IEC 61850 Protocol Fundamentals

By Eng. Sobhi Ali

Tel: +201112478990

Why 61850?

1- Interoperability: For Easy Interoperability between Systems from different vendors.
2- Avoid System Configuration Issues
3- Standard Configuration Mechanism
4- Use of TCP / IP – Ethernet Network.

Protocol Locations:

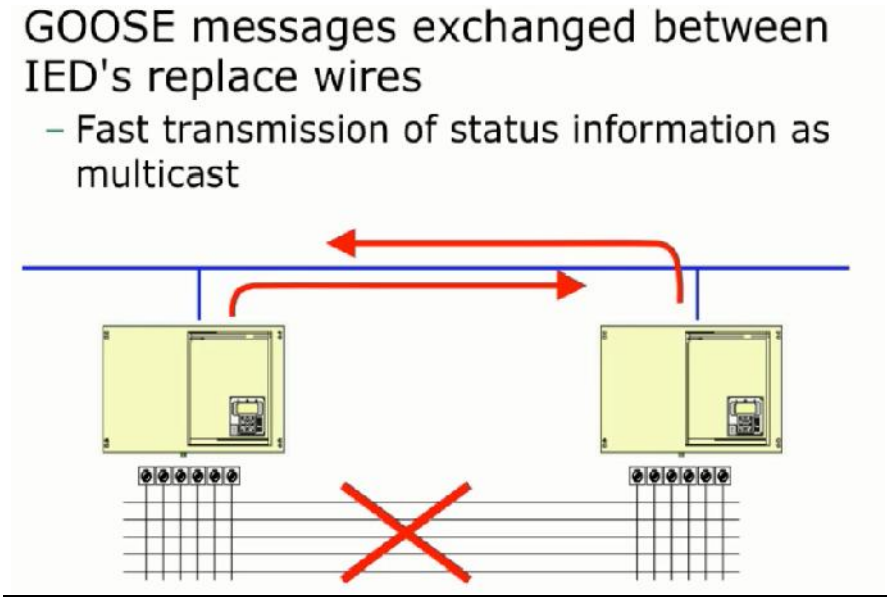
-IEC 61850 and MMS: Between Station Level SCADA and Bay Level IEDs

– IEC GOOSE: Between Bay Level IEDs

– IEC SMV (Sampled Value): From Process Level Devices to Bay Level IEDs.

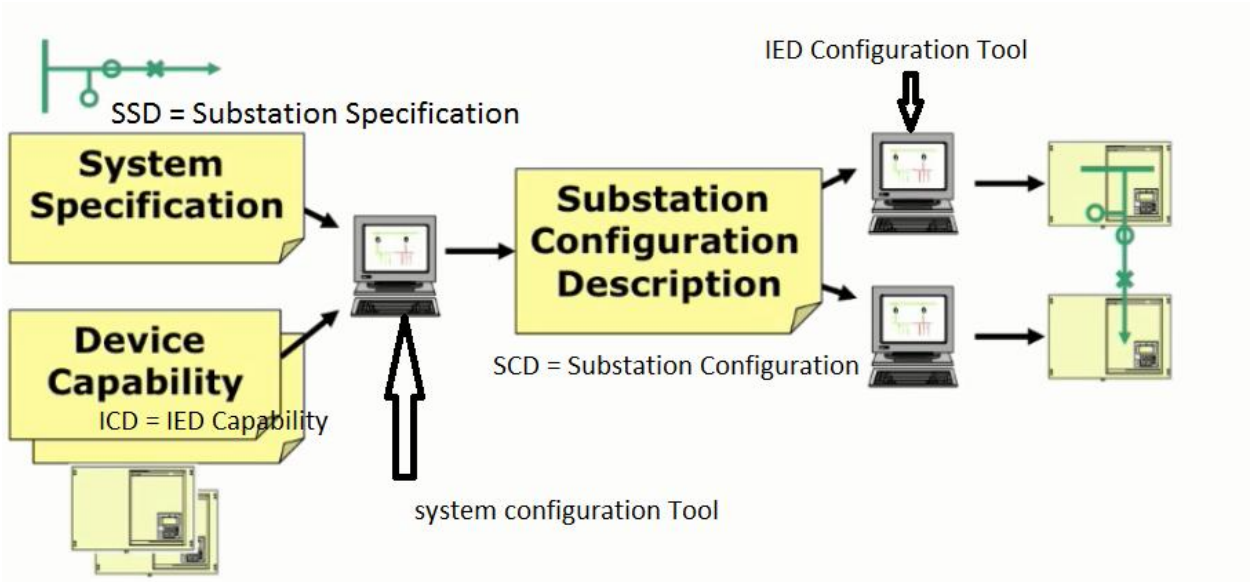
IEC GOOSE- Facilitates High Speed end to end Data Transfer within 4 milliseconds

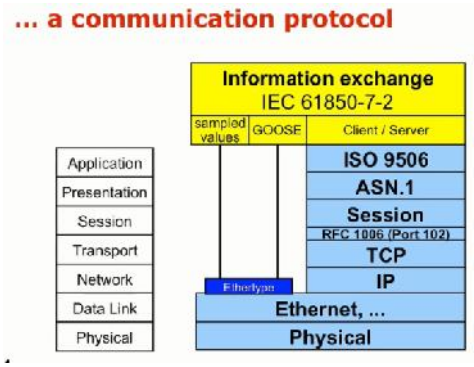
- Multicast Addressing allows One Source and any Number of Destinations within a Network
-Uses Virtual LAN addressing and Priority Tagging for dedicated and faster Packet delivery
-Uses only 3 Layers of the (OSI) (Application – DataLink – Physical).



The configuration files:

SCL: system configuration Language (XML)
SSD = Substation Specification Description : like SLD single line Diagram تعريف مبدئى يتم ادخالة الى system configuration tool لعمل الملف النهائىSCD
ICD = IED Capability Description : مثل داتا مودل ويتم ادخالها الى يتم ادخالهاالى سيستم كونفجيرشن تووول ايضا و communication capability
SCD = Substation Configuration Description
CID = Configured IED Description





Process Level consists of:

– Transducers like CTs & VTs which are connected to Electrical Network to measure Current. CB, Isolators.

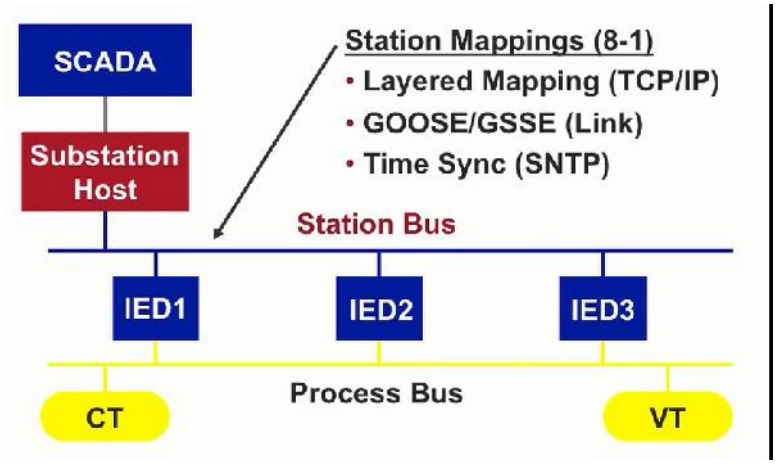
Bay level consists of

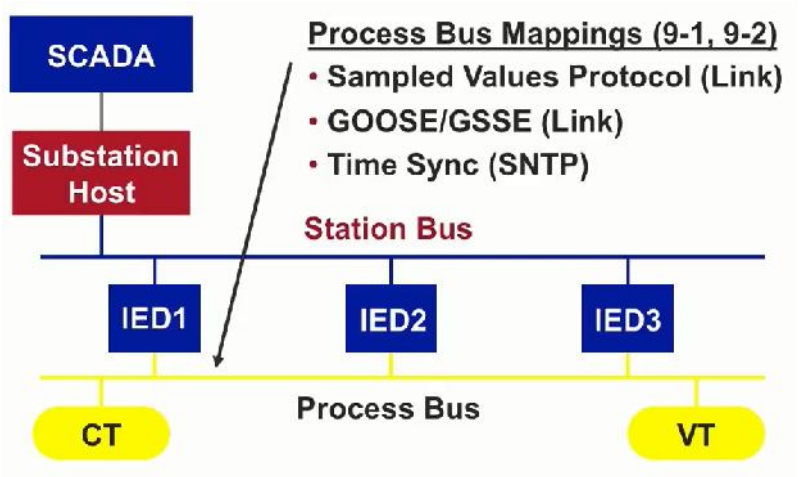
– (IED)
– Types of IEDs are
• Relays , RTU, Bay Controller Unit (BCU).

Station Level consists of

– SCADA ,Operators to Monitor.

Protocols of station Bus and process bus:





Logical node :IEC 61850 describes each function within a substation equipment (transformer, circuit breaker, protection function...) by a logical node (LN).

Logical device : Each physical device (called an IED) can perform functions that was formerly performedby different protection or control devices.
Those former devices are represented by Logical Devices within the physical device

Logical node classes: data classes : the type of the data if it is measurement or status (position).
X : for Switchgears
P: for protection function
C: for control
M: metering and measurements.

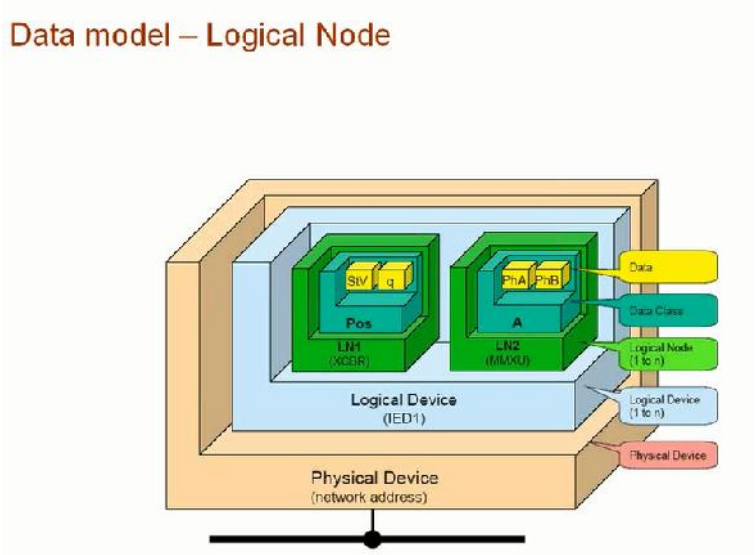
Logical node DATA objects:

XSWI

Data Name	Type	Explanation	
Mode	ENC	enable / disable	C
Loc	SPS	Local / remote control	M
EEHealth	ENS	ok / warning / alarm	O
EEName	DPL	Name plate	O
OpCnt	INS	Operation counter	O
Pos	DPC	position	M
BlkOpn	SPC	block opening	M
BlkCls	SPC	block closing	M
SwTyp	ENS	load break, dis, earth..	O

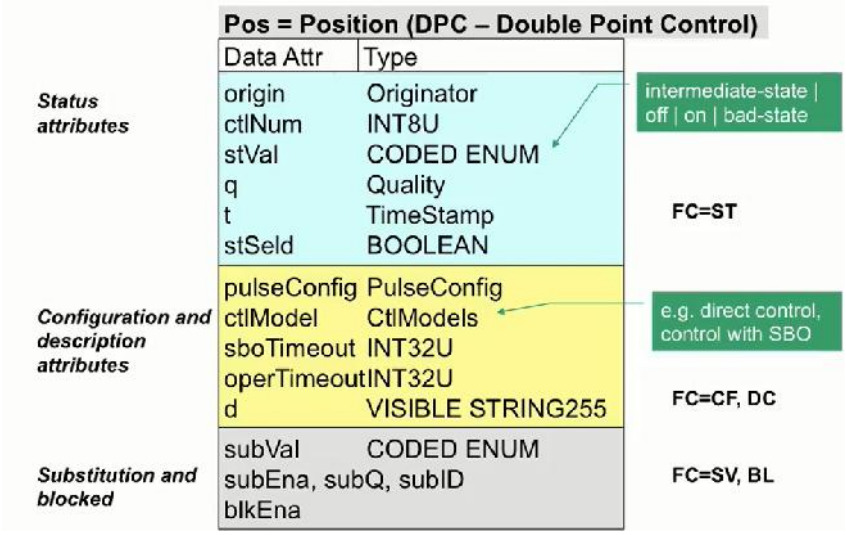
Mandatory

Optional



Data Model: standard to represent the function of an equipment , the data attributes and location . for example XCBR.POS. St Val (circuit breaker position) . And (MMXU.A.PhsA (the current value of Phase A).

DATA Objects & DATA Attributes:



Gate way:

An important part of the SAS (Substation Automation System), because is a central piece that translates all this data from both sides, between IEC-61850 devices to the Control Center, usually communicating with DNP3 or IEC-60870-5-101/104.

Summary of IEC TR 61850 -1

Definitions:

1-ACSI: abstract communication services interface, virtual comm. Interface independent than the actual interface.

2-Bay: subpart of S/S like switchgear, busbar, buscoupler , transformer…etc.

3-Data object: part of logical node object carry information like “status measurements..etc”

4-Logical Node “LN”: smallest part of function that exchange data

5-physical deice: PD, equivalent to IED.

6-interoperabilty: ability of two or more devices from one vendor or different vendor to exchange data.

7-PICOM: Piece of Information for COMmunication.

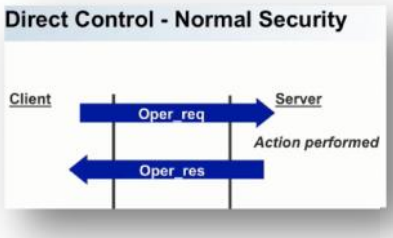
1-many functions supported by 61850 in communications as following:

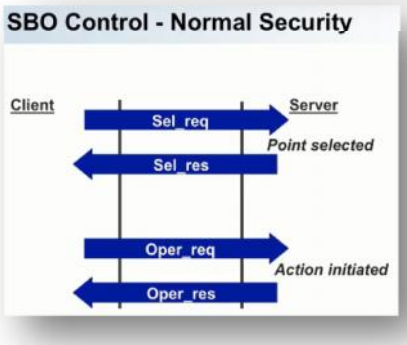
- sampled value exchange for CTs and VTs (1),
- – fast exchange of I/O data for protection and control (2),
- – control and trip signals (3),
- – engineering and configuration (4),
- – monitoring and supervision (5),
- – control-center communication (6),
- – time-synchronisation,
- – etc.

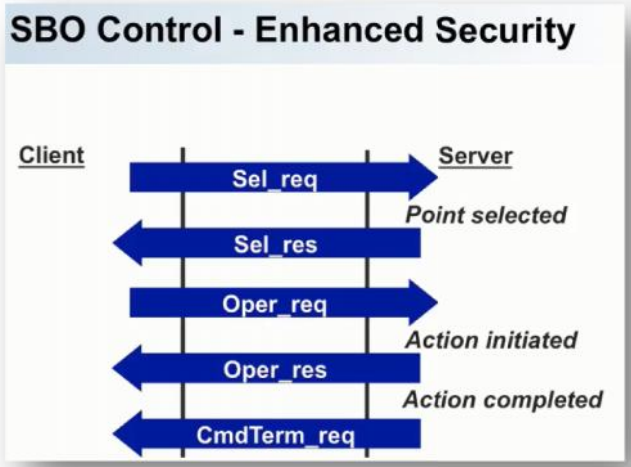
Able to communicate between many different IEDs even they have many functions.

Client /Server (client request) and server response and this happening in the un-critical time data reporting. It is called MMS protocol .Publisher / subscribers : multi-cast : the publisher send to all subscribers a multicasting data (like the status of CB) it is used in GOOSE and SV.

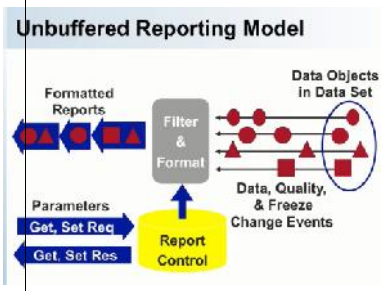
Control types:







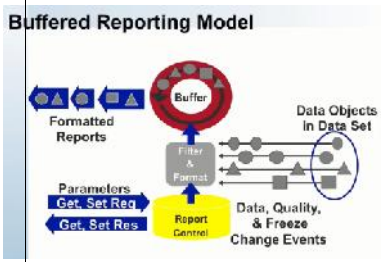
Reporting Types:



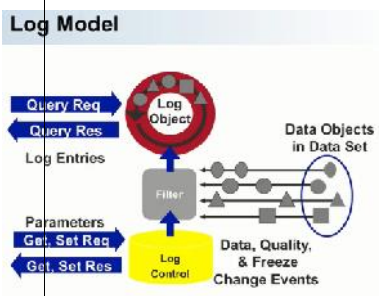
1-unbuffered:

Formatting logic: turns the sequence of chances in data into a sequence of messages, these messages can contain one or more data set of an event.

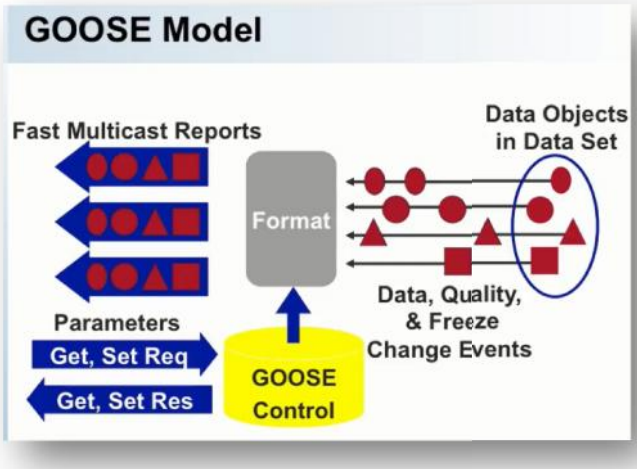
Filtering logic: removing the repeated messages and unuseful messages.

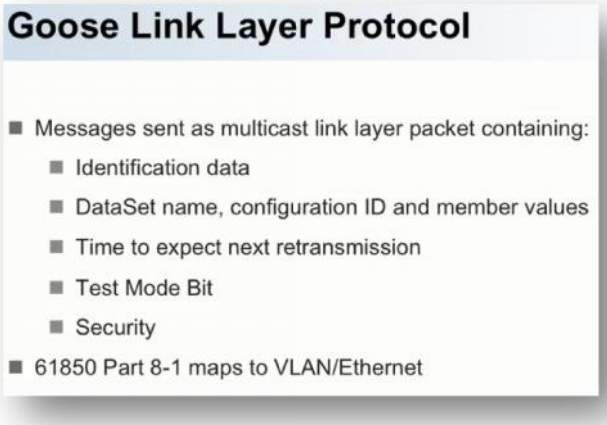


2-The main difference between unbuffered and buffered report: that the in buffer report the data after filtering and formatting stored in a buffer so it can be transmitted to client later if the network went down.



3- In log model: it is almost the same of buffered report but the only difference that the report messages do not send unless the client request that



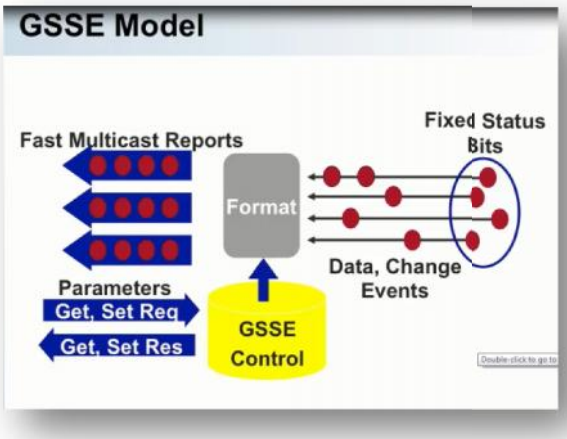


Goose is like layer packet uses Vlan/ ethernet

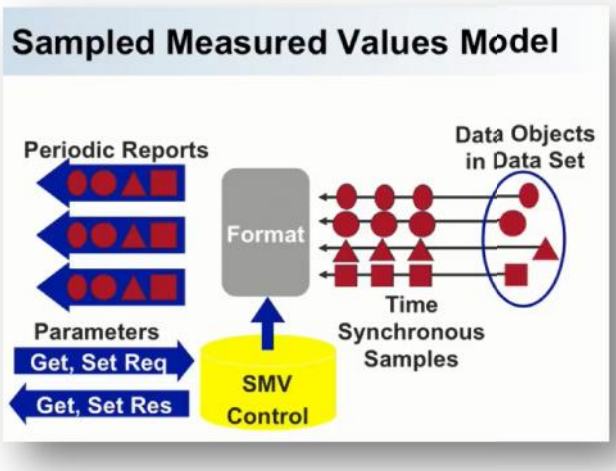
ID: name of the source

Time of the next packet : الوقت الى هتيجى فيه الباكت التاليه علشان لو ماجتش المستقبل يفهم ان الاتصال بالمرل اتقطع

Security: دا كود بيبعتها المرل علشان المستقبل يتاكد ان الباكت جايه من مصدر موثوق



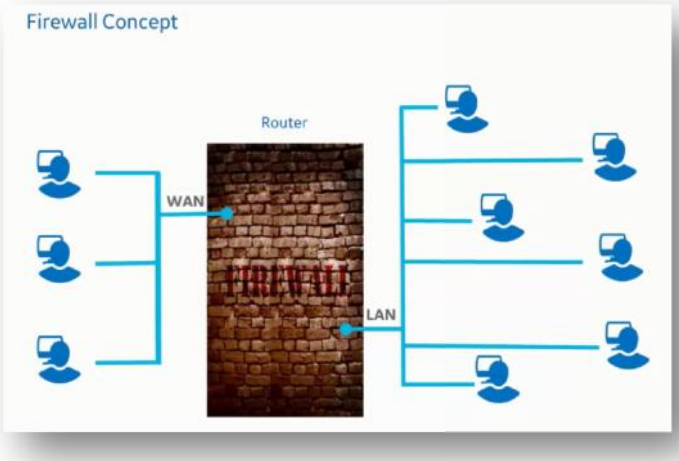
in GSSE it is the same like GOOE except of sending a fixed status bits rather than sending arbitrary data sets This protocol forward from UCA.2 to 61850.



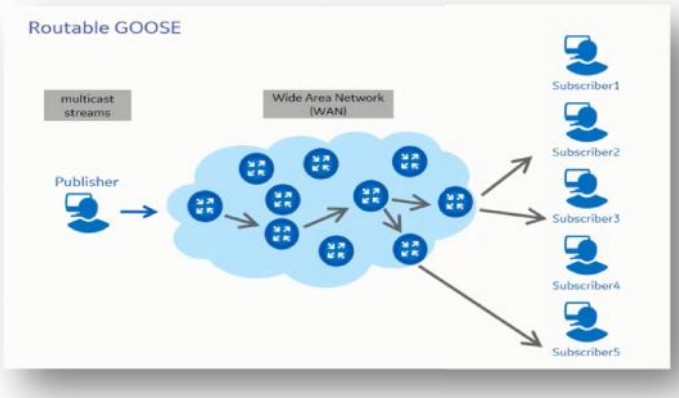
In SMV : same as GOOSE but instead of even driven it is Sampled here , this used in Process level to retrieve the samples from CT, VT to the merging unit.

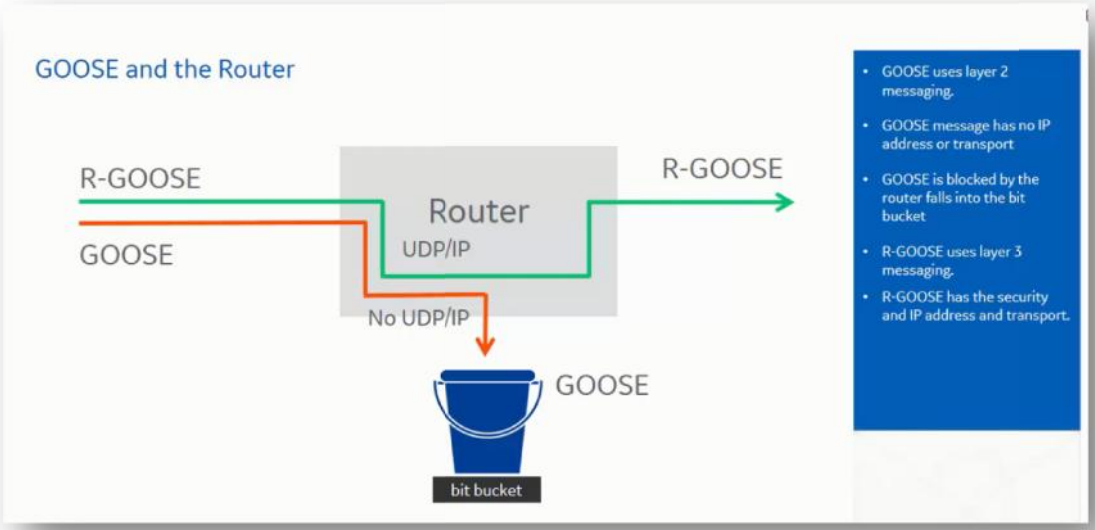
Goose Vs R-Goose(routable –Goose) R-GOOSE (IEC 61850-90-5)

فى حالة ال الجووس العادى الفير وول الى على الروتر بتمنع الباكت من المرور لو حاولت تمر من خلاله. وبكده الجووس العادى بيشتغل على لوكل نتورك.



R-GOOSE:





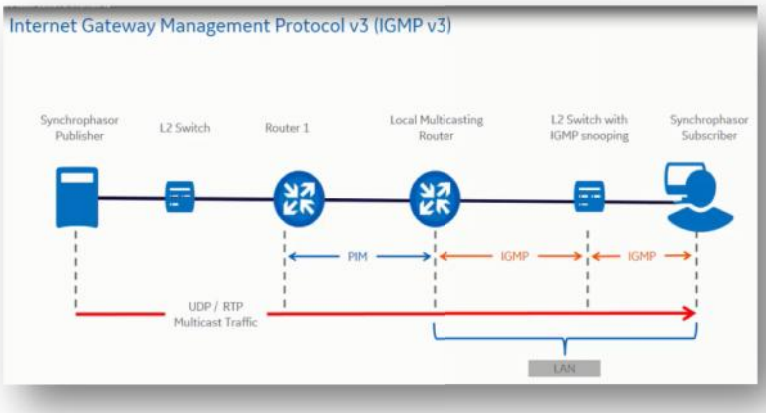
الماسدج تقدر تسافر خلال الروتر ولذلك لانها تحتوى على اى بى ادرس ولتحقيق دا طبعا بتقابلنا مشكله السيكورتى علشان كدا **بنستخدم** حماية اضافيه من خلال بعض البروتوكلات اولها

IGMP.V3

ودا بيخلى الروتر يعرف مين الى ارسل الداتا ورايحه فين وباءا عليه بيختار المسار الافضل الاقرب بدلا من ارسالها على جميع المسارات. The router selects the best path for the packet going to the subscribers

Additionally the IGMP filtering the source of information to make sure that the packet is coming from the intended source.

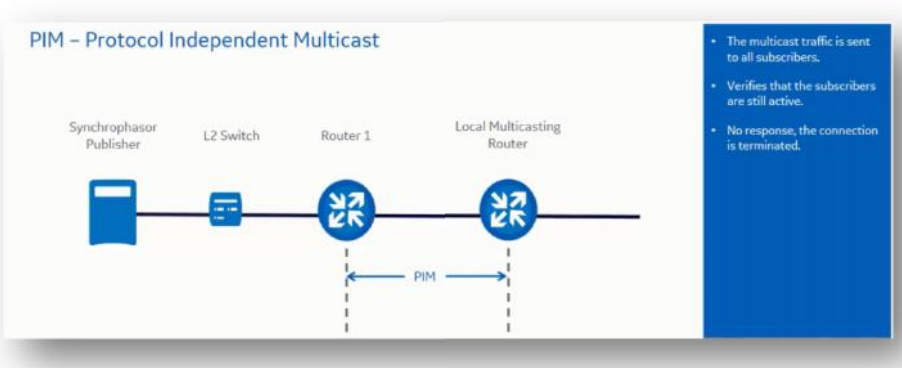
IGMP work between the subscriber and the local router.



بعدين عندنا بروتكول تانى اسمه

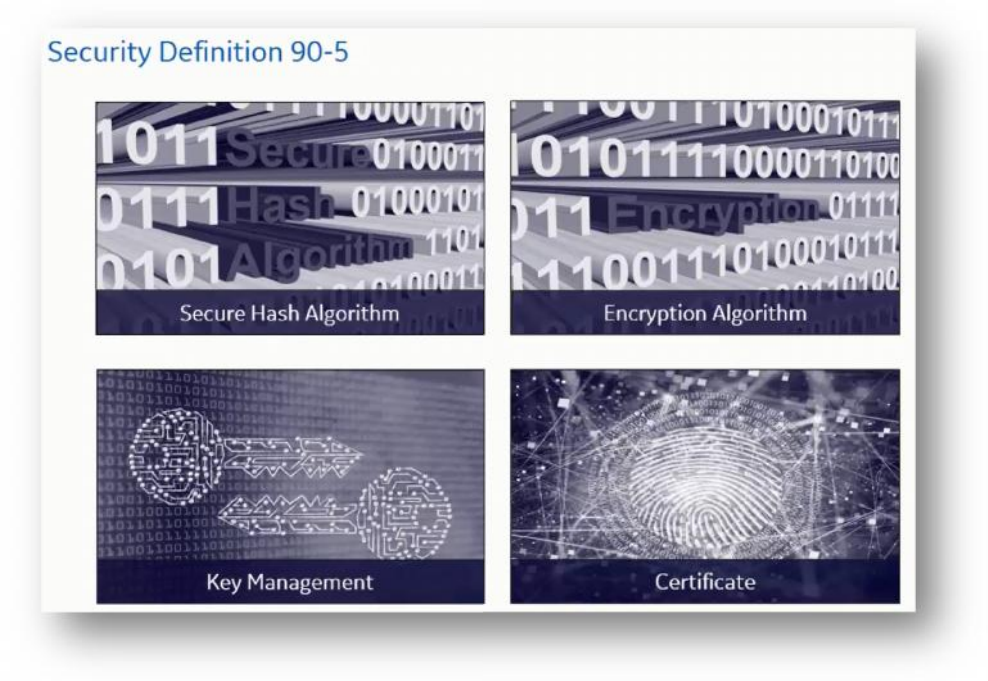
PIM

بتاكد ان المرسل لسه **متصل** لو ماردش عليه بيفصل الاتصال فورا: make sure the subscriber is a live if not responded the PIM breakdown the connection link


PIM – Protocol Independent Multicast
Synchrophasor Publisher
L2 Switch
Router 1
Local Multicasting Router
PIM
The multicast traffic is sent to all subscribers.
Verifies that the subscribers are still active.
No response, the connection is terminated.

Security of R-GOOSE:

بيستخدم الاربع طرق الى فى الصورة



R-goose Security:

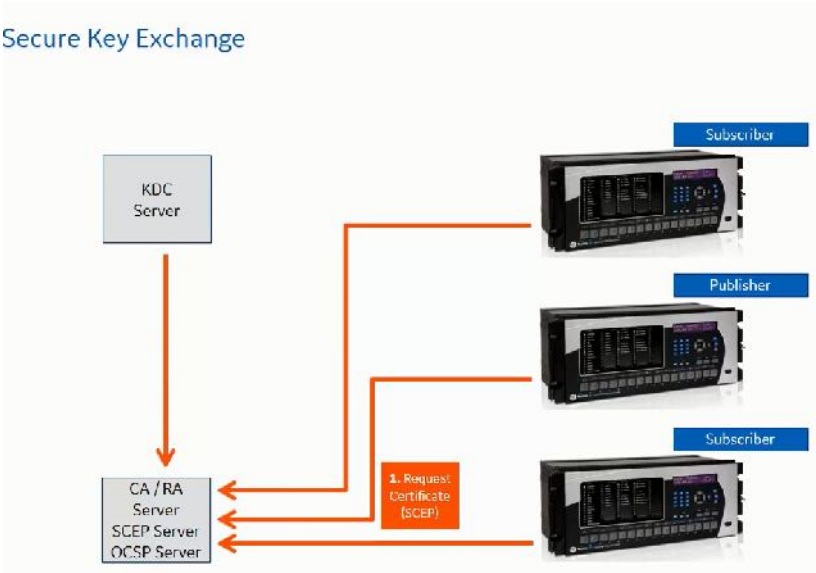
KDC Server : key distribution center

CA Server: certificate Authority server :

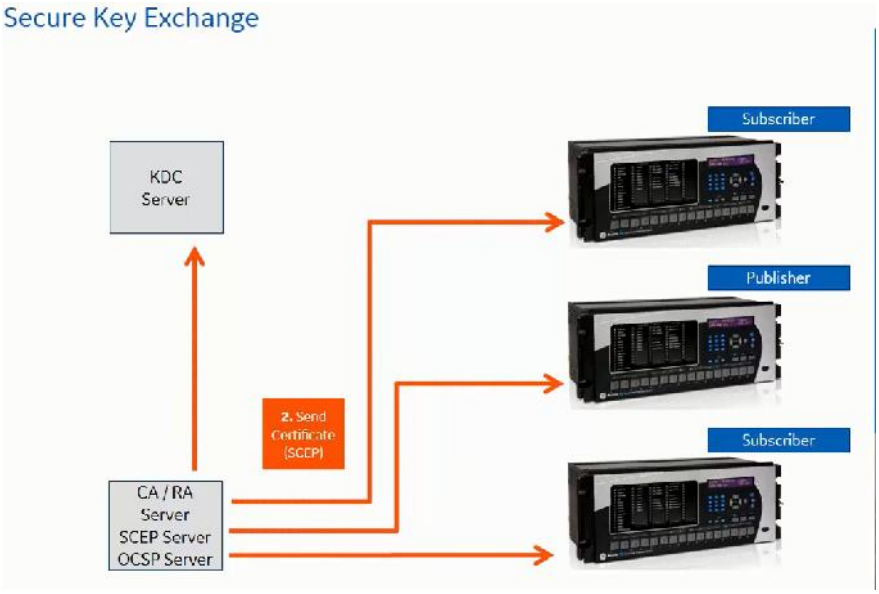
The Steps:

1-كل الاجهزة بتطلب شهاده معتمده من السيرفر سى ايه

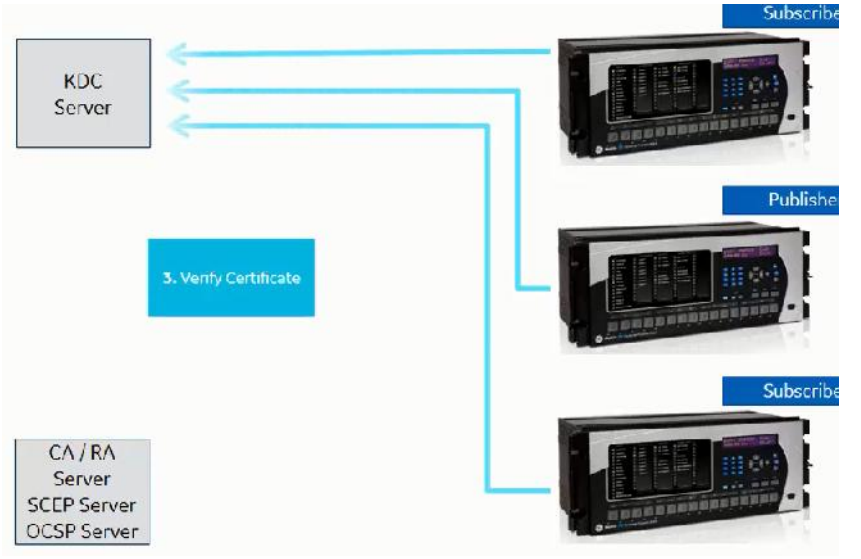
Each device request a certificate from CA server

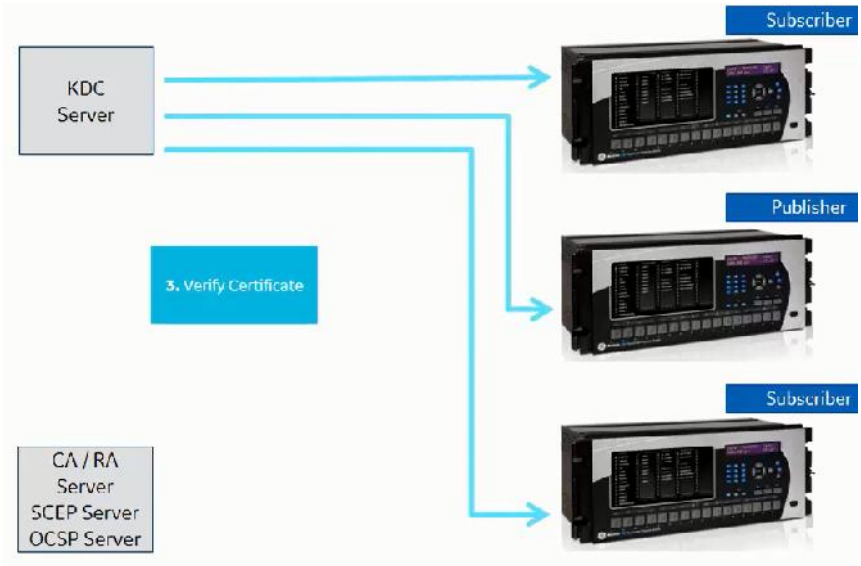


2- CA server sends a sign certificate for all devices.



3- All devices send their certificate to KDC server and request the KDC certificate so KDC and devices verify each other certificate.

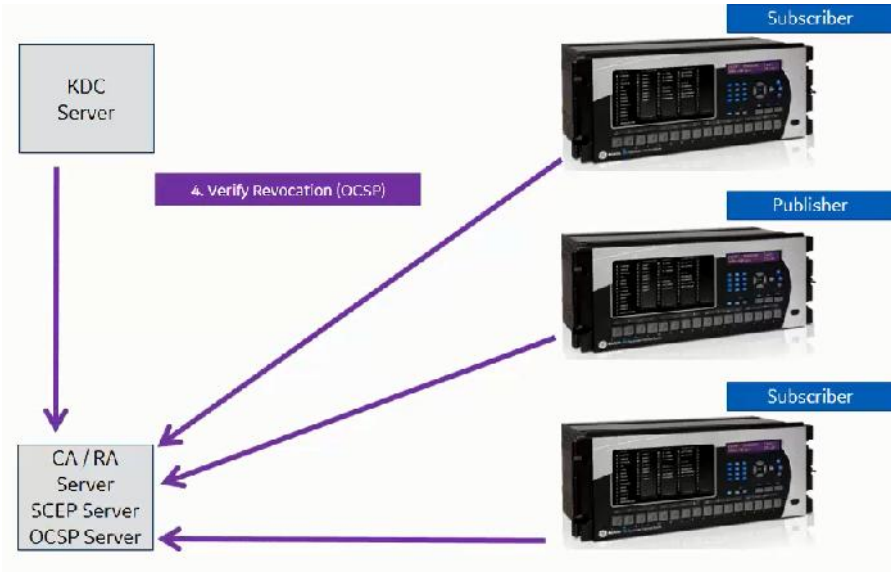


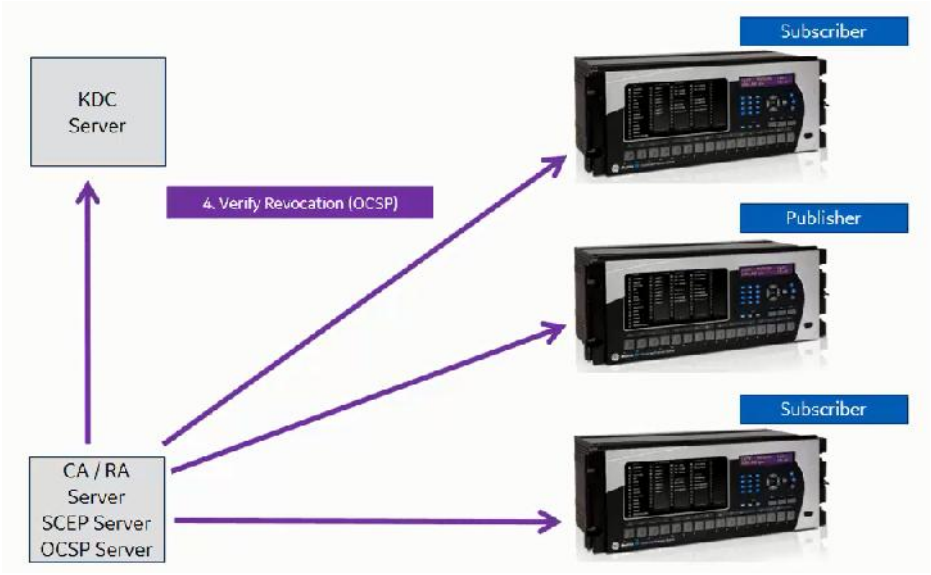


4-then each device end the other Certificate to the Registriation authority server to check if it is OK or not?

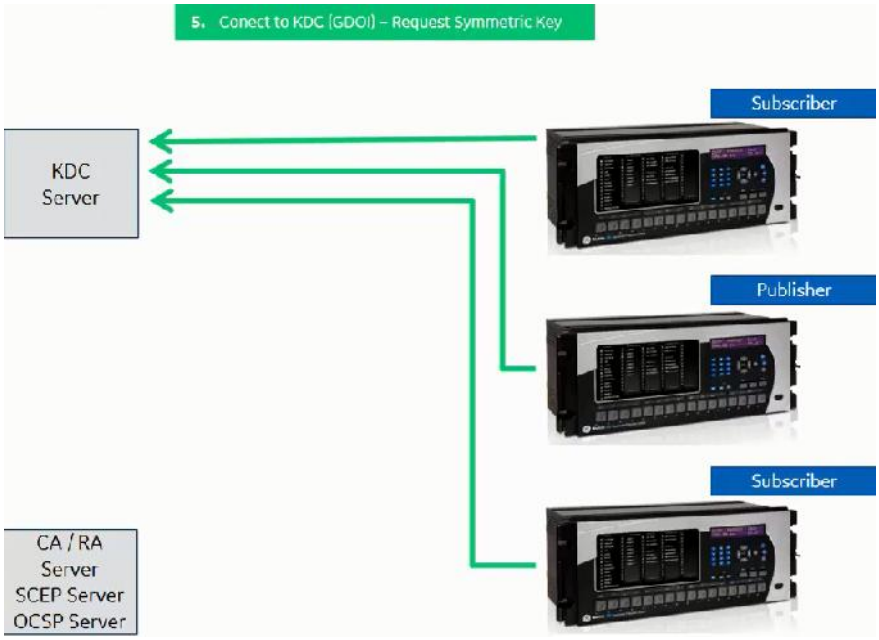
يعنى كل جهاز بيبعت الشهاده بتاع الكى دى سى لل هيئة التسجيل علشان يتاكد انها فعلا صحيحه بما فيهم كمان الكى دى سى بيرسل شهادات الاجهزه علشان يتاكد منها.

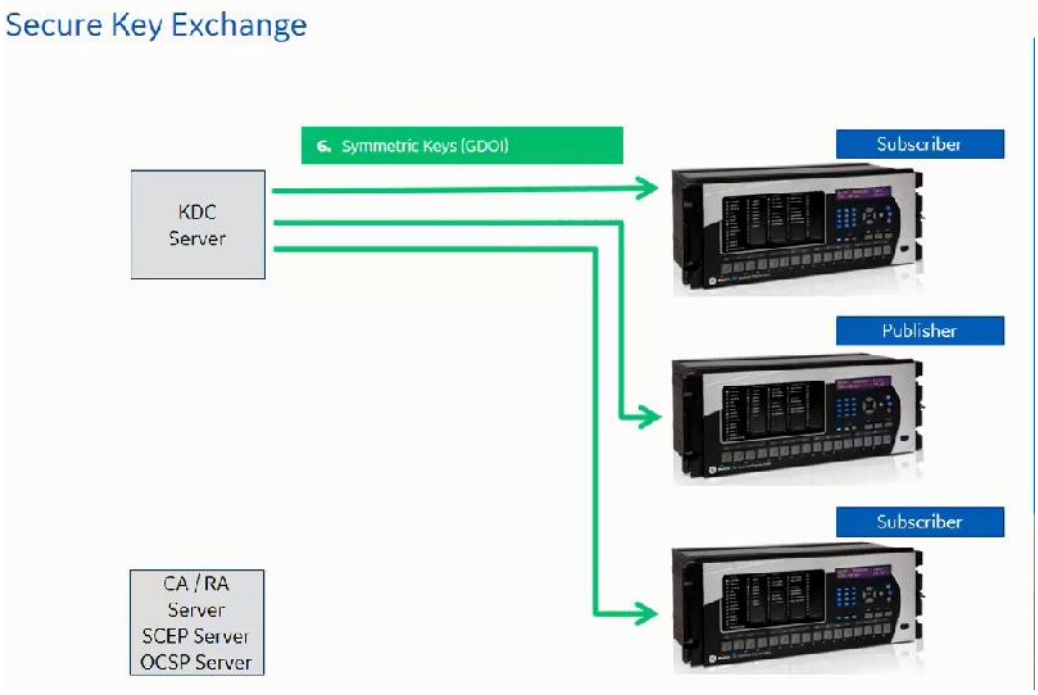
The RA response to each one to validate the certification



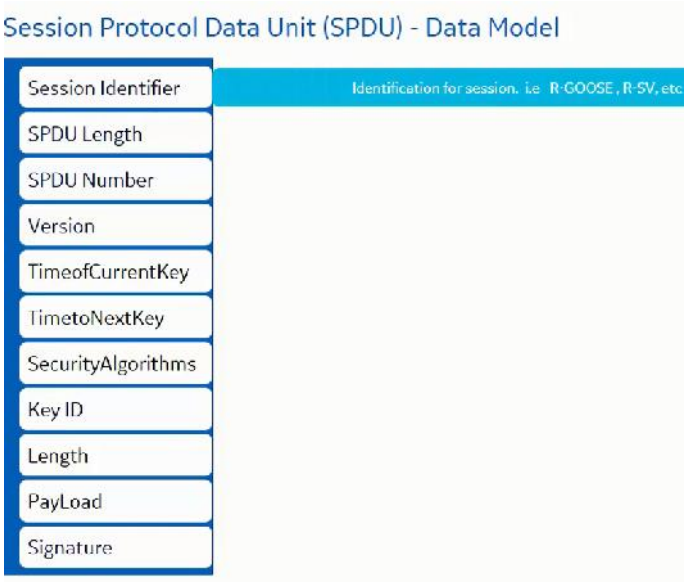


5-Then every device request symmetric key from KDC server , this key used for signing encrypted R-GOOSE message authentication and renewed each 2 days.





R- GOOSE (IEC61850-90-5) : using encapsulated data packet (SPDU)



HSR & PRP:

HSR has double data and PRP has double everything.

HSR and PRP advantage that RSTP protocol (rapid spanning tree protocol) that HSR & PRP has zero time recovery in case of failure.

HSR & PRP were originally designed for substation automation.

HSR & PRP: are un-visible to IP layer

HSR: High availability Seamless Redundancy Protocol

HSR implemented in a ring topology, each node in HSR has an internal Ethernet switch.

In HSR the frames are duplicated by the source/ transmitter and sending it through two paths to the receiver.

The distination accepts the first packet and discards the other packets.

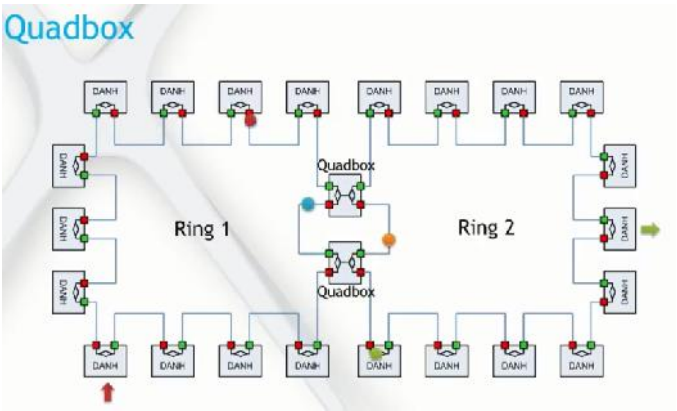
بتبدا عندى المشاكل فى حالة more complicated لما النتورك بتكبر

To solve this issue there is many ways:

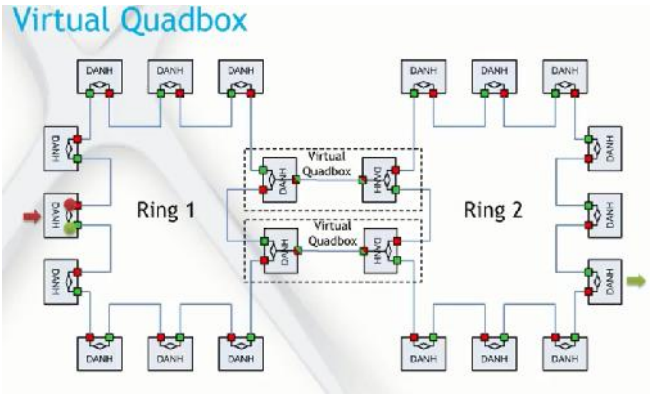
1-qouadbox: 2 Quad Boxes are need.

Divide the main Ring into 2 small rings to remove the repeated packets .

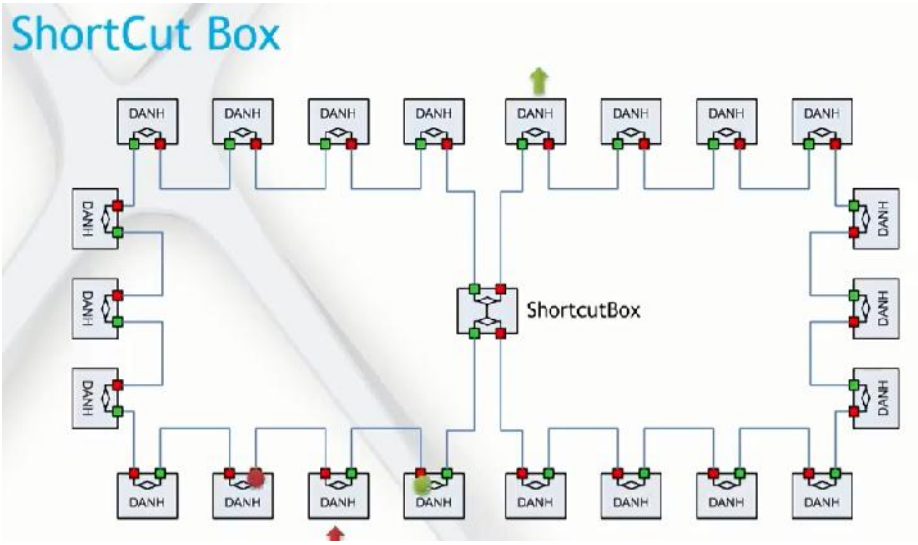
But in this solution 2 extra devices are needed, extra cost on the network.



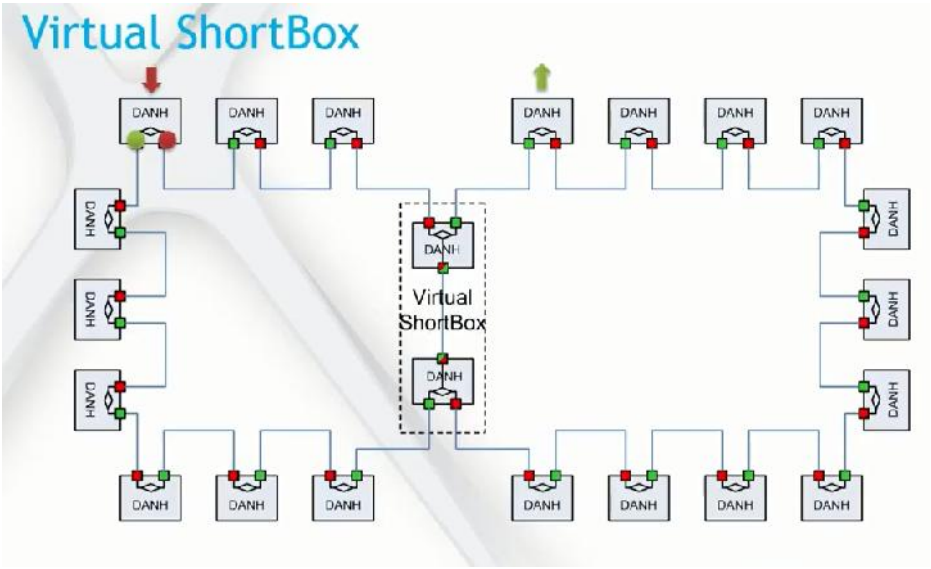
2- Virtual quad box:



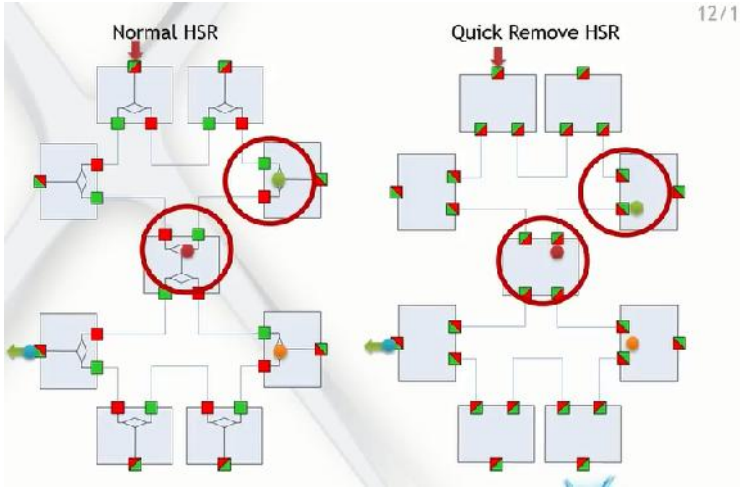
3-Shortcut box

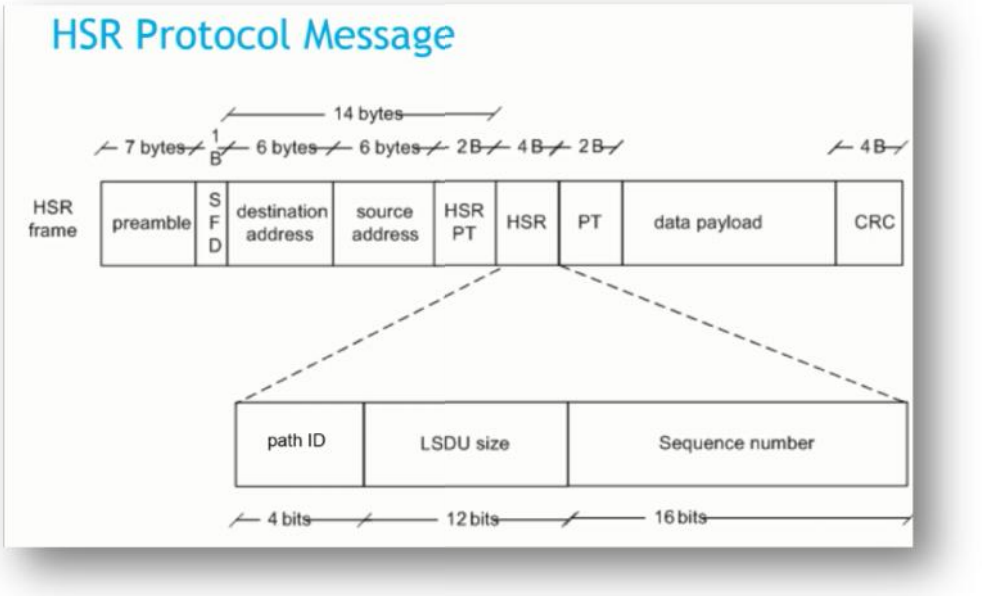


5- Virtual shortcut box:



6- New Quick removing nodes developed to eliminate the packet duplication: QR nodes.
This new node not allows the same packet to path through the network more than one time.





The most important in HSR frame message is the sequence number because HSR is compare packets and discard the duplicated based on it. اهم جزء فى الفرايم المدكونس نمبر لان البرتكول بيقارن الباكتس بناءا ويحذف المكرره بناءا على الرقم دا

Path ID: tells from which LAN this packet belong to. ودا كمان بيستخدم لمنع رجوع الباكت لنفس البورت الى جايه منه

Path ID used by the Red Boxes to prevent forwarding the packet to the original LAN.

PRP: Parallel Redundancy Protocol :

PRP implemented in a double star topology , in double star each DAN connected to different network.

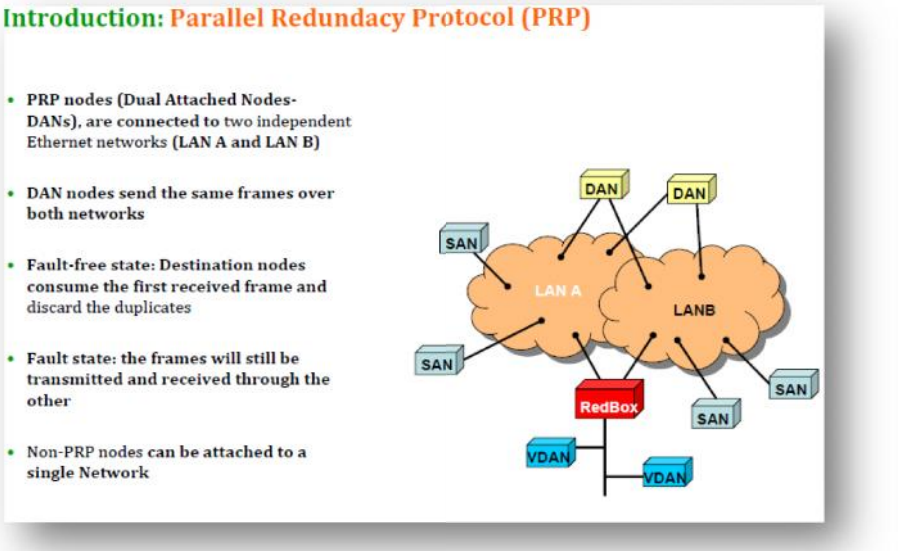
DANمثل ماهو واضح فى الصوره كل نوود بتتصل بشبكتين مختلفتين وتسمى

الدان بترسل نفس الباكت الى كلا من الشبكتين المتصله بهما.

المستقبل بيقبل اول باكت بعدين بيحذف اى رساله اخرى بتصله لنفس المعلومات

SAN single attached Node.ممكن طبعا نوود مش مفعل عليها البرتوكول دا تتصل باحد الشبكتين وتسمى

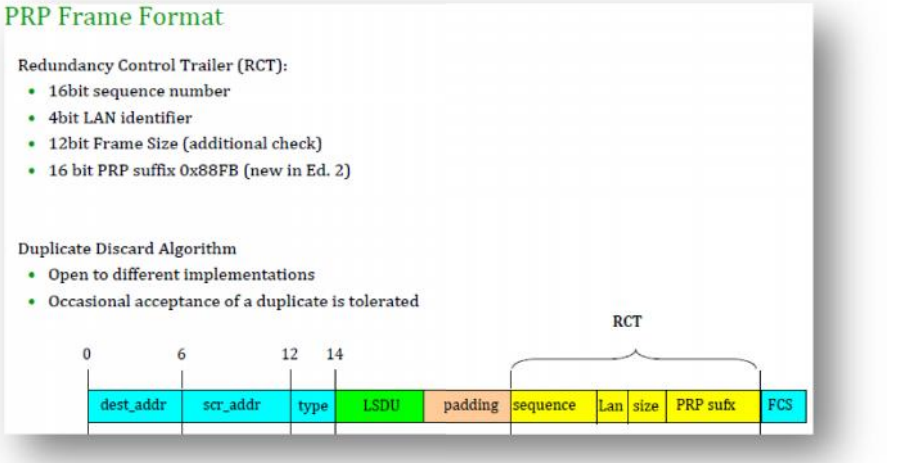
هنا بنقدر نوصل الاجهزه ال السنجل مباشرة لانIn PRP SAN device can connected directly to the network without RED Box that used in HSR because PRP protocol uses trailer and trailer is ignored by them. In the other hand HSR uses Header and Header in the front of the packet so the SAN devices do not understand it. من عيوبه لان المرسل يظل يبعت نفس الداتا



Network Supervision

- Monitor **the status of each node and LANs Each DAN sends periodically a** Supervision Frame

- **Supervision Frame Format:**
  - Multicast by each DANP over both ports every LifeCheckInterval
  - VLAN tag optional
  - MAC addresses
  - Protocol version
  - Mode of operation supported
  - Supervision frames sequence number

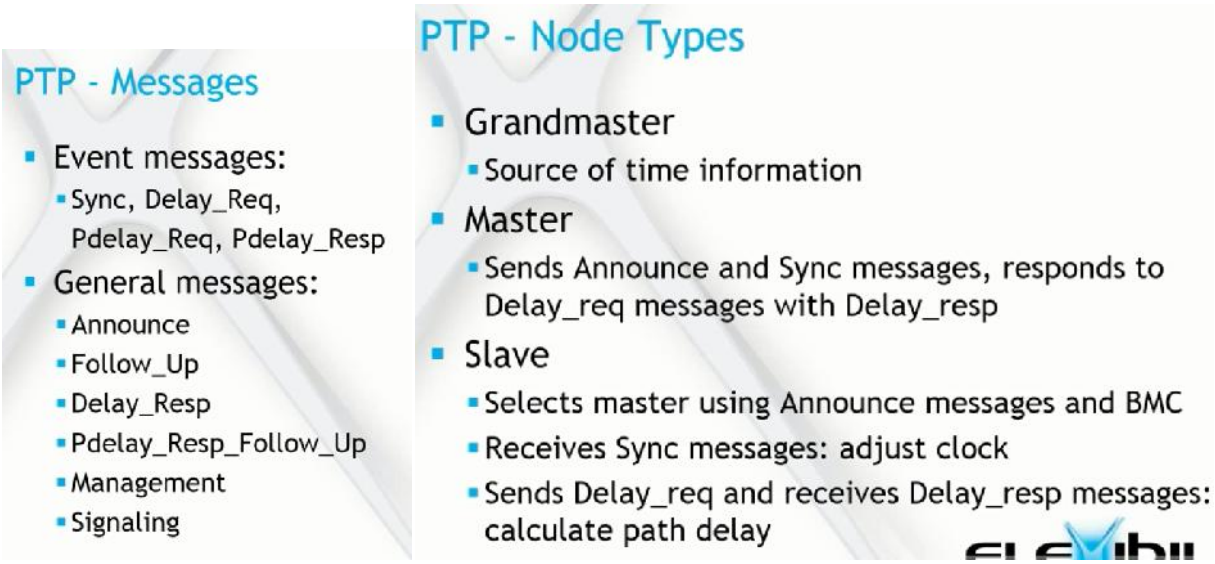


PTP: Precision Time Protocol (IEEE 1588 or IEC6 1588) : this protocol synchronize the network clock by sending packet over the network , the other clocks automatically synchronized to the most accurate clock in the network .

بيبعت باكت علشان يظبط الوقت بتاع كل اجهزه الشبكة كل الاجهزه بتاخد وقتها من افضل ساعه مضبوطه

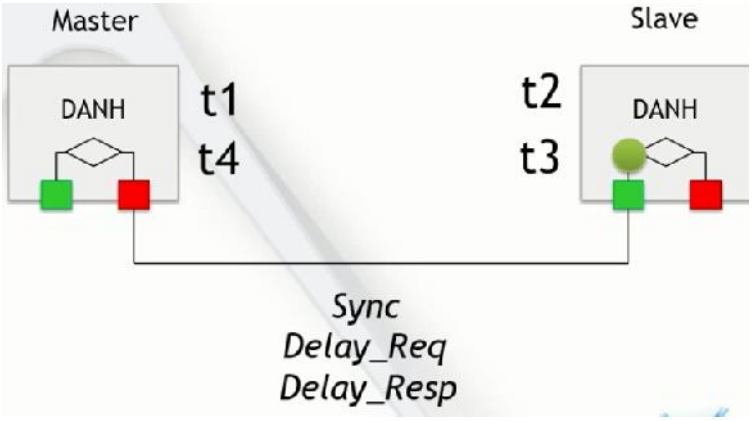
طبعاالبرتوكول غير مسؤل عن سرعه او بطء الشبكة هو بس بيضبط الساعه

PTP sends to types of Messages : 1- Event messages 2- General Messages.

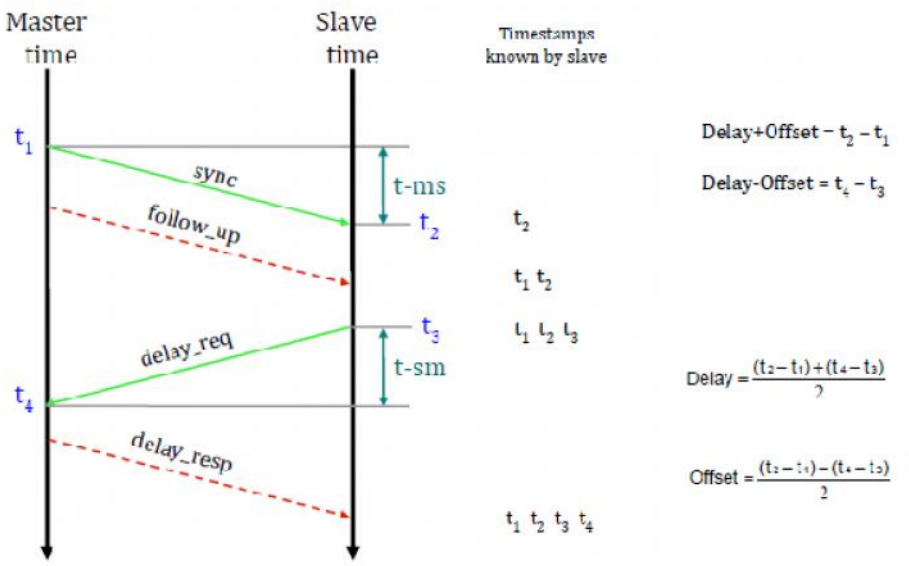


Clock types: Boundary clock, transparent clock, ordinary clock.

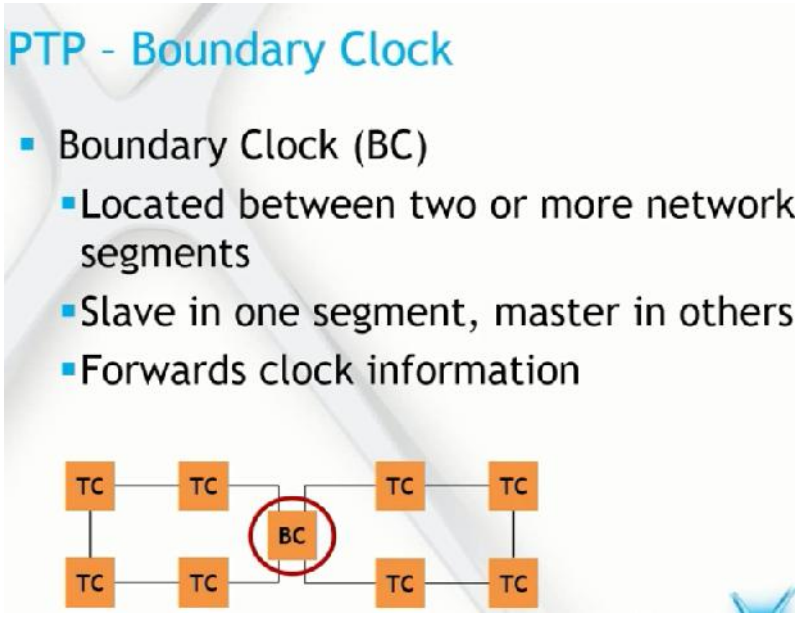
Ordinary clock (Master – Slaves).



الماستر بتبدا ترسل سينكورنيس ماسدج بالوقت الحالى ت1 بتوصل عند المستقبل بعد فتره معينه بنسميها ت2 وبعدين
المستقبل بيرسل للماستر رسالة عند ت3 اسمه ديلاى ريكوست بتوصل عند الماستر عند الوقت ت4 ويرد على المستقبل انه استقبل عند وقت كام بالظبط
وبناءا علية المستقبل بيحسب بقى الوقت عنده كام بناءا على ت1 وت2 وت3 وت4 .

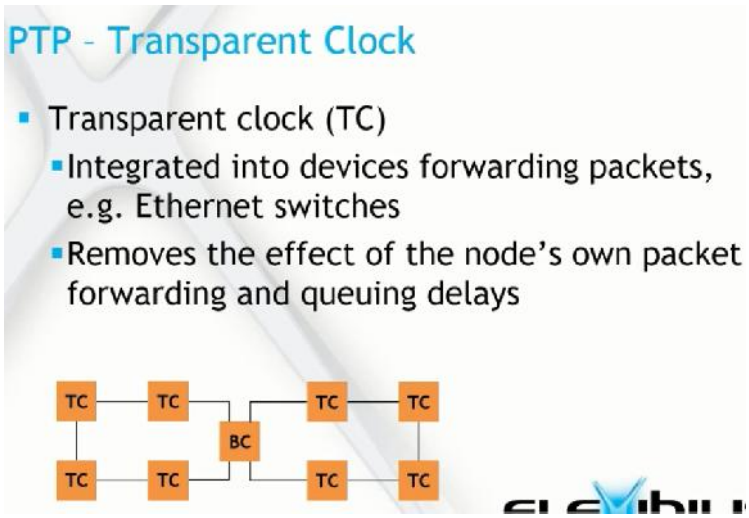


Boundary clock:



Boundary clock must be used if the PTP modes changes from peer to peer into end to end

.



Transparent clock:

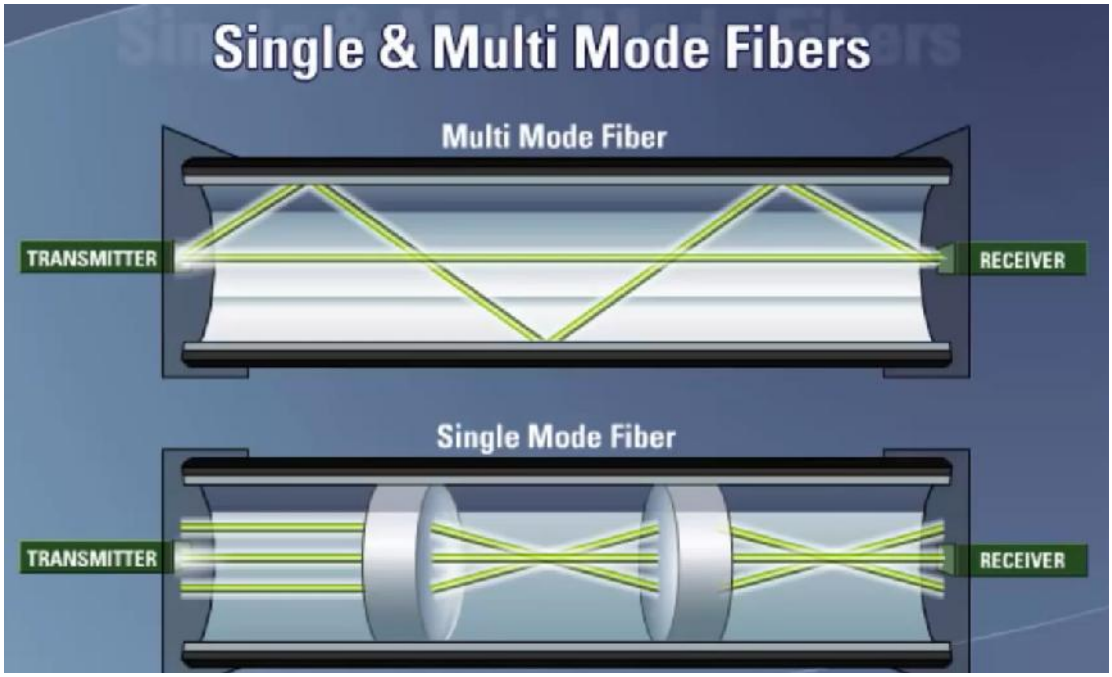
End to End يعنى بيحسب الوقت الى تم الارسال فيه ويشيل من التاخير على طول المسار من اول الماستر حتى المستقبل بصرف النظر عن كام نود فى الطريق.

Peer to peer: لازم يحسب كل تاخير بين كل اتنين نود لوحده ويجمع التاخير كله وبعدين يطرحه من زمن الارسال

In HSR peer to peer TC has to been to used because there are many routes the packet could use and the delay will be more accurate with it.

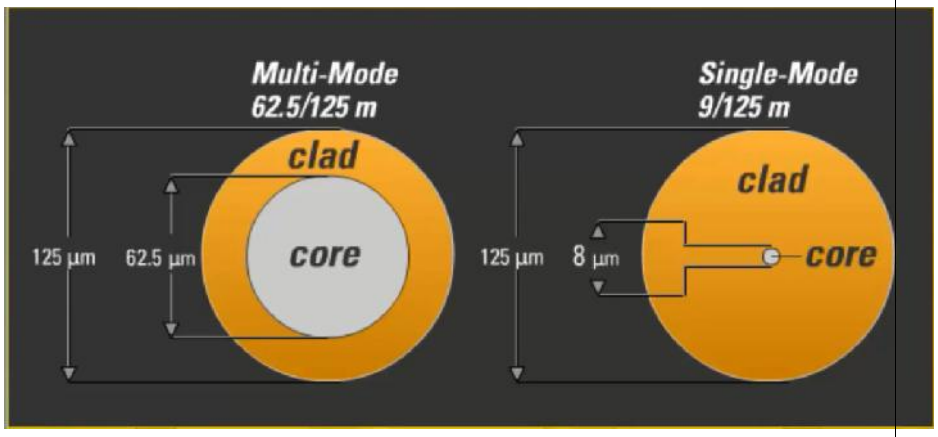
Fiber Optic media:

2 different types of fiber optic: single mode and multi mode

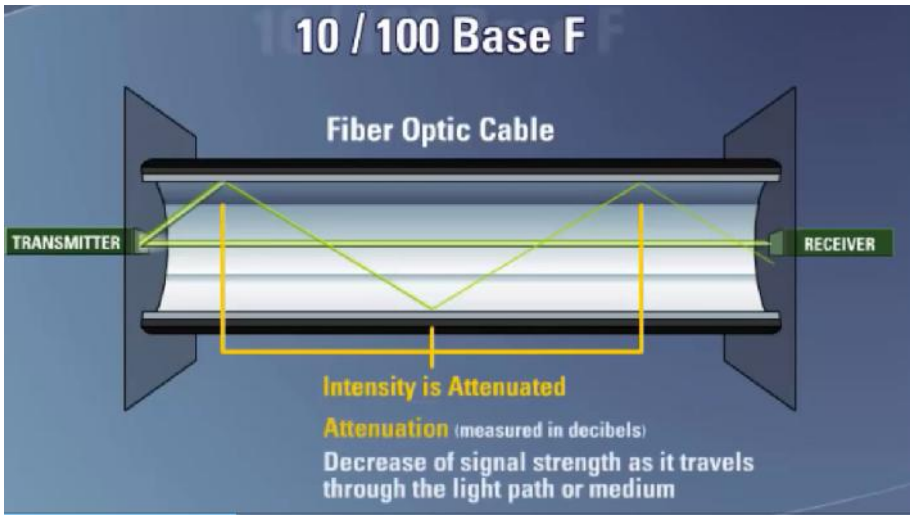


Multi mode: 2 Km distance

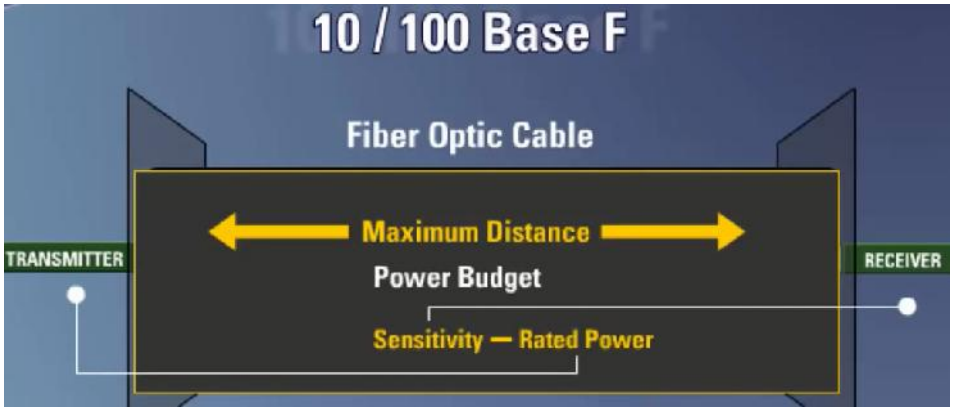
Single mode: less in attenuation



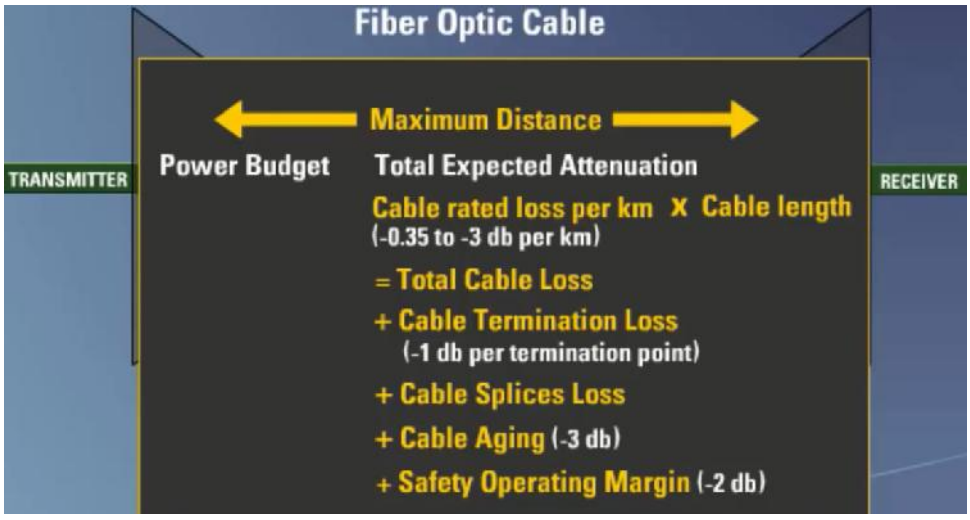
But practically what is the max distance using FO: Must be calculating the attenuation between TX and Rx:



If the light is not strong enough the receiver cannot detect the signal.



Power budget= sensitivity of Rx- rated power of Tx(هى اكبر كميه مسموح بها من ال اتنويشن



Total attenuations = (cable loss per Km * cable length + terminations (-1db for one termination) + splices loss (0.2 per one connection+ Aging + safety margin.

بعدين نقارن بقى الاتنين مع بعض

If Power budget > attenuation يبقى كدا تمام