

EINRICHTUNG EINES GÄSTE WLANS AUF EINER DIGITALISIERUNGSBOX

Basierend auf der Grundeinrichtung durch den Schnellstartassistenten



ERLEBEN, WAS VERBINDET.

1. VORBEMERKUNG

Wenn Sie Ihren Gästen Internetzugang zur Verfügung stellen, haften Sie ggf. nach der momentan vorliegenden Rechtsprechung für begangene Rechtsverstöße (z.B. Urheberrecht) Ihrer Gäste!

Ziel dieser Ausarbeitung ist die Beschreibung der Einrichtung eines Gäste WLANs ausgehend von der Konfiguration, welche nach Durchlauf des Schnellstartassistenten mit aktiviertem WLAN vorliegt.

Die angeführten Menüpunkte sind ggf. nur in der Ansicht „Vollzugriff“ zu erreichen.

Da beide SSIDs, das interne WLAN und das Gäste WLAN, auf dem gleichen Funkmodul „ausgestrahlt“ werden, sind natürlich auch die Einstellungen des Funkmoduls identisch und sehen nach der Inbetriebnahme durch den Schnellstartassistenten folgendermaßen aus:

The screenshot shows a web-based configuration interface for a wireless network. On the left is a navigation menu with the following items: **Konfiguration speichern**, Assistenten, Systemverwaltung, Physikalische Schnittstellen, VoIP, Nummerierung, Endgeräte, Anrufkontrolle, Anwendungen, LAN, **Wireless LAN**, **WLAN** (highlighted in pink), Verwaltung, Wireless LAN Controller, Netzwerk, and Multicast. The main content area is titled **Einstellungen Funkmodul Drahtlosnetzwerke (VSS)**. It contains a table of settings:

WLAN-Einstellungen	
Betriebsmodus	Access-Point
Frequenzband	2,4 GHz In/Outdoor
Kanal	Auto
Ausgewählter Kanal	8
Anzahl der Spatial Streams	2
Sendeleistung	Max.
Performance-Einstellungen	
Drahtloser Modus	802.11g/n
Airtime Fairness	<input checked="" type="checkbox"/> Aktiviert

At the bottom of the settings area, there is a link for **Erweiterte Einstellungen** and two buttons: **OK** and **Abbrechen**.

Werden hier Änderungen durchgeführt (wie z.B. die Umschaltung von 2.4 auf 5 GHz), dann wirken sich diese auch auf beide ausgestrahlten SSIDs aus!



2. ERSTELLUNG DER SSID

Fügen Sie unter: → Wireless LAN → WLAN →
Registerkarte „Drahtlosnetzwerke (VSS)“

mit „Neu“ ein weiteres VSS (Virtual Service Set)
hinzu (vss7-10 existiert schon):

Einstellungen Funkmodul **Drahtlosnetzwerke (VSS)**

Drahtlosnetzwerke (VSS)

VSS-Beschreibung	Netzwerkname (SSID)	MAC-Adresse	Sicherheit	Status	Aktion		
vss7-10	WLAN_intern	00:09:4f:6f:3a:3b	WPA-PSK	+	↑ ↓	🗑️	🔗

Neu

2. ERSTELLUNG DER SSID

Es öffnet sich das Konfigurationsmenü mit den Einstellungen für diese SSID.

Bitte setzen Sie den Namen der SSID und den Preshared Key!

Ebenso entfernen Sie die Haken bei „Intra-cell Repeating“ (Gäste können nicht untereinander kommunizieren) und „U-APSD“ (verlängert bei bestimmten Geräten die Laufzeit für VoWLAN) und setzen den „Sicherheitsmodus“ und den „WPA-Modus“ entsprechend.

Bitte beachten Sie, dass bei „WPA2“ die „WPA Cipher“ lt. Standard auf „AES“ gestellt wird, die Option „AES und TKIP“ stellt lediglich einen Kompromiss dar und wird nicht von allen Herstellern unterstützt.

Im vorliegenden Beispiel wurde die maximal mögliche Anzahl der Clients auf 10 begrenzt und jedem Client in Sende- und Empfangsrichtung nur max. 1 MBit/s (brutto) zugeteilt, um ggf. eine Auslastung der WAN-Anbindung durch einen einzelnen Client zu vermeiden.

Diese Werte können gerne an die eigenen Anforderungen und Gegebenheiten angepasst werden.

Einstellungen Funkmodul Drahtlosnetzwerke (VSS)

Ändern Sie unbedingt den Standard Preshared Key! Solange der Key nicht geändert wurde, ist ihr Gerät nicht gegen einen unautorisierten Zugriff geschützt!

Service Set Parameter	
Netzwerkname (SSID)	Guests_bintec-elmeg <input checked="" type="checkbox"/> Sichtbar
Intra-cell Repeating	<input type="checkbox"/> Aktiviert
U-APSD	<input type="checkbox"/> Aktiviert
Sicherheitseinstellungen	
Sicherheitsmodus	WPA-PSK
WPA-Modus	WPA 2
WPA2 Cipher	<input checked="" type="radio"/> AES <input type="radio"/> AES und TKIP
Preshared Key
Client-Lastverteilung	
Max. Anzahl Clients - Hard Limit	10
Max. Anzahl Clients - Soft Limit	10
Auswahl des Client-Bands	Deaktiviert, optimiert für Fast Roaming
MAC-Filter	
Zugriffskontrolle	<input type="checkbox"/> Aktiviert
Bandbreitenbeschränkung für jeden WLAN-Client	
Rx Shaping	1 Mbit/s
Tx Shaping	1 Mbit/s

Erweiterte Einstellungen

OK Abbrechen

2. ERSTELLUNG DER SSID

Danach ist die Definition abgeschlossen und die zusätzliche SSID steht als virtuelle Schnittstelle „vss7-11“ zur Verfügung.

Einstellungen Funkmodul **Drahtlosnetzwerke (VSS)**

Drahtlosnetzwerke (VSS)

VSS-Beschreibung	Netzwerkname (SSID)	MAC-Adresse	Sicherheit	Status	Aktion		
vss7-10	WLAN_intern	00:09:4f:6f:3a:3b	WPA-PSK	↑	↑ ↓	🗑️	🔧
vss7-11	Guests_bintec-elemg	02:09:4f:6f:3a:3b	WPA-PSK	↑	↑ ↓	🗑️	🔧

Neu

3. KONFIGURATION EINER IP ADRESSE AUF VSS7-11

Im nächsten Schritt wird der (virtuellen Schnittstelle) „vss7-11“ des Gäste WLANs eine IP-Adresse konfiguriert und der Schnittstellenstatus auf „Nicht vertrauenswürdig“ gesetzt.

Durch diesen Status sind erst einmal keine initialen Anfragen von dieser Schnittstelle erlaubt, das wird später in der Stateful Inspection Firewall (SIF) entsprechend konfiguriert.

Menü: → LAN → IP-Konfiguration → Registerkarte „Schnittstellen“

Öffnen Sie mit dem Edit Button das Konfigurationsmenü und vergeben die IP-Adresse und Netzwerkmaske sowie die Sicherheitsrichtlinie:

The screenshot shows a table titled 'Schnittstellen' with the following data:

Schnittstelle	IPv4-Adresse/Netzmaske	IPv6-Adresse/Länge	Status	Aktion
en1-4(VLAN-ID7)	Nicht konfiguriert/Nicht konfiguriert	-	⊖	⬆️⬇️⬆️
efm35-60(VLAN-ID7)	Nicht konfiguriert/Nicht konfiguriert	-	⊕	⬆️⬇️⬆️
en1-3	██████████ 255.255.255.0	Präfix: Germany - Telekom Entertain:0 Host: eui64	⊕	⬆️⬇️⬆️
ethoa35-5(VLAN-ID7)	Nicht konfiguriert/Nicht konfiguriert	-	⊖	⬆️⬇️⬆️
br0(VLAN-ID1)	██████████ 255.255.255.0	Präfix: Germany - Telekom Entertain:1 Host: eui64	⊕	⬆️⬇️⬆️
vss7-11	Nicht konfiguriert/Nicht konfiguriert	-	⊕	⬆️⬇️⬆️

The 'vss7-11' row is highlighted in yellow, and its edit icon (a pencil) is circled in red. A 'Neu' button is visible at the bottom of the table.

The screenshot shows the configuration page for the 'vss7-11' interface. The 'Schnittstellenmodus' is set to 'Untagged'. The 'Sicherheitsrichtlinie' is set to 'Nicht Vertrauenswürdig'. The 'Adressmodus' is set to 'Statisch'. The 'IP-Adresse / Netzmaske' field is filled with '192.168.3.1' and '255.255.255.0'. The 'IPv6' checkbox is checked.

Nach der Bestätigung mit „OK“ ist diese IP Adresse nun für die Schnittstelle vss7-11 des Gäste WLANs der Digitalisierungsbox konfiguriert.

4. DHCP SERVER FÜR GÄSTE WLAN EINRICHTEN UND AKTIVIEREN

Im nächsten Step muss nun ein DHCP-Pool erstellt werden, der zu dem Netzwerk der Schnittstelle vss7-11 passt (Im Beispiel aus dem Netz 192.168.3.0/24).

Menü: → Lokale Dienste → DHCP-Server → Registerkarte „IP-Pool-Konfiguration“ → „Neu“

The screenshot shows a configuration window with four tabs: IP-Pool-Konfiguration (selected), DHCP-Konfiguration, IP/MAC-Bindung, and DHCP-Relay-Einstellungen. The IP-Pool-Konfiguration tab contains a table with the following data:

Basisparameter	
IP-Poolname	Gast-Pool
IP-Adressbereich	192.168.3.100 - 192.168.3.109
DNS-Server	Primär: 8.8.8.8
	Sekundär: 8.8.4.4

At the bottom of the window are two buttons: OK and Abbrechen.

Als DNS-Server sind hier die beiden DNS-Server von Google angegeben und werden entsprechend via DHCP verteilt. Dies verhindert evtl. DNS Attacken der angeschlossenen Clients. Sollte das nicht gewünscht sein, bitte leer lassen (DB verteilt sich selber als DNS) und unter Punkt 5 eine zusätzliche Regel für DNS erstellen (analog zur Regel für DHCP).

Nun wird der soeben erstellte Pool der Schnittstelle zur Verteilung der Adressen zugeordnet und bei Bedarf zusätzliche DHCP-Optionen definiert. Im Beispiel ist das ein Zeitserver, es wird der interne Zeitserver der Digitalisierungsbox angegeben.

4. DHCP SERVER FÜR GÄSTE WLAN EINRICHTEN UND AKTIVIEREN

Menü: → Lokale Dienste → DHCP-Server → Registerkarte „DHCP-Konfiguration“ → „Neu“

IP-Pool-Konfiguration **DHCP-Konfiguration** IP/MAC-Bindung DHCP-Relay-Einstellungen

Basisparameter

Schnittstelle	vss7-11
IP-Poolname	Gast-Pool
Pool-Verwendung	Lokal

Erweiterte Einstellungen:

Gateway	Router als Gateway verwenden				
Lease Time	120 Minuten				
DHCP-Optionen	<table><thead><tr><th>Option</th><th>Wert</th></tr></thead><tbody><tr><td>Zeitserver</td><td>192.168.3.1</td></tr></tbody></table> <input type="button" value="Hinzufügen"/>	Option	Wert	Zeitserver	192.168.3.1
Option	Wert				
Zeitserver	192.168.3.1				

Mit Bestätigung durch „OK“ steht jetzt der Pool zur Verfügung!

Für eine kurzzeitige Deaktivierung kann die DHCP-Server Rolle auf dem Interface auch temporär durch das Entfernen des Hakens bei „aktiviert“ und Bestätigung mit „OK“ entfernt werden.

IP-Pool-Konfiguration **DHCP-Konfiguration** IP/MAC-Bindung DHCP-Relay-Einstellungen

Ansicht 20 pro Seite << >> Filtern in Keiner gleich

Schnittstelle	IP-Poolname	Gateway	Lease Time	Status		
br0	DHCP Adressbereich	Router als Gateway verwenden	120Min.	<input checked="" type="checkbox"/> Aktiviert	<input type="button" value="Löschen"/>	<input type="button" value="Aktivieren"/>
vss7-11	Gast-Pool	Router als Gateway verwenden	120Min.	<input checked="" type="checkbox"/> Aktiviert	<input type="button" value="Löschen"/>	<input type="button" value="Aktivieren"/>

Seite: 1, Objekte: 1 - 2

5. ERSTELLUNG DER FIREWALL REGELN FÜR INTERNETZUGRIFF VOM GÄSTE WLAN

Durch das Standardverhalten der Stateful Inspection Firewall und die Klassifizierung von vss7-11 als „Nicht vertrauenswürdig“ (siehe Punkt 3) sind initiale Anfragen über diese Schnittstelle zuerst verboten und werden geblockt. Das muss mit zwei Regeln noch angepasst werden.

Als erste Regel wird der DHCP Request der Clients dieses WLANs zugelassen.

Da ein Gäste WLAN normalerweise nur Zugriff auf das Internet bekommen soll, wird in diesem Beispiel mit der zweiten Regel auch nur dieses für die bereits vordefinierte Dienstegruppe „Internet“ (Gruppierung der gängigsten Services für den Internetzugriff wie z.B. http, https, POP3, IMAP, SMTP, ...) zugelassen.

Menü: → Firewall → Richtlinien → Registerkarte „IPv4-Filterregeln“ → „Neu“

IPv4-Filterregeln IPv6-Filterregeln Optionen

Basisparameter	
Quelle	WLAN_VSS7-11
Ziel	LAN_LOCAL
Dienst	dhcp
Aktion	Zugriff

OK Abbrechen

5. ERSTELLUNG DER FIREWALL REGELN FÜR INTERNETZUGRIFF VOM GÄSTE WLAN

Mit der jeweiligen Bestätigung durch „OK“ ist auch dieser Schritt abgeschlossen.

Sollen der Dienstgruppierung „Internet“ noch weitere Services hinzugefügt werden, so sind diese ggf. in den Diensten der Firewall noch zu definieren und der Gruppe „Internet“ hinzuzufügen.

Da IPv6 auf vss7-11 nicht aktiviert wurde muss hier auch nichts in den entsprechenden Sektionen konfiguriert werden.

Nach einem Test sollte nun die vorgenommene Konfiguration noch bootfest gespeichert werden:

Konfiguration speichern

IPv4-Filterregeln IPv6-Filterregeln Optionen

Basisparameter	
Quelle	WLAN_VSS7-11
Ziel	WAN_DTAG_VDSL50_ALL-IP
Dienst	Internet
Aktion	Zugriff

OK Abbrechen