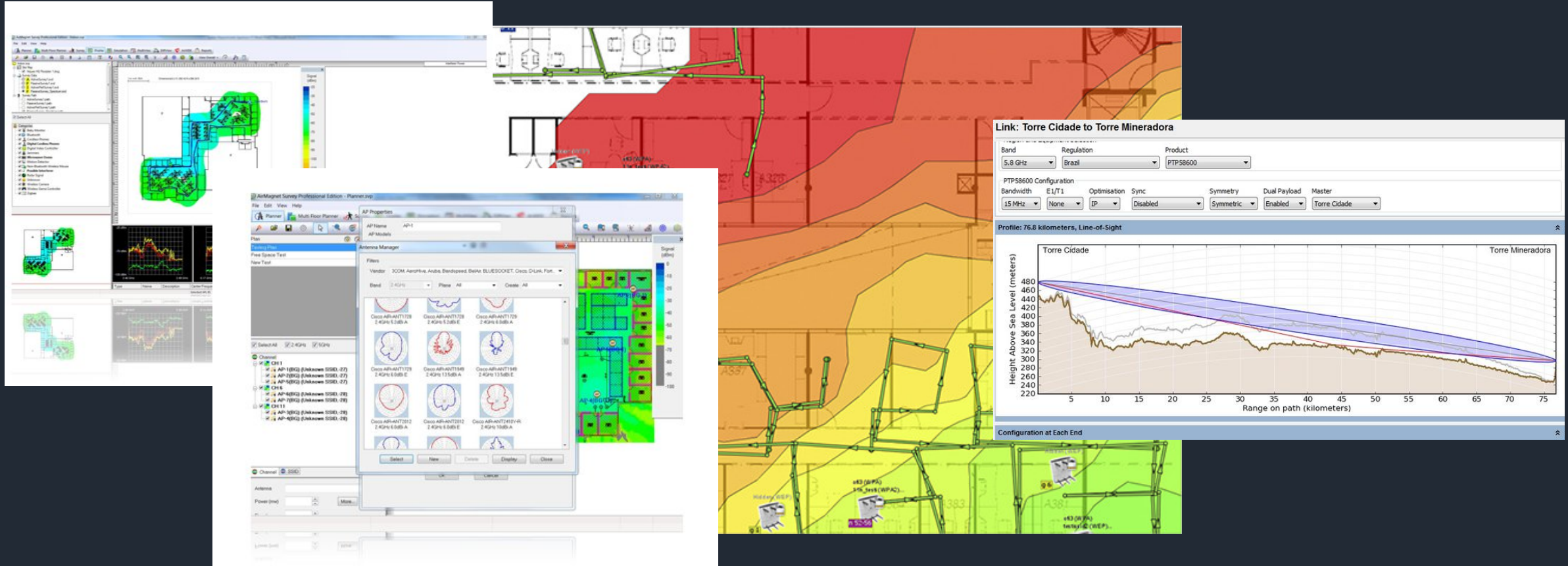


Seguridad WiFi ■

Diseñar una WiFi segura

- 1.Site Survey :: HeatMap/Spectrum
- 2.Planificación :: Channels/SSID
- 3.Estándares WiFi :: Protocolos y opciones
- 4.Seguridad :: Cifrado de datos
- 5.Seguridad :: Usuarios/Control de Acceso
- 6.Seguridad :: Rogue APs/Paranoia
- 7.El mejor consejo es ...

1. Site Survey – Estudio de Radiofrecuencia

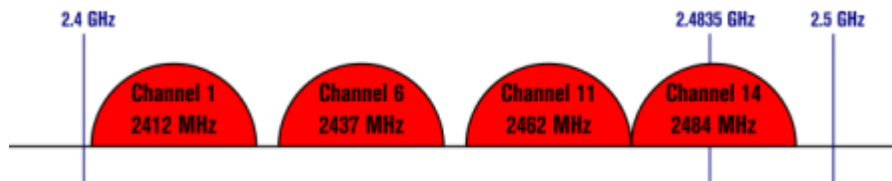


NetSpot, Ekahau, AirMagnet, Motorola PTP LinkPlanner ...

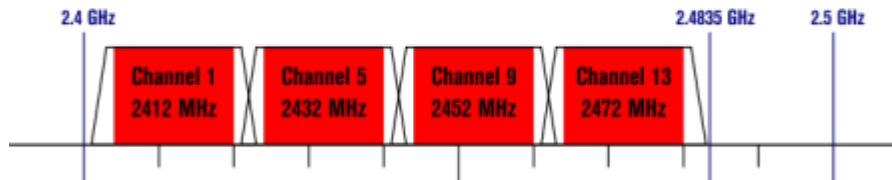
2. Planificación :: Channels/SSID

Non-Overlapping Channels for 2.4 GHz WLAN

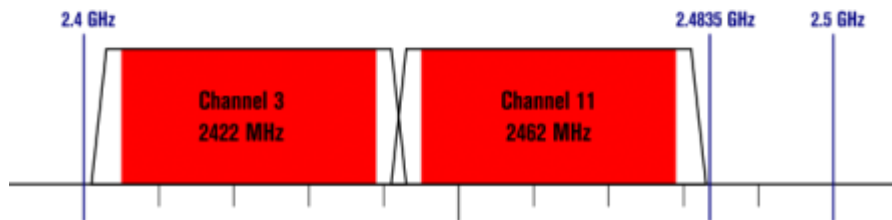
802.11b (DSSS) channel width 22 MHz



802.11g/n (OFDM) 20 MHz ch. width – 16.25 MHz used by sub-carriers



802.11n (OFDM) 40 MHz ch. width – 33.75 MHz used by sub-carriers

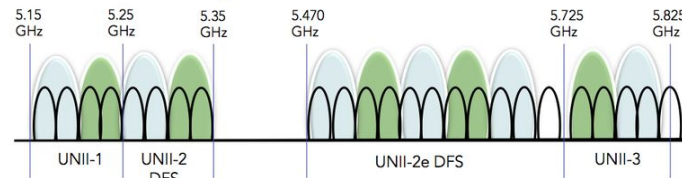


WLAN channels in Europe

2,4 GHz spectrum													
Channel	1	2	3	4	5	6	7	8	9	10	11	12	13
Channelwidth [MHz]	5	5	5	5	5	5	5	5	5	5	5	5	5
Frequency [MHz]	2412	2417	2422	2427	2432	2437	2442	2447	2452	2457	2462	2467	2472

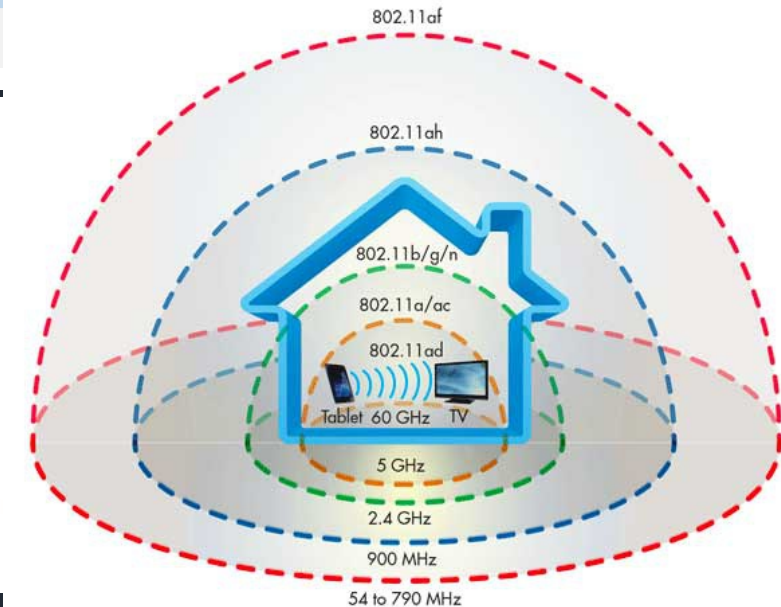
5 GHz spectrum																	
Base channels								Weather radar									
Channel	36	40	44	48	52	56	60	64	100	104	108	112	116	120	124	128	132
Channelwidth [MHz]	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20
Frequency [MHz]	5180	5200	5220	5240	5260	5280	5300	5320	5400	5420	5440	5460	5480	5500	5520	5540	5560

The Wi-Fi Spectrum: 5GHz



- 21 non-overlapping 20 MHz channels
- 9 non-overlapping 40 MHz channels
- Only 4 non-DFS channels for bonding
- Creates channel planning problems similar to 2.4 GHz
- 5 GHz isn't a panacea, RF management is still king

Figure 1: Existing 5 GHz Wi-Fi channels and the new channels we are making available



2. Planificación :: Channels/SSID

1. Definir canales o usar DFS según Survey
2. Definir ancho banda del canal (speed)
3. Analizar interferencias posibles
4. Ajustar potencia para limitar alcance
5. Usar WiFi Controller donde podamos
6. Planificar AP según velocidades clientes

2. Planificación :: Channels/SSID

1. Ocultar el SSID no sirve de nada (KALI)
2. NO usar un SSID del operador (WLAN_XXX)
3. NO usar un SSID que nos identifique
4. Jugar al despiste (WIFI_JAZZ en Vf)
5. SSID para invitados, separado por VLAN
6. Si podemos, tener un HoneyPot para jugar

3. Estándares WiFi :: Protocolos y opciones

1. 802.11b/g/n/ac/ad ... Evitar mezclar
2. Aislar clientes entre si.
3. WMM activo (VoIP, Streaming, ...)
4. Ajustar velocidades mínimas (QoS)
5. DESACTIVAR WPS!!!! DESACTIVAR WPS!!!!
6. Activar logs remotos

3. Seguridad :: Cifrado de datos

1. WiFi Abierta – NUNCA (Ojo LOPD/ENS)
2. WEP – 64/128bits – BASURA!*
3. WPA-PSK – 256bits – TKIP roto/AES – NO*
4. WPA2-PSK – 256bits – AES/CCMP –Mínimo!**
5. WPA-EAP – NO SALVO Hw LEGACY*
6. WPA2-EAP – 512bits – SI!
7. WPA2-EAP + 802.11x – WIN!!!!

* Equipos legacy pueden no soportar WPA2, o incluso WPA. Velocidad baja a 54Mbps

** Krack. Usemos EAP, que no es vulnerable, y con 802.11x lo más.

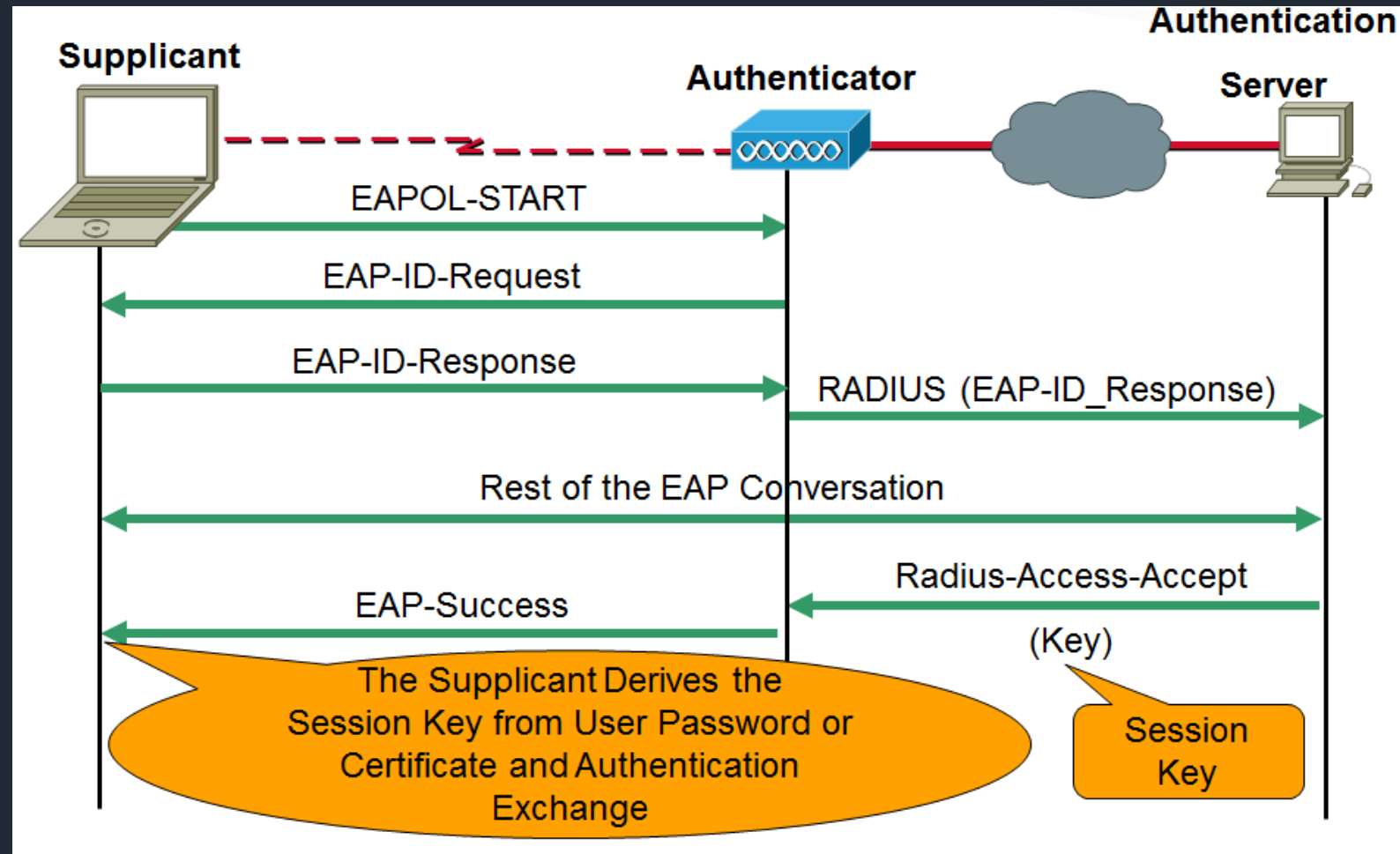
3. Seguridad :: Cifrado de datos – EAP/PEAP

- 1.EAP usa pass/cert por usuario, NO global
- 2.AD,Radius,Tacacs+,WiFi Controller,...
- 3.Primerá comprobación AP/Server->Client*
- 4.Luego Cliente contra el Servidor**
- 5.EAP se implementa EAP/CHAP2,PEAP/TLS,...
- 6.Hotspot WiFi, Portal cautivo
- 7.Cada usuario usa SU cifrado

* AP/Server(PEAP) comprueba que PC ID está OK para dar acceso a red. NO IP

** Usuario/Password o certificado del cliente.

3. Seguridad :: Cifrado de datos - EAP



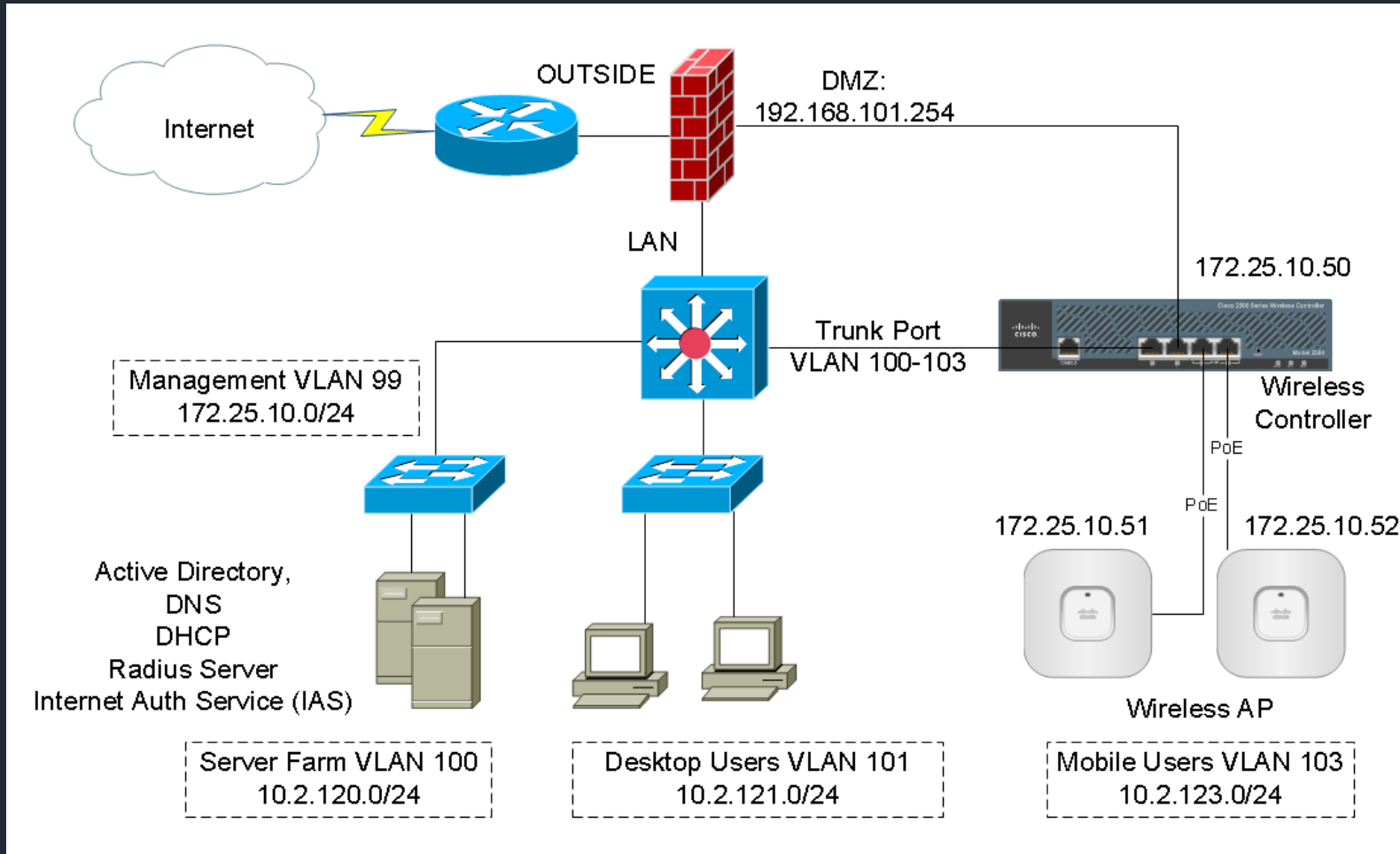
3. Seguridad :: Cifrado de datos - Krack

1. NO usar WPA2 AES+TKIP NUNCA!
2. Actualizar firmware Clientes y APs
3. Con WPA-TKIP o GCMP hay Packet Injection
4. Aprovecha fallo en 4-way Handshake
5. Sustituye las claves, NO las recupera
6. Problema en clientes, actualizar
7. EAP es inmune
8. Si EAP comprometido, solo ese usuario

3. Seguridad :: Usuarios/Control de acceso 802.11X

1. Control de acceso al medio físico
2. Implementado con Server Radius/IAS
3. Recomendando Zeroshell+Zerotruth, W2012/6
4. Implementar en switches y APs
5. Desactivar bocas no usadas de switch
6. Usuario/Contraseña o Certificado
7. Verificación acceso a red, NAC/NPS
8. Accounting

3. Seguridad :: Usuarios/Control de acceso



Protected EAP Properties

When connecting:

- ☒ Verify the server's identity by validating the certificate
- ☒ Connect to these servers (examples: srv1;srv2;.*\srv3\com):
nowiressecurity.com

Trusted Root Certification Authorities:

- ☐ GlobalSign
- ☐ GlobalSign Root CA
- ☐ Go Daddy Class 2 Certification Authority
- ☒ Go Daddy Root Certificate Authority - G2
- ☐ GTE CyberTrust Global Root
- ☐ Hotspot 2.0 Trust Root CA - 03
- ☐ Microsoft Root Authority

Notifications before connecting:

Don't ask user to authorize new servers or trusted CAs

Select Authentication Method:

Secured password (EAP-MSCHAP v2) Configure...

- ☒ Enable Fast Reconnect
- ☐ Disconnect if server does not present cryptobinding TLV
- ☐ Enable Identity Privacy

OK Cancel

3. Seguridad :: Cifrado de datos – Zeroshell + Zerotruth

Browser window showing the Zeroshell Net Services interface. The URL is https://192.168.0.254/. The interface includes a sidebar with navigation links (SYSTEM, USERS, NETWORK, SECURITY, ToDo List) and a main content area with tabs for NET BALANCER, Manage, Balancing Rules, and Statistics. The NET BALANCER tab is active, showing a table of gateways and a failover monitor section.

NET BALANCER

Status: **ACTIVE** Mode: Load Balancing and Failover

Gateway List: 5

Gateway Description	IP Address	Interface	Weight	Status	Faults	UP
DEFAULT GATEWAY			1	Disabled	0	<input type="checkbox"/>
Infostrada ADSL	192.168.1.254		7	Active	0	<input checked="" type="checkbox"/>
TIM Mobile		ppp0	1	Disabled	1	<input type="checkbox"/>
WIND Mobile		ppp1	1	Active	1	<input checked="" type="checkbox"/>
TRE Mobile		ppp2	1	Active	1	<input checked="" type="checkbox"/>

Failover Monitor Status: Active

ICMP failover checking: Enabled

Number of probes before marking DOWN: 3

Number of probes before marking UP: 5

Reply timeout (seconds): 4

Pause before starting a new cycle (seconds): 5

Oct 19 19:06,56 SUCCESS: Session opened from host 192.168.22.100 (Admin)
Oct 19 19:11,34 SUCCESS: Failover process has been tested. View NetBalancer logs for details.

Browser window showing the ZeroTruth interface. The URL is https://192.168.0.254/. The interface includes a sidebar with navigation links (User List, Add User, Classes, Email, SMS, Config, Esc) and a main content area with a table of registered users.

ZeroTruth
Interface For Zeroshell Captive Portal

Registered Users

N.	S.	Room	Username	Name	Surname	Email	Telephone	Up To	S.	I.	Actions
1	0	5A	bobby	Bob	Green	bob@green.com	3954678945	18/06/2015	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	0	1F	frank	Frank	Zappa	frank@zappa.com	39123654366	No limit	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	0	1B	john	John	Brown	johnbrown@example.net	393456478987	No limit	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	0	1A	kpjifs	Bob	Dylan	bob@dylan.org	3712346543	16/03/2013	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
				Trut	Hahn	nello@zerotruth.net	39333987654678	No limit	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
				pipo	top			No limit	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
				trut	hahn	truthahn@zerotruth.net	3933935765543	27/11/2012	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Copyright (C) 2012 truthahn v 0.8

ZeroTruth hot spot login page. The page includes a header with the ZeroTruth logo and a sidebar with navigation links (User List, Add User, Classes, Email, SMS, Config, Esc). The main content area contains a login form with fields for Username, Password, and Dominio (example.com). Below the form is a button labeled "Accesso alla rete".

ZeroTruth
Interface For Zeroshell Captive Portal

ZeroTruth hot spot

Username:

Password:

Dominio:

[Accesso alla rete](#)

[Info](#) - [Registrazione](#) - [Password dimenticata?](#)

Powered by Zeroshell & ZeroTruth

3. Seguridad :: Rogue APs/Paranoia

1. Filtrado MAC (fácil hacer spoofing)
2. APs para detectar Rogue APs
3. Deshabilitar conexión automática clients
4. Deshabilitar acceso APs (VLAN gestión)
5. Acceso vía HTTPS/SSH, fuera TR69 en CPE
6. Implementar WIPS/WIDS
7. PROXY/AntiMalware integrado
8. IPs estáticas/DHCP con reserva/DNS
9. Seguridad física/Acceso físico/Pintura

7. El mejor consejo es ...



Regla de la precisión: “Medir con micrómetro, marcar con tiza, cortar con hacha”

- Usar conexiones cableadas siempre que sea posible.
- Usar nuestra conexión LTE preferentemente a un Wifi público
- No “robar” el WiFi al vecino, nos puede troleear o algo peor
- Cifrar todo nuestro tráfico y tener un servidor VPN para conexiones remotas
- Configurar el WiFi como un BOFH
- Tener una política de caducidad de claves/certificados
- Monitorizar, revisar logs, repetir

7. That's all Folks!

