Punto de acceso inalámbrico con múltiples SSID y VLAN

El propósito de este documento es describir la implementación de un Punto de Acceso WiFi utilizando Zeroshell en un sistema con una tarjeta de red WiFi con un chipset Atheros. El documento se subdivide en las siguientes secciones:

¿Por qué implementar un punto de acceso inalámbrico con los módulos del kernel de Linux de el proyecto MadWifi?

Gracias a la utilización de los módulos MadWifi por el núcleo de Linux, es posible implementar un *punto de acceso inalámbrico* con un ordenador personal o un *dispositivo integrado* que tenga una tarjeta de red WiFi (PCI o MiniPCI) con un chipset Atheros. Esta función está disponible desde la versión 1.0.beta8 de Zeroshell, que introduce el soporte WiFi en cualquier AP (Access Point) o en modo STA (en el cual un Zeroshell router/bridge se puede asociar como un cliente en una LAN inalámbrica). La opción de utilizar los controladores Madwifi, combinados con el uso de *wpa_supplicant* y paquetes *hostapd*, se debe a su capacidad para desempeñar las funciones de un Punto de Acceso con características avanzadas, por ejemplo:

- Autenticación de acceso y cifrado del tráfico inalámbrico a través de *WPA/WPA2 (RSN).* Este es soportado también en modo *WPA-PSK*, en el que el cliente, a fin de estar asociado a un SSID, debe conocer el *Pre-Shared Key*, o el modo *WPA-EAP*, también conocido como *WPA Enterprise*, en el que un usuario puede llegar a ser autenticado con nombre de usuario y contraseña o un certificado digital X.509 validado por un *servidor* RADIUS. Tanto el algoritmo de cifrado *TKIP* y el mas seguro *CCMP*, basado en *AES*, son soportados;
- Modo de administración de múltiples *SSID* (también llamado *Virtual SSID)*, gracias al cual es posible crear hasta 4 puntos de acceso virtual independientes para cada tarjeta de red WiFi en el sistema. Es evidente que los SSID virtuales pertenecientes a la misma tarjeta de red WiFi compartiran el canal de radio que utilizan, y por lo tanto el ancho de banda disponible. Además, para cada SSID virtual es posible establecer un sistema de autenticación y esquema de cifrado independiente (texto sin formato, WPA-PSK, WPA Enterprise o WEP a 128 bits). De los cuatro posibles SSID también se puede trabajar en modo *administrado* y asociado a una WLAN como un cliente. Por ejemplo, esto es útil para ampliar el alcance de la red inalámbrica mediante la aplicación de autorepetidores que trabajan en *WDS* (Wireless Distribution System), pero no necesitan estar conectadas entre sí por medio de una red cableada.

- Compatibilidad con los canales de la red en la banda de 5GHz (802.11a) y la banda de 2,4 GHz (802.11by 802.11g). En particular, en caso de que el modo 802.11g sea seleccionado, la compatibilidad está garantizada para los clientes más antiguos que sólo tienen 802.11b.

Zeroshell identifica a cada SSID virtual como si se tratara de una interfaz Ethernet (ETHnn). Esto permite que operen en las redes Wi-Fi, utilizando una interfaz web, así como las interfaces de cable. En otras palabras, en el SSID es posible:

- Agregar direcciones IP, enrutamiento estático y también permite que el protocolo RIP V2 adquiera y propague las rutas dinámicas;
- Aplicar clases de calidad de servicio para hacer tráffic shaping mediante la asignación de diferentes niveles de prioridad, ancho de banda el máximo y garantizado a los diferentes tipos de tráfico (VoIP, P2P, SSH, HTTP, ...);
- Hacer de puente con las interfaces Ethernet, VLAN 802.1Q, VPN de LAN a LAN y otros SSID. En particular, la posibilidad de hacer un puente o enlace de capa 2 con un SSID virtual que funciona como un cliente con la calidad de un punto de acceso, permitiendo que funcione el llamado *repetidor WiFi* (o WDS) que extiende el área de cobertura de la WLAN;
- Activar los servicios, incluido el DHCP, portal cautivo y aplicar filtros de tráfico por medio del firewall.
- Aplicación *de bonding*, que es añadir dos o más interfaces de tal manera que se aumente el ancho de banda (balanceo de carga) y fiabilidad (tolerancia a fallos). Naturalmente, para tener enlaces inalámbricos, es necesario que los SSID virtuales que los componen pertenezcan a diferentes interfaces WiFi con el fin de equilibrar el tráfico en los diferentes canales de radio.

Administrar interfaces inalámbricas y múltiples SSID con el *WiFi-Manager*

Aunque mediante la interfaz web Zeroshell (véase figura) es posible administrar las interfaces de red que representan los SSID, las operaciones para la creación y gestión de estos últimos respecto a los parámetros inalámbricos como el canal a utilizar, la potencia de transmisión en dBm y el cifrado, todos son Gestionado por un script que es llamado por el comando de shell *wifi-gerente* por medio de una conexión serial RS232 o VGA por consola o mediante una sesión SSH remota. A continuación puedes ver el menú principal del *WiFi-Manager:*

```
root@gw-adsl root> wifi-manager

[wifi0]  Chipset  AR5413 802.11abg NIC (rev 01)
-- If -- Mode -- SSID --------------------------- Hide -- Security -
>> ETH02  AP     WLAN with Captive Portal          no     Plaintext
   ETH03  AP     WLAN with Pre-Shared Key          no     WPA-PSK
   ETH04  AP     WLAN with 802.1x Radius Auth.     no     WPA-EAP
   ETH05  AP     WLAN with WEP                     no     WEP128

[wifi1]  Chipset  AR5413 802.11abg NIC (rev 01)
-- If -- Mode -- SSID --------------------------- Hide -- Security -
   ETH06 STA     wrap-psk                          no     WPA-PSK

COMMANDS
```

```
  <N> New SSID                <M> Modify SSID
  <D> Delete SSID             <I> Show Information
  <C> Std/Channel/Tx-Power
  <L> List Stations           <S> Channel Scanning
  <R> Restarting Devices      <Q> Quit

>>
```

Como puede ver, este sistema se ilustra con un PC ALIX 2C2 Embebido con 2 interfaces WiFi con el chipset Atheros *AR5413 802.11abg*, capaz de operar tanto en 802.11bg como en 802.11a. En la interfaz inalámbrica *wifi0* con 4 puntos de acceso virtuales que comparten la misma frecuencia de radio, se definen cada uno con su propia autenticación y esquema de cifrado.

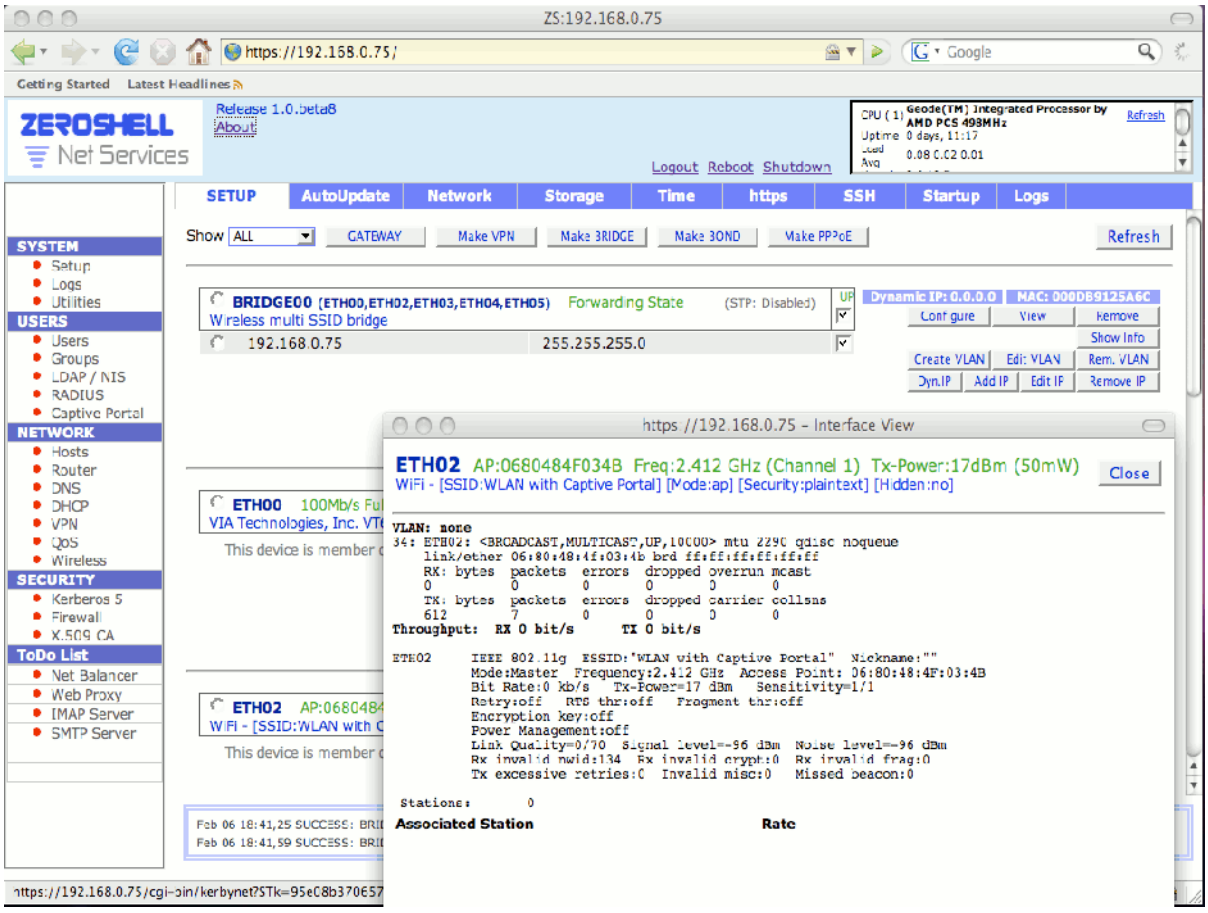
- La interfaz ETH02 corresponde a la WLAN con el SSID *"WLAN with Portal Cautivo"*. Sin cifrado (texto plano) se define para este SSID, pero la autenticación es sucesivamente delegada al portal cautivo;
- La interfaz ETH03 corresponde a la *WLAN con el* SSID *"with Pre-Shared Key"* con protección WPA-PSK, donde se puede acceder conociendo la clave compartida definida durante la creación del SSID. Este modo de protección, que sustituye a WEP, es muy vulnerables a la captura de un número determinado de paquetes, se considera suficientemente seguro si se utiliza una clave previamente compartida con el tamaño y complejidad adecuada. Naturalmente, como con WEP, el administrador debe comunicar este número a todos los usuarios que podrán acceder a la red inalámbrica, y se debe cambiar periódicamente. Esto es factible en configuraciones pequeñas, como el servicio doméstico o la configuración SOHO, pero se vuelve muy complicada cuando el número de puntos de acceso de usuarios crece;
- La interfaz ETH04 se refiere al punto de acceso virtual con SSID *"WLAN with Radius 802.1x Auth."* donde un esquema de encriptación WPA-EAP ha sido configurado. Este tipo de método de protección es la más segura y flexible, y por lo tanto se utiliza en configuraciones grandes y por eso que WPA-EAP es también conocida como *WPA Enterprise*. Su flexibilidad se debe al hecho de que las claves de cifrado no son generadas por el administrador, pero si de forma automática por un servicio de RADIUS mediante *802.1x*, que autentica al usuario mediante un nombre de usuario y una contraseña (con *PEAP* with MSCHAPv2 o *EAP-TTLS)* o por medio de un certificado digital X.509 (with *EAP-TLS).* Durante la configuración del SSID con WPA-EAP, se puede optar por utilizar el servidor local Zeroshell RADIUS o hacer una referencia a un servidor RADIUS externo. En el primer caso no es necesario configurar ningún *secreto compartido,* mientras que en el segundo caso utilizando un RADIUS externo es necesario especificarlo.
- WEP de 128-bits se define en la última interfaz. Es necesaria debido a la existencia de antiguos clientes que no son compatibles con WPA/WPA2, WEP en lo posible debe evitarse dado el bajo nivel de protección que garantiza.

En el *wifi1* una única interfaz es definida en modo cliente. Esta interfaz se conecta a la red inalámbrica con SSID llamada *"WRAP-PSK"*, protegida por una clave precompartida. Tenga en cuenta que con una tarjeta Wi-Fi puede tener un máximo de un SSID que actúe como un cliente. Los otros SSID deben corresponder a los puntos de acceso virtuales. Por otra parte, dado que todos los SSID pertenecen a la tarjeta WiFi y

comparten el mismo canal, éste coincidirá con el canal de radio de las WLAN externas. Esto inevitablemente significa compartir el ancho de banda.

Teniendo en cuenta la simplicidad del *WiFi-Manager*, es inútil describir ahora cada comando, ya que su uso debe ser muy intuitivo. El anuncio sólo es con respecto al "Std/Channel/Tx-Power" voz que se activa con la tecla *C* del menú. Con esto es posible aplicar la norma (802.11a, 802.11by 802.11g y después con las nuevas versiones del controlador de Madwifi, también para 802.11n, todavía en proyecto), la disposición del canal de radio de alta frecuencia para la norma elegida y una potencia de transmisión expresada en dBm o mW. En particular, es necesario establecer este último parámetro con cuidado para evitar pasar por el límite de potencia permitido por la ley donde se encuentran.

Como ya se ha insinuado, una vez que los SSID se crean y configuran con el *wifi-manager*, si éstas corresponden a los centros de Acceso Virtual o conexiones de cliente, aparecen en todos y para todos, como Ethernet (ETHnn) las interfaces que pueden ser manipulados a través de la interfaz web Zeroshell . En el ejemplo ilustrado en la figura siguiente, las cuatro interfaces inalámbricas Multi SSID y la interfaz de cable *ETH00* son enlazadas en un *BRIDGE00* único de la interfaz. *(ETH00, ETH02, ETH03, ETH04, ETH05)*



Interfaz de configuración. Haga clic en la imagen para ampliarla.

Haciendo esto, todas las 4 redes WLAN, independientemente de su modo de acceso (WPA-PSK, WPA-EAP, Portal Cautivo o WEP), comparten la misma capa 2 de la LAN que es accesible a través de la interfaz Ethernet ETH00. El hecho de compartir el nivel

de enlace de datos para varios componentes del SSID el cual hace posible utilizar el servidor LAN DHCP (si existe) o sólo se necesitara activar una subred con DHCP solo conectado a la interfaz del puente. Obviamente, como el firewall y la calidad de servicio también actúan en las interfaces de puente, es posible aplicar un acceso independiente y reglas de tráffic shaping para cada SSID. Por ejemplo, fuera posible para beneficiar a los usuarios que accedan a través de la WPA Enterprise con respecto a aquellos que utilizan el portal cautivo, ya que hemos visto que el tráfico de esta última no está cifrado.

Mapa de la LAN inalámbrica en la red VLAN con etiquetas tags

Si las LAN virtuales se definen en los switches LAN en el sensado de sus puertos son lógicamente reagrupados para que aparezcan como pertenecientes a diferentes (virtual) switches, la comunicación entre estos switches es posible por medio de puertos de *trunk* o *trunking*. Estos puertos se caracterizan por pertenecer simultáneamente a más de una VLAN, los paquetes a través de ellos deben ser identificados mediante marcas (o VIDs) que identifican la fuente/destino de la VLAN. Uno de los protocolos de trunking más utilizado es el definido en el estándar *IEEE 802.1Q,* que tiene una etiqueta de 12-bits con un intervalo de valores válidos desde 1 hasta 4094. Lo que es más se define el concepto de los *nativos de VLAN,* que es la VLAN cuyos paquetes van a través del trunk por defecto sin etiquetar las tramas Ethernet. VLAN nativas también se asignan a tareas de gestión. La difusión de esta norma ha permitido a la interoperabilidad entre diferentes marcas de dispositivos de red y modelos, incluso en las redes LAN virtuales están presentes. En particular, la función de mapeo de las redes VLAN en el que la LAN se subdivide en diferentes SSID inalámbrico se está volviendo más generalizada. Esto permite la homogeneidad en la asignación de direcciones IP de subred entre las VLANs que comprende la LAN y el SSID que constituyen la WLAN. Gracias al apoyo de Zeroshell de VLAN 802.1Q, la gestión de múltiples SSID para un único punto de acceso y la posibilidad de salvar las interfaces que representan a la VLAN con los representantes de los SSID, esto es ahora posible y económico, sin tener que utilizar un (físico) punto de acceso para cada LAN virtual que se alcanzara a través de la red inalámbrica.

Por ejemplo, supongamos que una organización tiene su LAN subdividida en 2 VLANs:

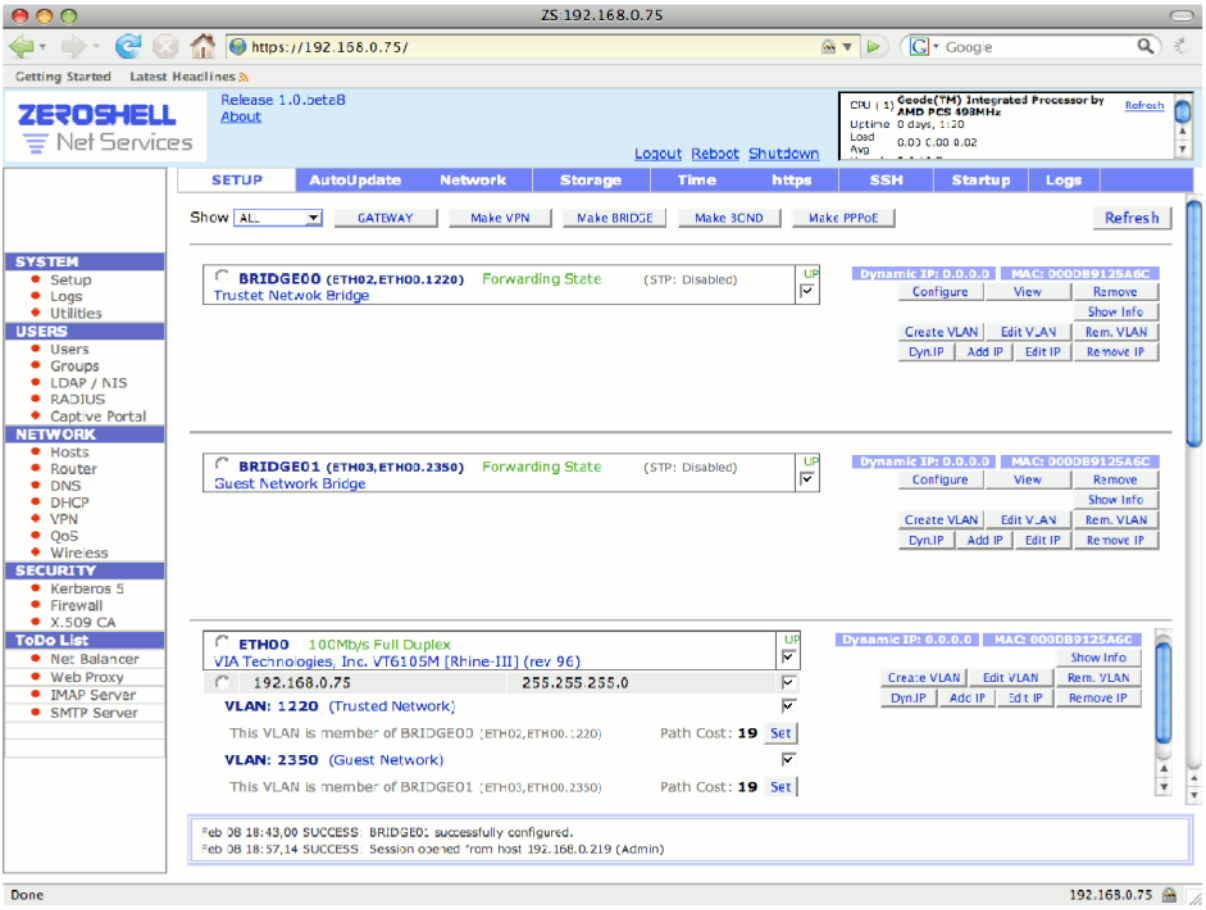
- Una VLAN para permitir el acceso a los hosts de servicios y los de escritorio del personal permanente de la organización. Esta VLAN, en la que no hay restricciones definidas por el firewall respecto a los recursos de la red interna, tiene un VID 1220 (VLAN ID) y debe ser accesible a través de SSID inalámbrico a través de un llamado *"Trusted Network"*. El acceso a este WLAN se debe permitir sólo a los poseedores de una tarjeta inteligente o eToken con un certificado personal X.509, esto a través de WPA-EAP con RADIUS activado para poder responder a EAP-TLS;
- Una VLAN para permitir que los clientes con computadores portátiles accedan a Internet pero con algunas reglas de firewall que limitan el acceso a los recursos de la red interna. Tal VLAN, cuyo VID se ha establecido como 2350, también a través de cifrado inalámbrico con un SSID llamado *"guest"*. Aunque el tráfico viaja sin codificar, en esta WLAN, la autenticación se solicita al acceso desde el

portal cautivo donde se concede el acceso a través de un nombre de usuario y contraseña temporal dado a los invitados. La decisión de utilizar el portal cautivo para esta VLAN está motivada por la simplicidad de acceso que no limita a los huéspedes a tener configurar su equipo WiFi para solicitar el acceso a Internet. Esta última operación no siempre es inmediata y soportada en todos los sistemas operativos, mientras que el portal cautivo provee acceso independientemente del tipo de sistema, siempre que tenga un navegador web.

Como se ilustra a continuación, dos SSID virtuales se crean a través de la *wifi-manager: "Trusted Network"* corresponde a la interfaz Ethernet ETH02 y con WPA Enterprise activa, *"guest"* corresponde a ETH03. A pesar de que el hardware que está utilizando tiene 2 tarjetas de red WiFi (wifi0 y wifi1), se decidió crear dos SSID en wifi0. Esto ahorraría un canal de radio, que es un recurso muy valioso cuando se utiliza 802.11b / g, ya que sólo hay tres canales sin solapamiento de frecuencias (1,6 y 11).

```
root@multi-AP root> wifi-manager

[wifi0]  Chipset  AR5413 802.11abg NIC (rev 01)
-- If -- Mode -- SSID -------------------------- Hide -- Security -
>> ETH02  AP     Trusted Network                 no     WPA-EAP
   ETH03  AP     Guest Network                   no     Plaintext

[wifi1]  Chipset  AR5413 802.11abg NIC (rev 01)
-- If -- Mode -- SSID -------------------------- Hide -- Security -

COMMANDS
  <N> New SSID              <M> Modify SSID
  <D> Delete SSID           <I> Show Information
  <C> Std/Channel/Tx-Power
  <L> List Stations         <S> Channel Scanning
  <R> Restarting Devices    <Q> Quit

>>
```

Ahora, supongamos que la interfaz Ethernet ETH00 está conectada a un switche en un puerto de trunking a través del cual las dos VLANs se cuentan con etiquetas 1220 y 2350, además de las VLAN nativas: con el botón [Crear VLAN] añadimos la mencionada LAN virtual . Una vez hecho esto, creamos dos puentes presionando [Hacer BRIDGE]: BRIDGE00 debe conectar ETH00.1220 (VLAN 1220) con ETH02 (SSID *"Trusted Network")* en la capa 2, mientras que BRIDGE01 debe conectar ETH00.2350 (VLAN 2350) con ETH03 (SSID *"guest").* Todo esto se ilustra en la figura siguiente:



SSID y VLAN bridging. Haga clic en la imagen para ampliarla.

Usted puede notar que no es estrictamente necesario asignar una dirección IP a los dos puentes, mientras que la interfaz ETH00 que corresponde a la VLAN nativa, se le asigna la dirección IP 192.168.0.75, conectándola para que ejecute las opciones de gestión de Zeroshell.

En este caso, para completar esta tarea es suficiente activar el portal cautivo en la sesión [Portal Cautivo] -> [Gateway] en interfaz ETH03 (SSID *"guest")* en *el modo Bridge.*

Amplíe la conexión inalámbrica geográficamente a través de OpenVPN

Zeroshell utiliza *OpenVPN* con dispositivos *Tap* (Ethernet virtual) como una solucion VPN sitio a sitio. Esto ofrece ventajas a través de protocolos como IPSec en el sentido de que permite conectar sitios de la organización que están geográficamente distantes usando la capa 2. De hecho, desde la interfaz *Tap* (Zeroshell la llama VPNnn) es muy similar a la interfaz Ethernet (ETHnn), la VPN puede ser puenteada con este último y también con el SSID inalámbrico. Por lo tanto, ya que no hay procesos de enrutamiento entre la LAN y la WLAN ya sean locales o remotos conectados a través de la VPN, la misma subred IP se puede utilizar en todas partes. Por lo tanto, no sólo un único servidor DHCP puede ser utilizado para distribuir la misma dirección IP a cada cliente independientemente del lugar y tipo de conexión (cableada o inalámbrica), pero como los protocolos de NetBIOS utilizados para compartir recursos como impresoras de

windows y carpetas puede operar sin tener que utilizar un servidor WINS con el fin de descubrir los recursos de red, ya que el tráfico de difusión se propaga de manera uniforme en la LAN y WLAN (local y remota).
Siempre gracias a la similitud de las VPN hechas con OpenVPN y las conexiones Ethernet reales, es posible generalizar el ejemplo anterior mediante el transporte de 802.1Q VLAN en sitios remotos, así ampliar su aplicación vía inalámbrica puenteando las interfaces que representan a la VLAN transportadas por la VPN (en el ejemplo anterior son VPN00.1220 y VPN00.2350) con SSID *"Trusted Network"* y *"guest"*.