↳ Naix ARPA → interconexió ordinadors xarxes telefòniques

↳ Es dissenya una pila de protocols → model TCP/IP rep el nom dels protocols més importants

↳ Primer es dissenya la pila i després es descriu el model al contrari de OSI.

↳ El model de capes estableix que la capa n ofereix serveis a capa n+1, i sols veu els serveis de la capa n-1. La capa n sols es comunica amb la capa n de l'altre sistema remot

↳ La pila de protocols de TCP/IP està formada per 4 capes.

(1) Capa host-red → equival a la capa física + enllaç

↳ Ha de ser capaç de connectar el host a la xarxa per algun protocol que permeti enviar IP

↳ En eixir una nova tecnologia → com enviar IP

(2) Capa de Internet

↳ Encamina els paquets de la forma més convenient.

↳ Dissenys ⇒ Donc servei de Commutació de paquets no orientat a conexió → poden arribar desordenats, i tampoc està garantida la entrega (consistència)

↳ Es defineix un format de paquet i protocol anomenat IP, de forma que aquest nivell el conformen IP, més protocols auxiliars ICMP, ARP, BGP que excepte ARP i RARP els demés fan ús dels datagrames IP.

El datagrama IP té 2 parts la capçalera i el text, actualment ~~està~~ Internet fa ús en un 99% de la versió 4. La versió 6 és la substituta de la versió 4 i en la UV ja hi han alts serveis que estan disponibles per a IPv6.

Dins capçalera podem destacar els següents camps:

- Versió → indica versió v4 o v6
- Serveis diferenciats → sempre per a implementar QOS
- Longitud → longitud del datagrama sencer capçalera + text
  - max 64 kbytes → fragmentar { ruta → no IPv6 / origen → en IPv6
- TTL → Temps de vida → contador regressiu → datagrama flotant.
- Protocol → Protocols de control ICMP → dosti inaccessible
  - ↳ ping
  - ↳ Protocols de resolució d'adreces ~~ARP~~ BOOTP DHCP
  - ↳ Protocols de Routing
- Adreces d'origen i destí
  - 4 bytes IPv4 red / host per mascara
  - 16 bytes IPv6 ~~no triat~~ 8 bytes xarxa 8 bytes host

③ Capa de transport

Ofereix un servei de transport que pot ser orientat a connexió o no orientat a connexió.

ex: no orientat UDP

- No fa control de errors (opcional) ni de flux
- Missatges UPD
- No fa control de flux o congestió
- No retransmet els perduts

↳ Per a multiplexar empra ports (65535 ports)
  ↳ IP + port → socket.
↳ Ex UPD → NFS → control d'errors en capa superior.

Ex. Orientat a connexió TCP i SCTP (emprat en SIP)

TCP
↳ ~~Orientat~~ Fiable → paquets (segments) arriben ordenats i sense errors
↳ Multiplexar → ports. IP + port socket igual que UDP
  ↳ ben coneguts (0-1023)
  ↳ registrats
  ↳ dinàmics → només tenen sentit dins de la connexió establerta
↳ Control d'errors (retransmetre)
↳ Control de flux → ~~Tam~~ Mida de la finestra. Si = 0 → bloqueja emisor
↳ Control de congestió
  ↳ Si hi ha congestió → baixa el ritme → supera xarxa molt pixable i que no té pèrdues.
  ↳ Mecanisme: slow-start (inici lent) → augmenta la tasa de forma exponencial fins que perd un segment.
  → llindar de perill → augmenta linealment
  ↳ Mecanismes més actuals → fast-recovery.
↳ Gestiona intercanvi de dades amb aplicacions
↳ Estableix i tanca connexions. (salutació a 3 vies)
  ↳ Simètrica → o asimètrica

(4) Capa d'aplicació
↳ protocols d'alt nivell → donen serveis a usuaris
  ↳ FTP, http (hi ha que van sobre UDP o TCP)

Xarxes, subxarxes i xarxes virtuals

127.0.0.1

↳ Adreça IP → part host i part xarxa
  ↳ ~~Pri~~ Classificació principal A B C D ↳ multicast i E ↳ reserva
    ↳ estableix quin es host i quin red ↳ xarxa UV (147.156. . .)
També IP privades. →
  ↳ En IPv4 → distingir part host / red → mascara. IPv6 i
  ↳ la mascara 32 bits, no apareix en els paquets IP. cal
    ↳ Tas permet fer subneting, o dividir una xarxa en varies més menudes, de dimensions potencia de 2
    ↳ Sistema sense clases (classless) → no afecta a D i E
    ↳ Al fer subxarxes → camp host a zeros → subred
      ↳ camp host a uns → broadcast.
      ↳ Subnet zero → Conflicte subred i red en ~~broadcast~~ broadcast i adreça subred.

↳ La xarxa més menuda: 30 bits → punt a punt
  ↳ 4 adreces → 2 útils
  ↳ rutes host → sols per a especificar una ruta a un host. (32 bits)

↳ Per contra subxarxes → superxarxes → reduir la taula de rutes dels routers. → CIDR.
  ↳ També s'assignen adreces amb criteris geografics
    ↳ abans sols cronologic
↳ D'aquesta forma → host vol enviar un paquet:
  ↳ Obté la part de xarxa de la IP destí: producte binari
  ↳ Compara la xarxa amb la seua pròpia directament
    ↳ coincideixen → ho envia ~~per eixe iface~~
    ↳ no coincideixen → ho envia per la ruta.

Redes Virtuales

↳ Desde el punto de vista de varias locales VLAN
↳ Desde el punto de vista de conectarse a la xarxa interna VPN

VLANS => Virtual LAN

↳ Equival a partir el conmutador en varis menuts a fin de aumentar el rendimiento (disminuim broadcast) i la seguretat i millorar la gestió.

↳ Varies VLANS → cadascuna construeix el seu Spanning Tree de forma independent.

↳ Habitualment la interconexión entre VLANS diferents es fa mitjançant un router, ~~pero si volem~~ ~~alta opció es unir~~.

↳ Si ~~conectem~~ interconectem 2 conmutadors per un port, sols estarem unint les VLAN's a les que pertanyen eixos ports, de forma que si volem unir varies caldria emprar varis ports.

↳ Una forma d'evitar açò és emprar enllaços Trunk o troncals, per a tal cosa s'etiqueten les trames segons el estandard 802.1Q, el que fa que la trama augmente 4 bytes de tamany. i augmenta els 1500 bytes.

↳ El protocol VTP (VLAN Trunking Protocol) és el que s'empra en aquests casos. → CISCO

Dins de les VLANS podem distingir estàtiques i dinàmiques:

↳ Les VLAN estàtiques definim a quina VLAN pertany

cada client en base a parametres fixos com per exemple el port del commutador.

Les VLAN dinàmiques son els ports dels commutadors que detecten automàticament a quina VLAN pertany el lloc de treball conectat, en base a característiques del equip conectat, com per exemple la MAC adress.

Això ens permetrà moure l'equip de a un altre commutador sense cap problema, com pot ser el cas d'un portatil.

↳ L'altre cas de les xarxes virtuals, son les VPN, que ens permiten connectarnos a la nostra organització des de fóra d'aquesta sense emprar enllaços dedicats.

↳ Es crea un tunell que simula un enllaç punt a pu

VPN's

↳ L'altre tipus de xarxes virtuals → VPN

↳ Permet la extensió de la xarxa local sobre una xarxa pública, o no controlada.

~~↳ Han de proveir~~

↳ Per a que siguen reparers han de proveir mecanismes per a garantir la integritat, autentificació, i confidencialitat

↳ Autentificació ⇒ qui es conecta, i quin accés disposa

↳ Integritat → les dades enviades no estan alterades.

↳ Confidencialitat > Dades xifrades → ~~no~~ ~~interceptades~~

↳ Basicament ∃ 3 arquitectures de conexió VPN

↳ VPN Acces remot ⇒ Permet acces remot a usuaris de l'empresa desde una xarxa pública com per exemple Internet. Es un reemplaç dels ~~les línies telefòniques~~ modems i permet tindre un acces molt similar al que tenen en la xarxa de l'empresa: ie: consultar un catalog que nds es pot veure si estas dins de la xarxa local. ex: VPN de la UV.

↳ VPN Conexió de xarxes a través d'Internet

↳ Per a conectar departaments remots a una seu central. Permet emprar Internet, ie adsl, en compte d'una línea dedicada entre el departament remot i la seu central.

↳ Es poden emprar certs models de routers que ja incorporen les caracteristiques necessaries per a tals conexions.

↳ VPN Interna

↳ Sempre la mateixa LAN de la empresa, i pot servir per a millorar la seguretat de les xarxes WIFI. En el cas de la uveg VPN
 sucum WEP.

↳ Establir VPN ⇒ Crear un canal virtual, anomenat túnel que ens permeta ~~salt~~ oblidarnos de la topologia intermitja de la red.

↳ En el tunel → paquets s'encapsulen sobre ela capçalera del protocol del tunel, i en el destí son desencapsulats

↳ El paquet encapsulat pot ser xifrat d'acord mutu sempre i quan ho soporte el protocol, i a aquest mode s'anomena mode tunel. ~~te~~

↳ El mode transport sols dona xifrat a les dades de nivell superior (i.e: es pot veure origen i destí)

Modo tunel → es xifra tot → capçaleres i dades

Modo transport → es xifra la carrega util

↳ Aquests tunels no tenen per que soportar xifrat, però lo convenient és emprar xifratge ja que accedim a través de xarxes d'acces públic.

↳ Els tunels es poden fer encapsulant dades a diferents nivells.

Nivell 2 → PPTP (M$) no molt segur

L2F → Cisco → sense xifratge

L2PP → IETF → ~~sha de contri~~ no te xifratge ni autentificació

L2TP (cont) -> Combinar amb IPSec.
Layer 2 tunel protocol.

Nivell 3 -> IPSec - Estandard IPv6 adaptat a IPv4
↳ Control d'acces, integritat i confidencialitat
↳ Sols encapsula IP.
↳ Mode tunel o transport

↳ Nivell 7 -> Capa aplicacions
↳ Tunels a nivell aplicació, VPN SSL, emprant un browser https.
↳ No cal configuració per part del client
↳ No hi ha estàndard definit sino que varies implementacions, com per exemple OpenVPN
↳ GPL.

~~a UV empra~~

Com a exemple, els edificis remots que es connecten a la ~~intran~~ xarxa de la UV ~~ho fan~~ mitjançant internet, com per exemple les conexions ADSL de la clínica podològica, ho fan emprant tunels. ~~a tra~~