP achieves sub-microsecond accuracy through hardware timestamping. PTP also enables switches, routers and other IT infrastructure to deliver time synchronization with much greater accuracy than NTP. This makes PTP more suitable for modern data center infrastructures, WANs and cloud networks.

To achieve exact clock synchronization, PTP relays packet messages between the receiver and primary time source to ascertain an accurate measurement of the path delay in the network. PTP conveys time in "event" packet messages transmitted from a Grand Master clock (GM), or another primary clock, to a secondary clock, and vice versa. The network nodes then synchronize to the GM, ensuring all clocks accurately synchronize within a PTP network.

Precise time synchronization for ZTA

Leveraging PTP and GNSS for ZTA applications

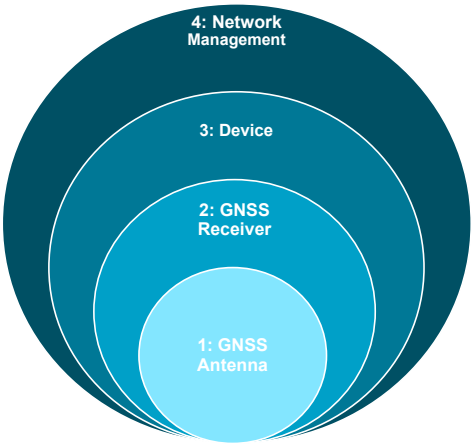
We have seen that PTP and GNSS are available for delivery of timing for ZTA applications. But what steps to take in implementing a robust timing architecture? The Oscilloquartz portfolio can help.

Our technology is the first in the industry to provide end-to-end timing distribution and assurance from the core to the last mile. With our solutions, IT teams can assess the accuracy of the network's phase and frequency synchronization every minute of every day. Embedded in all of our timing devices, our Syncjack™ technology includes a synchronization network management suite with an extensive set of tools for remote configuration and troubleshooting. That means no more sending field engineers to multiple sites in search of timing issues. With continuous updates while the network is up and running, operators can preempt synchronization degradation and take complete control.

Delivering accurate phase and timing from the core is challenging due to packet delay variation and delay asymmetry. Delay problems are correctable by locating one of our grandmaster/PRTCs closer to the end application, such as in the first aggregation node. This device can also manage network sync probing and assurance with minimal footprint and cost. Ideal for this application is our OSA 5401 SyncPlugTM™, a highly accurate and uniquely efficient SFP grandmaster clock and GNSS receiver with the smallest footprint and most compact design on the market. It brings precise timing deeper into access networks, including radio access and small cell networks.

Mitigating GNSS Jamming and Spoofing

GNSS signals at the ground level are very weak, with easy vulnerability to interferences that are both unintentional and intentional. To protect against interference, Oscilloquartz implements a layered protection strategy. The core functions of this strategy are to Prevent, Respond, and Recover. The four layers of GNSS signal protection functions are: Antenna, GNSS receiver, Device Software, and Management System.



Oscilloquartz provides four layers of GNSS signal protection

Mitigating GNSS Jamming and Spoofing (cont.)

Layer 1 – GNSS Anti-jamming antenna with modified antenna radiation pattern reduces signals arriving from low elevation sources. Since jamming typically originates at low elevations, this roof top antenna helps to mitigate jamming signals.

Layer 2 – GNSS receiver based jamming and spoofing detection functions.

- Jamming indicator mechanism measures continuous waves, sounding alarms at abnormalities
- Jamming monitor mechanism tracks background noise and alarm for significant signal variations
- Spoofing detection consists of GNSS Receiver based detection functions (L2) and Advanced Spoofing Detection Algorithm (L2+). These techniques successfully detect multi-constellations inconsistencies and position discrepancies.
- Advanced algorithm based on stateless detection, is able to distinguish genuine satellites signals and software-defined radio (SDR) signals. This Layer 2+ protection is capable of detecting multi-constellations and multi-band spoofing attacks. Can also detect attacks involving device locations and time discrepancies.

Additionally, GNSS Integrity monitoring functions include providing satellites in view AGC, C/No measurements and comprehensive alarm functions.

Precise time synchronization for ZTA

Layer 3 – Device based spoofing detection and protection functions

- Build-in SyncJack monitoring feature mitigates spoofed GNSS signal basing on reliable reference from other sources like PTP or PPS+ToD
- GNSS Jamming and Spoofing protection function can disqualify compromised PNT source and automatically switch to alternative reference

Layer 4 – Detection and protection provided by Network Management System

- GNSS Assurance functions of Ensemble Controller engage Machine Learning algorithms in searching for signal anomalies
- GNSS Firewall feature activates GNSS failover switch in case vulnerabilities detected

Enabling four layers of protection in Antenna, GNSS Receiver, Device Software, in tandem with management system support are the best ways to augment protection against vulnerabilities in GNSS signals.

Recommended Oscilloquartz solutions for ZTA networks

OSA 5412/22 – Secure time reference for ZTA networks

Reliable and accurate delivery of synchronization and time is essential to meet the stringent requirements of mission-critical applications in multiple market areas such as mobile backhaul, power utilities, defense, finance and broadcasting. Our OSA 5412/22 offers a unique flexibility for a versatile and accurate synchronization device that can meet the most stringent frequency, time and phase synchronization demands.

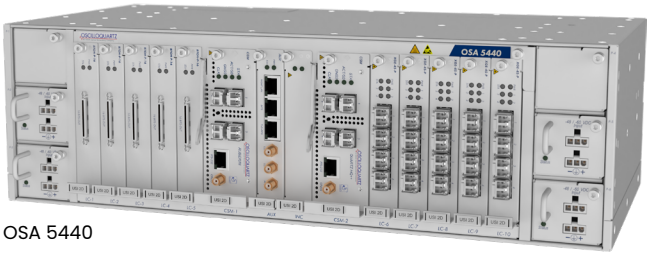
OSA 5422

OSA 5412

OSA 5430/40 – Carrier-grade time reference for ZTA networks

Delivering aPNT+ time and synchronization from the core to the network edge is essential to meet the stringent requirements of new mobile, fixed and cable networks. Our OSA 5430/40 are carrier-grade ePRTC, PRTC A/B, SSU, and IEEE 1588v2 grandmaster clock supporting 10Gbit/s and 1Gbit/s interfaces with hardware timestamping. Their modular design offers full redundancy and incomparable flexibility in the most compact design.

OSA 5430



OSA 5440

Security features in OSA 5412/22 and OSA 5430/40 families

User security

Access to any Oscilloquartz device, either over local or remote access, must be controlled and highly secured. Our OSA 5412/22 and OSA 5430/40 families manage users' access, including the highest security features.

- User access via different security levels
- Up to 5 levels of privileges for local users
- User security policy configurable per user with three pre-defined levels
- User management, including username and password creation, deletion, login timeout, CLI paging
- Secure Socket Layer (SSL)
- Support for security using Secure Hypertext Transfer Protocol (HTTPS) over TLS 1.2
- Use of Secure Shell (SSH) management protocol
- Use of remote authentication Radius or TACACS
- Support of SNMPv3
- Customizable post login security banner on web + CLI
- Access Control List (ACL) management
- Two factors authentication
- LDAP Authentication (release 12.5 and above)
- Adjustable session timeout

Why modern networks need Oscilloquartz time synchronization

Device
Ensure every device connected to your ZTA network has all the necessary features to keep your equipment and network safe and not create breaches for potential security concerns. Our OSA 5412/22 and OSA 5430/40 delivers the following features:

- High-level encryption SHA-512 with random salt of 8 characters to store sensitive information
- Enable / Disable ntpd symmetric key
- ntpd MD5 or SHA1 authentication
- ntpd Autokey Server and Autokey Client
- HTTP / HTTPS secure management over TLS 1.2
- Individually Enable/Disable protocol, Serial, Telnet, SSH, HTTP, HTTPS, FTP, SFTP, SCP, NTP, PTP, ToD
- Access via serial port enable/disable capability with automatic user log off
- Multiple LAN ports / virtual ports capability
- Management port separated from timing ports to protect from attacks
- 1 to 10 ports dedicated for timing in OSA5412 (not subject to potential attacks from management), with additional line cards expansion in OSA5422, OSA5430 and OSA5440 (up to 10 LC in 5440)

Application
To ensure OSA 5412/22 and OSA5430/40 software and applications are always kept operating at the highest security levels and ready to react against any new event, Oscilloquartz has instituted the following security guidance:

- Adtran security vulnerability management via PSIRT framework structure and CPSA (Customer Product Security Advisory)
- Software upgrade via Adtran authenticated customer portal
- Software download platform protected by highly secured authorization and encrypted image files

Network
Network connectivity continuously requires the highest degree of protection and security. OSA 5412/22 and OSA 5430/40 use the highest secured protocols and can cope with the most stringent requirements

- Configurable web session timeouts up to 99 mins
- Software locks the login account for 5 minutes after three failed login attempts
- Authentication via SNMPv3 MD5/SHA1 protocol and privacy cryptography selectable between DES / AES (128 bits)
- Connection through SSH and SSL-based protocol
- Remote network connection with four levels of users pre-configured (Admin, Monito, Operator, Provision)
- Remote source SSL certificate support in X.509 format (CRT)
- Support of Self-signed certificate or from tested certificate authority
- Up to 4 different CA authority profiles
- System default CA profile
- Automatic certificate enrollment using Secure Certificate Enrollment Protocol (SCEP)
- Traffic restriction per port and per IP addresses
- Hardware-based ACL on NTP and/or PTP to protect from Distributed Denial-of-Service (DDoS) attack
- RADIUS authentication IPv4/IPv6 with configurable port (default 1812)
- TACACS+ remote authentication IPv4/IPv6 with configurable port (default 49)
- Configurable timeout 2 to 10 sec and configurable maximum number of attempts 0 to 5
- supporting up to 3 servers and customizable port number

Data
Keep sensitive data perfectly protected while safeguarding everyone's privacy

- Enable/Disable Data Anonymity after a configurable period of up to 1096 days

Automatization – environment
Do not let anything be uncontrolled in your network. Prevent, respond, and recover are the keys for successful and 100% efficient protection.

- Full FCAPS Network Management ENC R.14.x or higher
- Advanced jamming and spoofing detection

Analytics – visibility
Centralization and monitoring of all logs are crucial in incident response, threat detection and compliance with the security environment. SYSLOG is an incontrovertible player for intrusion detection systems and intrusion prevention systems (IDS/IPS)

- Security, alarm, and audit logs support SYSLOG (RFC3164) with configurable port number

OSCILLOQUARTZ
A division of Adtran

TL9000
TL19.1270

ADTRAN Certified Supplier
ISO 9001
ISO 14001
TL 9000