UTN-FRBA-Dto.Sistemas
Redes de Información

Unidad 5: Protocolos TCP/IP
Clase 3: Aplicaciones

Fuentes: Stallings, cap. 18 y 20
Comer, vol.1 y otras
Versión: 2

1-La capa de aplicaciones

- En el modelo TCP/IP incluye los protocolos que manejan los programas del usuario
- Cada programa tiene dos capas:
  - —Interfaz con el usuario
  - —Manejo de protocolos
- Funciones típicas:
  - —Transferencia de archivos
  - —Correo electrónico

Características de servicios

APLICACIÓN	PERDIDA DE DATOS	ANCHO DE BANDA	SENSIBLE AL RETARDO
Transf.archivos	No tolerable	Elástico	No
Correo	No tolerable	Elástico	No
Navegación web	No tolerable	Elástico	No
Telefonía	Tolerable	<1Mbps	<300 ms
Música	Tolerable	<1Mbps	segundos
Juegos	Tolerable	<10kbps	cientos de ms
Mensajes	No tolerable	Elástico	depende

Protocolos para servicios

APLICACIÓN	PROTOCOLO APLICACION	PROTOCOLO TRANSPORTE
Transf. archivos	FTP	TCP
Correo	SMTP/POP	TCP
Navegación web	HTTP	TCP
Telefonía	SIP	UDP
Música	Propietario	UDP/TCP
Acceso remoto	Telnet	TCP
Ficheros remotos	NFS	UDP/TCP

Clasificación de aplicaciones

- Orientadas a la conexión:
  - — Navegación web
  - — Transferencia de archivos
  - — Correo electrónico
  - — Emulación de terminales
- No orientadas a la conexión:
  - — DNS
  - — DHCP
  - — Telefonía IP

2-Logeo remoto

- Son aplicaciones desarrolladas en la época de terminales ASCII que se debían conectar a un host
- Entre el cliente y el servidor se intercambian caracteres e interaccionan localmente
- **TELNET**: define una NVT (*Network Virtual Terminal) con negoc*ación de los parámetros del enlace
- Cliente y servidor Telnet mapean NVT en cada equipo
- Modo terminal no se adapta a la trasmisión de paquetes por lo que los caracteres de control se tratan como mensajes urgentes de TCP

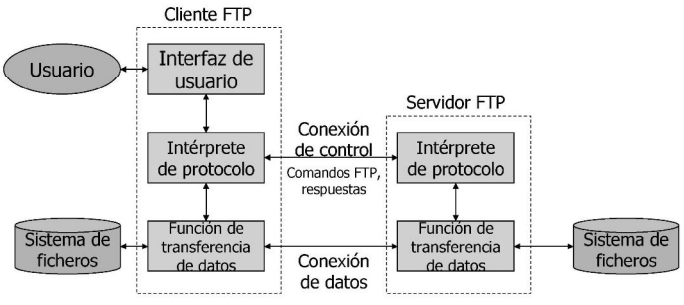
- **RLOGIN** (*Remote Login*): creado específicamente para Unix
- **RSHELL** (rsh): ejecuta comandos en forma remota
- **SECURE REMOTE LOGIN** (ssh): es una alternativa de la capa de transporte con autenticación y encripción
- Permite hacer *port forwarding* de las comunicaciones a través de un túnel, similar a NAT
- ***Remote Desktop***: permite ver pantalla y utiliza teclado y mouse propio para interfaces GUI

3-Transferencia de archivos

- ON LINE FILE SHARING: permite transferir todo o parte en forma opaca o transparente (igual para local o remoto)
- FILE TRANSFER: transfiere archivos completos bajo pedidos del cliente
- FTP (*File Transfer Protocol*) usa TCP con autenticación
- Para transferir los datos hay una inversión de los roles entre cliente y servidor utilizados en el establecimiento de la sesión
- Inicialmente usaban la línea de comandos pero hoy se usan browsers con dos ventanas (directorio local y remoto)
- Para los sitios públicos se usa:
  - usuario: anonymous
  - clave: guest

- PROTOCOLOS DE TRANSFERENCIA SEGURA:
  - SSL-FTP (*Secure Socket Layer*): transferencias confidenciales
  - SFTP (*Secure File Transfer Protocol*): usa un túnel ssh
  - SCP (*Secure Copy*): derivado de Unix, usa túnel
- TFPT (Trivial FTP):
  - Más reducido que FTP
  - Copia archivos enteros
  - Pensado para LAN
  - Usa UDP
  - En ambos extremos necesitan ACK o piden retrasmisión
  - La retrasmisión genera duplicación de paquetes

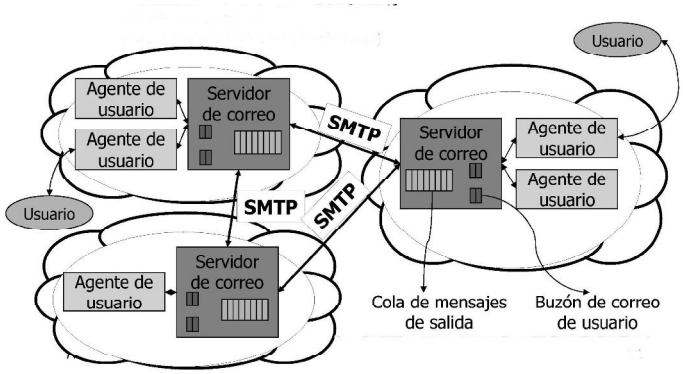
- NFS (*Network File System*):
  - sirve para administrar archivos, no para copiar
  - opera en forma transparente (como si el remoto fuera local)
- RPC (*Remote Procedure Call*)
  - usado para implementar NFS
  - permite representar items de datos de computadoras heterogéneas



4-Correo electrónico

- Es una tarea de segundo plano con dos partes:
  - Interfaz de usuario
  - Transferencia de mensajes
- El destino se identifica por el par:
  usuario@computadora
- Se permite el reenvío
- Mensajes normalizados en RFC 2822 tienen:
  - Encabezamiento con formato *clave: dato*
  - Línea en blanco
  - Cuerpo

- Para trasmisión: SMTP (*Simple Mail Transfer Protocol*)
  - trasmite en ASCII usando TCP
- Para recepción:
  - POP3 (*Post Office Protocol* versión 3)
  - IMAP (*Internet Message Access Protocol*)
- MIME (*Multipurpose Internet mail Extensions*) para transferir información no textual



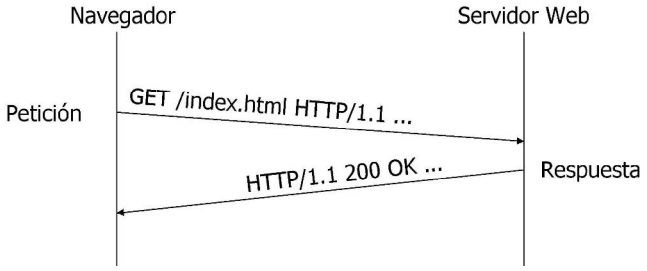
5-Web

- WWW (World Wide Web) es la aplicación principal en Internet desde 1995
- Las páginas se identifican por un URL (*Uniform Resource Locator*) con el formato:
  - http://hostname [:port] / path [; parametros]
- La URI (*Uniform Resource Identifier)* agrega información del contenido de la página (URL es un subconjunto)
- La representación se hace con HTML (*Hyper Text Markup Language*) con texto y enlaces
- Como la norma no da detalles, puede haber diferencias entre la presentación de los distintos browsers

HTTP

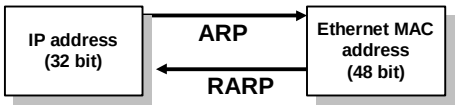
- La transferencia entre el browser y un servidor web se hace con HTTP (*Hyper Text Transfer Protocol*) mediante TCP
- Maneja pedidos y respuestas bidireccionales
- Permite caching e intermediarios
- Maneja mensajes de error en HTML
- Dos versiones: 1.0 (RFC 1946) y 1.1 (RFC 2616)
- Las nuevas versiones trasmiten la longitud en octetos antes de cada pedido indicando que mantienen la sesión abierta después de la respuesta
- Tiene encabezamiento con metainformación para negociar la representación y codificación del documento
- Los encabezamientos son como los de correo

- Browsers pueden ser configurados para contactarse con un proxy y permitir el caching de la organización
- Servidores pueden especificar:
  - Cantidad de proxy
  - Páginas a cachear
  - Tiempo de vida



6-Asignación de direcciones IP

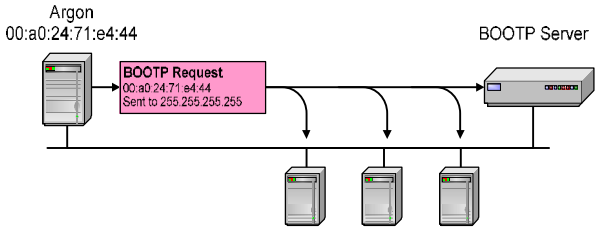
- La asignación de direcciones puede ser:
  - Manual
  - Automática
  - Dinámica (direcciones prestadas por un período)
- La asignación fija se debe hacer máquina por máquina y es engorrosa en redes grandes
- RARP: funciona al revés de ARP (*Reverse ARP*), ya que dada la MAC address consulta por la dirección IP
- Solamente se asigna la dirección IP

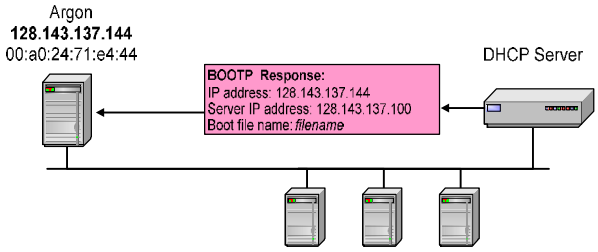


BOOTP

- *Bootstrap Protocol* aparece en 1985
- Los host configuran su IP durante el boot
- BOOTP supera al RARP porque no depende del hardware
- Asigna direcciones IP estáticas, máscara de red y default router
- Se envían en mensajes UDP (puerto 67 para el server y 68 para el host)

Operación



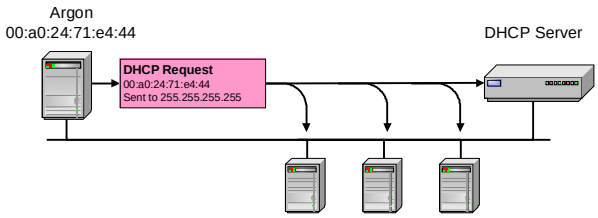


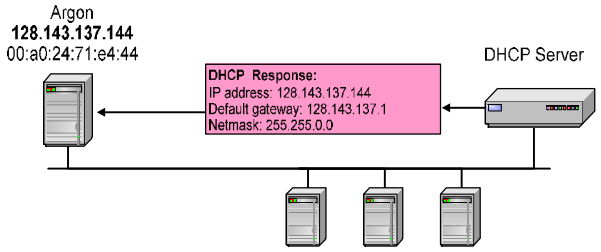
DHCP

- *Dinamic Host Configuration Protocol*
- Similar al BOOT pero lo reemplaza porque usa asignación dinámica de direcciones
- Aparece en 1993, basado en la RFC 1541
- Usa los mismos puertos que BOOT
- Puede interactuar con clientes BOOT
- Cuando arranca usa mensajes broadcast hasta que se asigne una dirección

- DHCP comunica dirección de un servidor y el nombre de un archivo con los datos de configuración que los clientes deben copiar
- En v6 es poco usado el DHCP
  - Se prefiere la autoconfiguración que embebe dirección MAC
  - Hay direcciones locales y globales

Operación





Formato de mensajes BOOT/DHCP

OpCode	Hardware Type	Hardware Address Length	Hop Count
Number of Seconds		Unused (in BOOTP) Flags (in DHCP)	
Transaction ID			
Client IP address			
Your IP address			
Server IP address			
Gateway IP address			
Client hardware address (16 bytes)			
Server host name (64 bytes)			
Boot file name (128 bytes)			
Options			

Campos del mensaje

- code: Indica pedido o respuesta
  - —1 Request
  - —2 Reply
- HWtype: es el tipo de hardware:
  - —1 Ethernet
  - —6 IEEE 802 networks
- length: longitud de dirección de hardware en bytes (en Ethernet son 6)
- hops: el cliente pone un 0, y cada router que repite el mensaje lo incrementa hasta llegar al servidor.

  Si el valor llega a 3 se ha detectado un loop.

- Transaction ID: número aleatorio para aparear pedidos y respuestas
- Seconds: lo pone el cliente, indica el tiempo en segundos desde que empezó el boot
- Flags field: El bit más significante se usa como indicador de broadcast y los otros en cero, reservados para uso futuro.

  La dirección destino en el encabezamiento IP es el DHCP *your IP address* y la MAC address es la DHCP *client hardware address*.

  Si un host es incapaz de recibir un datagrama IP, hasta que no conoza su dirección IP, el bit de broadcast debe ser 1 para indicar al servidor que la respuesta DHCP debe ser enviada como un broadcast de IP y MAC.

- Client IP address: lo pone el cliente (si no lo conoce será 0.0.0.0)
- Your IP address: lo pone el servidor si la dirección IP del cliente fuese 0.0.0.0
- Server IP address: puesto por el servidor
- Router IP address: es la dirección de un repetidor BOOTP, *no* la de un router usado por el cliente. Lo pone el agente de repetición cuando hay BOOTP forwarding
- Client hardware address: lo pone el cliente. DHCP define un identificador de cliente, pero si no se usa esta opción, el cliente se identifica por su dirección MAC

- Server host name: Opcional terminado por X'00'.
- Boot file name: el cliente o lo deja nulo o especifica un nombre genérico, tal como router, indicando el tipo de archivo a usar.

  En un pedido DHCPDISCOVER está en cero.

  El servidor devuelve un path name en la respuesta DHCPOFFER.

  El valor termina en X'00'.
- Options: Subnet Mask, Name Server, Hostname, Domain Name, Forward On/Off, Default IP TTL, Broadcast Address, Static Route, Ethernet Encapsulation, X Window Manager, X Window Font, DHCP Msg Type, DHCP Renewal Time, DHCP Rebinding, Time SMTP-Server, SMTP-Server, Client FQDN, Printer Name, ...

Tipo de mensajes DHCP

- El tipo de mensaje se envía como una opción.

Valor	Tipo de mensaje
1	DHCPDISCOVER
2	DHCPOFFER
3	DHCPREQUEST
4	DHCPDECLINE
5	DHCPACK
6	DHCPNAK
7	DHCPRELEASE
8	DHCPINFORM

- DHCPDISCOVER: es un broadcast de un cliente que busca un servidor DHCP disponible.
- DHCPOFFER: es la respuesta de un servidor a un DHCPDISCOVER que ofrece una dirección IP y otros parámetros.
- DHCPREQUEST: mensaje de un cliente a los servidores que:
  - —Acepta los parámetros ofrecidos por un servido y rechaza las otras ofertas.
  - —Verifica las direcciones previas depués de un reboot.

- DHCPACK: reconocimiento del servidor a un cliente con parámetros, incluyendo dirección IP.
- DHCPNACK: reconocimiento negativo del servidor a un cliente, indicando que la asignación ha expirado o que el pedido es incorrecto.
- DHCPDECLINE: mensaje del cliente al servidor indicando que la dirección ofrecida ya está usada.
- DHCPRELEASE: mensaje del cliente al servidor cancelando la dirección y pidiendo una nueva.
- DHCPINFORM: mensaje del cliente que ya tiene una dirección IP (configurada manualmente), pidiendo más parámetros del servidor DHCP.

7-Resolución de nombres

- Las direcciones IP se reemplazan por nombres de servidores o servicios.
- Resolver un nombre es hallar cuál es su dirección IP.
- Hay varios métodos a utilizar:
  - — NETBIOS
  - — WINS
  - — DNS
- Cada máquina guarda un caché de los nombres que usa frecuentemente.
- Cada vez que se debe resolver un nombre, se consulta al caché y luego al servidor.

NETBIOS

- Protocolo NETBEUI para LAN con máquinas en Windows
- Usa nombres de hasta 15 caracteres
- Permite direccionar hasta 255 máquinas
- Los pares nombre/dirección IP se guardan en el archivo de texto *lmhosts*
- Puede trabajar sobre TCP/IP según RFC 1001/2
- Debe ser transportado
- Provee servicios de sesión

WINS

- Permite trabajar con NETBIOS sobre TCP/IP
- Reduce el tráfico porque no hay broadcast sino consulta al servidor WINS
- Permite una tabla dinámica en entornos con DHCP
- Puede trabajar con DNS en el mismo entorno
- Sirve para hacer compatibles las viejas versiones de Windows

DNS

- *Domain Name System*
- Para facilitar recordar direcciones IP se usan nombres para los dominios
- Los servidores DNS traducen nombres en direcciones IP mediante mensajes en UDP
- La estructura es un árbol jerárquico con dominios delegados
- El cliente pregunta al DNS primario del ISP quien le contesta con la dirección del DNS raíz
- Cada nueva consulta cae en otro DNS hasta resolver
- Los pares nombre/dirección IP se guardan en el archivo de texto *hosts*

- Los DNS tiene cache para recordar consultas frecuentes
- Todos los DNS usan el programa BIND (*Berkeley Internet Name Domain*)
- Las redes medianas deben tener su DNS para agilizar el tráfico a Internet
- DNS usa:
  - —UDP entre cliente y servidor (no es confiable)
  - —TCP entre servidores
- Regido por las RFC 1591, 1034 y 1035

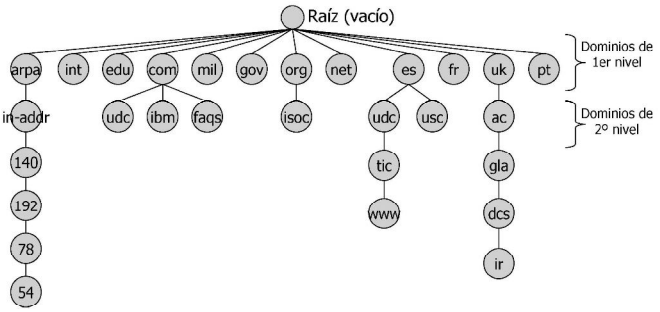
- DNS usa el formato:

  webcampus.sistemas.frba.utn.edu.ar
- Dominios genéricos: .com ; .net ; .org;
- Otros: .edu ; .gov ; .mil
- Cada dominio en cada nivel debe tener una autoridad que asigna los nombres
- En los servidores DNS se registra la correspondencia entre nombres en formato completo y direcciones

- Los clientes usan programas resolvedores de nombres que consultan a los servidores y permiten abreviaturas
- Un host puede manejar varios niveles de nombres
- El root tiene todos los topes de cada nivel
- No se consulta al root sino al servidor más cercano
- Se guardan consultas en un cache con tiempo de vida
- La consulta reversa es poco usada
- Consulta de puntero: averigua el nombre poniendo la dirección invertida como string agregada al nombre del root

Servidores root

- Hay 13 servidores raíz de nombres de dominio (DNS Root Servers) que incluyen la información sobre los nombres de dominio de primer nivel (.com, .org, etc.) y los regionales (.es, .it, etc.).
- Se identifican con letras A/M
- Distribución geográfica:
  - —10 en Estados Unidos
  - — 1 en Suecia
  - — 1 en Inglaterra
  - —1 en Japón.



Administración

- Ante problemas con la resolución de nombres hay varios recursos:
  - —Uso de la utilidad Ipconfig
  - —Uso de la utilidad Ping
  - —Uso de la utilidad Tracert
  - —Uso de la utilidad Nslookup
- Para administrar la resolución de nombres NetBIOS
  - —Uso del comando Net para ver la configuración de la red
  - —Uso del comando Nbtstat para administrar la caché

DNS dinámicos

- Los DNS guardan la dirección IP fija de Internet asignada a cada dominio.
- Si no tiene una dirección IP fija se debe utilizar un servicio de DNS dinámico al cual asociar el dominio (hay algunos gratuitos).
- Cada vez que se conecta al ISP, éste asigna una dirección IP transitoria, y el cliente avisa al DNS dinámico para que actualice este dato en los servidores DNS.

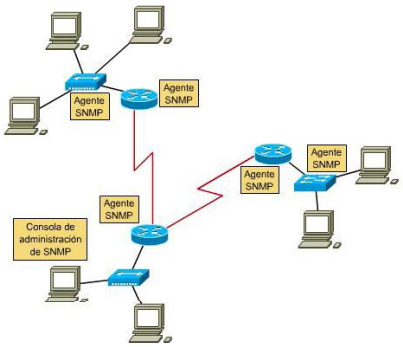
8-SNMP

- *Simple Network Management Protocol*
- La gestión de la red se puede hacer a nivel red o enlace por enlace
- Como Internet agrupa redes heterogéneas la gestión se hace a nivel de aplicación
- La gestión la realiza un software de gestión que corre en la estación de trabajo y envía pedidos a los agentes
- MIB (*Management Information Base*)
  - — Todos los comandos son operaciones sobre variables
  - — La información está dividida en categorías
- SMI (*Structure of Management Information*)
  - — Reglas para definir nombres de variables
  - — Define direcciones y contadores
  - — Usa ASN.1

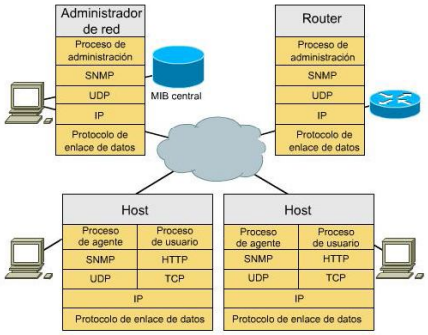
Arquitectura

- La Arquitectura de Administración de Red se compone de cuatro componentes principales:
  - — estación de administración
  - — agente de administración del dispositivo administrado
  - — base de información de administración,
  - — protocolo de administración.
- SNMP facilita la comunicación entre la estación administradora y el agente de un dispositivo de red (o nodo administrado), permitiendo que los agentes transmitan datos estadísticos (*variables*) a través de la red a la estación de administración.

Agentes SNMP



Componentes de la arquitectura



Funcionamiento

Sondeo: (forma normal de uso):

- **Pregunta**: la estación administradora envía una solicitud a un agente pidiéndole información o mandándole actualizar su estado de cierta manera.
- **Respuesta**: la información recibida del agente es la respuesta o la confirmación a la acción solicitada.

El problema del sondeo que se incrementa con los nodos administrados y en ocasiones puede llegar a perjudicar el rendimiento de la red.

Interrupción *(trap)*: un agente manda la información al nodo administrador puntualmente, ante una situación predeterminada (una anomalía detectada en la red, etc.)

Protocolos

- SNMP es independiente del protocolo (IPX de SPX/IPX de Novell, IP con UDP)
- SNMP se puede implementar usando comunicaciones UDP o TCP
- Se usa comunicaciones UDP en la mayoría de los casos.
- Con UDP, el protocolo SNMP se implementa utilizando los puertos:
  - 161: se utiliza para las transmisiones normales de comando SNMP
  - 162: se utiliza para los mensajes de tipo “trap” o interrupción.

9-Aplicaciones de voz y video

- Protocolos diseñados para datos pueden transportar aplicaciones de tiempo real como voz y video
- Estas señales analógicas se convierten en digitales y viceversa mediante un circuito CODEC
- Señales usan codificación PCM
- Como el tráfico en Internet es en ráfagas, se usan:
  - buffers que se descargan a velocidad fija
  - protocolos especiales
  - marcas de tiempo en los paquetes de datos
- RTP (*Real Time Transport*)
  - provee marcas de tiempo y número de secuencia
  - no es protocolo de transporte sino de aplicación sobre UDP
  - Combina hasta 15 fuentes de voz y video

- RTCP (*RTP Control Protocol*)
  - Parte de RTP
  - Coordina sesiones entre Tx y Rx enviando informes
  - Utiliza número de port para separar señales
- VoIP (Voz sobre IP)
  - Usa RTP para manejar las señales
  - Necesita un protocolo para la señalización telefónica (H.323, SIP)
  - Mediante un gateway se conecta a la Red Telefónica Pública, que usa la señalización SS7
- Protocolo H.323
  - Normalizado por la ITU
  - Es una serie de protocolos que manejan las distintas funciones
  - Algunos operan sobre TCP y otros sobre UDP

- SIP (*Sesion Initiation Protocol*)
  - Normalizado por el IETF
  - Más reducido que H.323
  - No usa RTP
- SDP (*Sesion Description Protocol*)
  - Acompaña al SIP
  - Se encarga de la codificación y direccionamiento

- QoS (*Quality of Service*)
  - Es una garantía estadística del funcionamiento
  - Requiere cambios en los protocolos
- RSVP (*Resource reSerVation Protocol*)
  - Normalizado por IETF como alternativa a ATM
  - Provee QoS en una o ambas direcciones, pero necesita otro protocolo para el tráfico, tal como COPS (*Common Open Policy Service*)