UTN-FRBA-Dto.Sistemas
Redes de Información

Unidad 6
Redes WAN y protocolo PPP

Fuente: Varias
Versión: 2

1-Redes WAN

- Vinculan redes LAN ubicadas en edificios mediante enlaces punto a punto.
- Mientras las LAN pertenecen a los usuarios, los enlaces WAN pertenecen a los proveedores de servicios.
- La red de acceso incluye el equipamiento del cliente y los enlaces hasta el punto de presencia (POP) más cercano de la red del proveedor.
- La red de transporte (*backbone*) vincula los nodos del proveedor.

Red de acceso

Hay varias técnicas para acceso residencial:

- Cableada: Red telefónica conmutada, ADSL, cablemoden
- Inalámbrica: GPRS, WiFi

Para acceso corporativo hay enlaces dedicados o WiMax.

Red de transporte

Hay tres tipos de routers unidos por enlaces:

- Servidores de acceso remoto (RAS) en los POP con muchos puertos de baja velocidad.
- Router troncales o de backbone con pocos puertos de alta velocidad vinculados a Internet o a otros proveedores.
- Concentradores que unen varios POP hacia los router troncales, con características intermedias.

Acceso residencial por ADSL

Se utiliza la infraestructura basada en PPP.

El enlace entre el abonado y el nodo de acceso del proveedor se realiza mediante un DSLAM (*Digital Subscriber Line Access Multiplexer*) y una WAN ATM.

Se pueden establecer dos variantes entre ambas:

- PVC ATM entre ambas, usando PPP sobre este CV (*PPPoA*).
- intercambiar tramas PPP encapsuladas en tramas Ethernet (*PPPoE*).

2-Protocolo PPP

(*Point to Point Protocol*) aparece en la RFC 1661

-Originado por la necesidad de transmitir Datagramas IP a través de vínculos punto a punto.

PROVEE SERVICIOS DE:

- •Configuración del enlace.
- •Multiplexación de protocolos de red (IPX, IP, etc.)
- •Testeo de la calidad del enlace.
- •Asignación dinámica de direcciones IP.

Su antecesor es el protocolo SLIP (*Serial Link Interface Protocol*)

Componentes

- Un protocolo de encapsulamiento de datagramas sobre enlaces seriales de la familia HDLC.
- Un protocolo de control del enlace:
  - LCP (*Link Control Protocol*)
- Una familia de protocolos de red:
  - NCP (*Network Control Protocol*)

Capa física

Se utilizan enlaces serie de distinto tipo:

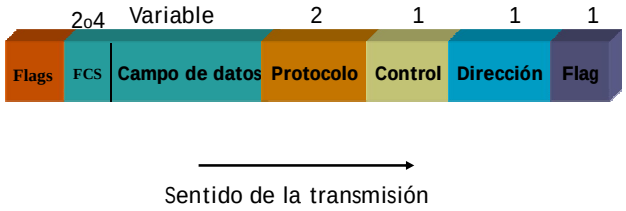
-enlaces RDSI

-enlaces E1/T1

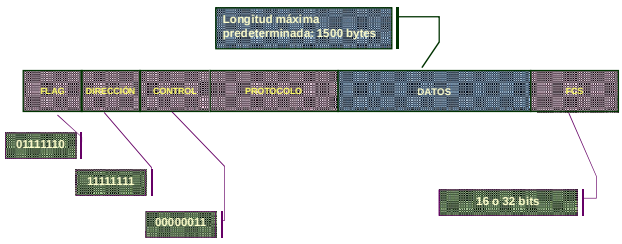
-enlaces SDH

-enlaces de modems sincrónicos o asincrónicos

Trama de capa de enlace



- Utiliza los principios, terminología y estructura de la trama de los procedimientos HDLC de la ISO



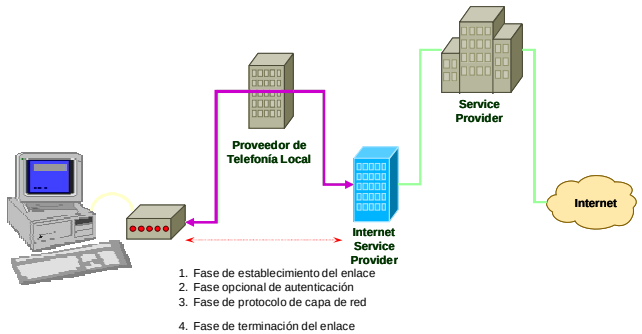
- **Flag** : “01111110”
- **Dirección** : Se utiliza siempre la secuencia binaria “11111111”
- **Control** : Un único byte con la secuencia “00000011” que indica tramas sin numeraciòn.
- **Protocolo** : 2 bytes, identifican el protocolo de nivel 3 que se transporta en el campo de datos. IP, IPX, etc
- **Datos** : Longitud variable de 0 o más bytes, hasta un máximo de 1500
- **FCS** : 16 o 32 bit

Fases de la operación

- Fase de enlace muerto, capa física no lista:
  - Detecta la presencia del dispositivo y/o portadora.
- Fase establecimiento del enlace:
  - Se intercambian tramas LCP para configurar el enlace: MRU (unidad maxima de recepción), etc.
- Fase de validación:
  - Proceso PAP o CHAP.

Conexión por enlace telefónico

Establecimiento



1. Fase de establecimiento del enlace
2. Fase opcional de autenticación
3. Fase de protocolo de capa de red
4. Fase de terminación del enlace

Fases de la operación

- Fase de Red:
  - El protocolo NCP debe configurar el protocolo de red; IP, IPX o AppleTalk.
- Fase abierta de intercambio de datos:
  - Se intercambian paquetes de datos y también LPC y NCP.
- Fase de Terminación del Enlace:
  - Puede ocurrir por:
    - perdida de señal de portadora
    - falla de autenticación
    - baja calidad del enlace
    - expiraciòn de timers
    - cierre administrativo del enlace.

Autenticación

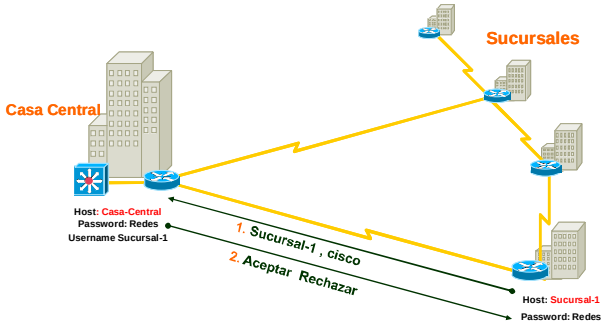
- PPP soporta autenticación PAP y CHAP.
  - PAP: *Password Authentication Protocol.*
  - CHAP: *Challenge Authentication Protocol*.
- El proceso de autenticación se efectúa durante el establecimiento del enlace (LCP).
- No se pasa a la etapa NCP sin haber completado la autenticación.

PAP

- PAP es poco seguro dado que envía la clave en claro conjuntamente con la identificación de la estación cliente.
- Durante el establecimiento de la sesión LCP se negocia dicho protocolo, en caso que el servidor requiera este protocolo.

Autenticación PAP

- Se utiliza sólo en el establecimiento inicial del enlace
  - luego de establecido el enlace, se envía al router el nombre de usuario y la contraseña.
- La contraseña viaja en claro, sin cifrar
- No hay protección ante ataques de prueba y error
  - el nodo remoto controla la frecuencia y la temporización de los intentos de acceso.
- Puede ser aceptable en entornos que cambian la contraseña en cada autenticación.



- Se utiliza en el inicio de un enlace y periódicamente para comprobar la identidad del nodo remoto.
  - ✓ Puede repetirse en cualquier momento posterior al establecimiento del enlace.
  - ✓ Esa comprobación la hace a través de un valor *hash* que se calcula en ambos extermos.
- Hay protección ante ataques de prueba y error
  - ✓ Utiliza un "mensaje" que es variable.

- El servidor CHAP envía un "mensaje" en claro que el cliente cifra con su clave y se lo devuelve cifrado al servidor.
- El servidor realiza el cifrado del mensaje en claro, debiendo coincidir ambos textos cifrados.
- El proceso en ambos casos es hashing.
- Durante el periodo de actividad del enlace se envian frecuentes verificaciones de autenticación.

Challenge / response protocol

- El cliente se comunica con el servidor.
- El server responde con el envio de un "Challenge" (mensaje aleatorio).
- El cliente combina su nombre con el Challenge y lo cifra con su password.
- El resultado de la operación es devuelto al server, quien realiza las mismas operaciones.
- El servidor compara los resultados y si son iguales autentica al cliente.

Ventajas de PPP sobre HDLC

- Es más confiable
- Puede trabajar con diversos enlaces (E1, modems)
- Está bien normalizado por las RFC
- Permite mayor seguridad
- Permite compresión de datos