Treball d'Internet

INTE 2023-2024 Q5

Nom: Mariona Farré Tapias
Data: 21/11/2023
Curs: 2023-24

Índex:

Enunciat

El treball consisteix en entendre i analitzar les possibles problemàtiques en una connexió entre dos equips de xarxa. Es divideix en tres apartats complementaris que es descriuen a continuació.

a) Identificar els possibles punts de fallida en una connexió entre dos equips de xarxa i proposar un algorisme teòric senzill que permeti fer-ne el seguiment. Es pot utilitzar, a títol d'exemple, la connexió de l'ordinador personal a la web de la UPC. Es valorarà que es contempli la major quantitat possible de casuística, el plantejament amb una visió general i la sistemàtica d'anàlisi.
b) Proposar, en cada situació problemàtica de l'algorisme anterior, una solució teòrica al problema identificat.
c) Proposar les proves pràctiques que cal fer, en cada possible situació problemàtica de l'algorisme anterior, per a verificar el funcionament. Les proves es realitzaran amb la distribució Debian més actual, mitjançant línia de comandes, i s'hauran de documentar. No es poden fer captures de pantalla per demostrar el funcionament, cal copiar el resultat de les comandes.

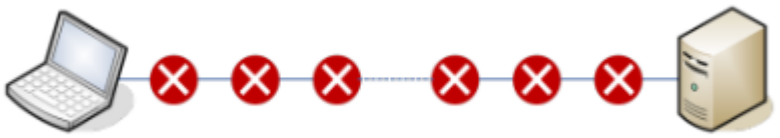


Figura 1. Possibles errors en la comunicació entre dos equips de xarxa.

1. Identificació de punts problemàtics

Per poder estudiar d'una manera ordenada els diferents punts problemàtics entre dos equips de xarxa, una de les maneres que es pot organitzar és seguir el model OSI (Open Systems Interconnect) i centrar-se en cada capa, la seva funcionalitat i quins són els possibles problemes que ens podem trobar.

1.1. Capa Física

La capa física és la primera capa en la connexió del model OSI, es basa en la transmissió i recepció de dades no estructurades o processades entre dispositius, les tradueix per a la següent capa d'Enllaç en forma de ones eléctriques o óptiques o de ràdio o viceversa per la recepció de dades.
Els possibles problemes que ens podem trobar són:

- Dany en els cables:

Els cables poden patir desgast del seu ús amb trencades, ruptures, danys pel medi ambient etc que poden fer que hi hagi problemes de connectivitat.

- Problema amb els connectors:

Els connectors poden acabar trencats físicament, solts entre ells o corroir, interrompent els senyals de transmissió.

- Interferències elèctriques:

Les interferències externes electromagnètiques d'altres dispositius o línies elèctriques, poden distorsionar els senyals de la xarxa que sent transmeses en forma d'ones.

- Falles del hardware:

Tots els components que formen part d'aquesta capa, com els adaptadors de xarxa, els routers, els ports estàndard o d'Ethernet dels routers, els switches, els hubs o els mòdems poden fallar per diferents problemes com serien els defectes de fabricació, el temps d'ús i el sobreescalfament entre altres.

- Factors ambientals:

Tenir els equips exposat a factors ambientals com les temperatures extremes, la humitat o l'exposició a l'aigua, pot impactar negativament els components físics de la connexió.

- Limitacions de distància:

Les grans distàncies entre equips poden portar problemes de disminució de senyals o la pèrdua completa d'aquestes.

1.2. Capa d'Enllaç

La segona capa del model OSI, està entre la capa Física i la capa de Xarxa, té la funció de comunicar les dades de les capes més físiques a les capes més abstractes.
Té la funció de transferir dades entre dispositius de la mateixa xarxa, on les dades que rep de la capa de Xarxa les divideix entre parts més petites formant trames per la capa Física. Controla el flux de la transmissió de dades entre dos punts per rebaixar el tràfic, té controls d'error de les comunicacions, per això ha de controlar la topologia de la xarxa, sent conscient de la topologia física i lògica, gestionant i finalitzant connexions entre dispositius per garantir una comunicació fiable.
Fa servir les adreces MAC (Media Accés Control) per atribuir adreces als diferents dispositius per assegurar-se que s'entreguen correctament els paquets dins la xarxa.
El protocol ARP (Address Resolution Protocol) i DHCP (Dynamic Host Configuration Protocol), tenen la funció de configurar una adreça IP a través de les adreces MAC de manera automàtica i sincronitzada, és tenen guardades dins una taula per cada dispositiu amb totes les equivalències de les adreces MAC i les adreces IP amb qui es pot comunicar.
Els possibles problemes que ens podem trobar són:

- Conflictes amb adreces MAC:

Es poden donar casos que dos dispositius a la mateixa xarxa tinguin la mateixa adreça MAC, fent que hi hagi problemes d'enviament de paquets on arribin dispositius erronis o la pèrdua d'aquests.

- Protocol ARP:

Fallades en la resolució de les adreces IP a adreces MAC, ja sigui atribuint les mateixes adreces, adreces incorrectes o no trobar l'adreça que li correspon.

- Canvi de bucles:

Camins redundants d'una xarxa amb switches, pot crear bucles infinits fent que s'arribi al col·lapse o creació de congestió en la xarxa.

- Corrupció de Fragmentació:

Els fragments que crea separant les dades, poden ser creats erròniament amb dades que falten o repetides, per exemple per culpa d'interferències, fent que hi hagi errors en les dades i la retransmissió.

- Col·lisió i problemes de broadcast:

Tenint dos equips, si estan connectats amb half-duplex, on només els dispositius poden transmetre enviant o rebent informació per una direcció alhora pot fer que hi hagi col·lisions o tenim masses missatges de broadcast que arribin a saturar la xarxa.

- Configuració incorrecta de la VLAN:

Si hi ha una configuració incorrecta a la VLAN (Virtual Local Area Network), les subxarxes lògiques creades o en els ports dels switches, poden haver problemes de connectivitat entre dispositius que no rebin, envin incorrectament les dades o vulnerabilitats a la seguretat.

- Problemes d'enllaç:

Problemes en connexions origen i destí, poden ser per problemes de la capa Física o per què hi hagi problemes de comunicació entre dos dispositius.

1.3. Capa de Xarxa

La capa de Xarxa, és la tercera capa del model OSI, com el seu nom indica, es responsable per l'adreçament lògic i l'encaminament de les dades.
Inclou el protocol IP (Internet Protocol), ja sigui la versió 4 o versió 6, per què és la base dels protocols de la capa de Transport amb els protocols TCP i UDP.
Amb el protocol DHCP (Dynamic Host Configuration Protocol), permet als dispositius d'una xarxa IP, obtenir els paràmetres de configuració d'aquesta automàticament. Per exemple, amb un client i servidor, el servidor anirà assignant a cada client adreces IP a mesura que aquestes estiguin lliures, tenint la informació per cada adreça qui la té assignada, la máscara, la porta d'enllaç (gateway), el servidor DNS i el nom del domini (capa d'Aplicació), quan de temps té aquesta adreça IP i a qui se li assigna després.
També inclou protocols de control de missatges com l'ICMP (Internet Control Message Protocol) per reconèixer i alertar d'errors de la xarxa.
El protocol OSPF (Open Shortest Path First), quin és el millor camí per les dades en que poden ser transmeses, des de l'origen al seu destí, involucra analitzar les condicions de la xarxa, la distància entre routers etc.
El protocol RIP (Routing Information Protocol), determina la distància a través de salts entre routers com a mètrica, per trobar el millor camí serà el que tingui menys salts a fer.
La fragmentació i tornar a ajuntar paquets, és per tenir transmissió més eficient amb paquets petits i assegurar que es poden tornar a muntar de manera correcta en el seu destí.
Els possibles problemes que ens podem trobar són:

- Conflictes d'adreces IP:

Poden haver-hi problemes quan més d'un dispositiu de la mateixa xarxa, tenen assignada la mateixa adreça IP, fent que hi hagi problemes de comunicació o problemes amb la compatibilitat entre versions entre IPv4 i IPv6.

- Assignació dinàmica DHCP:

En l'assignació dinàmica d'adreces IP en un servidor DHCP, es poden produir problemes com: assignar adreces ja utilitzades, adreces errònies, màscares de subxarxa incorrectes o adreces fora de la xarxa.

- Protocol ICMP:

La incapacitat de crear missatges ICMP en la xarxa, pot fer que hi hagi errors en la xarxa sense ser alertats i que aquests després afectin en la comunicació entre dispositius.

- Problemes d'encaminament amb RIP o OSPF:

Si s'utilitzen aquests protocols, i estan mal configurats, pot afectar a la capacitat de la xarxa per determinar el millor camí pels paquets i fer una tria incorrecte o menys efectiva.

- Subnetting:

Si hi ha errors en la creació de subxarxes, en les màscares configurades o en la configuració de rutes per els paquets, pot resultar a problemes de redirecció errònia del tràfic i llocs en la xarxa que no es pot arribar mai.
És important respectar les adreces de gateways i les màscares de cada subxarxa per no tenir problemes de connexió.

- Configuració del Router:

Els routers si tenen qualsevol error en la seva configuració poden tenir encaminaments ineficients, bucles o molt tràfic en segments específics.

- Configuració de Firewalls:

Una configuració molt estricte o mal creada de Firewalls (tallafocs), pot bloquejar el trànsit de connexions desitjades i permetre accés a dades no autoritzades.

- Congestió i caps d'ampolla:

Tenir segments de xarxa amb una sobrecàrrega de tràfic amb congestió o un rendiment lent a punts específics, pot afectar a una connexió lenta i ineficient.

1.4. Capa de Transport

La capa de transport, és la quarta capa del model OSI,on es gestiona la comunicació des d'un origen a un destí, assegurar-se que les dades siguin transmeses entre dispositius de manera fiable i eficient igualment del tipus de xarxa sigui a les capes de baix.
Divideix els blocs de dades en segments més petits per tenir una transmissió més fàcil i eficient, després aquests són reagrupats a la destinació.
Regula el flux de dades amb la velocitat de transmissió entre dos punts per no sobrecarregar el receptor.
Pot detectar i corregir potencialment errors en la transmissió de dades, a través de checksums dels paquets i missatges de reconeixement ACK (acknowledgement).
Aquesta capa fa servir els protocols TCP (Transmission Control Protocol) i UDP (User Datagram Protocol), on TCP proporciona connexió fiable i orientada a la connexió i UDP proporciona velocitat i no està orientat a la connexió.
Els possibles problemes que ens podem trobar son:

- Conflictes en els ports:

Si els ports estan mal configurats o bloquejats, pot fer que aplicacions i serveis no es puguin comunicar amb el dispositiu, o si hi ha múltiples aplicacions o serveis utilitzant el mateix port, poden haver-hi conflictes i errors de comunicació.

- Congestió i control de flux:

Com amb anteriors capes, una gestió inadequada de les dades pot portar a una congestió i saturació de la xarxa provocant pèrdua de paquets i retards.

Assegurar-se que les transmissions de dades entre l'emissor i receptor tinguin les mateixes taxes de transmissió, sinó pot ser que el buffer de transmissió es desbordi o guardi molt poques dades entre dispositius.

- TCP: (Transmission Control Protocol)

Pot incloure problemes com un inici lent o erroni, problemes per culpa de la congestió en la xarxa, problemes amb la segmentació del paquet TCP, creant retards i reduint el rendiment de la xarxa.

- UDP: (User Datagram Protocol)

Pot incloure problemes amb la pèrdua de paquets, al no tenir mecanismes per assegurar-se la fiabilitat, l'ordre i la seguretat de les dades, comporta possibles pèrdues de dades i possibles errors.

- Temps d'espera:

El temps d'espera (Timeout) d'un paquet pot arribar a gastar-se i fer que aquell paquet sigui invàlid per culpa de retards fent que hi hagi retransmissions i una connexió ineficient.

- Reordenació dels paquets:

És possible que els paquets fragmentats que arribin a la seva destinació de forma desordenada, afectant en la totalitat de les dades rebudes.

- Establiment i acabament de la connexió:

Els problemes per establir o tancar correctament les connexions poden provocar un malbaratament de recursos i retards en la comunicació.

- Recuperació d'errors:

Tenir mecanismes de recuperació insuficients poden provocar la corrupció o pèrdua de dades.

1.5. Capa de Sessió

La capa de Sessió és la cinquena capa en el model OSI, on es gestiona i es controla els diàlegs (les sessions) entre els dispositius de la xarxa. Estableix, manté i finalitza aquestes sessions assegurant-se que les dades són intercanviades ordenadament i correctament.
Té mecanismes per la sincronització de les dades, característica essencial per transmissions llagues o en aplicacions multimèdia, incloent punts de control per recuperar dades si hi ha interrupcions en la transmissió de dades.
Pot participar o facilitar en els processos d'autenticació i autorització per establir sessions segures.
Els possibles errors que ens podem trobar són:

- Inicialització de la sessió:

Problemes en l'inici de sessions a causa de problemes de comunicació, configuracions incorrectes o limitacions de recursos.

- Sincronització de sessions:

Dificultats per mantenir l'estat de la sessió i la sincronització, sobretot en comunicacions complexes o de llarga durada.

- Finalització de la sessió:

Les sessions que no finalitzen correctament, sessions amb inactivitat prolongada o problemes de connexió provoquen un malbaratament de recursos.

- Autenticació i Autorització:

Dificultats per verificar les identitats entre els dispositius connectats per assegurar-se que tenen les permisos adequats per establir i passar-se informació.

- Amenaces en la seguretat:

Possibles vulnerabilitats en la gestió de sessions que poden provocar fallides en la seguretat exponent dades vulnerables a ser robades per usuaris o dispositius externs.

1.6. Capa de Presentació

La capa de presentació és la sisena capa del model OSi, té com a funció la traducció entre la capa d'Aplicació i les altres capes anteriors del protocol de comunicació.
Converteix el format de les dades pel que la xarxa o l'aplicació vol, garanteix seguretat encriptant les dades abans que siguin enviades i poder ser desencriptades a l'arribar al seu destí i té la funció de poder compactar dades, ja sigui sense pèrdues de cap dada o amb algunes pèrdues, però mantenint l'essència de les dades originals.
Els problemes que ens podem trobar són:

- Incompatibilitat de format:

Diferents dispositius poden utilitzar diferents formats de dades, detall que pot comportar problemes d'incompatibilitat en serveis o aplicacions.

- Encriptació/Desencriptació de dades:

Si hi ha problemes amb l'encriptació o desencriptació, pot resultar en dades siguin il·legibles o es vulneri la seva privacitat durant la seva transmissió.

- Compressió i Descompressió:

Els problemes en la compressió de dades poden provocar la pèrdua de dades o possibles errors a l'hora de descomprimir les dades.

- Errors de codificació de caràcters:

La falta de coordinació entre sistemes, pot fer que la codificació dels caràcters tingui una mala interpretació de les dades (com a ASCII o Unicode)

- Corrupció de dades:

Les dades es poden malmetre en els processos de transformació i traducció de format, afectant la integritat de les dades originals.

1.7. Capa d'Aplicació

La capa d'aplicació és la setena i última capa en el model de OSI, és la capa més a prop de l'usuari, té la funció de proveir una interfície interactiva entre les aplicacions d'una capa anterior i el dispositiu físic que utilitza l'usuari.
Ha de gestionar les dades com són presentades, formatejades, creades i convertides per assegurar compatibilitat entre diferents tipus de software i sistemes.
Inclou varis protocols específics per aquesta capa, com podria ser: els certificats SSL (Secure Sockets Layers), TLS (Transport Layer Security) , HTTP o HTTPS (HyperText Transfer Protocol Secure) i FTP (File Transfer Protocol), per navegadors d'internet per una transferencia de dadesi fitxers segura i eficaç.
També fa servir el protocol DNS (Domain Network System) sistema de noms jeràrquic que permet obtenir informació associada a un nom d'un domini on el tradueix a una adreça necessària pel protocol IP.
El protocol SSH (Secure SHell) és un protocol per connectar els servidors fent servir la xarxa d'internet per comunicar-se, sempre és segur perquè la informació està encriptada i garanteix confidencialitat entre usuaris.
També té la responsabilitat de gestionar la identificació de l'usuari, els seus drets d'accés i assegurar.se que només usuaris autoritzats puguin accedir a la xarxa.
Els problemes que ens podem trobar són:

- Protocols HTTP i FTP:

Errors en la implementació de protocols com el HTTP o FTP, poden provocar errors en la comunicació o una mala interpretació de les dades.

- Certificats SSL, TLS i HTTPS:

Errors en la negociació o encriptació en SSL,TLS o HTTPS, poden fer que aquestes dades ja no estiguin segures i no es pugui donar els certificats de seguretat en la connexió, convertint-la en una connexió no segura.

- Configuració de SSH:

Si es tenen problemes en la configuració o l'execució del protocol SSH, les dades que s'estan comunicant poden estar compromeses.

- Configuració del DNS:

Una configuració incorrecta o una fallida en el servei DNS, pot donar errors de connexió sigui donant una adreça incorrecta o que no existeix.

- Error de l'aplicació:

Fallades en el programari (software) de l'aplicació pot portar errors de comunicació i pèrdua de dades.

- Mesures de seguretat inadequades:

La manca de mesures de seguretat robustes poden provocar vulnerabilitats en l'aplicació, poden donar accés no autoritzat a usuaris externs o vulneració de dades comunicades.

- Rendiment de l’aplicació:

Les aplicacions mal optimitzades o amb funcions irrellevants poden provocar temps de resposta lents, alta latència o sobrecàrrega del servidor.

- Problemes d'interoperabilitat:

La incompatibilitat entre diferents sistemes o plataformes pot dificultar la comunicació o provocar errors en l'intercanvi de dades.

- Escalabilitat:

Les aplicacions que no estan dissenyades per la seva escalabilitat poden tenir problemes amb una càrrega més gran on no poden gestionar un gran nombre d'usuaris alhora. També l’alta demanda de serveis, pot sobrecarregar els servidors d'aplicacions amb una baixada en el rendiment.

- Autenticació i autorització de l’usuari:

La mala gestió de l’accés dels usuaris i la seva verificació d’identitat o problemes amb els seus drets d’accés, pot portar riscos de seguretat i afectar a la usabilitat del servei o aplicació.

- Integritat i sincronització de dades:

Garantir que les dades es mantenen coherents i sincronitzades entre els diferents sistemes pot comportar molt treball, sobretot si l'aplicació aconsegueix les dades en vàries bases de dades.

2. Solucions teòriques per cada punt problemàtic

Per cada un dels nivells del model OSI, hem exposat els possibles problemes i punts problemàtics en l'inici, establiment i finalització d'una connexió, ara donarem vàries solucions teòriques per cada punt exposat, per així en el següent apartat poder donar una o vàries solucions pràctiques.

2.1. Capa Física

Per cada problema exposat anteriorment, les solucions teòriques proposades són:

- Danys en els cables:

Per cables danyats és important fer inspeccions regulars, implementar una gestió adequada i substituir els cables danyats amb recanvis d'alta qualitat.

- Problema amb els connectors:

Comprovar regularment l'estat dels connectors, ajustar si s'han desajustat, netejar si és possible o directament substituir connectors corroïts o trencats.

- Interferències elèctriques:

Intentar ubicar els cables i l'equips en zones sense interferències elèctriques, es pot utilitzar cables blindats per minimitzar les interferències.

- Falles del hardware:

Implementar rutines de manteniment a tot el equip físic de la xarxa, tenir microprogramari (firmware) i programari (software) sempre actualitzats, substituir els components trencats, defectuosos o que comencen a fallar el més aviat possible i amb components de xarxa de qualitat.

- Factors ambientals:

Tenir els equips en zones amb climatització controlada, ja sigui amb aire acondicionat, amb una ventilació adequada per evitar el sobreescalfament i amb sistemes per detectar i protegir contra els danys que pot provocar el contacte amb l'aigua.

- Limitacions de distància:

Si hi ha una gran distància usar repetidors o extensors de senyal per augmentar la força del senyal i triar el tipus de cable adequat pel rendiment i la distància necessària.

2.2. Capa d'Enllaç

Per cada problema exposat anteriorment, les solucions teòriques proposades són:

- Conflictes amb adreces MAC:

Implementar protocol automàtic d'adreces MAC utilitzant el servidor DHCP, aquest serà el responsable d'assignar automàticament adreces IP als seus clients d'adreces MAC. Regulament controlar els dispositius dins de la xarxa per veure que cap adreça MAC està mal configurada o duplicada.

- Protocol ARP:

Revisar i gestionar la taula ARP del dispositiu per trobar inconsistències, es pot reiniciar el dispositiu per reiniciar el protocol o usar comandes des de la terminal d'un dispositiu per actualitzar, crear o borrar entrades a la taula.

- Canvi de bucles:

Ultilitzar protocols com STP (Spanning Tree Protocol) per prevenir la creació de bucles infinits en la xarxa només tenint un camí actiu entre dispositius (però guardar els camins redundants com a reserva si l'actiu falla)

- Corrupció de Fragmentació:

Implementar mecanismes de detecció d'errors com el mecanisme CRC (cyclic redundancy check) en dispositius d'emmagatzematge per detectar canvis accidentals en les dades.

- Col·lisió i problemes de broadcast:

Intentar transmetre les dades en configuracions full-duplex on els dispositius poden enviar i rebre dades alhora i evitar així les col·lisions.
Establir límits d'adreces per la missatgeria broadcast i intentar utilitzar switches abans de hubs per reduir el número d'aquestes adreces.

- Configuració incorrecta de la VLAN:

Realitzar revisions i verificacions de la configuració VLAN, mantenint normes estrictes de la seva gestió i els controls d'accés en aquesta.

- Problemes d'enllaç:

Assegurar-se que l'enllaç existeix, que els dos dispositius són compatibles i que funciona correctament.

2.3. Capa de Xarxa

Per cada problema exposat anteriorment, les solucions teòriques proposades són:

- Conflictes d'adreces IP:

Implementar el protocol DHCP per tenir una assignació correcta i automàtica de les adreces IP per cada dispositiu, anar monitoritzant les adreces assignades per evitar conflictes.
Per els conflictes de versió IPv4 o IPv6, implementar configuracions dual-stack (doble pila) per tenir una pila de la xarxa de connexió per cada possible versió i fer compatibles les dues versions a l'hora.

- Assignació dinàmica DHCP:

Verificar la configuració DHCP, reiniciar el servidor si hi ha problemes o assignar manualment adreces estàtiques com a solució temporal.

- Protocol ICMP:

Si no es creen missatges ICMP, pot ser que sigui perquè la configuració del firewall estigui blocant aquest tipus de missatges.

- Problemes d'encaminament amb RIP o OSPF:

Revisar les taules de rutes creades per RIP o OSPF, corregir les rutes si són incorrectes i actualitzar la configuració d'aquests protocols per evitar possibles problemes.

- Subnetting:

Planificar abans i provar la implementació de les subxarxes, usar protocols d'encaminament dinàmics com OSPF, per automàticament ajustar els canvis en la xarxa.
Anar revisant i actualitzant regularment les taules d'encaminament de cada dispositiu.

- Configuració del Router:

Sempre tenir actualitzat el microprogramari (firmware) i programari (software) dels routers i utilitzar protocols per evitar bucles en la xarxa.

- Configuració de Firewalls:

Revisar i verificar regularment les normes implementades en el firewall i en les llistes ACL (Acces Control List) per controlar qui té accés a la xarxa.

- Congestió i caps d'ampolla:

Expandir l'amplada de banda o implementar balanceig de la càrrega de dades quan sigui necessari, optimitzar les rutes per distribuir el tràfic uniformement per la xarxa.
Monitoritzar el tràfic i el rendiment en diversos punts de la xarxa contínuament.

2.4. Capa de Transport

Per cada problema exposat anteriorment, les solucions teòriques proposades són:

- Conflictes en els ports:

Utilitzar protocols dinàmics d'assignació de ports per evitar conflictes i configurar les aplicacions a un únic port quan sigui necessari.

- Congestió i control de flux:

Implementar mecanismes de control dinàmics anar calculant el flux i anar ajustant la freqüència de transmissió de dades depenen de les condicions de la xarxa.
Monitoritzar l'ús del buffer i ajustar la mida segons les dades.
Considerar actualitzar l'amplada de banda (bandwidth) per alleujar la congestió en la xarxa.

- TCP: (Transmission Control Protocol)

Optimitzar els paràmetres TCP com la mida de la finestra, les estratègies de retransmissió o timeouts adaptius, triar protocol UDP si la velocitat de transmissió és clau.

- UDP: (User Datagram Protocol)

Utilitzar protocols a nivell d'aplicació que puguin afegir característiques de fiabilitat sobre l'UDP, triar protocol TCP si la fiabilitat de transmissió és clau.

- Temps d'espera

Ajustar els temps d'espera basant-se en les condicions de la xarxa, utilitzar algorismes de retransmissió adaptius a la xarxa.

- Reordenació dels paquets:

Implementar numeració en seqüència dels paquets de dades per facilitar l'ordenació en arribar a destinació i optimitzar els protocols d'encaminament per reduir la probabilitat de reordenar paquets.

- Establiment i acabament de la connexió:

Assegurar-se de la robustesa de l'inici de sessió en les aplicacions, optimitzar el firewall i la configuració de seguretat per assegurar que no es bloquegen connexions acceptades.
monitoritzar i tancar connexions inactives per alliberar recursos.

- Recuperació d'errors:

Fer servir protocols de detecció i correcció d'errors, com ara TCP, que té funcions de recuperació d'errors integrats.
Monitoritzar el rendiment de la xarxa i trobar possibles patrons d'errors per localitzar el problema.

2.5. Capa de Sessió

Per cada problema exposat anteriorment, les solucions teòriques proposades són:

- Inicialització de la sessió:

Assegurar fiabilitat a la xarxa tenint una correcta configuració a cada dispositiu.
Utilitzar protocols de sessió fiables i implementar mecanismes com el temps d'espera o número de reintents per la inicialització.

- Sincronització de sessions:

Crear punts de control per mantenir la sincronització i estratègies per gestionar els diferents estats de les sessions.

- Finalització de la sessió:

Crear sistemes per automàticament tancar sessions inactives a l'acabar un temporitzador, fent servir senyals de terminació en els protocols de sessió per aconseguir una correcta finalització.

- Autenticació i Autorització:

Implementar protocols d'autenticació robustos com Kerberos, on dos dispositius en una xarxa insegura demostren la seva identitat mútuament de manera segura.
Tenir polítiques estrictes d'accés a la sessió.

- Amenaces en la seguretat:

Utilitzar protocols d'encriptació i tokens per protegir les dades de la sessió, intentar tenir sempre actualitzats els sistemes per assegurar-se que s'arreglen vulnerabilitats en la xarxa conegudes.
Monitoritzar les sessions per veure si hi ha activitat inusual que podria indicar problemes en la seguretat.

2.6. Capa de Presentació

Per cada problema exposat anteriorment, les solucions teòriques proposades són:

- Incompatibilitat de format:

Implementar mecanismes de conversió de formats de les dades o utilitzar formats estandarditzats com XML o JSON.

- Encriptació/Desencriptació de dades:

Regularment, actualitzar i gestionar les claus criptogràfiques usades per mantenir la seguretat i millor utilitzar protocols estandarditzats d'encriptació com les SSL o TLS.

- Compressió i Descompressió:

Tenir algorismes de compressió fiables i que siguin compatibles a través dels diferents sistemes i tenir controls d'errors en els processos de compressió i descompressió.

- Errors de codificació de caràcters:

Implementar un format comú de codificació de caràcters per tota la xarxa i tenir eines de detecció i conversió de caràcters en cada dispositiu.

- Corrupció de dades:

Fer servir els checksums dels paquets per verificar la integritat de les dades i implementar mecanismes de gestió i recuperació d'errors si aquests estan incorrectes.

2.7. Capa d'Aplicació

Per cada problema exposat anteriorment, les solucions teòriques proposades són:

- Protocols HTTP i FTP:

Fer proves fent tests i depurant per qualsevol cas possible els protocols d'aplicació. Intentar estandarditzar els protocols seguint els estàndards de xarxa.

- Certificats SSL, TLS i HTTPS:

Verificar certificats i les configuracions SSL/TLS, sempre tenir actualitzades les llibreries criptogràfiques que s'utilitzin.

- Configuració de SSH:

Verificar les claus i configuracions de SSH, sempre intentar tenir el programari actualitzat .

- Configuració del DNS:

Revisar la configuració DNS, utilitzar altres servidors DNS com a alternatives o consultar la memòria del DNS local.

- Error de l'aplicació:

Reiniciar l'aplicació i el dispositiu, si continua donant error al mateix lloc, avisar als creadors de l'aplicació de l'error perquè ells puguin donar una solució o una actualització de l'aplicació amb l'error solucionat.

- Mesures de seguretat inadequades:

Implementar encriptació i protocols de comunicació segurs com HTTPS, SSL o TLS.

- Rendiment de l’aplicació:

Optimitzar codi i les configuracions del dispositiu per aconseguir un millor rendiment, si es necessita utilitzar mecanismes de distribució de serveis.

- Problemes d'interoperabilitat:

Intentar que el programari sigui compatible per multiplataformes, utilitzant dades i API amb formats estandarditzats i per tenir una integració més fàcil.

- Escalabilitat:

Des de l'inici pensar en la possible escalabilitat de l’aplicació. Implementar serveis cloud (núvol) i una arquitectura per donar suport a una escalabilitat dinàmica de l’aplicació.

- Autenticació i autorització de l’usuari:

Implementar protocols d'autenticació robustos o tenir una autenticació de múltiples factors. Tenir mecanismes de gestió per verificar quins usuaris tenen accés a l’aplicació.

- Integritat i sincronització de dades:

Implementar comprovacions de validació de dades, sistemes de gestió de bases de dades que de propietats ACID (atomicitat, coherència, aïllament i durabilitat).

3. Solucions pràctiques per cada punt problemàtic

Per cada un dels nivells del model OSI, hem exposat els possibles problemes i punts problemàtics en l'inici, establiment i finalització d'una connexió, ara a base de les solucions teòriques podem exposar una o diverses solucions pràctiques.
Si el problema es pot consultar o solucionar a través de la terminal, s'explicarà les instruccions usades escrites amb el color blau, amb una simple descripció de la seva funció, el resultat de la seva execució i una breu descripció del resultat aconseguit.
Si no es pot solucionar a través de la terminal, s'explicarà que es pot fer pel contrari:
Es necessita haver instal·lat dins de Debian net-tools.

3.1. Capa Física

Per cada problema exposat anteriorment, les solucions pràctiques són:

- Danys en els cables i Problema amb els connectors:

Fer una inspecció visual dels cables i connectors per detectar danys físics.

- Interferències elèctriques:

Reubicar físicament els cables en zones sense interferències elèctriques.

- Falles del hardware:

Es pot visualitzar la llista de hardware connectat utilitzant les següents comandes:

lspci: informació detallada sobre els dispositius connectats al sistema

```
root@debian95-INTE-server:~# lspci
00:00.0 Host bridge: Intel Corporation 440FX - 82441FX PMC [Natoma] (rev 02)
00:01.0 ISA bridge: Intel Corporation 82371SB PIIX3 ISA [Natoma/Triton II]
00:01.1 IDE interface: Intel Corporation 82371AB/EB/MB PIIX4 IDE (rev 01)
00:02.0 VGA compatible controller: InnoTek Systemberatung GmbH VirtualBox Graphi
cs Adapter
00:03.0 Ethernet controller: Intel Corporation 82540EM Gigabit Ethernet Controll
er (rev 02)
00:04.0 System peripheral: InnoTek Systemberatung GmbH VirtualBox Guest Service
00:05.0 Multimedia audio controller: Intel Corporation 82801AA AC'97 Audio Contr
oller (rev 01)
00:06.0 USB controller: Apple Inc. KeyLargo/Intrepid USB
00:07.0 Bridge: Intel Corporation 82371AB/EB/MB PIIX4 ACPI (rev 08)
00:0b.0 USB controller: Intel Corporation 82801FB/FBM/FR/FW/FRW (ICH6 Family) US
B2 EHCI Controller
00:0d.0 SATA controller: Intel Corporation 82801HM/HEM (ICH8M/ICH8M-E) SATA Cont
roller [AHCI mode] (rev 02)
```

(Dona la *informació de l'ordinador, la interfície que s'està fent servir (Virtual Box), els ports de Ethernet, d'audio, usb i els diferents controladors del dispositiu*)

dmesg : mostra els missatges de kernel que el dispositiu dona a l'arrencada i en el seu funcionament.
dmesg | grep -i error: filtre de només els missatges d'error del kernel, retornant els errors de maquinari o del sistema.

```
root@debian95-INTE-server:~# dmesg |grep -i error
[    2.934299] EXT4-fs (sda1): re-mounted. Opts: errors=remount-ro
```

(*S'ha trobat un missatge d'error on els fitxers ext4. sda1 i ha errors en l'escriptura o lectura d'aquests, on l'opció per solucionar-ho és fer un remontatge (remount-ro) dels fitxers*)
Si es troben errors en el hardware substituir els components de forma manual.

- Factors ambientals:

Tenir els equips en zones amb sistemes del control climàtic.

- Limitacions de distància:

Instal·lar repetidors o extensors de senyal segons sigui necessari.

3.2. Capa d'Enllaç

Per cada problema exposat anteriorment, les solucions pràctiques són:

- Conflictes amb adreces MAC:

Implementar l'assignació dinàmica amb un servidor DHCP, des de la terminal de Debian es pot veure l'adreça MAC i quina adreça IP té assignada.

ip addr: extreu tota la informació de les adreces del dispositiu

```
root@marionaF (Tue Nov 21):<~># ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:41:ea:92 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 86243sec preferred_lft 86243sec
    inet6 fe80::a00:27ff:fe41:ea92/64 scope link
       valid_lft forever preferred_lft forever
```

(*La adreça MAC del Debian és: 08:00:27:41:EA:92 amb mascara FF:FF:FF:FF:FF:FF:FF*)

- Protocol ARP:

Revisar les taules ARP dels dispositius i modificar les entrades si és necessari.
arp -a: retorna la taula ARP del dispositiu:

```
root@marionaF (Tue Nov 21):<~># arp -a
? (10.0.2.2) at 52:54:00:12:35:02 [ether] on enp0s3
```

(l'adreça ip 10.0.2.2 està associada a l'adreca MAC 52:54:00:12:35:02)

arp -d adreçaIP: instrucció per eliminar una entrada específica de la taula.

- Canvi de bucles:

La informació dels possibles bucles només es poden veure des dels switches de la xarxa.

- Corrupció de Fragmentació:

Implementar mecanismes de detecció d'errors són implementats a nivell de microprogramari dels dispositius de d'emmagatzematge.

- Col·lisió i problemes de broadcast:

Fer que la configuració del sigui de full-duplex i canviar els switches de la xarxa per hubs.
ethtool nominterfice: Mirar la configuració de la interfície del dispositiu:

(*En l'apartat de Duplex podem veure que ja està configurat en FULL que implica que ja té la connexió full-duplex*)

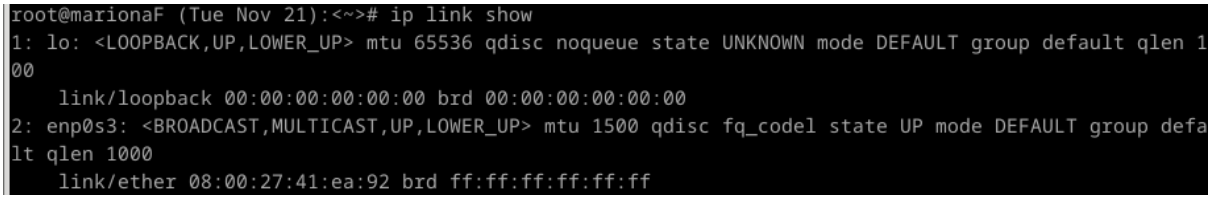
ethtool -s nominterfice duplex full: canvi manual per implementar full duplex

(Després de l'execució d'aquesta instrucció s'haurà implementat la configuració desitjada)

- Configuració incorrecta de la VLAN:

Gestionar la VLAN:

ip link show: veure la informació lligada a la ip on també es pot veure el nom de la VLAN



(*En aquest dispositiu les VLAN configurades son lo (local) i enp0s3*)

També es pot entrar al fitxer de xarxes dins de les interfícies, i observar les xarxes VLAN configurades.

(*En aquest dispositiu hi ha configurada una VLAN dinàmica anomenada enp0s3 i utilitza el protocol DHCP per la seva configuració*)

- Problemes d'enllaç:

La configuració de LACP es realitza en els switches de la xarxa.

3.3. Capa de Xarxa

Per cada problema exposat anteriorment, les solucions pràctiques són:

- Conflictes d'Adreces IP

Implementar el servidor DHCP, es pot veure des del fitxer de la xarxa i aplicar en la interfície que es vol el protocol, en aquest cas el VLAN dinàmica ja utilitza el protocol DHCP per l'assignació adreces IP.

```
iface enp0s3 inet dhcp
```

(*Dins del fitxer /etc/network/interficies es pot configurar els diferents protocols d'assignació d'adreces IP*)

Implementar la configuració dual-stack per fer compatibles les dues versions de IPv4 i IPv6:

ip -6 addr add adreçaIPv6 dev nominterficie: estableix una adreça IP de v6 a la interficie

```
root@marionaF (Tue Nov 21):<~># ip -6 addr add 2001:db8:3333:4444:5555:6666:7777:8888 dev enp0s3
```

(*En la interficie enp0s3 hi haurà dues adreces assignades per cada versió 4 i 6*)

Fent un ip addr es poden veure les dues versions correctament configurades:

```
inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
   valid_lft 71147sec preferred_lft 71147sec
inet6 2001:db8:3333:4444:5555:6666:7777:8888/128 scope global
   valid_lft forever preferred_lft forever
```

- Assignació dinàmica DHCP:

Com hem implementat abans el servidor DHCP, ens hem assegurat una correcta configuració del servidor.

ip addr add adrecaIP dev nominterficie :assignar una adreça IP estàtica:

```
root@marionaF (Tue Nov 21):<~># ip addr add 192.168.1.100/24 dev enp0s3
```

(*Es crea una adreça IP 192.168.1.100 estàtica en la interfície enp0s3*)

- Protocol ICMP

Es pot mirar la configuració del Firewall implementat en el dispositiu, i mirar si no bloqueja els missatges ICMP:

iptables -L: ensenya totes les normes que aplica el Firewall del dispositiu.

```
root@marionaF (Tue Nov 21):<~># iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

(*El nostre dispositiu no té cap norma aplicada, verificant que no tenim cap bloqueig per l'enviament dels missatges ICMP*)

- Problemes d'encaminament amb RIP o OSPF:

Revisar la ruta d'encaminament del dispositiu

ip route show: ensenya la ruta creada per aquest únic dispositiu

```
root@marionaF (Tue Nov 21):<~># ip route show
default via 10.0.2.2 dev enp0s3
10.0.2.0/24 dev enp0s3 proto kernel scope link src 10.0.2.15
```

(*Ens dona la ruta del dispositiu, on exposa que passa per la interficie VLAN enp0s3*)

- Subnetting:

Per la configuració de les subxarxes s'han de fer servir eines específiques per la creació i encaminament d'aquestes.

- Configuració del Router:

Les actualitzacions del microprogramari es realitzen a fora dels dispositius de la xarxa.

- Configuració de Firewalls:

Podem veure la llista ACL de cada usuari i qui hi té accés.
getfacl /user/: mostra els permisos actuals de l'usuari triat

```
root@marionaF (Tue Nov 21):<~># getfacl /root/
getfacl: Removing leading '/' from absolute path names
# file: root/
# owner: root
# group: root
user::rwx
group::---
other::---
```

(Si mirem l'usuari root podrem veure tots els permisos d'aquest, que serà tots els seus directoris)

- Congestió i caps d'ampolla:

Dependrà de l'equip i la configuració de la xarxa.

3.4. Capa de Transport

Per cada problema exposat anteriorment, les solucions pràctiques són:

- Conflictes en els ports:

El conflicte dels ports es gestiona des de la capa d'aplicació, ja que serà aquesta la que assigni manualment o dinàmicament l'ús dels ports.

- Congestió i control de flux:

Dependrà de la configuració i els mecanismes triats per la gestió del flux de dades.
Es pot canviar la mida del buffer del sistema de manera manual.
sysctl -w net.core.rmem_max=número: canvia la mida del buffer segons la mida entrada.

```
root@marionaF (Tue Nov 21):<~># sysctl -w net.ipv4.core.remem_max=524288
```

(El buffer del dispositiu tindrà la mida màxima de 524288 bits)

- TCP: (Transmission Control Protocol)

Es poden ajustar diferents paràmetres del protocol TCP per millorar la seva eficàcia en la xarxa.

sysctl -w net.ipv4.tcp_window_scaling=1: modificació del paràmetre de la finestra del protocol TCP en la versió 4 de adreça IP

```
root@marionaF (Tue Nov 21):<~># sysctl -w net.ipv4.tcp_window_scaling=1
net.ipv4.tcp_window_scaling = 1
```

(Varia la possible escala del protocol TCP, ara s'inicialitzarà a 1 unitat)

- UDP: (User Datagram Protocol)

Si es vol aplicar característiques de fiabilitat en el protocol UDP, s'ha de fer des de la capa d'aplicació.

- Temps d'espera:

Es pot ajustar els temps del protocol TCP de manera manual
sysctl -w net.ipv4.tcp_retries2=15: modifica el nombre de retransmissions que pot fer el dispositiu.

```
root@debian95-INTE-server:~# sysctl -w net.ipv4.tcp_retries2=15
net.ipv4.tcp_retries2 = 15
```

(El nombre de possibles retries s'ha canviat a 15 vegades)

- Reordenació dels paquets:

La implementació de numeració en seqüència dels paquets de dades s'ha de fer en la fragmentació d'aquests.

- Establiment i acabament de la connexió:

Es poden observar les connexions actualment obertes depèn de quins protocols es vulguin mostrar.
netstat -t: ensenya les connexions amb aplicacions o serveis que utilitzen TCP
netstat -tuln: ensenya les connexions amb aplicacions o serveis que utilitzen UDP

```
root@marionaF (Tue Nov 21):<~># netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 10.0.2.15:55636         93.243.107.34.bc.:https ESTABLISHED
tcp        0      0 10.0.2.15:57138         239.237.117.34.bc:https ESTABLISHED
tcp        0      0 10.0.2.15:54638         209.100.149.34.bc:https TIME_WAIT
root@marionaF (Tue Nov 21):<~># netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 0.0.0.0:5353            0.0.0.0:*
udp        0      0 0.0.0.0:68              0.0.0.0:*
udp        0      0 0.0.0.0:43082           0.0.0.0:*
udp6       0      0 :::5353                 :::*
udp6       0      0 :::59075                :::*
```

(Es poden veure les connexions actualment obertes dels protocols TCP i UDP)

- Recuperació d'errors:

Dependrà dels protocols usats de detecció i correcció d'errors, el seu funcionament i les seves característiques per la implementació.

3.5. Capa de Sessió

Per cada problema exposat anteriorment, les solucions pràctiques són:

- Inicialització de la sessió:

Dependrà dels protocols de sessió implementats el seu funcionament i la seva implementació en el sistema.
Dins del dispositiu es poden veure quines aplicacions estan actualment actives
ss -t: llista dels ports actius que estan fent servir aplicacions de protocol tcp

```
root@marionaF (Tue Nov 21):<~># ss -t
State       Recv-Q       Send-Q             Local Address:Port              Peer Address:Port
ESTAB       0            0                     10.0.2.15:55636            34.107.243.93:https
```

(Podem veure que actualment hi ha una aplicació activa sent el navegador d'internet (https))

- Sincronització de sessions:

La sincronització de la sessió estan directament relacionades amb l'aplicació utilitzada i no amb el sistema dins la xarxa.

- Finalització de la sessió:

El tancament de la sessió estan directament relacionades amb l'aplicació utilitzada i quins protocols de finalització de sessió usa.

- Autenticació i Autorització:

Dependrà dels protocols implementats en autenticació i autorització que l'aplicació vol utilitzar.
Des del dispositiu hi ha vàries instruccions per la creació de nous usuaris,eliminar-los o canviar els seus permisos.
useradd // usermod: creació i modificació dels permisos d'usuaris del dispositiu

- Amenaces en la seguretat:

Dependrà dels protocols implementats de seguretat que la xarxa vulgui fer servir.
Tenir sempre els dispositius actualitzats:
apt-get update // apt-get upgrade: actualitza a l'última versió aprovada del sistema Debian.

```
root@marionaF (Tue Nov 21):<~># apt-get update
```

```
root@marionaF (Tue Nov 21):<~># apt-get upgrade
```

(Executant les dues instruccions el dispositiu està actualitzat a l'última versió)

3.6. Capa de Presentació

Per cada problema exposat anteriorment, les solucions pràctiques són:

- Incompatibilitat de format:

La conversió de format de les dades es realitza a dins l'aplicació, usant Json o Xml per tenir formats estàndard de dades.

- Encriptació/Desencriptació de dades:

Dependrà dels estàndards d'encriptació triats el seu funcionament i la seva implementació en el sistema.
Tenint les SSL instal·lades a Debian podem utilitzar-ho.
openssl genrsa -out private.key 2048: genera una nova clau d'encriptació SSL

```
root@marionaF (Tue Nov 21):<~># openssl genrsa -out private.key 2048
```

(Sha generat una nova clau d'encriptació amb el protocol SSL)

- Compressió i Descompressió:

La compressió i descompressió de dades, es pot fer automàticament dins de les aplicacions o manualment
tar -czvf arxiu.tar.gz : comprimeix arxiu tirat
tar -xzvf arxiu.tar.gz: descomprimeix l'arxiu triat

- Errors de codificació de caràcters:

Dependrà de la codificació de caràcters tirada per la xarxa el seu funcionament i la seva implementació en el sistema.

- Corrupció de dades:

A través del checksum de fitxers, es pot veure si les dades d'aquests han estat corrompudes
sha256sum fitxer > fitxer.sha256sum : Crea un checksum del fitxer i el guarda en un fitxer .sha256sum

```
root@marionaF (Tue Nov 21):<~/Documents># sha256sum user_stats.py >user_stats.sha256sum
```

(*Crea el fitxer user_stats.sha256sum on guarda el checksum del fitxer*)

sha256sum -c fitxer.sha256sum: comprova si el checksum es correcte

```
root@marionaF (Tue Nov 21):<~/Documents># sha256sum -c user_stats.sha256sum
user_stats.py: OK
```

(Retorna resultat correcte del checksum creat del fitxer user_stats.py, volen dir que aquestes dades no han estat modificades ni corrompudes)

3.7. Capa d'Aplicació

- Protocols HTTP i FTP:

Dependrà del programari creat de l'aplicació el seu funcionament i la seva implementació en el sistema.

- Certificats SSL, TLS i HTTPS:

Donat que les SSL estan ja instal·lades en Debian, podem connectar-nos de manera segura a aplicacions de manera manual:
openssl s_client -connect dominitriat:numport: crea una connexió segura al domini triat dins del número de port que s'hagi especificat.

```
root@marionaF (Tue Nov 21):<~/Documents># openssl s_client -connect www.google.com:443
CONNECTED(00000003)
depth=2 C = US, O = Google Trust Services LLC, CN = GTS Root R1
verify return:1
depth=1 C = US, O = Google Trust Services LLC, CN = GTS CA 1C3
verify return:1
depth=0 CN = www.google.com
verify return:1
```

(*Sha creat una connexió segura des de google al port 443 del dispositiu*)

- Configuració de SSH:

La configuració de les SSH dependrà de l'ús en l'aplicació i del seu funcionament i la seva implementació en el sistema.

- Configuració del DNS:

Dins del dispositiu podem entrar en el fitxer de la configuració del DNS per veure quin servidor fa servir en la resolució de noms del domini a adreces IP:

```
root@marionaF (Tue Nov 21):<~/Documents># cat /etc/resolv.conf
nameserver 172.20.10.1
```

(*En aquest dispositiu per defecte en la resolució de noms retornarà l'adreca IP 172.20.10.1*)

- Mesures de seguretat inadequades:

Dependrà de les mesures de seguretat triades el seu funcionament i la seva implementació en el sistema.

- Rendiment de l'aplicació:

El rendiment de l'aplicació dependrà del programari fet d'aquesta.
Es Poden mirar els diferents recursos utilitzats del dispositiu i mirar quins usa l'aplicació quan està en funcionament.
top: mostra els recursos en ús actualment.

```
top - 19:32:53 up  5:54,  2 users,  load average: 0.05, 0.05, 0.00
Tasks: 185 total,   1 running, 178 sleeping,   6 stopped,   0 zombie
%Cpu(s):  0.0 us,  0.0 sy,  0.0 ni, 99.9 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :   3913.8 total,   1819.6 free,   1068.7 used,   1272.0 buff/cache
MiB Swap:   2048.0 total,   2048.0 free,      0.0 used.   2845.1 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
    923 root      20   0  408768  33508  25056 S   0.3   0.8   0:34.65 panel-8-pulseau
   3227 root      20   0       0      0      0 I   0.3   0.0   0:02.92 kworker/7:2-events_freezable_powe
   3274 root      20   0       0      0      0 I   0.3   0.0   0:00.60 kworker/5:2-events
```

(Estadístiques del dispositiu basat en les tasques actuals, actives, tancades, "dormint" o "zombie".
Després surt la lista de processos i les columnes de recursos com CPU i Memòria i quan fa servir de cada recurs)

- Problemes d'interoperabilitat:

El disseny de l'aplicació s'ha de crear pensant en la compatibilitat i les possibles plataformes que pot interactuar.

- Escalabilitat:

El disseny de l'aplicació s'ha de crear pensant en la seva escalabilitat i el seu monitoratge es gestiona des de les eines del núvol.

- Autenticació i autorització de l'usuari:

Dependrà de les mesures de seguretat per autenticació i autorització dels usuaris en l'aplicació el seu funcionament i la seva implementació en el sistema.

- Integritat i sincronització de dades:

Dependrà de les bases de dades triades, la seva estructura i controls de sincronització el seu funcionament i la seva implementació en el sistema.
Intentar sempre utilitzar bases de dades conegudes com les SQL per no tenir problemes de compatibilitat entre intercanvis de dades.