# Protocolos

Protocolos de red y protocolos de aplicación

# En esta presentación…

- Protocolos de Aplicación.
  - Son los que usan las aplicaciones para enviar los datos.
- Protocolos de Transporte.
  - Encapsulan los datos de las aplicaciones para que puedan trasportarse por una red de computadores.
- Herramientas de diagnóstico de red.
  - Nos permiten saber si algo falla o funciona bien o ayudarnos a encontrar soluciones a problemas de conectividad.

# Protocolos de Aplicación

# Protocolo HTTP

- *HyperText Transfer Protocol.*
- Inventado junto con HTML en los orígenes de la World Wide Web
- Transmite hipertextos: textos que contienen enlaces a otros textos
  - Este concepto hoy se extiende a todo tipo de contenidos web.
- Los enlaces de llaman hipervínculos (hyperlinks).
- Su puerto predeterminado es el tcp/80.

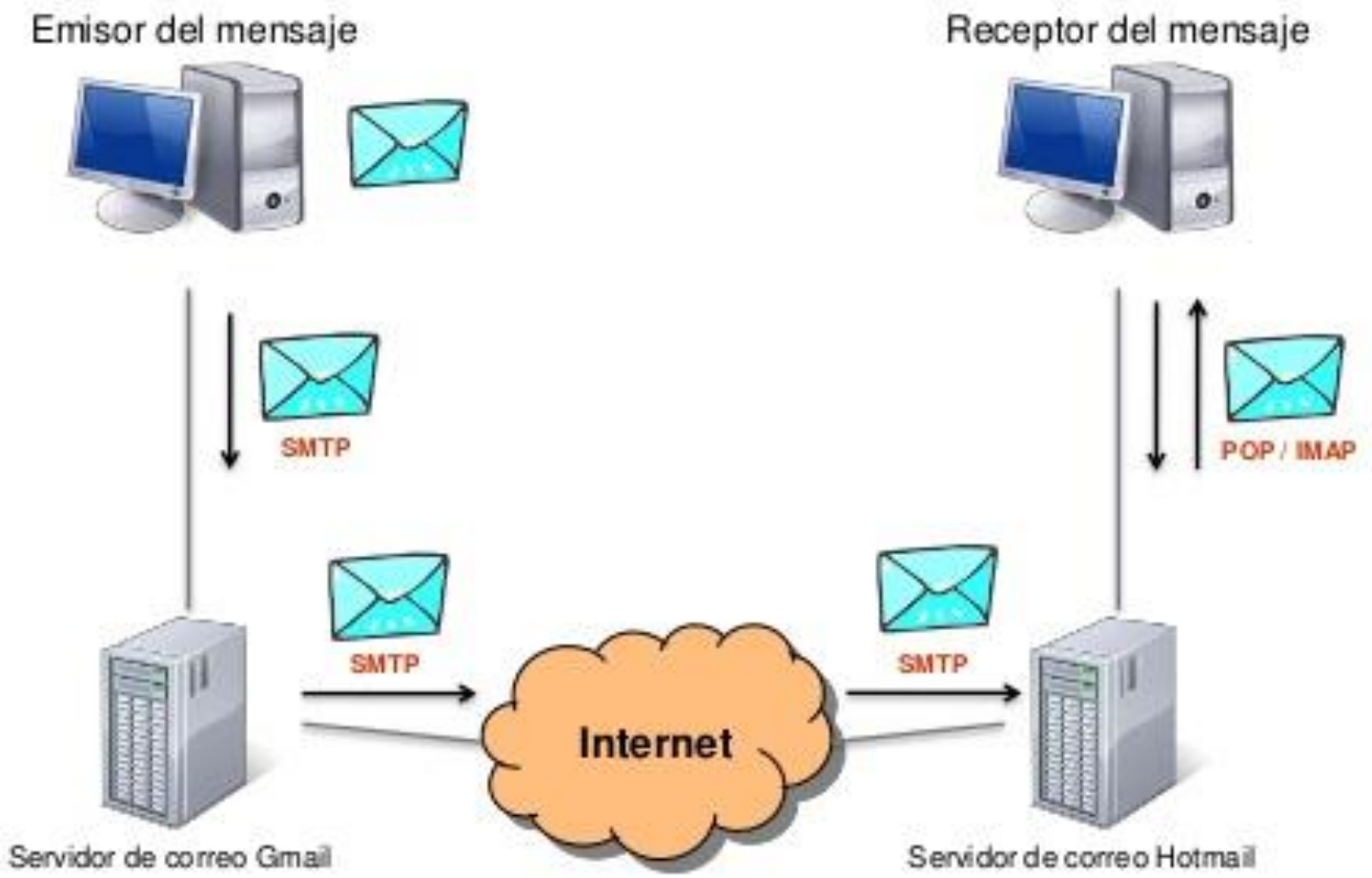
# Protocolo HTTPS

- Es la versión segura de HTTP.
- Requiere de la implementación de certificados digitales en el servidor.
- Cifra la información que el cliente y el servidor intercambian.
- Originalmente poco usado por generar carga de trabajo en los equipos. Hoy es un estándar de la industria y se lo prefiere sobre HTTP siempre que sea posible su implementación.
- Su puerto predeterminado es el tcp/443.

# Protocolo SMTP

- *Simple Mail Transport Protocol.*
- Protocolo de comunicación para envío de correos.
- Utilizado por los servidores de correo para comunicarse entre ellos.
- Se complementa con otros servicios (POP, IMAP, webmail) para que los usuarios puedan acceder a leer sus correos.
- Su puerto predeterminado es el tcp/25. En algunas circunstancias se usan los puertos tcp/587 (autenticación de clientes) y tcp/465 (SMTP-S).

# Envío de un Correo Electrónico en Internet



# Protocolo FTP

- *File Transfer Protocol.*
- Protocolo cliente-servidor para transferencia de archivos.
- Su implementación básica prioriza la velocidad de transferencia por sobre la seguridad de los datos que se transfieren.
- Alternativas seguras: SFTP (SSH) , FTP-S (TLS).
- Su puerto predeterminado es el tcp/21.
  - Pero utiliza el puerto tcp/20 para transferir los datos en modo activo.
  - O puertos altos en modo pasivo.

# Protocolo FTP

- Puede trabajar en modo activo (PORT) o pasivo (PASV)
  - En ambos casos el puerto en el que el servidor “escucha” es el 21. Lo que cambia es la manera en que se definirán los puertos de transferencia.
- El modo pasivo permite fijar los puertos por los que se transfieren los datos. Es el que se debe utilizar cuando hay dispositivos de red como routers o firewalls entre el cliente y el servidor.

# TCP y UDP

Protocolos de transporte

# Definición

- TCP = Transmission Control Protocol
- UDP  = User Datagram Protocol

- Son los protocolos de Internet más ampliamente usados para transportar datos.

- Encapsulan los datos generados por las aplicaciones para transferirlos entre dispositivos.

# Diferencias

- TCP: Es un protocolo de comunicación en donde los datos se transmiten entre nodos de una red. Los datos se transmiten en forma de paquetes. La transmisión incluye verificación de errores, garantiza la entrega del paquete y preserva el orden de los paquetes.

- UDP: Es también un protocolo de comunicación, excepto que no garantiza la verificación de errores y reenvío de paquetes y recuperación de errores. Si se usa UDP, los datos se mandan en forma continua, sin importar los problemas que se encuentren en la parte receptora.

# Diseño

- TCP: Protocolo orientado a conexión.
- UDP: Protocolo sin control de conexión.

# Transmisión de datos

- TCP: Los datos se transmiten en una secuencia específica. Cuando llegan a destino se reordenan. Si faltan, se vuelven a pedir.
- UDP: NO hay secuenciamiento de datos en UDP. Los paquetes pueden llegar en un orden diferente al generado.

# Desempeño

- TCP: Es más lento, dado que tiene mayores controles y verificaciones por cada paquete.
- UDP: Al no existir verificación ni control de paquetes, ni bidireccionalidad, se desempeña en forma mas rápida que TCP.

# Retransmisión

- TCP: Es posible la retransmisión de paquetes perdidos en caso de ser necesario.
- UDP: No es posible la retransmisión de paquetes que se pierdan.

# Uso por parte de protocolos de Aplicación

- TCP: HTTP, SMTP, POP, IMAP, FTP y otros.
- UDP: Video conferencia, streaming, DNS, DHCP, VoIP, y otros.

# Acerca de los puertos TCP / UDP

- Puerto 0 a 1023: estos números de puerto TCP / UDP se consideran puertos conocidos. Estos puertos son asignados a un servicio de servidor específico por la Autoridad de Números Asignados de Internet (IANA). Por ejemplo, los servidores web utilizan el puerto tcp/80 para HTTP y tcp/443 para HTTPS.
- Puerto 1024 a 49151: estos son puertos que una organización, como los desarrolladores de aplicaciones, puede registrar en IANA para utilizarlos en un servicio en particular. Estos deben tratarse como semi-reservados.
- Puerto 49152 a 65535: estos son los números de puerto que utilizan los programas cliente, como un navegador web. Cuando visita un sitio web, su navegador web asignará a esa sesión un número de puerto dentro de este rango. Como desarrollador de aplicaciones, puede utilizar cualquiera de estos puertos.

# Analogía

- Imagínate un edificio de apartamentos:
  - La numeración de la puerta es el análogo a la dirección IP.
  - El número de apartamento es el análogo al número de puerto.
- Si tu le envías una carta a alguien en un edificio, necesitas saber tanto la dirección de la puerta como el número de apartamento.
- Dos servicios diferentes no se pueden brindar en el mismo puerto.

# Herramientas de Diagnóstico de Red

# IPCONFIG

- Herramienta para ver la configuración básica de la red en un equipo
- Se ejecuta desde una línea de comandos (cmd o PowerShell)
- Puede ejecutarse con el modificador /all para que muestre información adicional
- https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/ipconfig
- En Linux y macOS el nombre de la herramienta es ifconfig.

# PING

- Herramienta de diagnóstico de conectividad en una red
- Permite verificar si otro equipo está disponible
  - Importante: Algunos equipos no responden a este comando.
- Permite verificar si el equipo propio tiene una configuración de red correcta:
  - Ping localhost (127.0.0.1): tarjeta de red y el protocolo responden correctamente
  - Ping IP del equipo: dirección IP se inició correctamente
  - Ping IP del router: hay conexión con otros equipos de mi red
  - Ping IP de un equipo remoto: hay conexión con otras redes
- Utiliza el protocolo ICMP (protocolo de red)

# Usar PING

```
C:\>ping www.ort.edu.uy

Haciendo ping a cie.ort.edu.uy [164.73.96.20] con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 164.73.96.20:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos),

C:\>ping www.google.com.uy

Haciendo ping a www.google.com.uy [172.217.172.67] con 32 bytes de datos:
Respuesta desde 172.217.172.67: bytes=32 tiempo=17ms TTL=115
Respuesta desde 172.217.172.67: bytes=32 tiempo=19ms TTL=115
Respuesta desde 172.217.172.67: bytes=32 tiempo=18ms TTL=115
Respuesta desde 172.217.172.67: bytes=32 tiempo=18ms TTL=115

Estadísticas de ping para 172.217.172.67:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 17ms, Máximo = 19ms, Media = 18ms

C:\>
```

https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/ping

# TRACERT/PATHPING

**Comandos que permiten diagnosticar la conexión a un equipo remoto verificando los pasos intermedios que ocurren entre un equipo y otro.**

```
C:\>tracert www.google.com

Traza a la dirección www.google.com [172.217.172.36]
sobre un máximo de 30 saltos:

  1     4 ms     2 ms     2 ms  192.168.252.1
  2     7 ms     7 ms     7 ms  rtia2bras1.antel.net.uy [200.40.78.196]
  3     5 ms     7 ms     5 ms  ibb2agu4-0-3-0-1.antel.net.uy [200.40.78.18]
  4     7 ms     7 ms     6 ms  ibe2tia1-0-6-0-0.antel.net.uy [179.31.59.252]
  5    18 ms    17 ms    17 ms  ibe2mln1-be20.antel.net.uy [179.31.62.85]
  6    16 ms    15 ms    16 ms  crton1.eze-ae1003.antel.net.uy [179.31.62.103]
  7    20 ms    14 ms    16 ms  72.14.216.159
  8    15 ms    16 ms    17 ms  72.14.216.158
  9    18 ms    18 ms    19 ms  172.253.53.33
 10    18 ms    16 ms    17 ms  142.250.62.31
 11    17 ms    18 ms    14 ms  eze06s05-in-f4.1e100.net [172.217.172.36]

Traza completa.
```

```
C:\>pathping www.google.com

Seguimiento de ruta a www.google.com [172.217.172.36]
sobre un máximo de 30 saltos:
  0  [redacted] [192.168.252.171]
  1  192.168.252.1
  2  rtia2bras1.antel.net.uy [200.40.78.196]
  3  ibb2agu4-0-3-0-1.antel.net.uy [200.40.78.18]
  4  ibe2tia1-0-6-0-0.antel.net.uy [179.31.59.252]
  5  ibe2mln1-be20.antel.net.uy [179.31.62.85]
  6  crton1.eze-ae1003.antel.net.uy [179.31.62.103]
  7  72.14.216.159
  8  72.14.216.158
  9  172.253.53.33
 10  142.250.62.31
 11  eze06s05-in-f4.1e100.net [172.217.172.36]

Procesamiento de estadísticas durante 275 segundos...
           Origen hasta aquí    Este Nodo/Vínculo
Salto  RTT    Perdido/Enviado = Pct  Perdido/Enviado = Pct  Dirección
  0                                                [redacted] [192.168.252.171]
                                0/ 100 =  0%   |
  1    2ms     0/ 100 =  0%     0/ 100 =  0%  192.168.252.1
                                0/ 100 =  0%   |
  2    6ms     0/ 100 =  0%     0/ 100 =  0%  rtia2bras1.antel.net.uy [200.40.78.196]
                                0/ 100 =  0%   |
  3    6ms     0/ 100 =  0%     0/ 100 =  0%  ibb2agu4-0-3-0-1.antel.net.uy [200.40.78.18]
                                0/ 100 =  0%   |
  4    6ms     0/ 100 =  0%     0/ 100 =  0%  ibe2tia1-0-6-0-0.antel.net.uy [179.31.59.252]
                                0/ 100 =  0%   |
  5   ---     100/ 100 =100%   100/ 100 =100%  ibe2mln1-be20.antel.net.uy [179.31.62.85]
                                0/ 100 =  0%   |
  6   ---     100/ 100 =100%   100/ 100 =100%  crton1.eze-ae1003.antel.net.uy [179.31.62.103]
                                0/ 100 =  0%   |
  7   25ms     0/ 100 =  0%     0/ 100 =  0%  72.14.216.159
                                0/ 100 =  0%   |
  8   17ms     0/ 100 =  0%     0/ 100 =  0%  72.14.216.158
                                0/ 100 =  0%   |
  9   18ms     0/ 100 =  0%     0/ 100 =  0%  172.253.53.33
                                0/ 100 =  0%   |
 10   17ms     0/ 100 =  0%     0/ 100 =  0%  142.250.62.31
                                0/ 100 =  0%   |
 11   18ms     0/ 100 =  0%     0/ 100 =  0%  eze06s05-in-f4.1e100.net [172.217.172.36]

Traza completa.
```

Tracert está disponible en Linux y macOS como “traceroute”. Pathping está solo disponible en Windows.

# TRACERT/PATHPING

**tracert**

- Herramienta de línea de comando que puede ser usada para trazar la ruta que un paquete IP toma para llegar a su destino.
- Ayuda a encontrar la ruta exacta que un paquete usa para llegar a su destino.

**pathping**

- Herramienta de línea de comando que combina la funcionalidad de ping con tracert.
- Ayuda a localizar puntos en la red que presentan latencia y pérdidas.

# TELNET

- Herramienta de diagnóstico de disponibilidad y funcionamiento de un servicio
  - Acceso en modo CLI o terminal para ejecutar comandos específicos de cada servicio. Suele restringirse por razones de seguridad.
  - Se suele utilizar para verificar que un servicio está disponible en un equipo. Para esto es necesario conocer el puerto del servicio.
- Sirve para puertos TCP.
- Utiliza el puerto tcp/23.

```
S: 220 Servidor SMTP
C: HELO miequipo.midominio.com
S: 250 Hello, please to meet you
C: MAIL FROM: <yo@midominio.com>
S: 250 Ok
C: RCPT TO: <destinatario@sudominio.com>
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: Subject: Campo de asunto
C: From: yo@midominio.com
C: To: destinatario@sudominio.com
C:
C: Hola,
C: Esto es una prueba.
C: Hasta luego.
C:
C: .
C: <CR><LF>.<CR><LF>
S: 250 Ok: queued as 12345
C: quit
S: 221 Bye
```

# NSLOOKUP

- Herramienta de diagnóstico de infraestructuras DNS.
- Dado un equipo o un dominio de Internet, las herramientas de diagnóstico de DNS permiten verificar que la resolución de nombres sea correcta.
- Utilizan los puertos de DNS (tcp y udp/53).

```
C:\>nslookup
Servidor predeterminado:  ns3.antel.net.uy
Address:  200.40.30.245

> set q=all
> www.ort.edu.uy
Servidor:  ns3.antel.net.uy
Address:  200.40.30.245

Respuesta no autoritativa:
www.ort.edu.uy  canonical name = cie.ort.edu.uy

ort.edu.uy      nameserver = uni.ort.edu.uy
ort.edu.uy      nameserver = ns1.ort.edu.uy
ns1.ort.edu.uy  internet address = 164.73.96.19
uni.ort.edu.uy  internet address = 164.73.96.38
> exit

C:\>
```