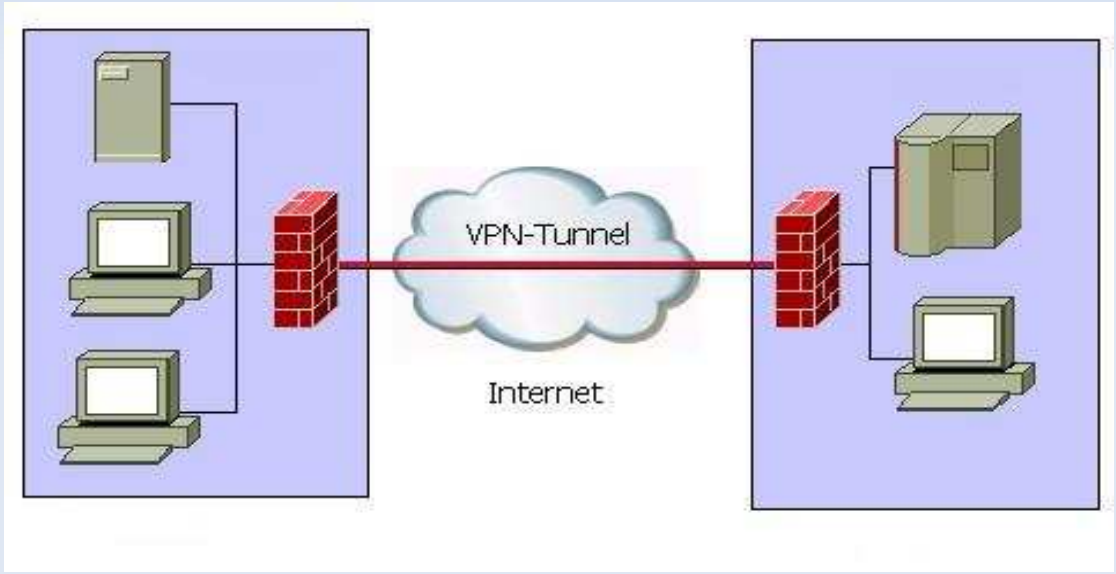
Virtual Private Network

Liliana Castillo Devoto
Aldo Lovera Raffo

Ingeniería de Telecomunicaciones - GST

¿Qué es una VPN?

- Es un sistema para simular una red privada sobre una red pública.

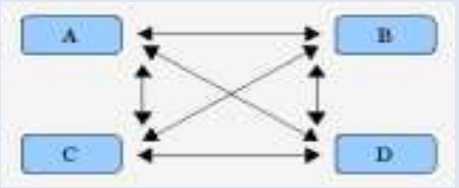


Surgimiento de las VPNs

- Intercambio flexible y rápido de información.
- Sucursales en diferentes ubicaciones.
- Trabajadores remotos.
- Necesidad de altos estándares de seguridad: autenticidad, integridad, y disponibilidad.

Posibles soluciones

- Módem:
  - Costo de llamada por minuto conectado
  - Equivalente a llamada de larga distancia
  - Calidad pobre y baja velocidad
- Líneas dedicadas:
  - Se necesitan conexiones físicas reale
  - Costo muy alto

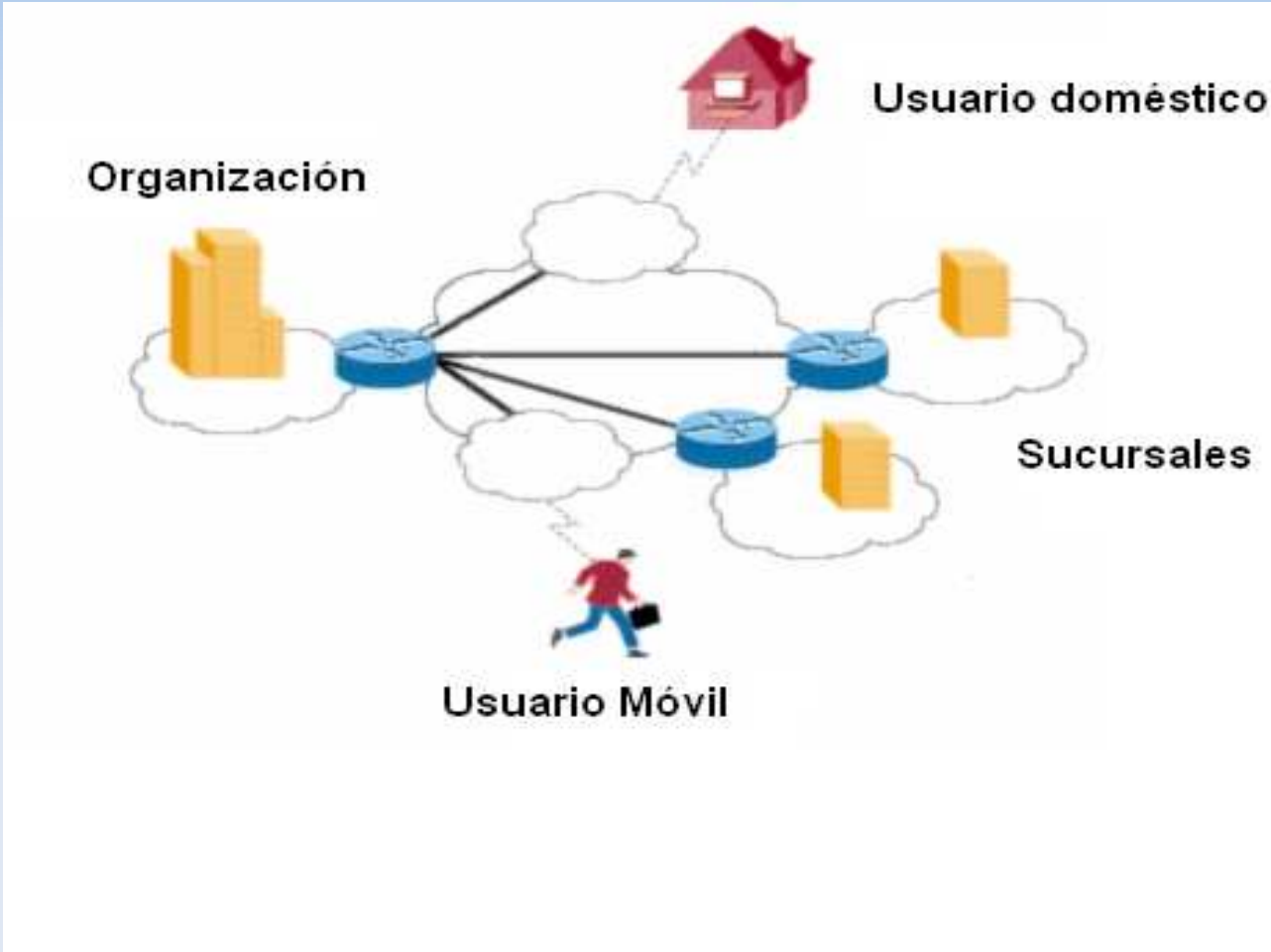


- VPN:
  - Solo requiere conexión a Internet → Costo bajo
  - Virtual, privado y seguro.
  - Buena calidad y velocidad

Arquitecturas Básicas

- Acceso Remoto:
  - Usuarios que se conectan de manera remota (domicilios, hoteles, cafés..) utilizando Internet como vía de acceso.
- Punto a Punto:
  - Conexión entre diversos puntos de una organización a través de Internet.
- Interna VLAN:
  - Utiliza la LAN de la organización como vía de acceso.
  - Sirve para aislar zonas y servicios de la red interna

Arquitecturas Básicas



Implementación

- Capa de Enlace:
  - Permite transferencia sobre protocolos no-IP
  - PPTP, L2F, L2T, L2Sec
- Capa de Red:
  - Solo trabaja con protocolo IP
  - IPsec: ESTANDARD
- Capa de Aplicación:
  - Se accede a través de un browser
  - Seguridad es lograda a través de mecanismos SSL/TLS

GST

Seguridad VPN

- Cifrado Simétrico y clave pre-compartida:

Seguridad VPN

- Cifrado Asimétrico

Protocolo SSL

- Encriptación:
  - Datos intercambiados son cifrados simétricamente usando una llave de sesión
  - La llave de sesión es intercambiada con cifrado asimétrico (RSA)
- Autenticación:
  - Autoridad Certificante (CA) que entrega una firma digital
- Integridad:
  - Basta que un carácter cambie en el mensaje enviado para que sea inválido en el servidor

GST

OpenVPN

- Creado por James Yonan en el año 2001
- Implementa conexiones de capa 2 ó 3
- Utiliza el protocolo SSL/TLS
- Las interfaces virtuales permiten la implementación de reglas de firewall muy específicas
- Se pueden usar IPs dinámicas a cada lado del túnel (no hay problema con NAT)
- Instalación y uso sencillo

GST

OpenVPN

- Un único puerto TCP o UDP
- Se puede ejecutar en espacio de usuario
- Todo concepto de reglas, restricciones, reenvío y NAT pueden ser usados
- Configuración escalable
- Multiplataforma
- Velocidad (más de 20 Mbps en máquinas de 1Ghz)
- Compatibilidad con firewall y proxies

Comparación entre OpenVPN e IPsec VPN

IPsec	OpenVPN
Estándar	Aun desconocida (no compatible con IPsec
En diferentes HW	Solo en computadoras
Interfaz gráfica	Sin interfaz gráfica
Modificaciones al Kernel	Interfaces Virtuales
Tecnología compleja	Facilidad de configuración y uso
Muchos puertos	Un solo puerto
Problema con direcciones dinámicas	Soporte transparente para IPs dinámicas
Problemas de seguridad	SSL/TLC

OpenVPN

- Paquetes
  - OpenVPN (versión 2)
  - OpenSSL
  - LZO
  - Controlador TUN/TAP (2.4.7)
  - bridge-utils
- Instalación OpenVPN
  - *sudo apt-get install openvpn*
  - *cp -R /usr/share/doc/openvpn/examples/ /etc/openvpn/*

OpenVPN: Seguridad

- Static Key: La llave es generada y compartida a ambos hosts antes de que se establezca el túnel.
  - ***openvpn --genkey --secret static.key***
- TLS: Método más seguro (certificados y llaves RSA)
  1. Generamos certificado CA maestro.
     - cd /etc/openvpn/easy-rsa
     - . ./vars
     - ./clean-all
     - ./build-ca (¡¡Common Name!!)
     - ./build-dh (parámetros Diffie-Hellman)
     - Archivos: **ca.crt, ca.key, dh1024.pem**

OpenVPN: Seguridad

2. Generamos certificado y llave del servidor.
   - ./build-key-server servidor (CN=servidor)
   - Archivos: **servidor.crt, servidor.key**
3. Generamos certificado y llave del cliente.
   - ./build-key cliente1 (CN=cliente1)
   - Archivos: **cliente1.crt, cliente1.key**
4. Copiamos los archivos a los equipos correspondientes:
   - Servidor: **ca.crt, ca.key, dh1024.pem, servidor.crt, servidor.key**
   - Cliente: **ca.crt, cliente1.crt, cliente1.key**

GST

OpenVPN: Seguridad

- Otra opción: Cliente genera su propia llave y envía un Certificate Signing Request (CSR) al equipo firmador, obteniendo su certificado firmado. El archivo secreto *.key no saldrá del equipo que lo generó.
- CA es el mismo Servidor en la mayoría de casos.

OpenVPN: Configuración

- local: IP que OpenVPN debe escuchar
- port: puerto para las conexiones (1194 puerto oficial)
- proto: udp o tcp
- dev: tun o tap
- ca: certificado CA
- cert: certificado del servidor/cliente
- key: llave del servidor/cliente
- dh: parámetros Diffie–Hellman

GST

OpenVPN: Configuración

- server: modo servidor y subred VPN
- server-bridge: Bridged VPN.
- push: agrega rutas al cliente luego de la conexión.
- client-config-dir: directorio para configuración por cliente (**iruote**)
- route: enrutamiento del kernel al servidor
- client : modo cliente
- remote: IP pública del servidor y puert

OpenVPN: Configuración

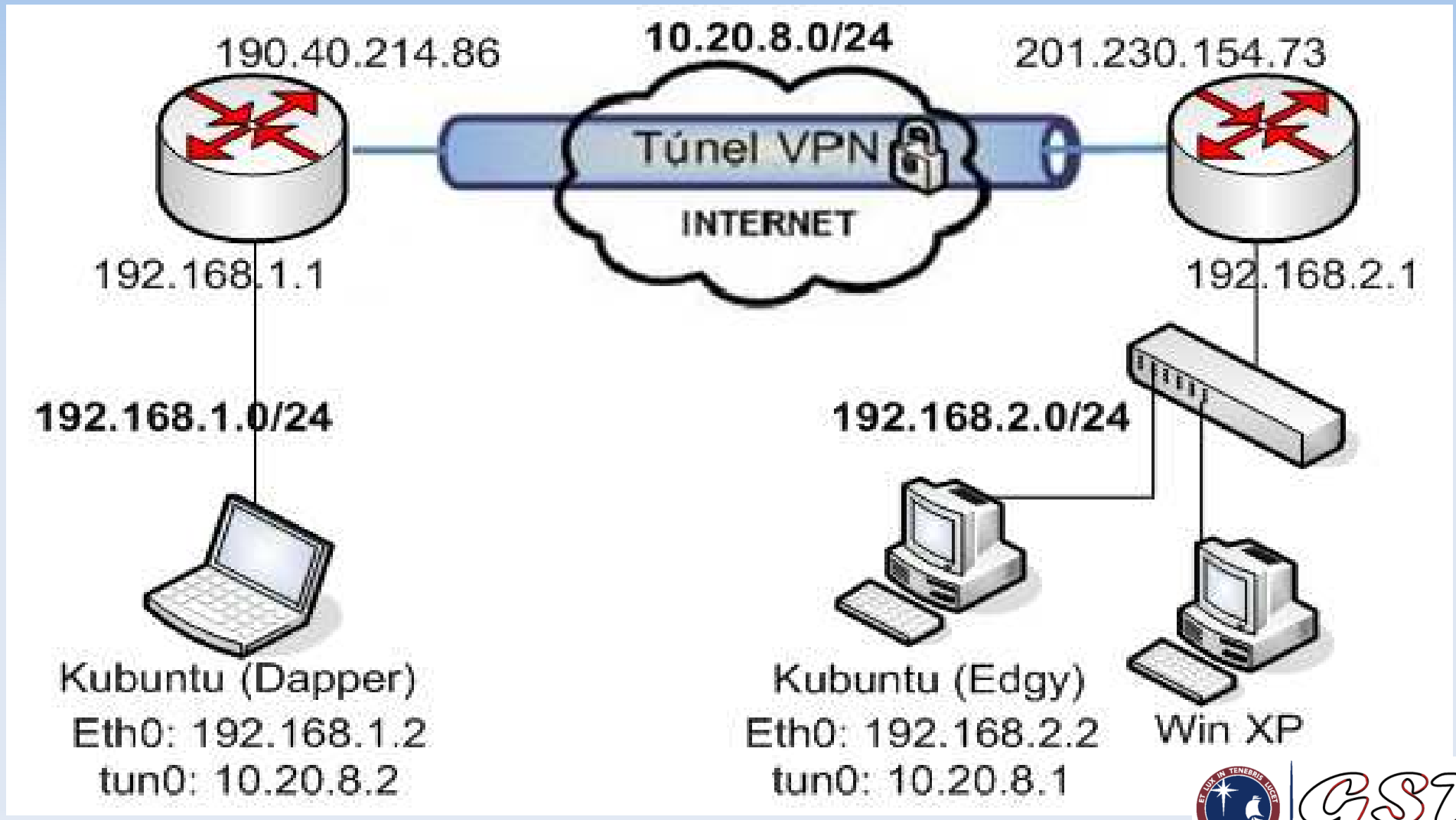
- client-to-client: conexiones entre clientes
- float: remoto tiene IP dinámica
- keepalive: estado del enlace
- cipher: Blowfish, AES, Triple-DES
- comp-lzo: compresión en el enlace
- max-client
- user nobody, group nobody: reducir permisos
- log, verb

GST

OpenVPN

- Casos:
  - Conexión entre redes privadas (P2P)
  - Acceso para un Road-warrior (Cliente-Servidor)
  - Puente Inalámbrico (Cliente-Servidor)
- Routed vs Bridged VPN.
  - Routed: Solución más sencilla y común.
  - Bridged: Recomendado sólo en ciertos casos (IPX; broadcast; otros OS)

Conexión entre redes privadas



LAN-LAN

arudo@arudo-desktop: /etc/openvpn - Terminal Nº 2 - Konsole

Sesión Editar Vista Marcadores Preferencias Ayuda

```
arudo@arudo-desktop:~$ cd /etc/openvpn/
arudo@arudo-desktop:/etc/openvpn$ cat vpn_aldo_lili.conf
remote 190.40.214.86
port 1194
float
proto udp
dev tun                         # dispositivo virtual.

ifconfig 10.20.8.1 10.20.8.2     # nodo local - nodo remoto.
route 192.168.1.0 255.255.255.0  # enrutamos lo que vaya a la otra red

#secret /etc/openvpn/clave1.txt
keepalive 10 120
#comp-lzo
verb 3

persist-tun                      # no cerrar el tunel despues del ping restart
persist-key                      # no volver a leer la llave despues del ping restart

user nobody
group nogroup
chroot /var/empty                # por seguridad.
arudo@arudo-desktop:/etc/openvpn$ ifconfig tun0
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:10.20.8.1  P-t-P:10.20.8.2  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
```

Terminal | Terminal Nº 2

arudo@arudo-desktop: /etc/openvpn - Te

Sesión Editar Vista Marcadores Preferencias Ayuda

```
arudo@arudo-desktop:/etc/openvpn$ sudo 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
arudo@arudo-desktop:/etc/openvpn$
```

Terminal

GST

LAN-LAN

arudo@arudo-desktop: /etc/openvpn - Terminal - Konsole

Sesión Editar Vista Marcadores Preferencias Ayuda

```
arudo@arudo-desktop:/etc/openvpn$ sudo openvpn --config vpn_aldo_lili.conf
Tue Mar 20 15:21:40 2007 OpenVPN 2.0.7 i486-pc-linux-gnu [SSL] [LZO] [EPOLL] built on Sep 13 2006
Tue Mar 20 15:21:40 2007 ******* WARNING *******: all encryption and authentication features disab
 all data will be tunnelled as cleartext
Tue Mar 20 15:21:40 2007 TUN/TAP device tun0 opened
Tue Mar 20 15:21:40 2007 ifconfig tun0 10.20.8.1 pointopoint 10.20.8.2 mtu 1500
Tue Mar 20 15:21:40 2007 route add -net 192.168.1.0 netmask 255.255.255.0 gw 10.20.8.2
Tue Mar 20 15:21:40 2007 Data Channel MTU parms [ L:1500 D:1450 EF:0 EB:4 ET:0 EL:0 ]
Tue Mar 20 15:21:40 2007 Local Options hash (VER=V4): '65254739'
Tue Mar 20 15:21:40 2007 Expected Remote Options hash (VER=V4): '35db84e0'
Tue Mar 20 15:21:40 2007 chroot to '/var/empty' and cd to '/' succeeded
Tue Mar 20 15:21:40 2007 GID set to nogroup
Tue Mar 20 15:21:40 2007 UID set to nobody
Tue Mar 20 15:21:40 2007 UDPv4 link local (bound): [undef]:1194
Tue Mar 20 15:21:40 2007 UDPv4 link remote: 190.40.214.86:1194
Tue Mar 20 15:21:40 2007 read UDPv4 [ECONNREFUSED]: Connection refused (code=111)
Tue Mar 20 15:21:49 2007 Peer Connection Initiated with 201.230.244.184:50971
Tue Mar 20 15:21:50 2007 Initialization Sequence Completed
```

Terminal | Terminal Nº 2

sole

```
conf
EPOLL] built on Sep 13 2006
uthentication features disa


 mtu 1500
5.0 gw 10.20.8.2
3:4 ET:0 EL:0 ]

4e0'
d
```

```
Tue Mar 20 14:57:47 2007 UDPv4 link local (bound): [undef]:1194
Tue Mar 20 14:57:47 2007 UDPv4 link remote: 190.40.214.86:1194
Tue Mar 20 14:58:06 2007 TCP/UDP: Incoming packet rejected from 201.230.244.184:50687[2], expecte
d peer address: 190.40.214.86:1194 (allow this incoming source address/port by removing --remote
or adding --float)
Tue Mar 20 14:58:16 2007 TCP/UDP: Incoming packet rejected from 201.230.244.184:50687[2], expecte
d peer address: 190.40.214.86:1194 (allow this incoming source address/port by removing --remote
or adding --float)
```

Terminal | Terminal Nº 2

LAN-LAN

arudo@arudo-desktop: /etc/openvpn - Terminal Nº 2 - Konsole

Sesión Editar Vista Marcadores Preferencias Ayuda

```
arudo@arudo-desktop:/etc/openvpn$ ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=27.6 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=28.1 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=64 time=27.9 ms

--- 192.168.1.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2010ms
rtt min/avg/max/mdev = 27.643/27.938/28.180/0.261 ms
arudo@arudo-desktop:/etc/openvpn$ ping 10.20.8.2
PING 10.20.8.2 (10.20.8.2) 56(84) bytes of data.
64 bytes from 10.20.8.2: icmp_seq=1 ttl=64 time=28.1 ms
64 bytes from 10.20.8.2: icmp_seq=2 ttl=64 time=26.0 ms
64 bytes from 10.20.8.2: icmp_seq=3 ttl=64 time=29.1 ms

--- 10.20.8.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2006ms
rtt min/avg/max/mdev = 26.079/27.765/29.101/1.258 ms
arudo@arudo-desktop:/etc/openvpn$
```

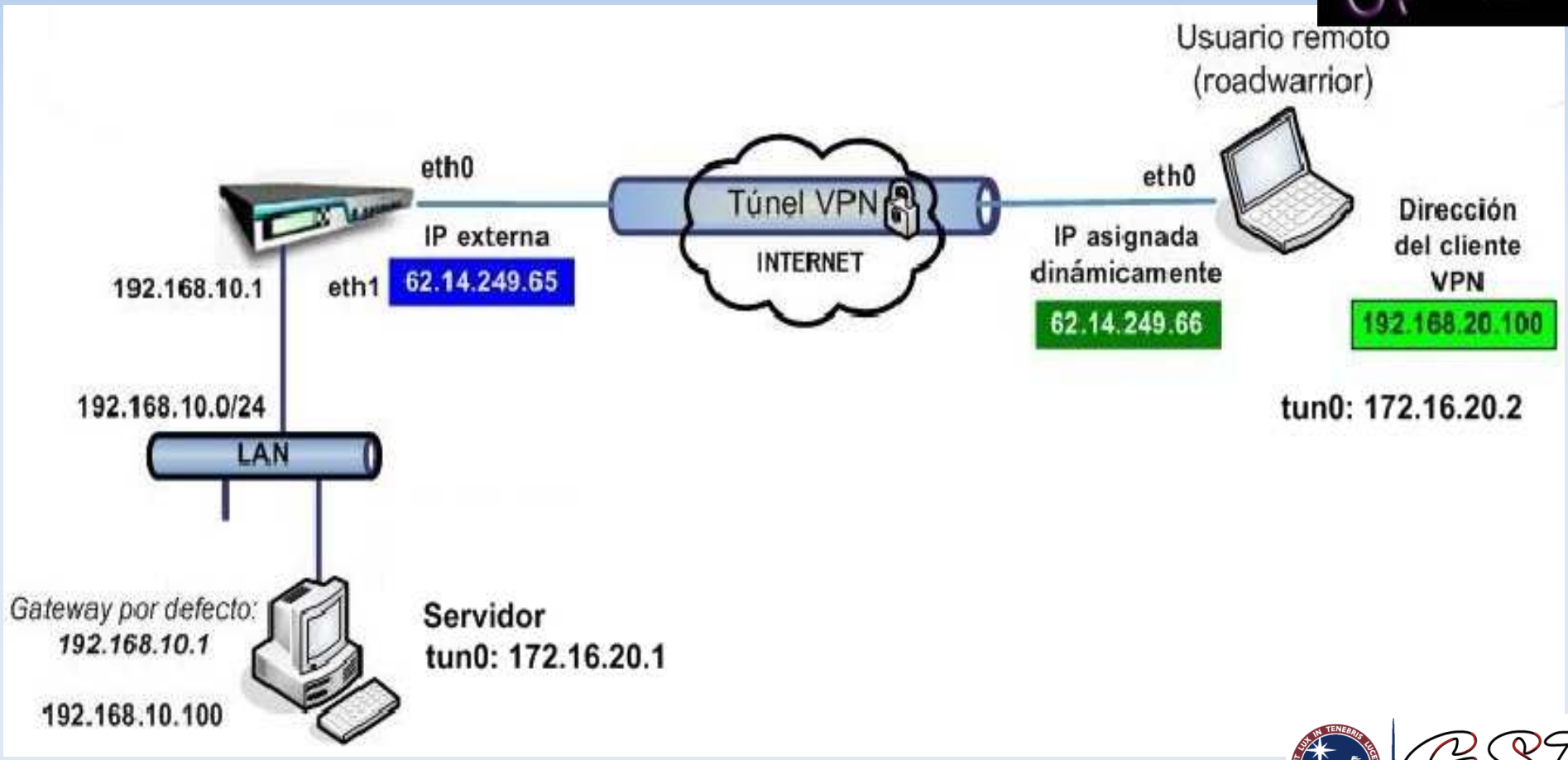
Terminal | Terminal Nº 2

GST

LAN-LAN: Consideraciones

- Firewall:
  - iptables -A INPUT -i tun+ -j ACCEPT
  - iptables -A OUTPUT -o tun+ -j ACCEPT
  - iptables -A FORWARD -i tun+ -j ACCEPT
  - iptables -A FORWARD -o tun+ -j ACCEPT
- Configuración del MODEM-Router (NAT)

Road-warrior



RoadWarrior: Servidor


```
#### Configuración de servidor ####
port 1194
dev tun
tls-server
mode server

dh /etc/openvpn/easy-rsa/dh1024.pem
ca /etc/openvpn/easy-rsa/ca.crt
cert /etc/openvpn/easy-rsa/servidor.crt
key /etc/openvpn/easy-rsa/servidor.key
duplicate-cn

ifconfig 172.16.20.1 172.16.20.2
ifconfig-pool 172.16.20.5 172.16.20.100 # rango para clientes

#mantener el túnel abierto
push "ping 10"
push "ping-restart 60"
ping 10
ping-restart 120
```

RoadWarrior: Servidor


```
#client-to-client

tun-mtu 1500

#rutas para el servidor
route 192.168.20.0 255.255.255.0
#rutas para los clientes
#push "route 10.10.10.0 255.255.255.0"          #Red de Servidores

comp-lzo
status-version 2
status openvpn-status.log
verb 5

####Fin de configuración####
```

RoadWarrior: Cliente

####Configuración del cliente ####

port 1194 #udp by default
dev tun
remote 62,14.249.65
tls-client

ca /etc/openvpn/easy-rsa/ca.crt
cert /etc/openvpn/easy-rsa/cliente1.crt
key /etc/openvpn/easy-rsa/cliente1.key

tun-mtu 1500
pull
comp-lzo
verb 4

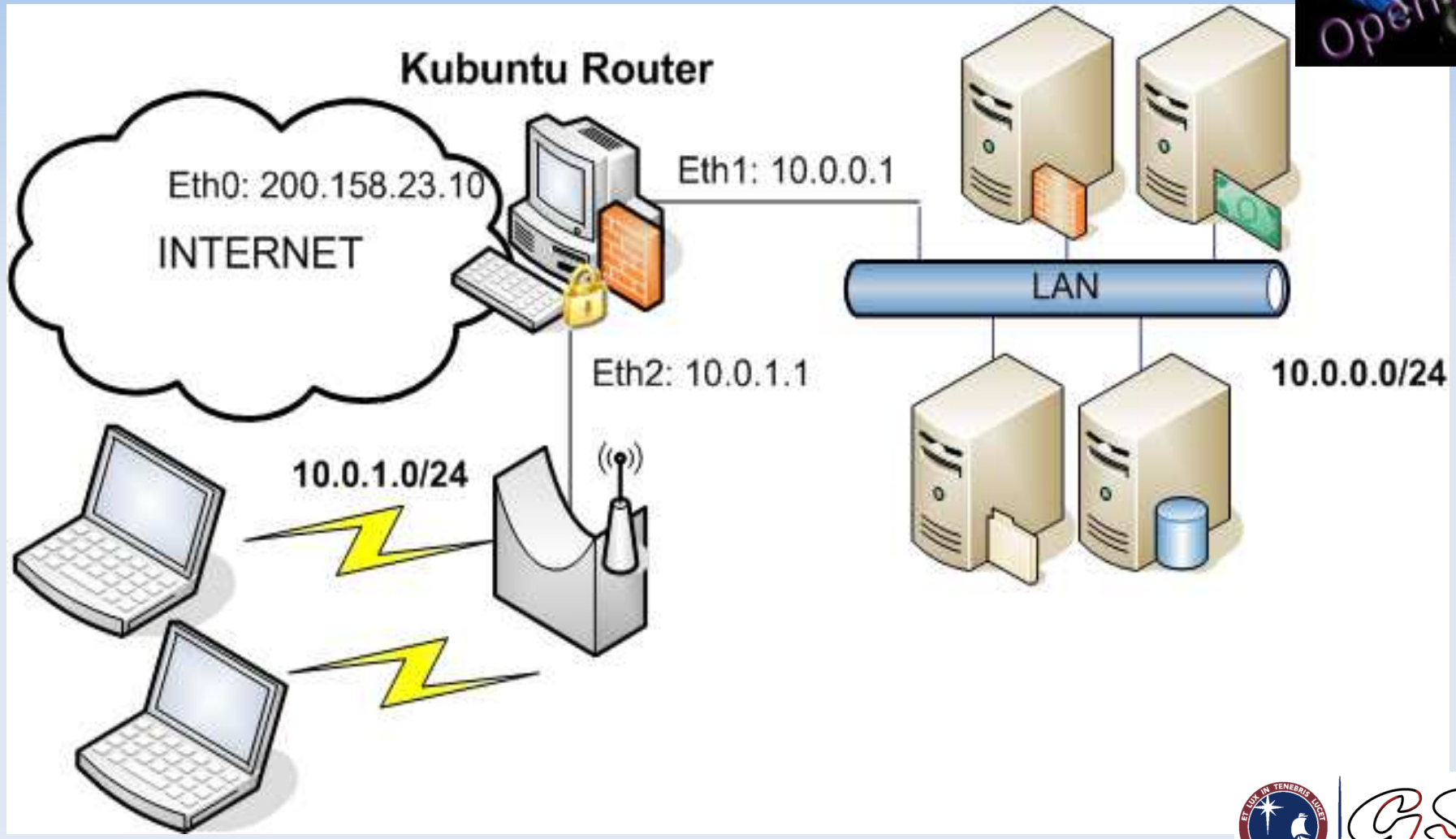
###Fin de configuración###

GST

RoadWarrior: Consideraciones

- Configuración del MODEM-Router (NAT).
- Configuración del Firewall.
- Habilitar IP FORWARDING en caso de conexiones entre clientes:
  - sudo vim /etc/sysctl.conf
  - net/ipv4/ip_forward=1
  - Otra opción: script OpenVPN

Puente Inalámbrico



Puente Inalámbrico: Servidor


```
##Configuración del servidor OpenVPN ##
port 1194
dev tap0                                #pre-creada
mode server

dh /etc/openvpn/easy-rsa/dh1024.pem
ca /etc/openvpn/easy-rsa/ca.crt
cert /etc/openvpn/easy-rsa/servidor.crt
key /etc/openvpn/easy-rsa/servidor.key

#dirección ip del servidor y rango e direcciones a dar a los cliente
server-bridge 10.0.0.1 255.255.255.0 10.0.0.100 10.0.0.200
#todo tráfico IP de clientes pasará por el servidor (DNS, HTTP Proxy)
push "redirect-gateway local def1"

client-config-dir /usr/local/etc/openvpn/bridge-clientes
client-to-client
keepalive 10 120
```

Puente Inalámbrico: Servidor


```
cipher AES
comp-lzo
max-clients 100
user nobody
group nobody
persist-key
persist-tun
verb 3
## Fin configuración ##


## /usr/local/etc/openvpn/bridge-clientes/clientevip ##
ifconfig-push 10.0.0.20 255.255.255.0
## fin ##
```

Puente Inalámbrico: Cliente


```
##Configuración del cliente OpenVPN ##
client
dev tap0
remote 10.0.1.1 1194
resolv-retry infinite
nobind                          # No asociado a un puerto local específico
    (retorno)
user nobody
group nobody
persist-key
persist-tun
ca /etc/openvpn/easy-rsa/ca.crt
cert /etc/openvpn/easy-rsa/cliente1.crt
key /etc/openvpn/easy-rsa/cliente1.key
cipher AES
comp-lzo
verb 3
mute 20
## Fin ##
```

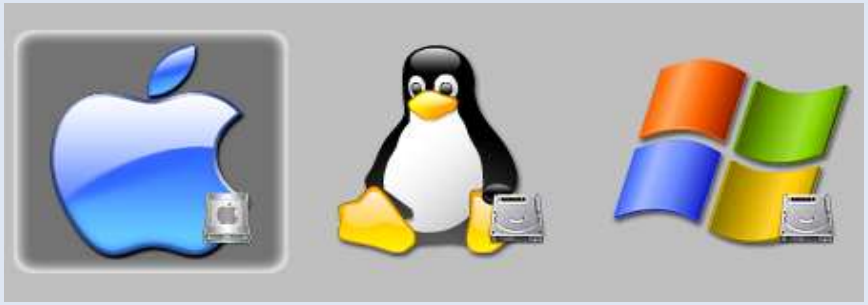
Puente Inalámbrico: Consideraciones

- Configurar las interfaces virtuales:
  - openvpn --mktun --dev tap0 (S y C)
  - brctl addbr br0
  - ip link set tap0 up
  - brctl addif br0 tap0
  - brctl addif br0 eth1
- Configurar el firewall:
  - iptables -A INPUT -i tap0 -j ACCEPT
  - iptables -A INPUT -i br0 -j ACCEPT
  - iptables -A FORWARD -i br0 -j ACCEPT
  - iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -o eth0 -j MASQUERADE
- Habilitar IP FORWARDING

GST

Ayuda

- man openvpn
- Windows: http://openvpn.net/
- MAC OS X: http://www.tunnelblick.net/



- Openswan: http://www.openswan.org/

openswan™

GST

Gracias por su atención

Liliana Castillo Devoto a20034689@pucp.edu.pe
Aldo Lovera Raffo a20030254@pucp.edu.pe

Ingeniería de Telecomunicaciones - GST