

Access convergé a consolidé la référence rapide pour les modèles Sans fil de RÉSEAU LOCAL

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Degré de sécurité de la couche 2](#)

[OUVREZ le WLAN aucune Sécurité](#)

[Confidentialité équivalente aux transmissions par fil \(WEP\) statique](#)

[Filtre d'adresses MAC - Base de données locale](#)

[Filtre d'adresses MAC - Rayon externe](#)

[Clé pré-partagée Sans fil du Protected Access 2 \(WPA2\) \(PSK\)](#)

[authentification locale de Protocole EAP \(Extensible Authentication Protocol\) de 802.1x \(NGWC utilisés en tant que RAYON local\)](#)

[802.1x sur le rayon externe](#)

[Degré de sécurité de la couche 3](#)

[Fonction émulation de Web](#)

[Authentification locale d'authentification Web](#)

[Authentification Web avec l'authentification externe de RAYON \(ISE\)](#)

[Authentification de Web externe](#)

[Authentification Web personnalisée avec l'authentification locale](#)

[Authentification Web automatique d'ancre](#)

Introduction

Ce document fournit des modèles de configuration CLI de référence rapide pour des configurations Sans fil du RÉSEAU LOCAL de base et connu de la couche 2 et de la couche 3 (WLAN). Des modèles de base sont donnés pour une copie rapide et les collent dans l'armoire de câblage de nouvelle génération de Cisco installations initiales Sans fil de client (NGWC) 5760 et 3850 récréations de laboratoire du contrôleur LAN (WLC) et.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance de version 3.3 NGWC ou de plus tard. On le

prévoit que Switch Virtual Interfaces (SVI) et des pools DHCP/pillant sont préconfigurés par pratiques recommandées.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Degré de sécurité de la couche 2

OUVREZ le WLAN aucune Sécurité

```
wlan 1 name testwlan ssid testwlan
  client vlan 20
  no security wpa
  no shut
```

Confidentialité équivalente aux transmissions par fil (WEP) statique

```
wlan staticWEP 6 staticWEP
  client vlan 79
  no security wpa
  no security wpa akm dot1x
  no security wpa wpa2
  no security wpa wpa2 ciphers aes
  security static-wep-key encryption 40 ascii 0 Cisco 1
  session-timeout 1800
  no shutdown
```

Filtre d'adresses MAC - Base de données locale

```
username 24770319eB75 mac
```

```
aaa new-model
aaa authorization network test_mac local
```

```
wlan macfiltering 6 macfiltering
  client vlan Vlan7
  mac-filtering test_mac
  no security wpa
  no security wpa akm dot1x
  no security wpa wpa2
  no security wpa wpa2 ciphers aes
  no shutdown
```

Filtre d'adresses MAC - Rayon externe

```
aaa new-model
aaa group server radius wcm_rad

server name RAD_EXT
subscriber mac-filtering security-mode mac
mac-delimiter colon

radius server RAD_EXT
address ipv4 x.x.x.x auth-port 1812 acct-port 1813
key cisco

aaa authorization network wcm_macfilter group wcm_rad

wlan macfiltering 1 macfiltering
client vlan Vlan7
mac-filtering wcm_macfilter
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
no shutdown
```

Clé pré-partagée Sans fil du Protected Access 2 (WPA2) (PSK)

```
wlan wpa2psk 1 wpa2psk
client vlan 20
no security wpa akm dot1x
security wpa akm psk set-key ascii 0 Cisco123
no shutdown
```

authentification locale de Protocole EAP (Extensible Authentication Protocol) de 802.1x (NGWC utilisés en tant que RAYON local)

```
user-name test
privilege 15
password 0 cisco
type network-user description pass=cisco
aaa new-model
aaa authentication dot1x default local
aaa authorization credential-download author_list local
aaa authentication dot1x authen_list local
aaa local authentication authen_list authorization author_list
dot1x system-auth-control
eap profile PEAPProfile
method ?
fast      EAP-FAST method allowed
gtc       EAP-GTC method allowed
leap      EAP-LEAP method allowed
md5       EAP-MD5 method allowed
mschapv2  EAP-MSCHAPV2 method allowed
peap      EAP-PEAP method allowed
tls       EAP-TLS method allowed

method peap
method mschapv2
```

```
wlan TestNGWC 1 TestNGWC
  client vlan VLAN0080
  ip dhcp server 192.168.80.14
  local-auth PEAPProfile
```

802.1x sur le rayon externe

```
user-name test
  privilege 15
  password 0 cisco
  type network-user description pass=cisco
aaa new-model
aaa authentication dot1x default local
aaa authorization credential-download author_list local
aaa authentication dot1x authen_list local
aaa local authentication authen_list authorization author_list
dot1x system-auth-control
eap profile PEAPProfile
method ?
  fast      EAP-FAST method allowed
  gtc       EAP-GTC method allowed
  leap      EAP-LEAP method allowed
  md5       EAP-MD5 method allowed
  mschapv2  EAP-MSCHAPV2 method allowed
  peap      EAP-PEAP method allowed
  tls       EAP-TLS method allowed
```

```
method peap
method mschapv2
wlan TestNGWC 1 TestNGWC
  client vlan VLAN0080
  ip dhcp server 192.168.80.14
  local-auth PEAPProfile
```

Degré de sécurité de la couche 3

Fonction émulation de Web

```
user-name test
  privilege 15
  password 0 cisco
  type network-user description pass=cisco
aaa new-model
aaa authentication dot1x default local
aaa authorization credential-download author_list local
aaa authentication dot1x authen_list local
aaa local authentication authen_list authorization author_list
dot1x system-auth-control
eap profile PEAPProfile
method ?
  fast      EAP-FAST method allowed
  gtc       EAP-GTC method allowed
  leap      EAP-LEAP method allowed
  md5       EAP-MD5 method allowed
  mschapv2  EAP-MSCHAPV2 method allowed
  peap      EAP-PEAP method allowed
```

```
tls          EAP-TLS method allowed

method peap
method mschapv2
wlan TestNGWC 1 TestNGWC
client vlan VLAN0080
ip dhcp server 192.168.80.14
local-auth PEAPProfile
```

Authentification locale d'authentification Web

```
user-name test
  privilege 15
  password 0 cisco
  type network-user description pass=cisco
aaa new-model
aaa authentication dot1x default local
aaa authorization credential-download author_list local
aaa authentication dot1x authen_list local
aaa local authentication authen_list authorization author_list
dot1x system-auth-control
eap profile PEAPProfile
method ?
  fast      EAP-FAST method allowed
  gtc       EAP-GTC method allowed
  leap      EAP-LEAP method allowed
  md5       EAP-MD5 method allowed
  mschapv2  EAP-MSCHAPV2 method allowed
  peap      EAP-PEAP method allowed
  tls       EAP-TLS method allowed
```

```
method peap
method mschapv2
wlan TestNGWC 1 TestNGWC
client vlan VLAN0080
ip dhcp server 192.168.80.14
local-auth PEAPProfile
```

Authentification Web avec l'authentification externe de RAYON (ISE)

```
user-name test
  privilege 15
  password 0 cisco
  type network-user description pass=cisco
aaa new-model
aaa authentication dot1x default local
aaa authorization credential-download author_list local
aaa authentication dot1x authen_list local
aaa local authentication authen_list authorization author_list
dot1x system-auth-control
eap profile PEAPProfile
method ?
  fast      EAP-FAST method allowed
  gtc       EAP-GTC method allowed
  leap      EAP-LEAP method allowed
  md5       EAP-MD5 method allowed
  mschapv2  EAP-MSCHAPV2 method allowed
  peap      EAP-PEAP method allowed
  tls       EAP-TLS method allowed
```

```
method peap
method mschapv2
wlan TestNGWC 1 TestNGWC
client vlan VLAN0080
ip dhcp server 192.168.80.14
local-auth PEAPProfile
```

Authentification de Web externe

```
user-name test
privilege 15
password 0 cisco
type network-user description pass=cisco
aaa new-model
aaa authentication dot1x default local
aaa authorization credential-download author_list local
aaa authentication dot1x authen_list local
aaa local authentication authen_list authorization author_list
dot1x system-auth-control
eap profile PEAPProfile
```

method ?

```
fast      EAP-FAST method allowed
gtc       EAP-GTC method allowed
leap      EAP-LEAP method allowed
md5       EAP-MD5 method allowed
mschapv2  EAP-MSCHAPV2 method allowed
peap      EAP-PEAP method allowed
tls       EAP-TLS method allowed
```

```
method peap
method mschapv2
wlan TestNGWC 1 TestNGWC
client vlan VLAN0080
ip dhcp server 192.168.80.14
local-auth PEAPProfile
```

Authentification Web personnalisée avec l'authentification locale

```
ip http server
ip device tracking
```

```
aaa new-model
aaa authentication login local_webauth local
aaa authorization network default local
aaa authorization credential-download default local
```

```
username <username> password 0 <password>
```

FTP Configuration for file transfer:

```
ip ftp username <username>
ip ftp password <password>
```

Upload custom html files to flash: with command:

```
5760# copy ftp://x.x.x.x/webauth_login.html flash:
```

Example of flash content:

w-5760-2#dir flash:

Directory of flash:/

```
64649 -rw-      1164   Oct 7 2013 04:36:23 +00:00  webauth_failure.html
64654 -rw-      2047   Oct 7 2013 13:32:38 +00:00  webauth_login.html
64655 -rw-      1208   Oct 7 2013 04:34:12 +00:00  webauth_success.html
64656 -rw-       900   Oct 7 2013 04:35:00 +00:00  webauth_expired.html
64657 -rw-     96894   Oct 7 2013 05:05:09 +00:00  web_auth_logo.png
64658 -rw-     23037   Oct 7 2013 13:17:58 +00:00  web_auth_cisco.png
64660 -rw-      2586   Oct 7 2013 13:31:27 +00:00  web_auth_aup.html
```

```
parameter-map type webauth global
virtual-ip ipv4 1.1.1.1
```

```
parameter-map type webauth custom
type webauth
redirect on-success http://www.cisco.com
banner text ^C CC global ip for redirect ^C
custom-page login device flash:webauth_login.html
custom-page success device flash:webauth_success.html
custom-page failure device flash:webauth_failure.html
custom-page login expired device flash:webauth_expired.html
```

```
wlan cisco 1 cisco
client vlan Vlanx
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list local_webauth
security web-auth parameter-map custom
session-timeout 1800
no shutdown
```

Authentification Web automatique d'ancre

```
//Verify//
```

```
show wireless mobility summary
```

```
<snip>
```

IP	Public IP	Group Name	Multicast IP	Link Status
192.168.100.8	-	ngwc	0.0.0.0	UP : UP
192.168.100.15	192.168.100.15	5760		UP : UP

```
radius server ise
address ipv4 192.168.154.119 auth-port 1812 acct-port 1813
key Cisco123
aaa group server radius rad_ise
server name ise
```

```
aaa authentication login ext_ise group rad_ise
parameter-map webauth global
virtual-ip ipv4 1.1.1.1
parameter-map type webauth test_web
type webauth
```

banner

WLAN configs on the Foreign 5760

```
wlan ngwc_guest 3 ngwc_guest
  client vlan 254
  mobility anchor 192.168.100.8 //Anchor
  no security wpa
  no security wpa akm dot1x
  no security wpa wpa2
  no security wpa wpa2 ciphers aes
  security web-auth
  security web-auth authentication-list wcm_local
  security web-auth parameter-map test_web
  no shutdown
```

WLAN configs on the Anchor 5760

```
wlan ngwc_guest 3 ngwc_guest
  client vlan 254
  mobility anchor 192.168.100.8 //Local
  no security wpa
  no security wpa akm dot1x
  no security wpa wpa2
  no security wpa wpa2 ciphers aes
  security web-auth
  security web-auth authentication-list rad_ise
  security web-auth parameter-map test_web
  no shutdown
```