TSM_SecIndOpT

Communication technology relevant to OT environment (II) Version: 1.2

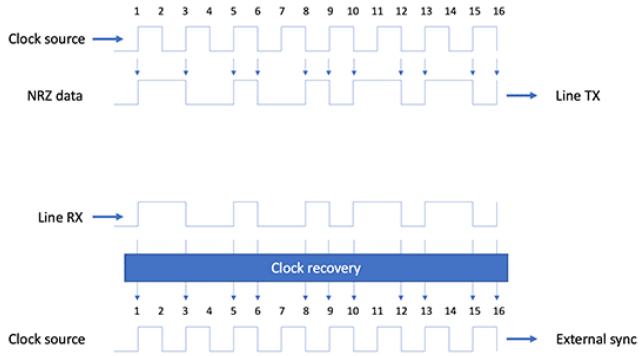
Luca Haab | 16/03/2026 | Cours MSE

LAN Continued

SyncE and PTP 1588

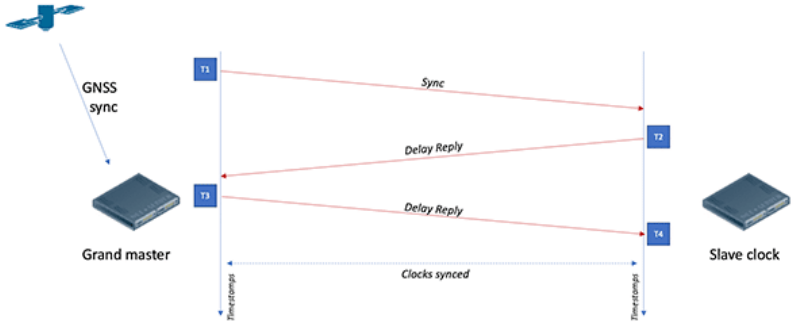
SyncE

- **Sync**hronous **E**thernet (ITU-T Rec. G.8261, G.8262 and G.8264) uses a traditional synchronisation delivery method where synchronisation is derived from the edges of the pulses being sent across the transmission medium.
- A high-quality clock reference (e.g. GPS clock source or a caesium clock) is used to time the



PTP

- **P**recision **T**ime **P**rotocol uses a protocol (IEEE 1588-2019) to deliver the timing to the edge of the network.
- PTP Grandmaster takes a sync source (usually a GPS based source) and uses this source to create a series of timestamped PTP packets sent out across the network to slave clocks that use the PTP protocol to create a sync signal for use on its local



Images from: https://frame.co.uk/understanding-the-difference-between-ptp-and-synchronous-ethernet/

SyncE and PTP 1588

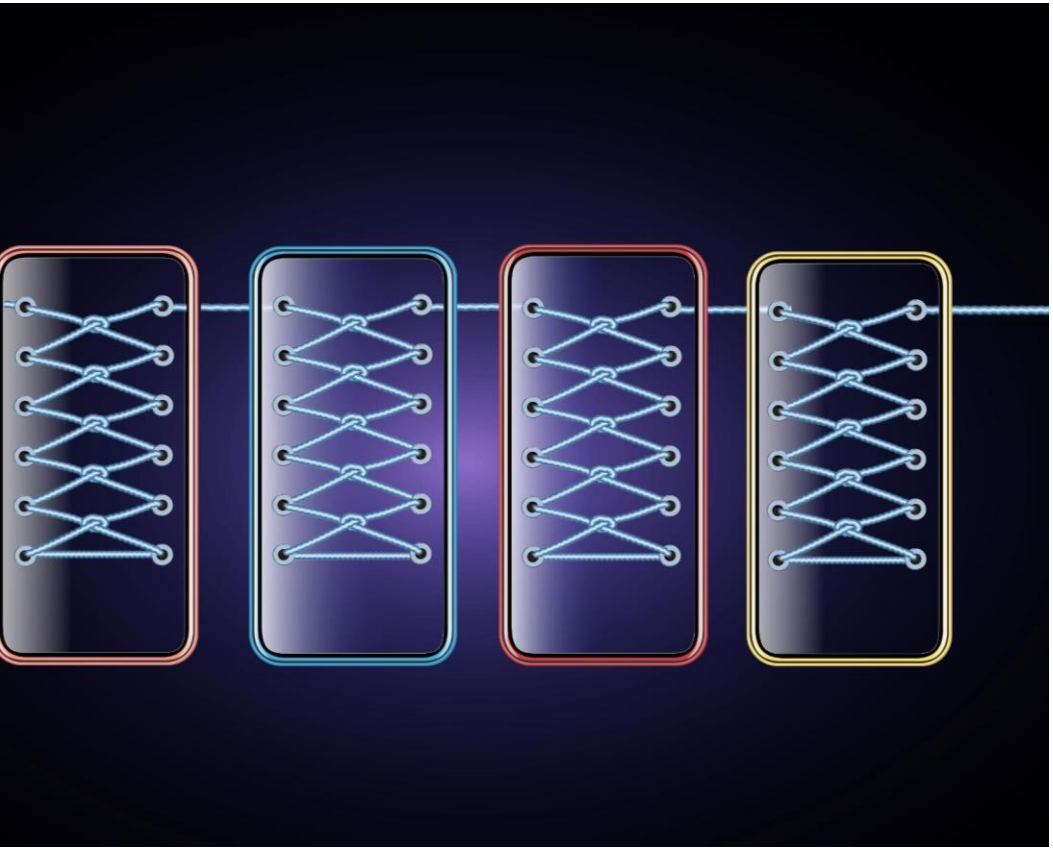
	SyncE	IEEE 1588	IEEE 1588 + Transparent Clocking
Timing Path Continuity	All nodes in the timing path must support SyncE. Any ±100 ppm free-running nodes in the timing path will break chain of synchronization.	Only Master and Slave nodes need to support 1588. Nodes between these are totally unaware of the timing packets and can run using ±100 ppm free-running clocks.	All nodes between Master and Slave need to support 1588. Nodes between these can run using ±100 ppm free-running clocks.
Number of Nodes in the Synchronous Timing Path	Frequency accuracy can be distributed over several nodes (<60) before being re-timed by a higher level clock.	Number of ±100 ppm free-running nodes in the timing path between the master and slave is limited (<10)	Number of ±100 ppm free-running nodes in the timing path between the master and slave is improved (>10). The maximum limit is dependant on the application and the loop algorithms.
Frequency Accuracy	Meets the same performance requirements as SONET/SDH line timing.	Much lower frequency accuracy than SyncE. Performance is dependent on the network's PDV.	Lower frequency accuracy than SyncE. Performance is much less dependent on the network's PDV.
Phase Alignment	Not supported	Phase alignment up to 1 µs is possible depending on PDV.	Phase alignment much less than 1 µs is possible.
Time Of Day	Not supported	Supported	Supported

May be combined

Feature	SyncE	PTP
Primary Goal	Frequency Sync	Time & Phase & Frequency
Layer	Physical Layer	Data Link/Network Layer
Network Requirement	All devices need to support SyncE	Optimized by PTP-aware nodes (BC/TC)
Best For	Stable frequency references	Phase/Time-sensitive apps

PDV: Packet Delay Variation resulting from store&forward behaviour

Source: Silicon Labs AN420 "SYNCE AND IEEE 1588: SYNC DISTRIBUTION FOR A UNIFIED NETWORK"



Time Sensitive Networking (TSN)

Deterministic Data Transmission

TSN enables deterministic data transmission, allowing for predictable delivery of critical data packets.

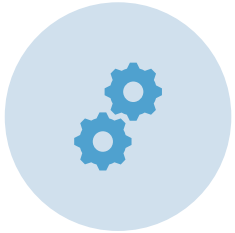
Industrial Automation Applications

TSN is particularly suitable for industrial automation applications where timely data delivery is essential for operations.

Standardized

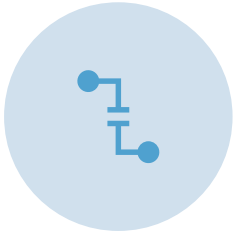
TSN is part of the IEEE 802.1 working group

Time Sensitive Network (TSN)

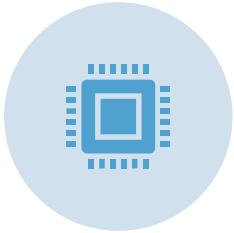


Precise Time Synchronization
TSN facilitates synchronization among devices, ensuring that data transmission aligns precisely with the defined time parameters. This synchronization capability is crucial in applications where coordinated actions are fundamental, such as industrial automation.

Bandwidth Allocation and Prioritization
TSN allows for the allocation and prioritization of network bandwidth, enabling critical data streams to take precedence over non-time-sensitive traffic. This feature ensures that mission-critical information reaches its destination without delay, vital in scenarios where split-second decisions are imperative.



Enhanced Reliability
By minimizing latency and packet loss, TSN elevates the reliability of data transmission, thereby fostering a more dependable network infrastructure. Industries reliant on real-time data, like those employing industrial switches, benefit immensely from this improved reliability.



Interoperability
One of the significant strengths of TSN is its interoperability with existing Ethernet standards, providing a seamless integration path for legacy systems. This compatibility ensures a smoother transition for industries adopting TSN technology.

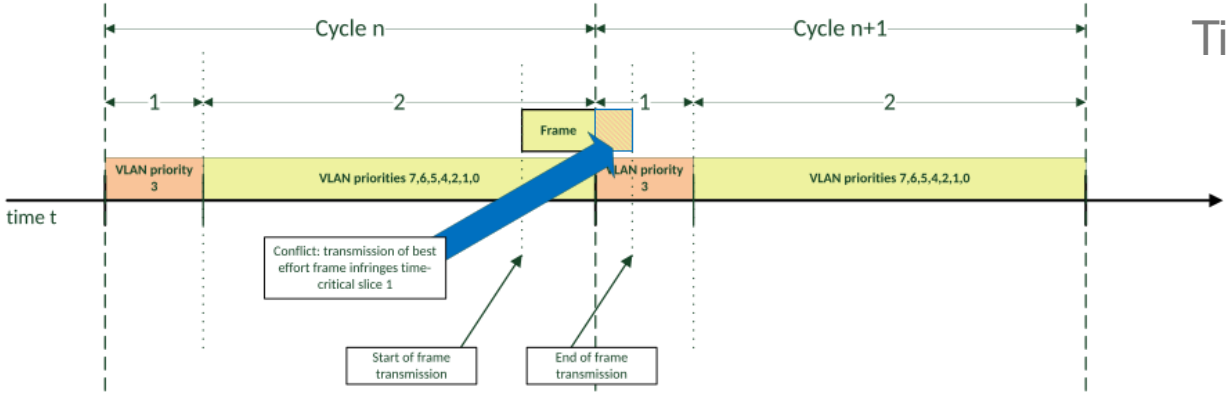
Source: https://community.fs.com/article/the-introduction-of-timesensitive-networking-tsn.html

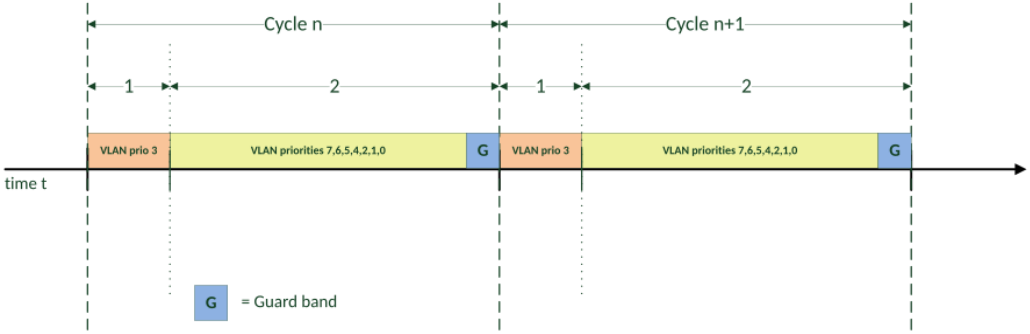
Standard	Definition	Title of Standard	Functionality
IEEE 802.1ASrev, IEEE 1588	Timing and synchronization	Enhancements and performance improvements	It establishes a common timebase among TSN-enabled devices, allowing them to operate with a shared perception of time, ensuring that clocks across the network are precisely synchronized.
IEEE 802.1Qbu and IEEE 802.3br	Forwarding and queuing	Frame preemption	It enables the quick transmission of urgent data by preempting lower-priority frames, minimizing latency for critical information.
IEEE 802.1Qbv	Forwarding and queuing	Enhancements for scheduled traffic	This protocol enables the allocation of time slots for different types of data traffic, ensuring that time-critical data gets precedence over less time-sensitive information.
IEEE 802.1Qca	Path control and reservation	Path control and reservation	It enables dynamic path management, configuration, and resource reservation within TSN, ensuring efficient and reliable transmission of critical data streams by optimizing network paths.
IEEE 802.1Qcc	Central configuration method	Enhancements and performance improvements	It offers improved stream management and control, optimizing network performance for time-sensitive applications.
EEE 802.1Qci	Time-based ingress policing	Per-stream filtering and policing	It allocates resources and reserves bandwidth for specific streams or traffic classes, ensuring that essential data streams receive the required network resources for timely transmission.
IEEE 802.1CB	Seamless redundancy	Frame replication and elimination for reliability	It allows for redundancy in data transmission paths, ensuring that if one path fails, an alternate path can be used to maintain uninterrupted communication.

Time Sensitive Network

IEEE 802.1Qbv in more detail:

Time slices and guard bands





G = Guard band $= \frac{1542\ \text{byte}}{12.5 \cdot 10^6\ \text{byte} \cdot \frac{1}{s}} = 123.36 \cdot 10^{-6} s$

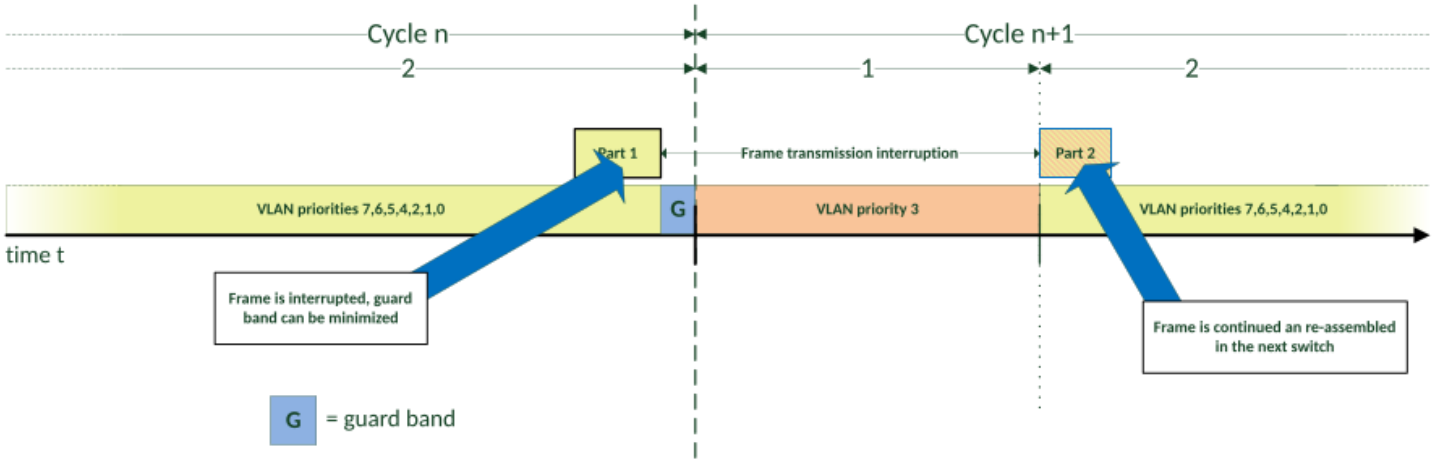
Source: https://en.wikipedia.org/wiki/Time-Sensitive_Networking

swissuniversities

Time Sensitive Network

Requires both ends to support this feature

IEEE 802.3br and 802.1Qbu
Interspersing Express Traffic (IET) and Frame Preemption



Source: https://en.wikipedia.org/wiki/Time-Sensitive_Networking

Air-Gapped

Network Working Group R. Shirey
Request for Comments: 4949 August 2007
FYI: 36
Obsoletes: 2828
Category: Informational

Internet Security Glossary, Version 2

$ air gap
(I) An interface between two systems at which (a) they are not connected physically and (b) any logical connection is not automated (i.e., data is transferred through the interface only manually, under human control). (See: sneaker net. Compare: gateway.)

Example: Computer A and computer B are on opposite sides of a room. To move data from A to B, a person carries a disk across the room. If A and B operate in different security domains, then moving data across the air gap may involve an upgrade or downgrade operation.

$ sneaker net
(D) /slang/ A process that transfers data between systems only manually, under human control; i.e., a data transfer process that involves an air gap.

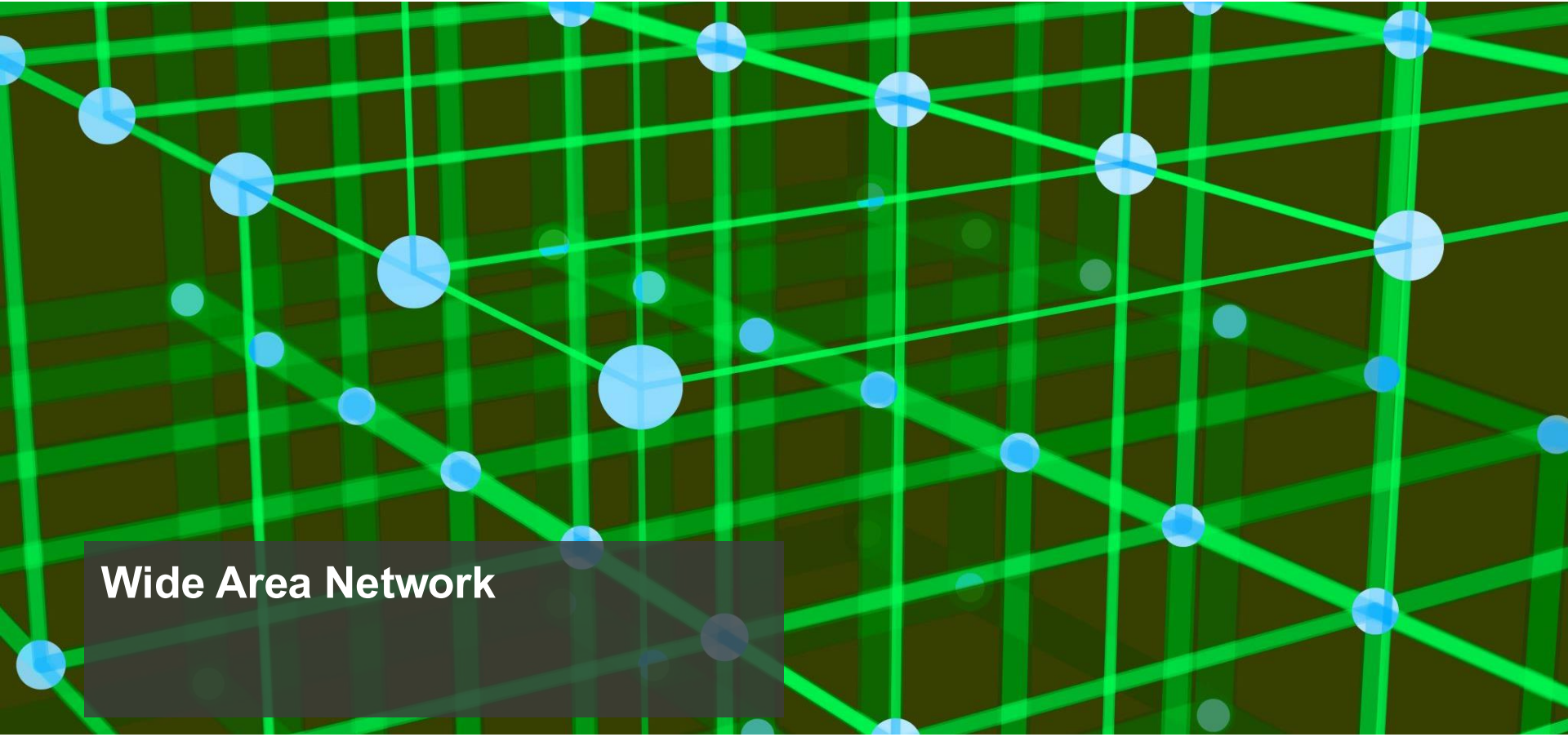
Source: https://datatracker.ietf.org/doc/html/rfc4949

Benefits

- Increased threat mitigation
- Regulatory and Audit compliance
- Data integrity and control

Challenges

- Infrastructure requirements
- Insider threats and security breaches
- Updates and maintenance



Wide Area Network

WAN Requirements

Main requirements
- Deterministic end-to-end performance
- Guaranteed QoS, (symmetric) delay & Jitter
- Precision time & clock
- Encrypted packet real-time operation
- Path protection switching (<50ms)

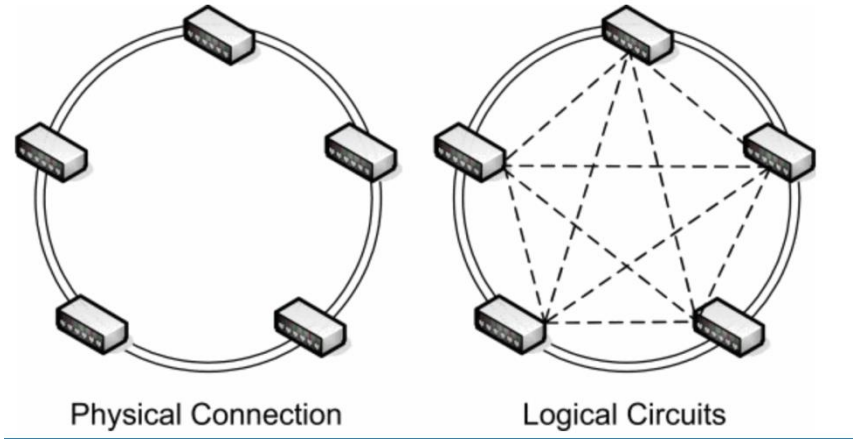
But also
- 5x9's availability
- Fanless & harsh environment* operation
- Meets regulatory standards

*: typically -25° - 60°C with up to 100% humidity

Source: https://hk.element14.com/

Former established WAN technology

- Connection-oriented
- Synchronous frames
- Clock distribution
- Fast Protection Switching (<50ms)
- OAM (Operation And Maintenance)
- Limited topology
- Bandwidth waste

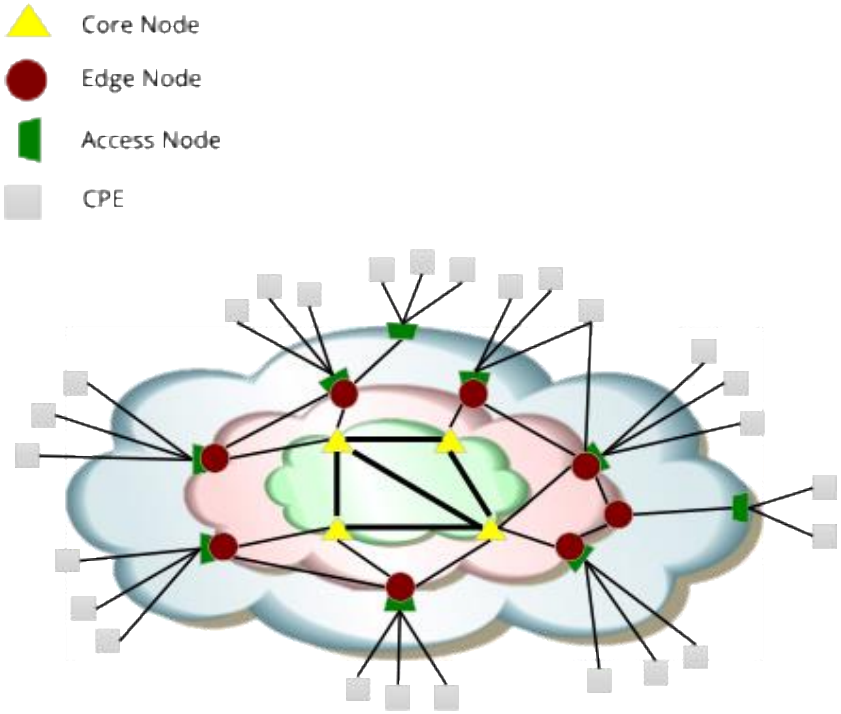


- Examples: SDH and predecessors…

Source: https://ieeexplore.ieee.org/document/4075833

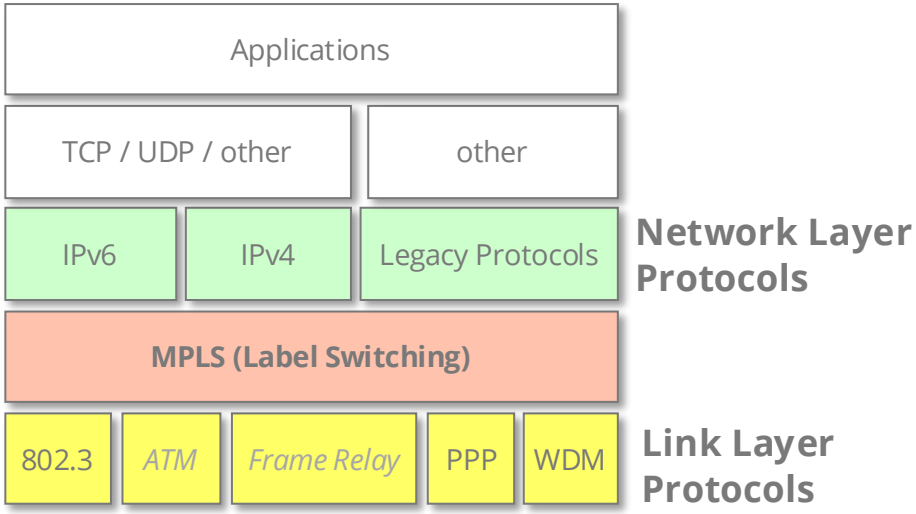
SDH: Synchronous Digital Hierarchy, see also https://en.wikipedia.org/wiki/Synchronous_optical_networking as well as standards ITU G.707, G.783, G.784 and G.803

Routers too slow, what to do?



Source: https://due.com/4-things-business-slow/

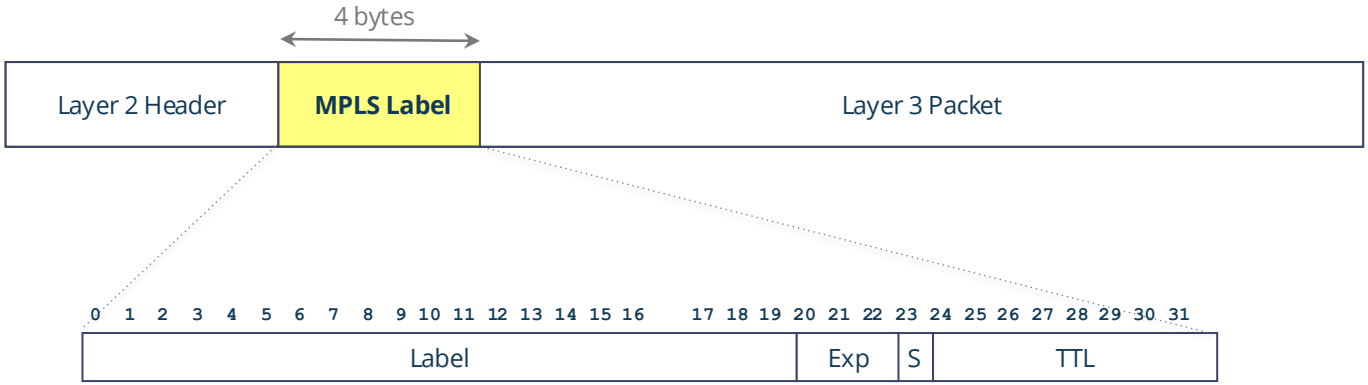
Multi Protocol Label Switching



- Defined in RFC 3031 (January 2001), RFC 6178 (2011) and RFC 8012 (2016)
- Data transport protocol based on label switching or '***labels***'
- Operates between layer 2 & 3 of the OSI model referred to as a **layer *2.5*** protocol
- **Independent of** layer 2 and 3 protocols
- Linking the recipient's IP address with an **entry reference** in the network (labels)
- Interface to existing routing protocols
- Allows the deployment of various applications such as:
  - *Virtual Private Network*
  - *Access Network traffic aggregation*
  - *Traffic Engineering*
  - *Quality of Service*
  - *Any Protocol over MPLS (Pseudo Wire)*

MPLS slides: credits to F. Buntschu, Ass. Professor @ HTA-FR

MPLS Frame



***Label* [20 bits]**	Label value
***Exp* [3 bits]**	Experimental, currently used as *Class of Service* (CoS) in« *Diffserv over MPLS* » [RFC3270]
***S* [1 bits]**	End of label stack
***TTL* [8 bits]**	Time to live

Note: the *MPLS Label* may be oftentime called "*shim*" header (or "*sham*")

MPLS Terms

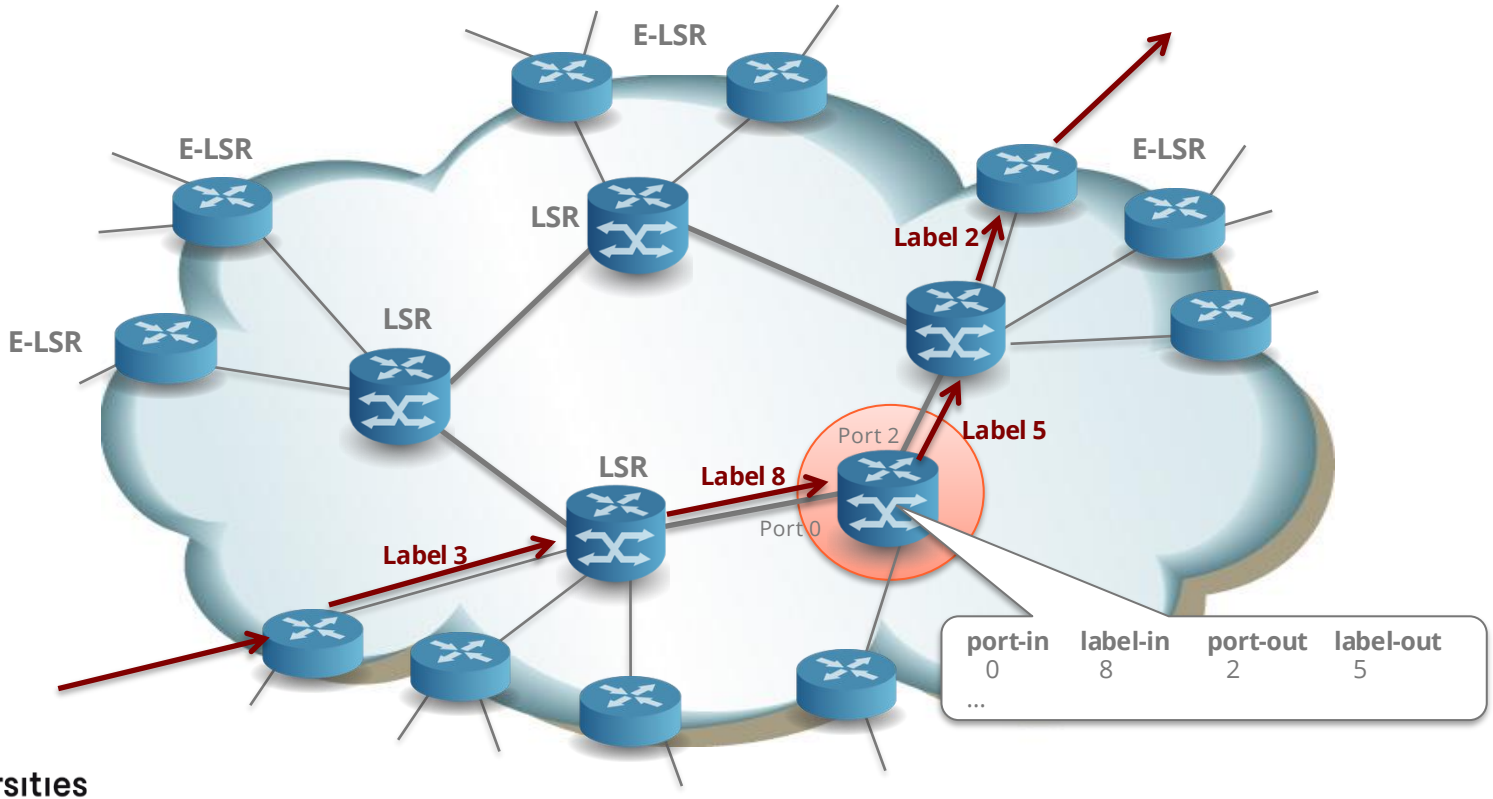
- **Label** and *label stack*

- **FEC** – *Forwarding Equivalence Class*
- **LIB** – *Label Information Base*
- **LFIB** – *Label Forwarding Information Base*

- **LER** – *Label Edge Router*
- **LSR** – *Label Switching Router*

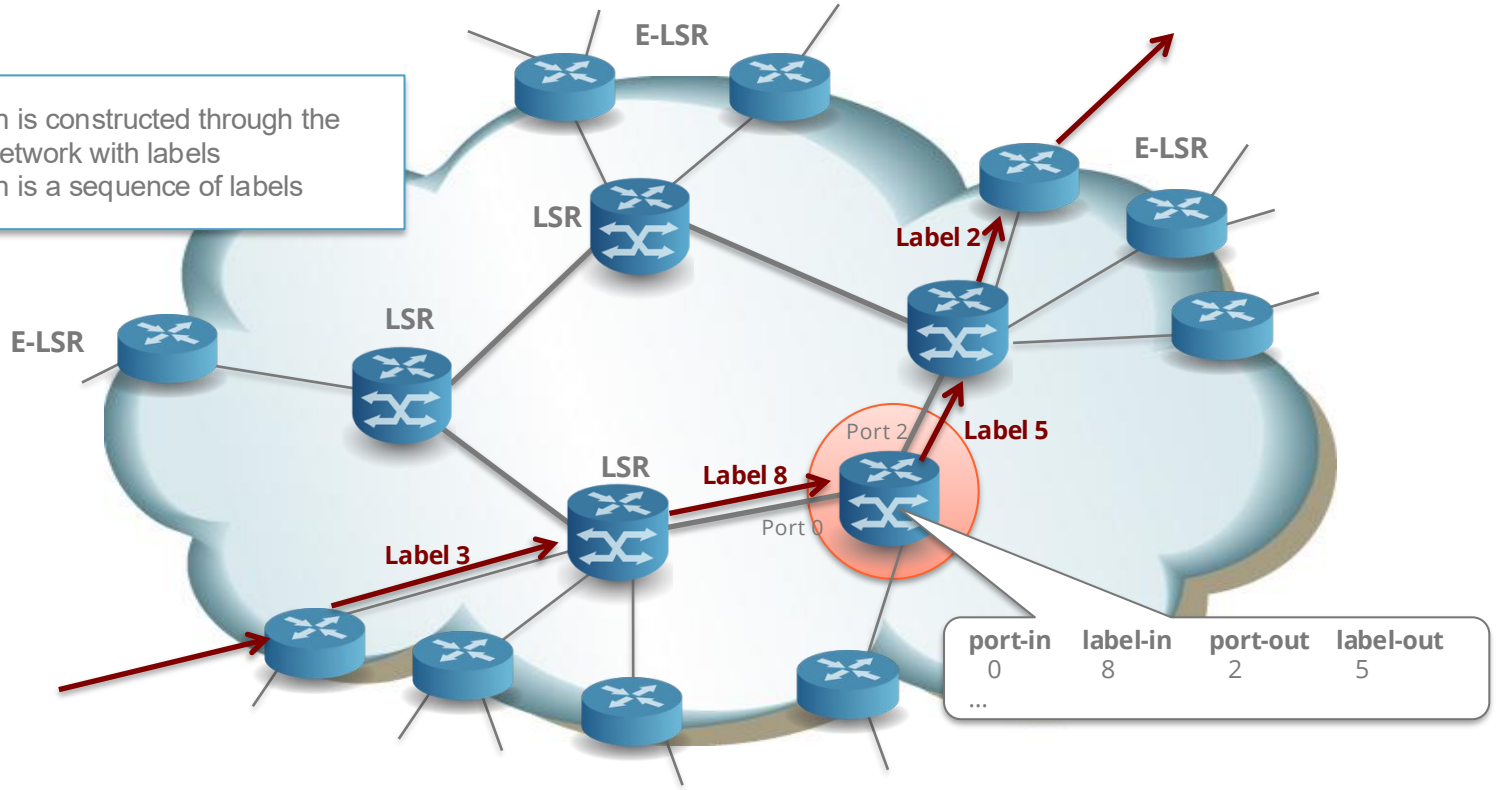
- **LDP** – *Label Distribution Protocol*
- **LSP** – *Label Switched Path*

MPLS : topology example



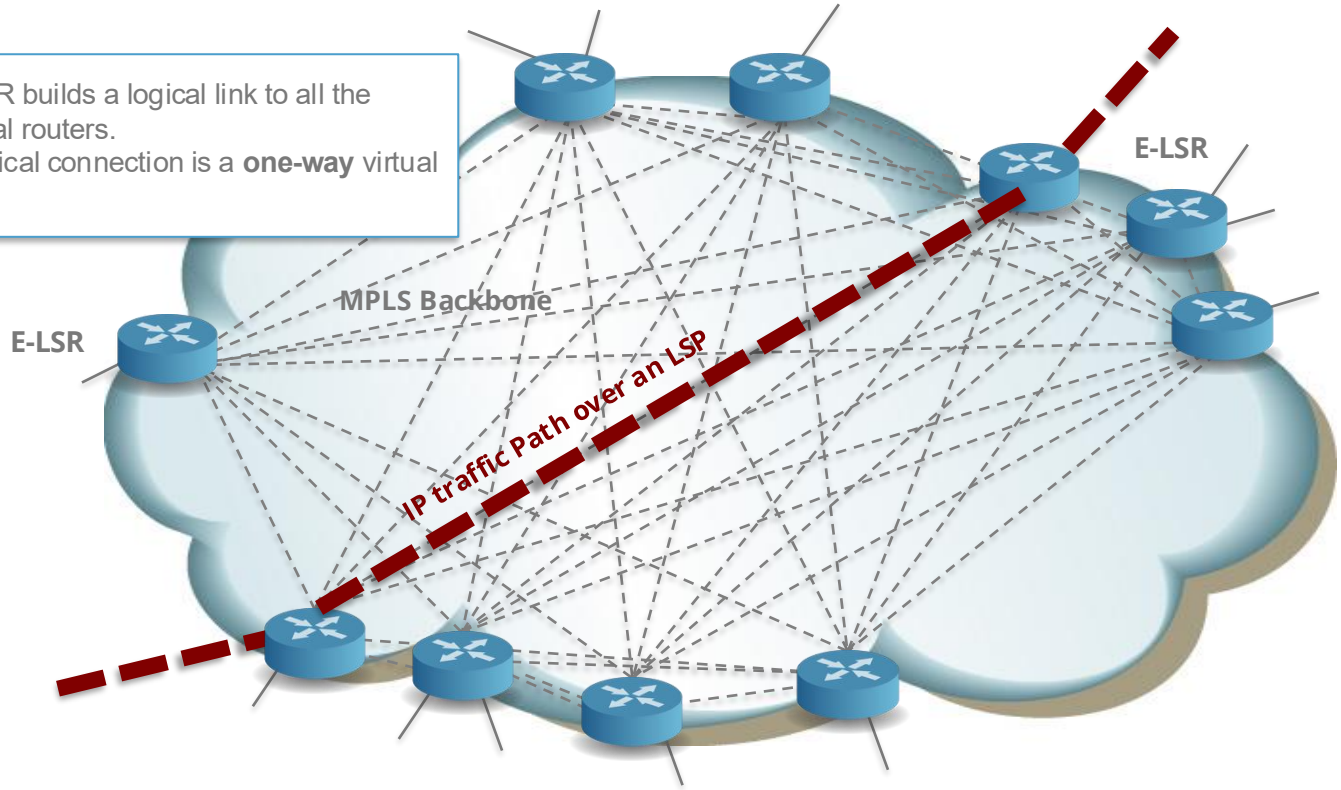
Label Switched Path (LSP) (1)

- The path is constructed through the MPLS network with labels
- The path is a sequence of labels

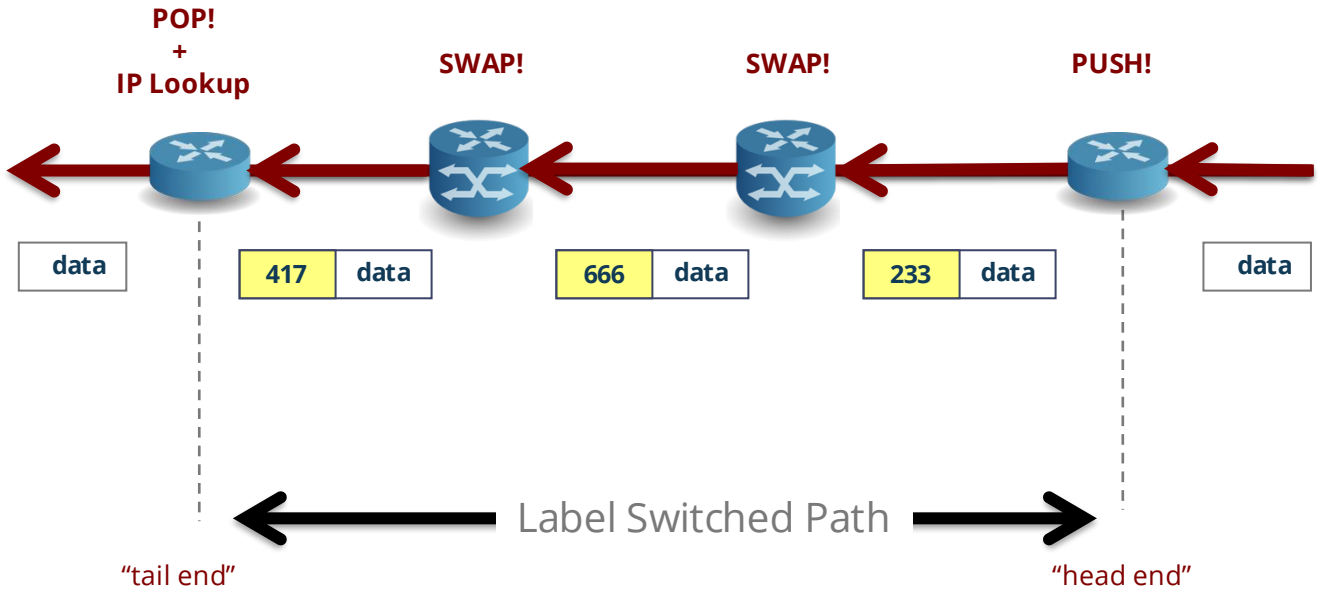


Label Switched Path (LSP) (2)

- Each LER builds a logical link to all the peripheral routers.
- Each logical connection is a **one-way** virtual link



Label Switched Path (LSP) (3)



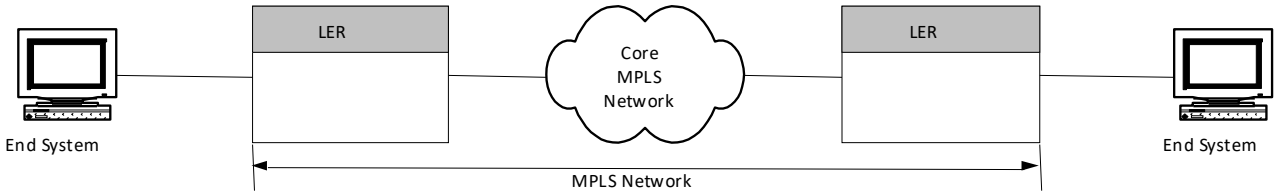
Often called a tunnel (path) MPLS: the headers contained in the data are not inspected in an LSP.

LSR vs E-LSR (or LER)

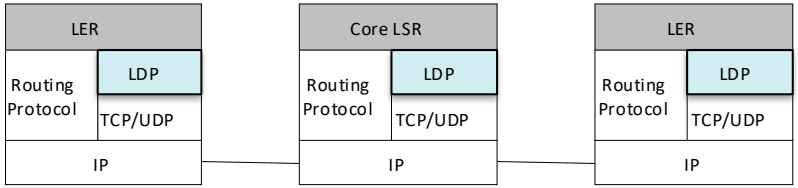
- **LSR**: *Label Switching Routers*
  - Generally core routers
  - High-speed data switching
  - Participates in the establishment of LSPs (Label Switching Paths)

- **E-LSR** or **LER**: *Edge LSR* or *Label Edge Routers*
  - Operates on the periphery of MPLS networks
  - Supports multiple ports connected to different networks
  - Transmits traffic through the LSPs established in the MPLS network (ingress)
  - Redistributes traffic to the access network (egress)
  - Allocation & deletion of labels associated with the FEC

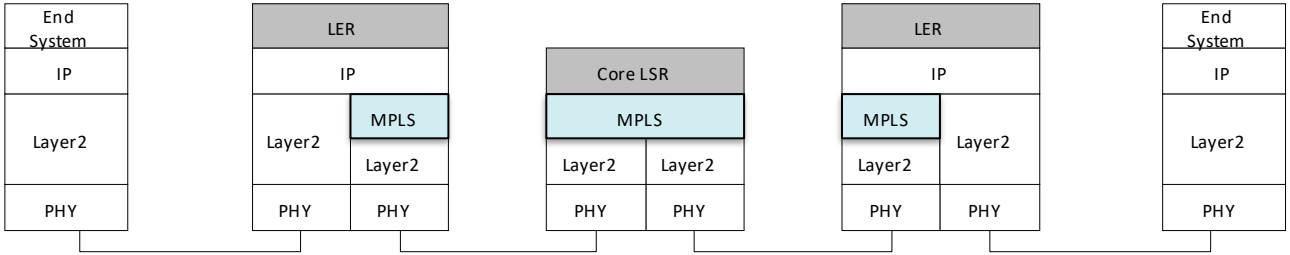
MPLS : Protocol stack (2)



MPLS Interworking Architecture



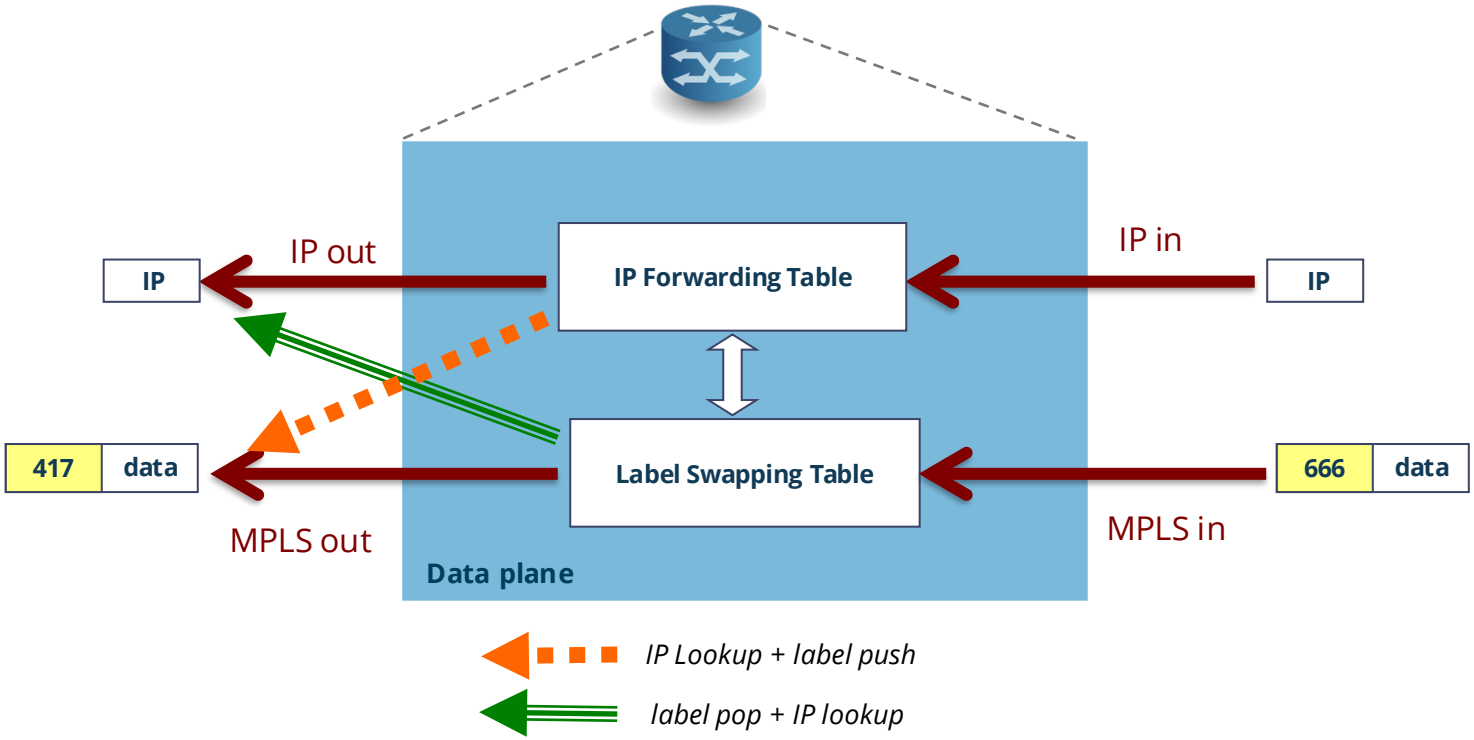
MPLS Control protocol Stack Architecture



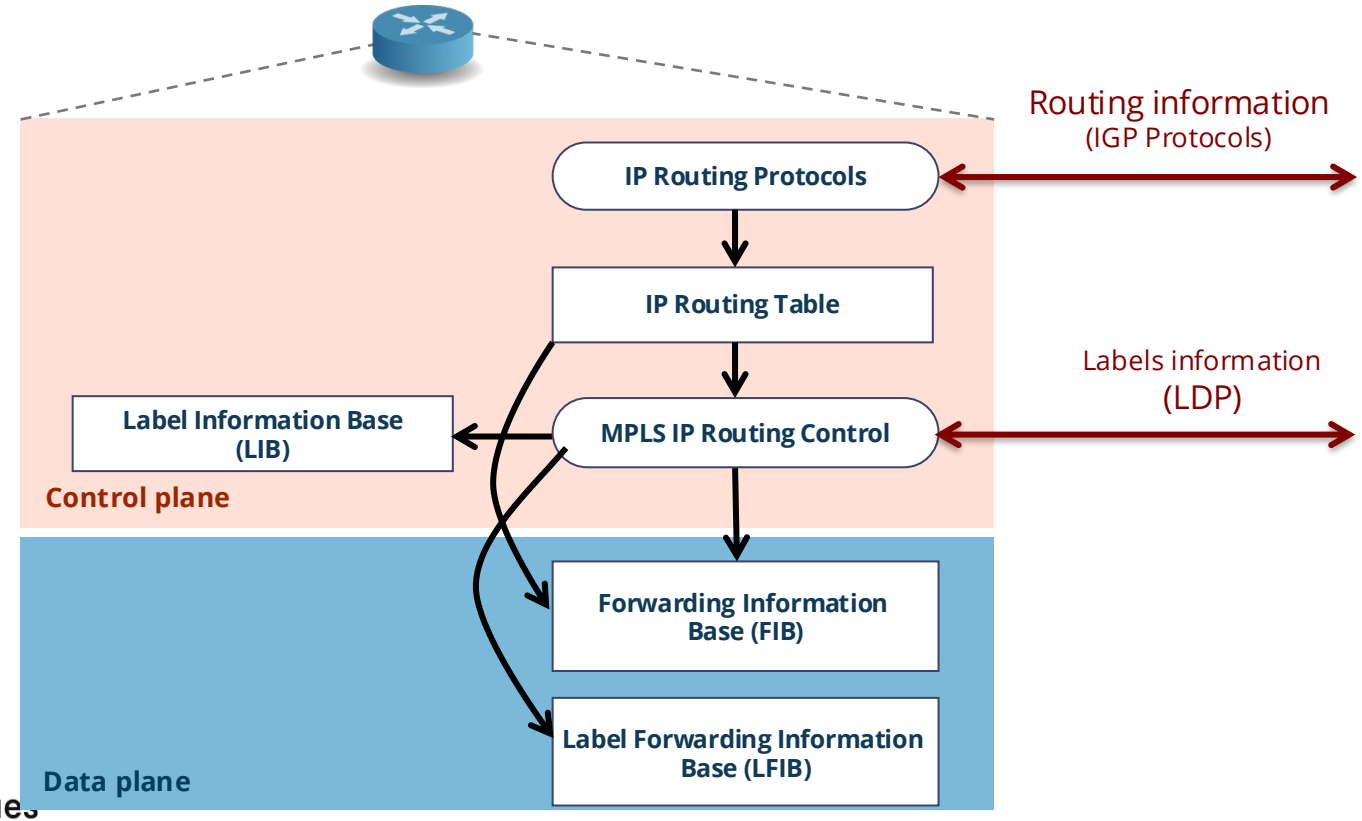
MPLS Data Protocol Stack Architecture

Source: LG Information & Communications, Ltd.

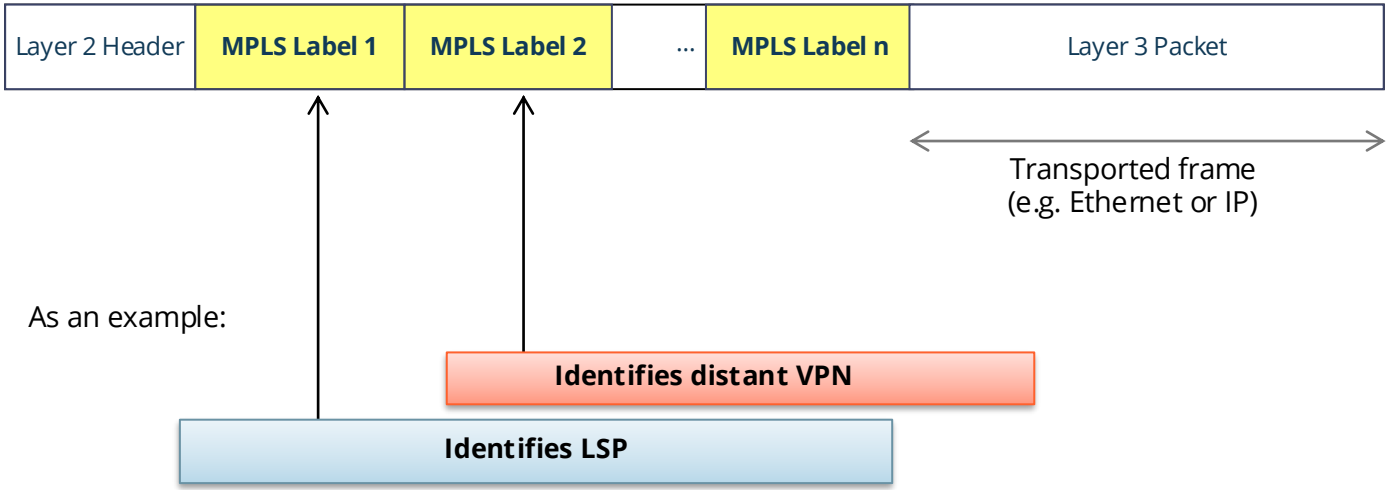
Label Switching Router (LSR)



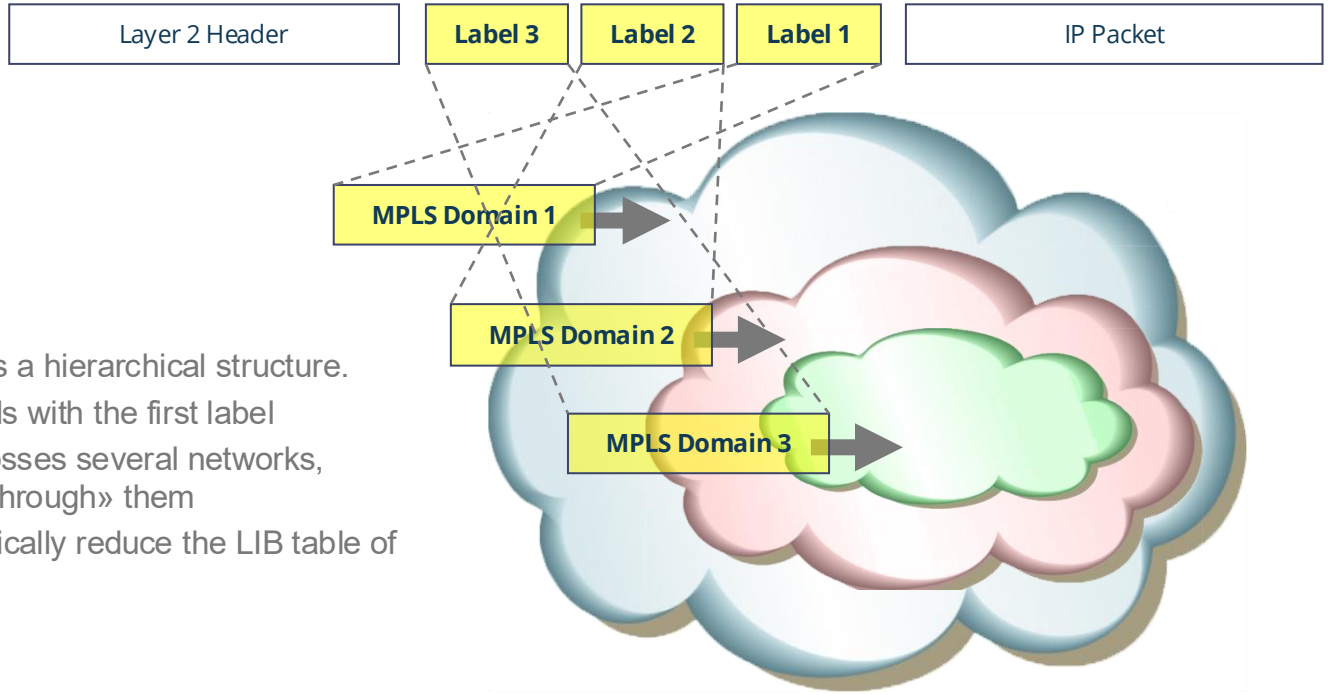
Edge Label Switching Router (E-LSR)



Labels stacking (1)



Labels stacking (2)



- MPLS supports a hierarchical structure.
- Each LSR deals with the first label
- If the traffic crosses several networks, it can «tunnel through» them
- Benefit – drastically reduce the LIB table of each router

MPLS: IP and Transport Protocol (I)

Source: https://www.noction.com/blog/mpls-tp-multi-protocol-label-switching-transport-profile

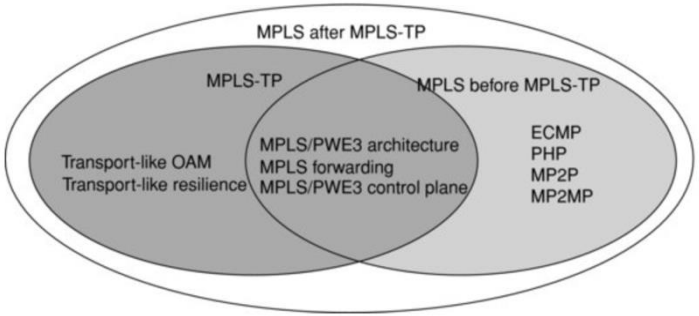
MPLS: IP and Transport Protocol (II)

Data Plane
- Bidirectional LSPs
- No LSP merging, ECMP or PHP

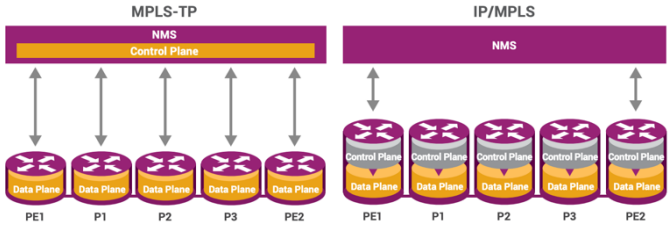
Control Plane
- Optional
- NMS static control

OAM
- In band OAM channel
- Proactive grade OAM

Protection and Resiliency
- Sub 50 msec protection switch for any topography



Source: MPLS-Enabled Applications: Emerging Developments and New Technologies,
Third Edition, ISBN 978-0-470-66545-9



Source: https://ribboncommunications.com/

swissuniversities

Intrusion Detection / Protection Systems

Network Traffic Monitoring

IDPS continuously monitors network traffic for any suspicious activities, ensuring prompt detection of potential threats.

Real-Time Threat Detection

These systems provide real-time detection of threats, enabling immediate responses to security incidents and vulnerabilities.

Enhanced Security Layer

IDS adds an additional layer of security for operational technology (OT) communication, safeguarding critical infrastructure against intrusions.

Intrusion Detection / Prevention System

An intrusion detection system (IDS) is software that automates the intrusion detection process. An intrusion prevention system (IPS) is software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents. IDS and IPS technologies offer many of the same capabilities, and administrators can usually disable prevention features in IPS products, causing them to function as IDSs. Accordingly, for brevity the term intrusion detection and prevention system (IDPS) is used throughout the

- Network-based
- Host-based
- Hybrid
- Behavioural

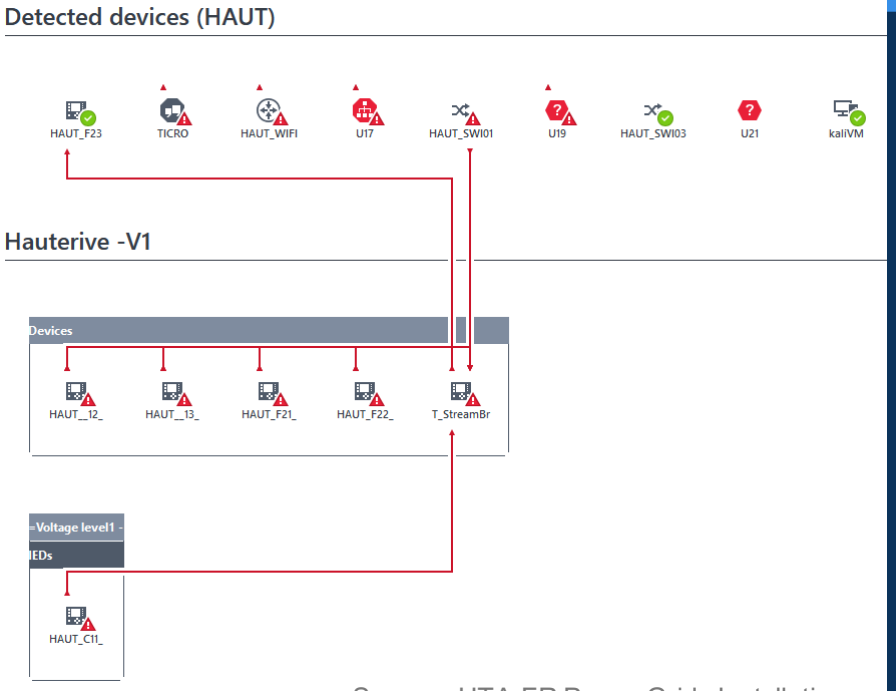
Source : Guide to Intrusion Detection and Prevention Systems (IDPS) - https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf

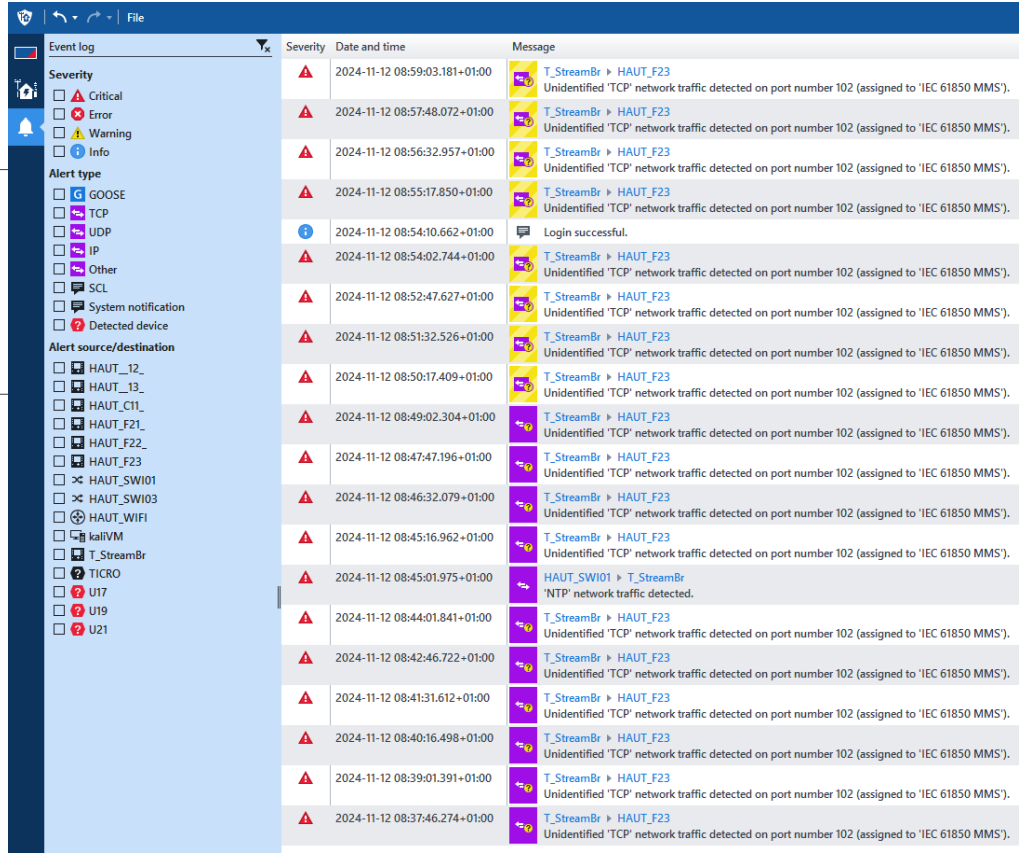
Intrusion Prevention System

- Danger

Acting on an identified potential threat will impact the control loop (or other critical functions) with potentially catastrofic effects

IDS – An example

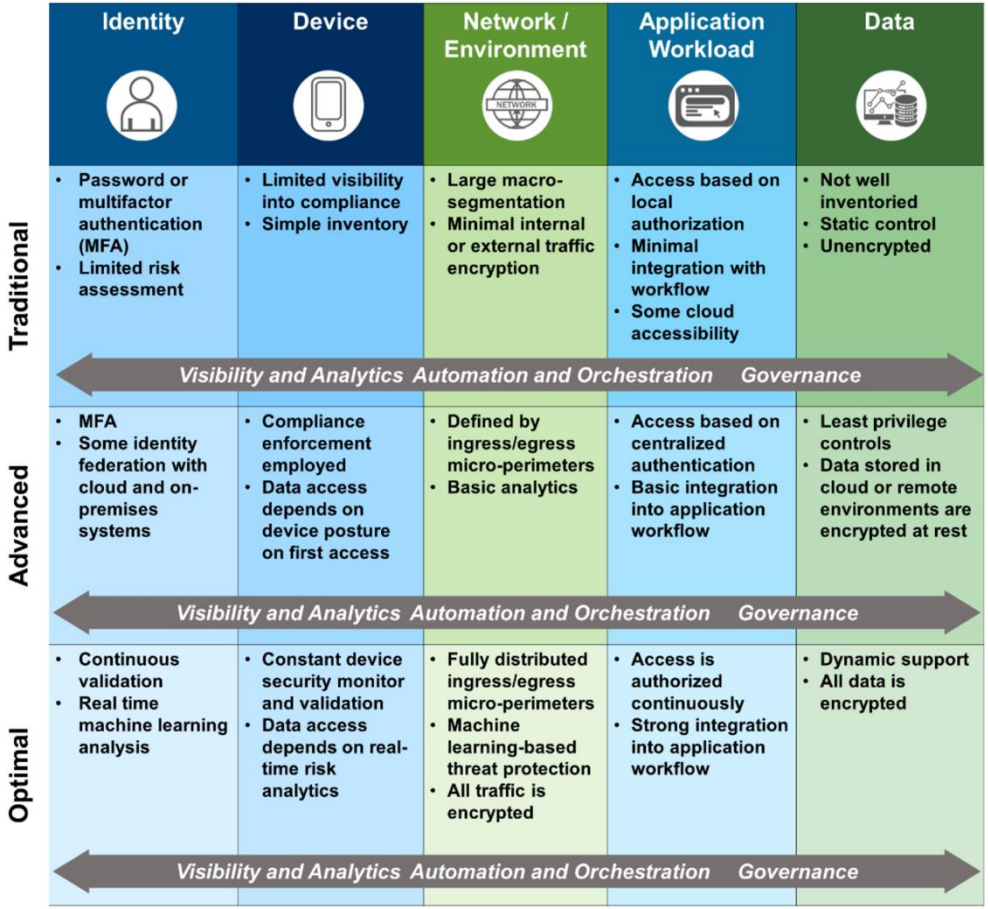




Source : HTA-FR Power Grids Installation

Zero Trust

- All data sources and computing services are considered resources
- All communication is secured regardless of network location
- Access to individual enterprise resources is granted on a per-session basis
- Access to resources is determined by dynamic policy and may include other behavioral and environmental attributes
- The enterprise monitors and measures the integrity and security posture of all owned and associated assets
- Resource authentication and authorization are dynamic and strictly enforced before access is allowed
- The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture

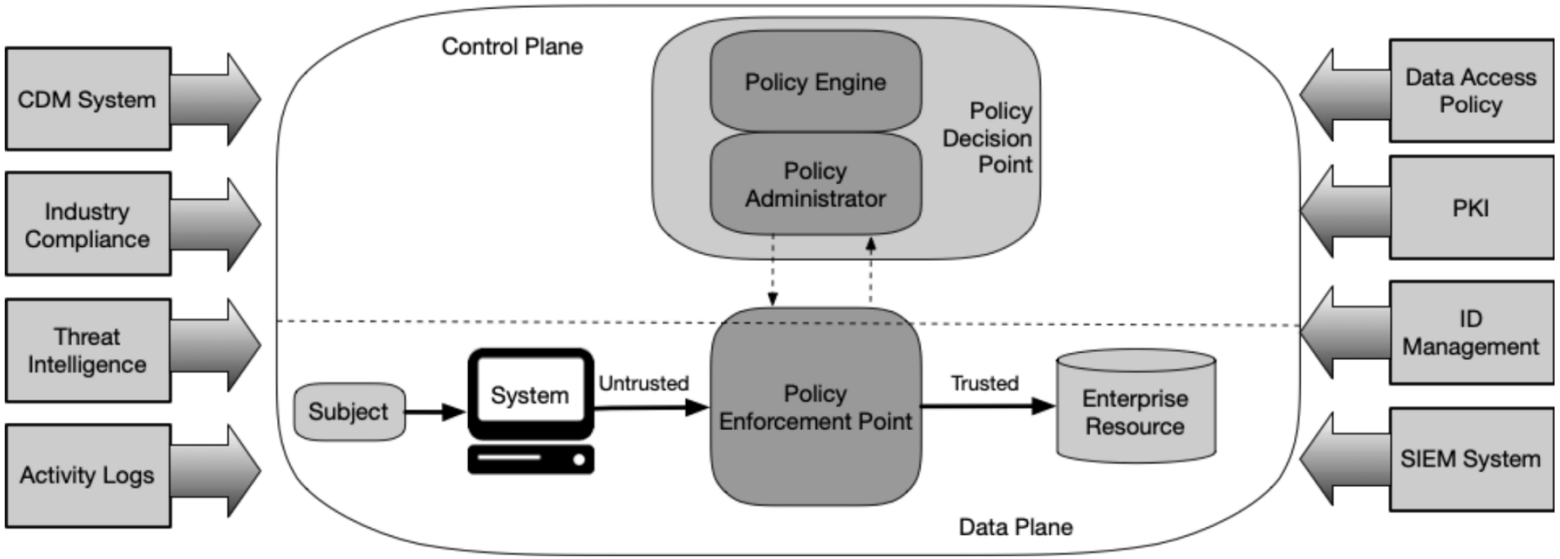


Source: https://www.cisa.gov/sites/default/files/2023-04/CISA_Zero_Trust_Maturity_Model_Version_2_508c.pdf

CISA: Cybersecurity and Infrastructure Security Agency

Source: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Policy Decision Point & Policy Enforcement Point

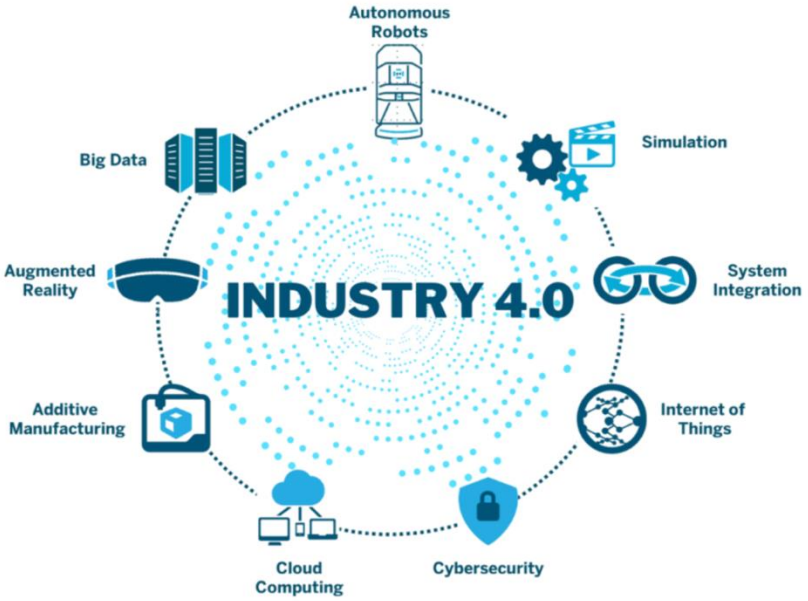


NIST 800-207: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Industry 4.0

Industry 4.0 (IIoT)

Manufacturing that improves its performance aspects with integrated and intelligent use of processes and resources in cyber, physical, and human spheres to create and deliver products and services, which also collaborates with other domains within enterprises' value chains.



Source: https://www.acemicromatic.net/the-role-of-iot-solutions-in-the-manufacturing-industry/

Note 1: Performance aspects include agility, efficiency, safety, security, sustainability, or any other performance indicators identified by the enterprise.
Note 2: In addition to manufacturing, other enterprise domains can include engineering, logistics, marketing, procurement, sales, or any other domains identified by the enterprise.

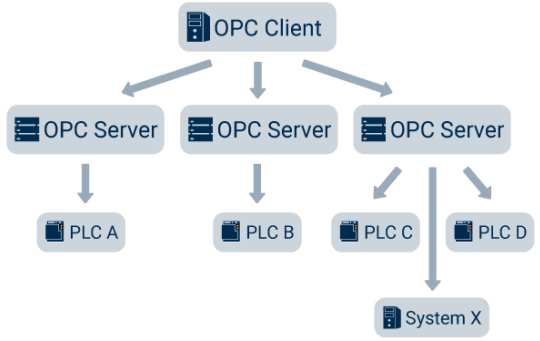
Source: https://www.isa.org/intech-home/2022/august-2022/features/introduction-the-birth-of-industry-4-0-and-smart-m

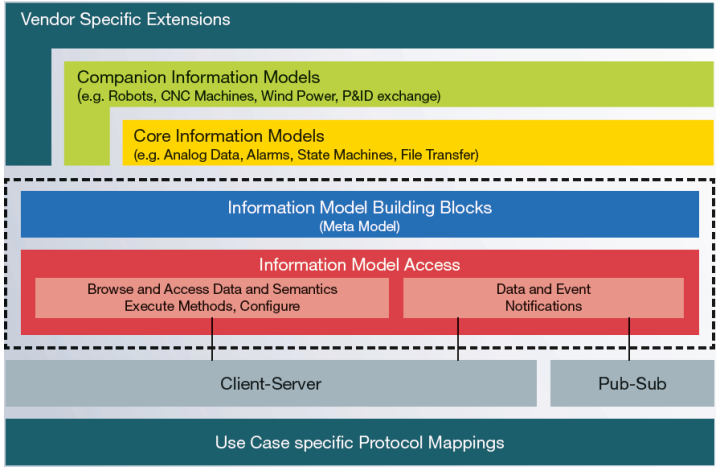
swissuniversities

OPC UA – A standardized solution

Open **Pl**atform **C**ommunications **U**nified **A**rchitecture

- Important communication standards for Industry 4.0 and the IoT
- Grants access to machines, devices and other systems is standardized
- Enables similar and manufacturer-independent data exchange
- Platform independent*
- Specified by IEC62541 and https://opcfoundation.org/

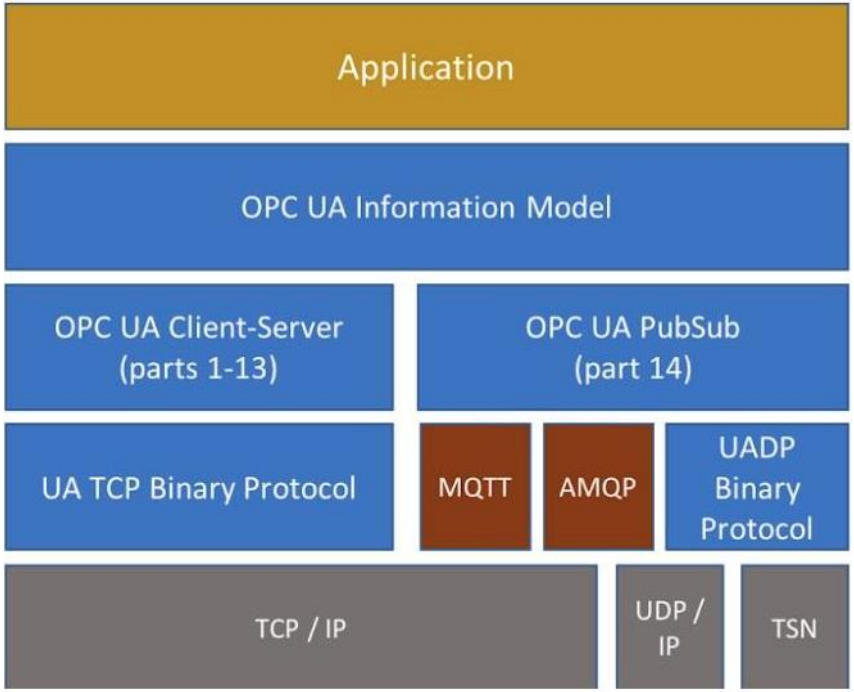


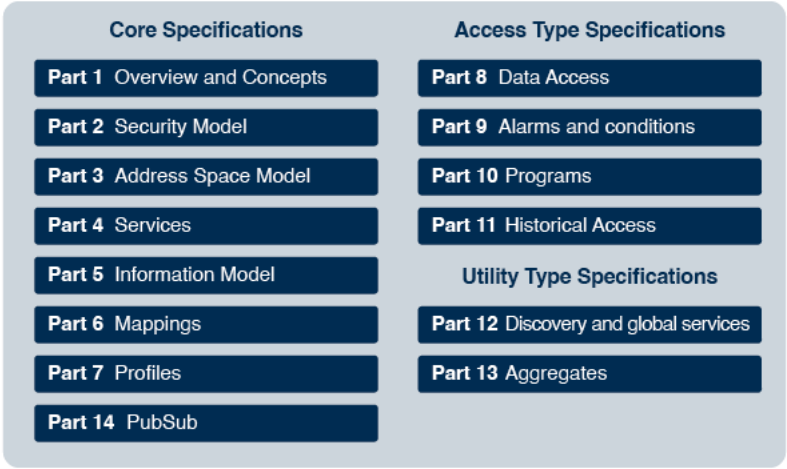


*: OPC Classic depends on MS Windows

Source: https://opcfoundation.org/about/opc-technologies/opc-ua/

OPC UA – A standardized solution

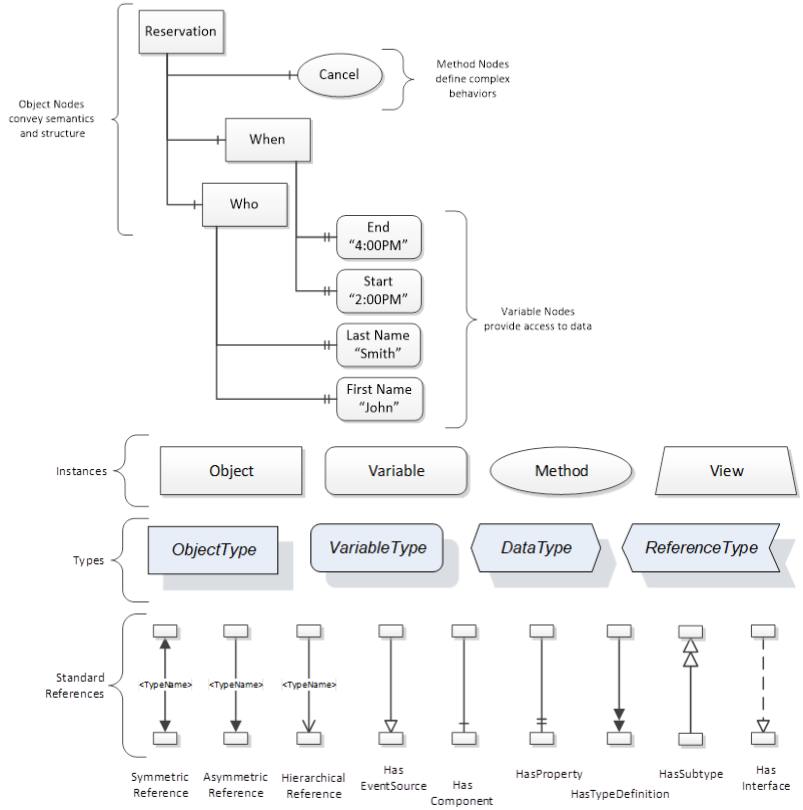




Source: https://wiki.st.com/stm32mpu/index.php?title=OPC_UA_overview&oldid=83328

Image source: https://www.opc-router.com/what-is-opc-ua/
Specifications: https://reference.opcfoundation.org/

OPC UA – A standardized solution



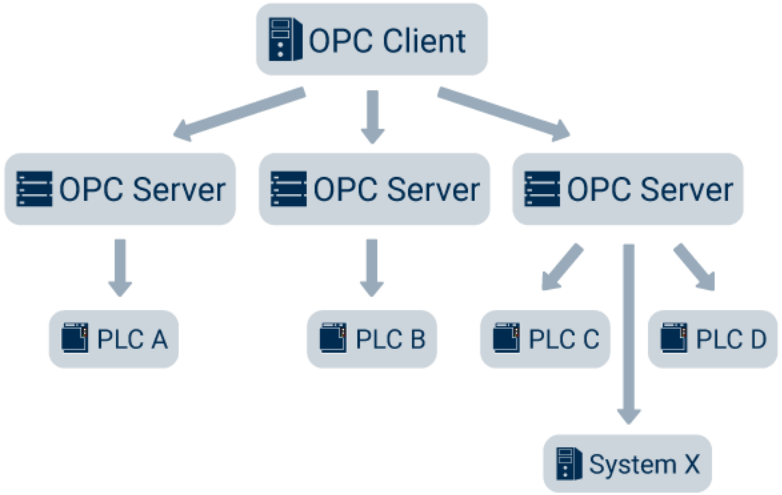
- Formal, yet flexible, extensible information model with complex types
- State of art security model
- Allows Functional equivalence

swissuniversities

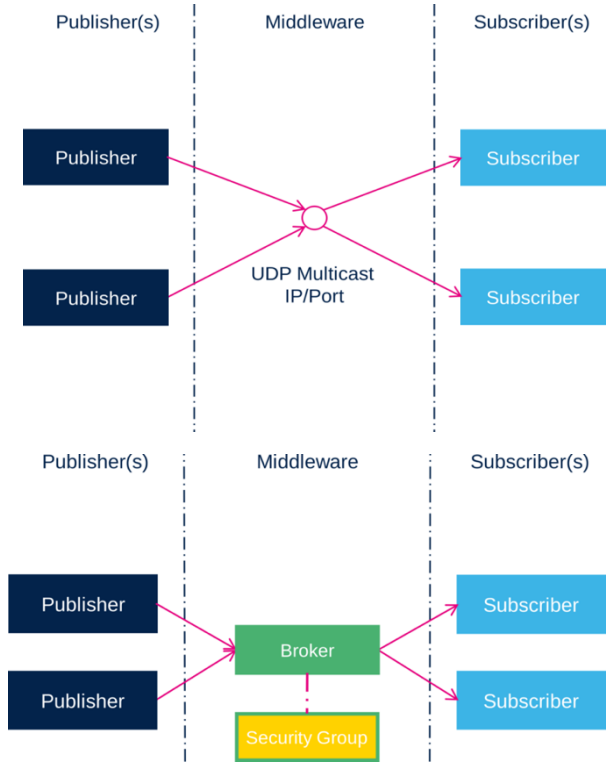
Source: https://reference.opcfoundation.org/Tightening/v100/docs/4.3

OPC UA – A standardized solution

Client-Server



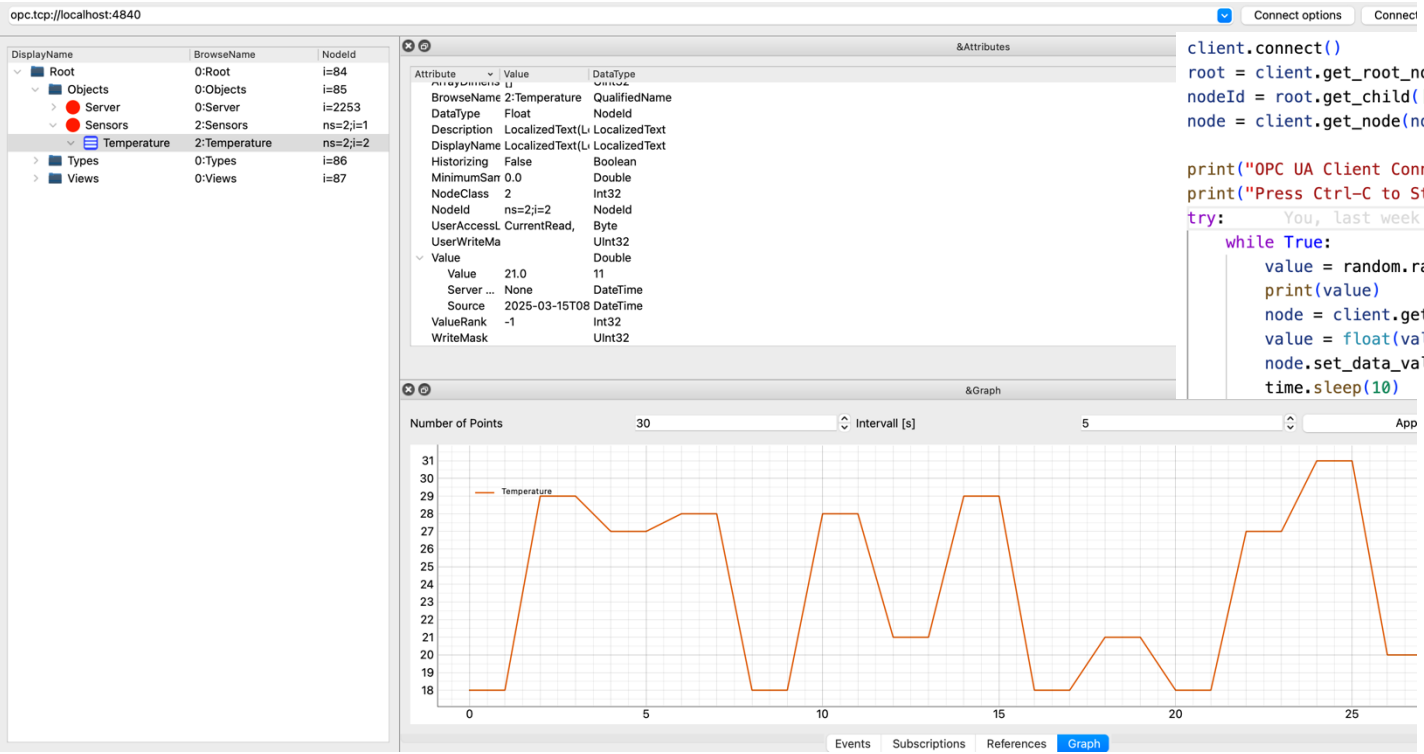
Publisher-Subscriber (PubSub)



swissuniversities

Source: https://wiki.st.com/stm32mpu/index.php?title=OPC_UA_overview&oldid=83328

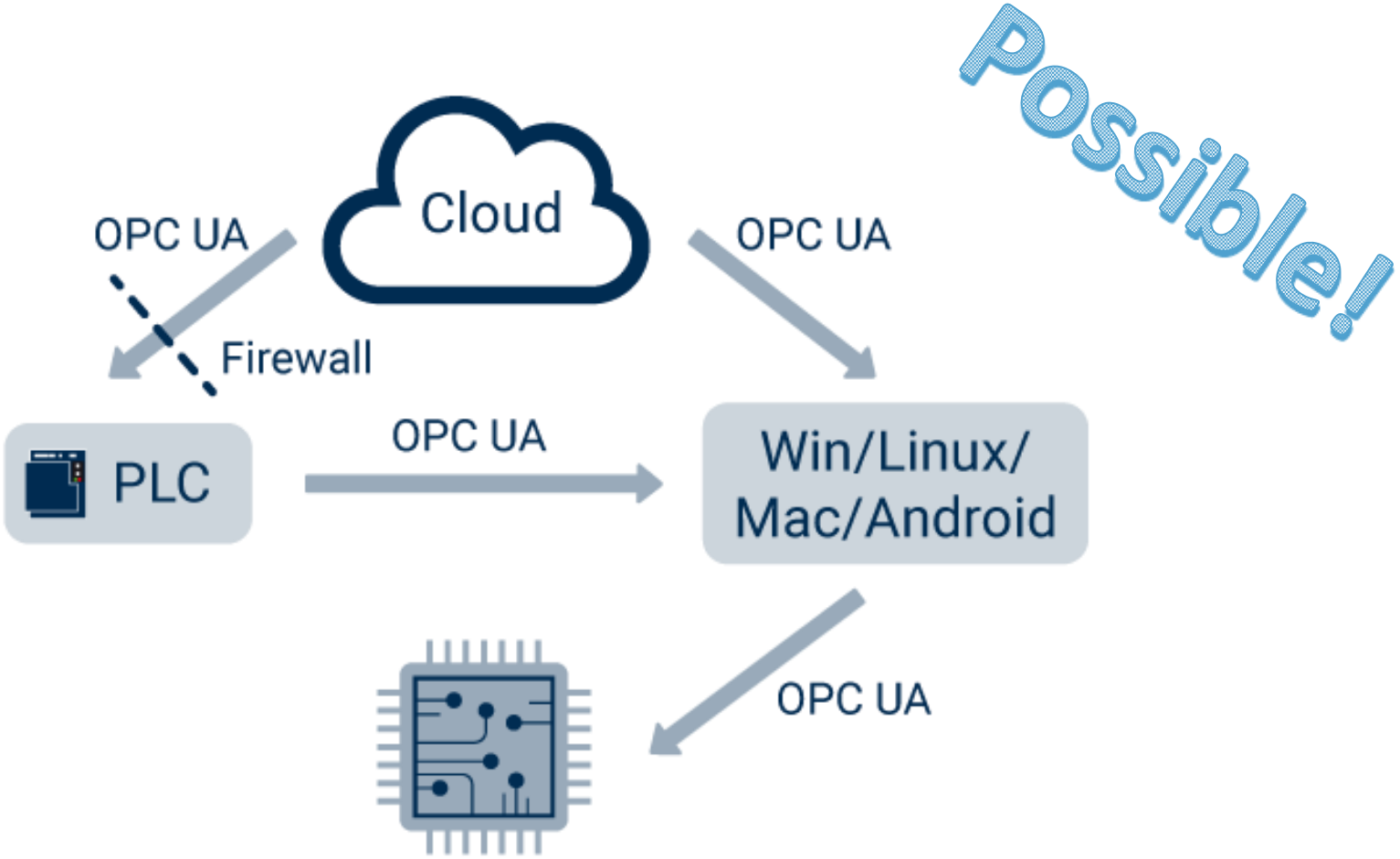
OPC UA – A standardized solution

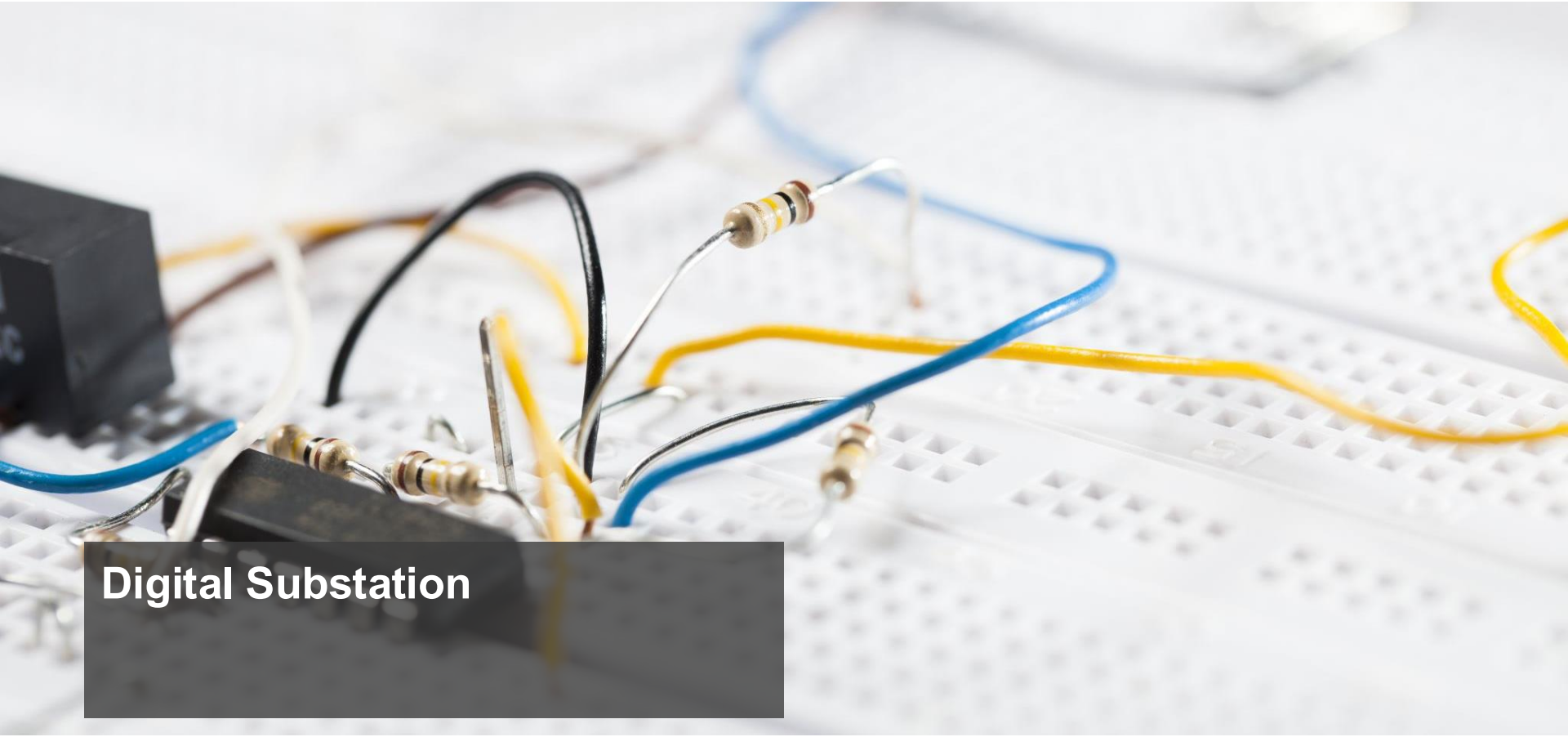



```python
client.connect()
root = client.get_root_node()
nodeId = root.get_child(["0:Objects", "2:Sensors", "2:Temperature"])
node = client.get_node(nodeId)

print("OPC UA Client Connected")
print("Press Ctrl-C to Stop Program")
try:      You, last week • feat: 1st OPC-UA setup
    while True:
        value = random.randint(18,32)
        print(value)
        node = client.get_node(nodeId)
        value = float(value)
        node.set_data_value(value)
        time.sleep(10)
```

swissuniversities


Possible!
Cloud
OPC UA
OPC UA
Firewall
PLC
OPC UA
Win/Linux/
Mac/Android
OPC UA

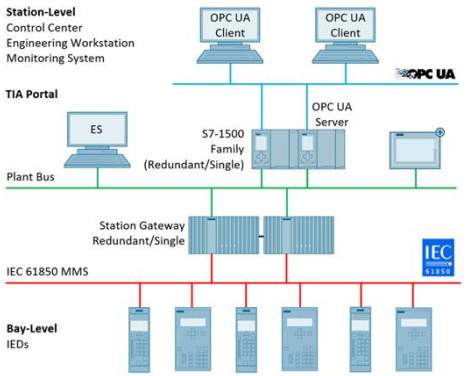


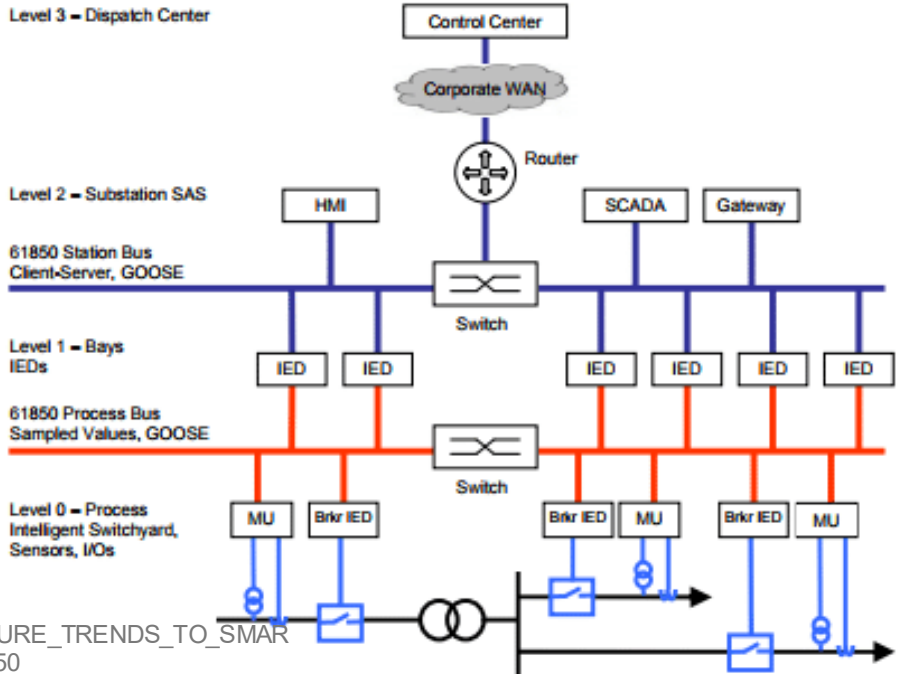
Digital Substation

Source: https://support.industry.siemens.com/cs/document/109977049/setting-up-an-iec-61850-mms-opc-ua-gateway-with-tia-portal-and-station-gateway-for-tia

IEC 61850

- IEC 61850 is the international standard for defining devices within substation automation systems and how their interactions





https://www.researchgate.net/publication/325069210_FUTURE_TRENDS_TO_SMART_GRID_AUTOMATION_ARCHITECTURE_BY_IEC_61850

IEC 61850

Platform for designing, integrating and maintaining

- Communications
- Protection
- Control
- Automation
- Measurements
- Recording
- Monitoring

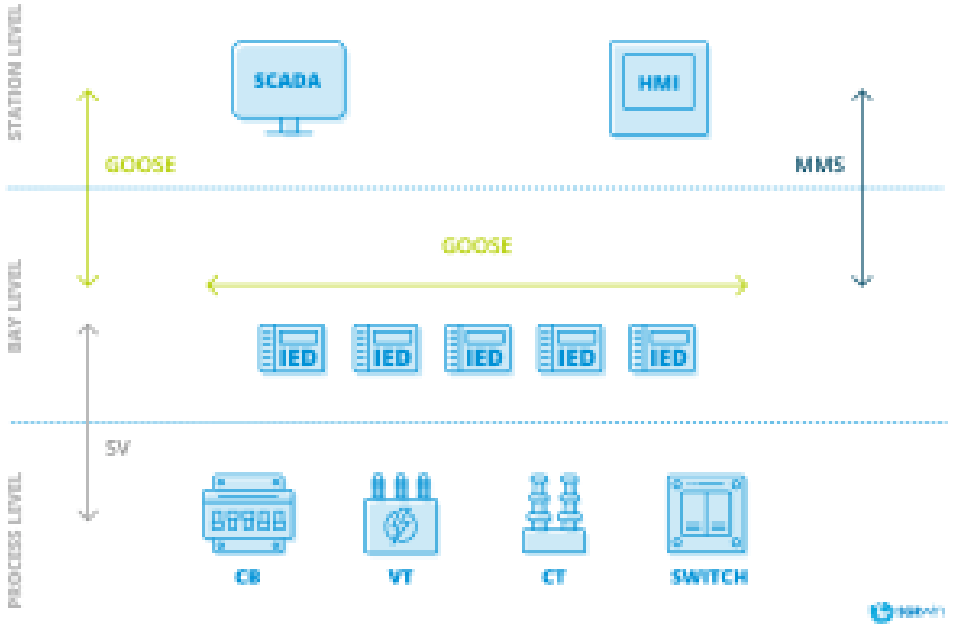
Features of IEC 61850

- Self description capability (supports Interrogation)
- Fast peer-to-peer communication for tripping, blocking, interlocking
- Reduction of hard-wired connections
- Reporting features

IEC 61850

Standardizes

- Design
- Language
- Services
- Protocol
- Configuration
- Substation Information
- Device Information
- Device Services
- Naming Convention
- Fault Records
- Conformance Tests

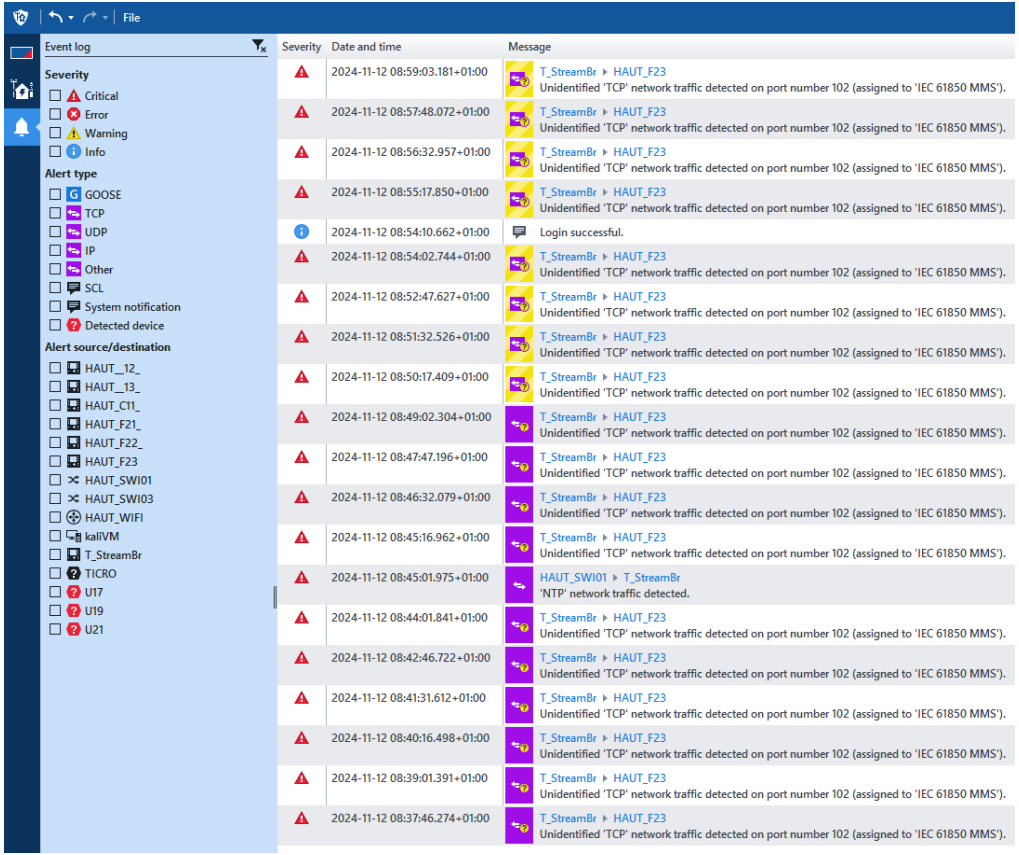


Source: https://www.sgrwin.com/goose-mms-and-sv-protocols/

MMS (Manufacturing Message Specification) Protocol
GOOSE (Generic Object-Oriented Substation Event) Protocol
Sampled Values (SV) Protocol

IEC 61850

- The IDS example was using this standard to interpret the composition of a substation and extracted the corresponding rules



Summary

Communication Technology Relevant to OT Environment

Encryption and Network Segmentation

Data Protection

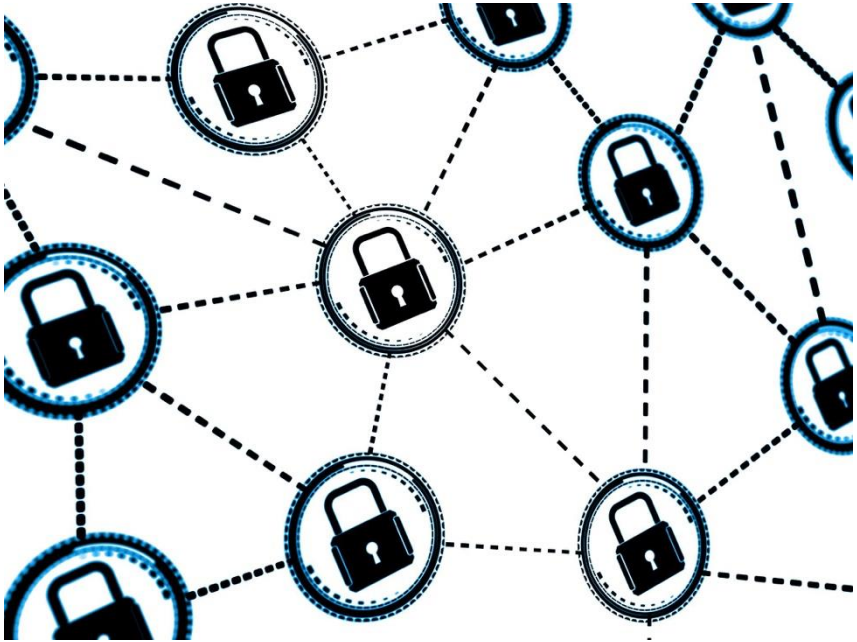
Encryption is essential for protecting sensitive data from unauthorized access and potential breaches.

Access Limitation

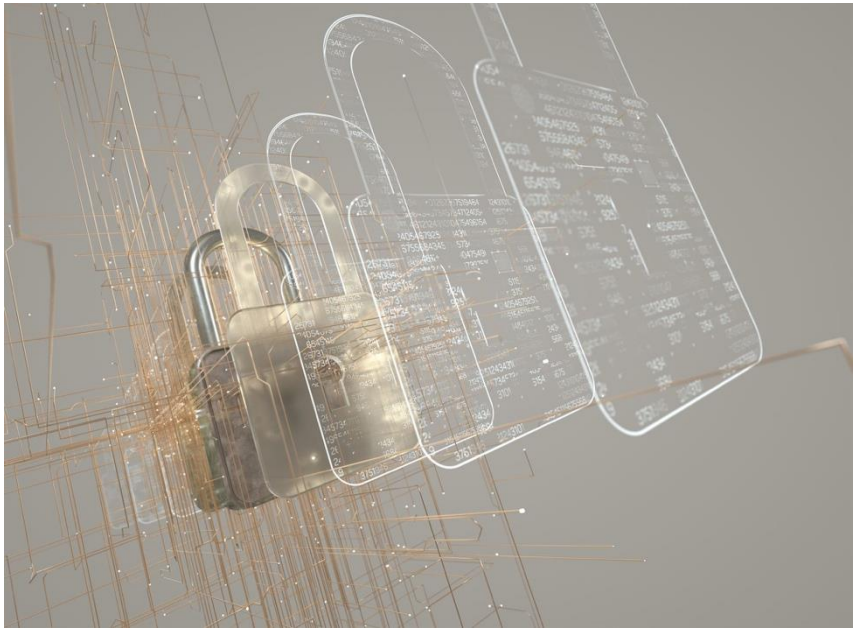
Network segmentation helps to limit access to critical systems, reducing the risk of cyber attacks.

Enhanced Security Posture

Together, encryption and segmentation enhance the overall security posture of operational technology environments.



Use of Secure Protocols



Importance of Secure Protocols

Secure communication protocols like TLS and SSH are vital for ensuring data privacy and integrity in operational technology environments.

Preventing Eavesdropping

Using secure protocols helps prevent unauthorized access and eavesdropping on sensitive data during transmission.

Protecting Against Tampering

Secure protocols protect data from being altered or tampered with during transmission, ensuring its authenticity.

Heterogeneity of OT Systems

Variety of Devices & Applications

Operational Technology (OT) environments include a wide range of devices, each with unique specifications and functionalities – with hard real-time and environmental requirements.

Protocols in OT

Different communication protocols in OT systems can complicate interoperability, requiring careful management and integration.

Interoperability Challenges

Understanding the heterogeneity of OT systems is essential for addressing interoperability challenges and improving communication.

Open Standards for Interoperability

Importance of Open Standards

Adopting open standards is crucial for ensuring interoperability among various operational technology systems.

Facilitating Communication

Standards like OPC UA enable seamless communication between devices from different manufacturers, enhancing system integration.

Enhanced Data Exchange

Open standards promote efficient data exchange, allowing diverse systems to work together effectively.

Conclusion

Importance of Communication Technology

Communication technology is essential for improving efficiency in operational technology environments, ensuring smooth operations.

Core Technologies and Protocols

Understanding the core technologies and protocols helps optimize their operations and enhance security.

Security Measures

Implementing robust security measures is critical to protecting OT environments from potential threats and vulnerabilities.

Interoperability Challenges

Addressing interoperability challenges ensures that various technologies work together seamlessly for optimal performance.