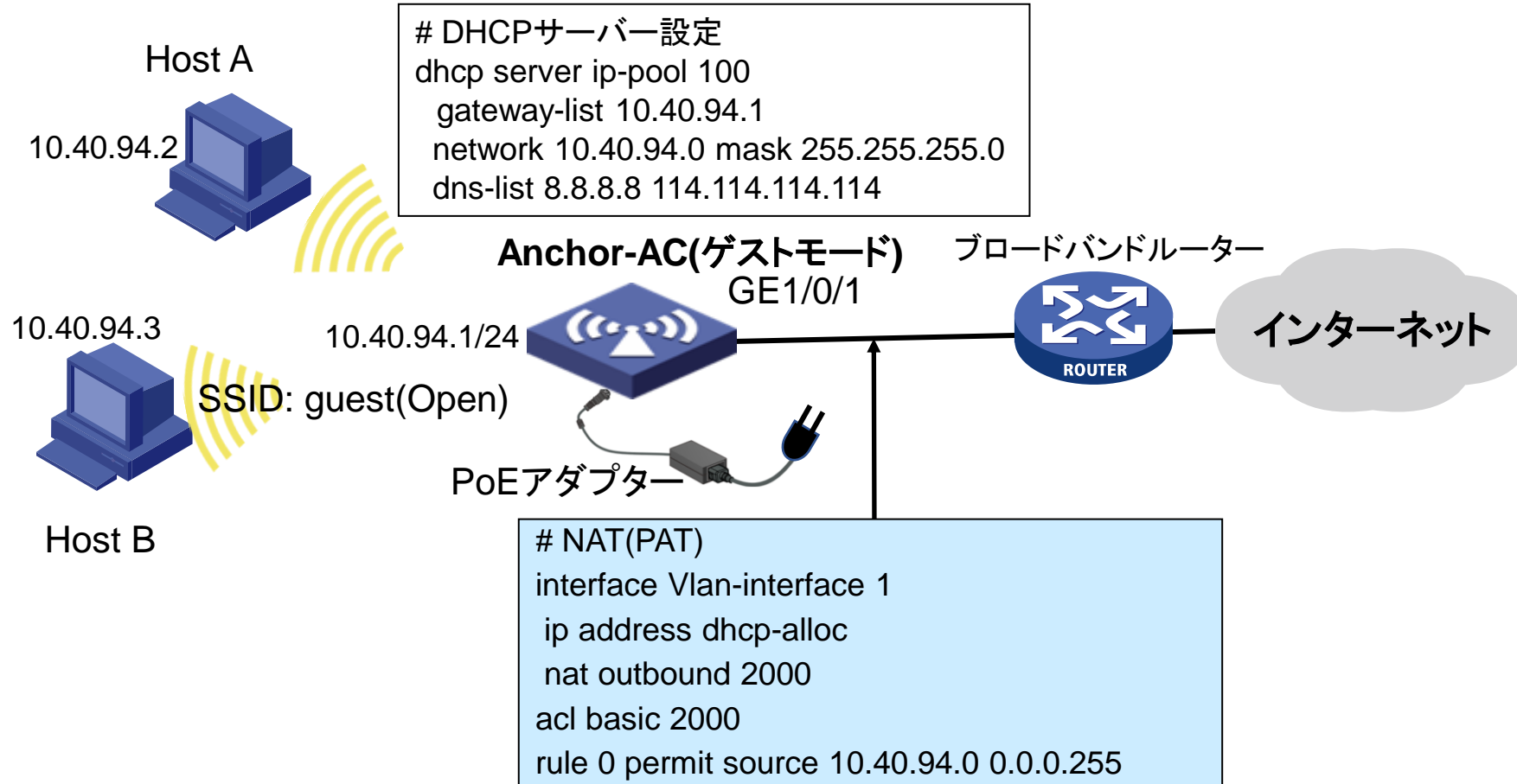




H3C Anchor-ACゲストモードベストプラクティスガイド

ゲスト(オープン認証)





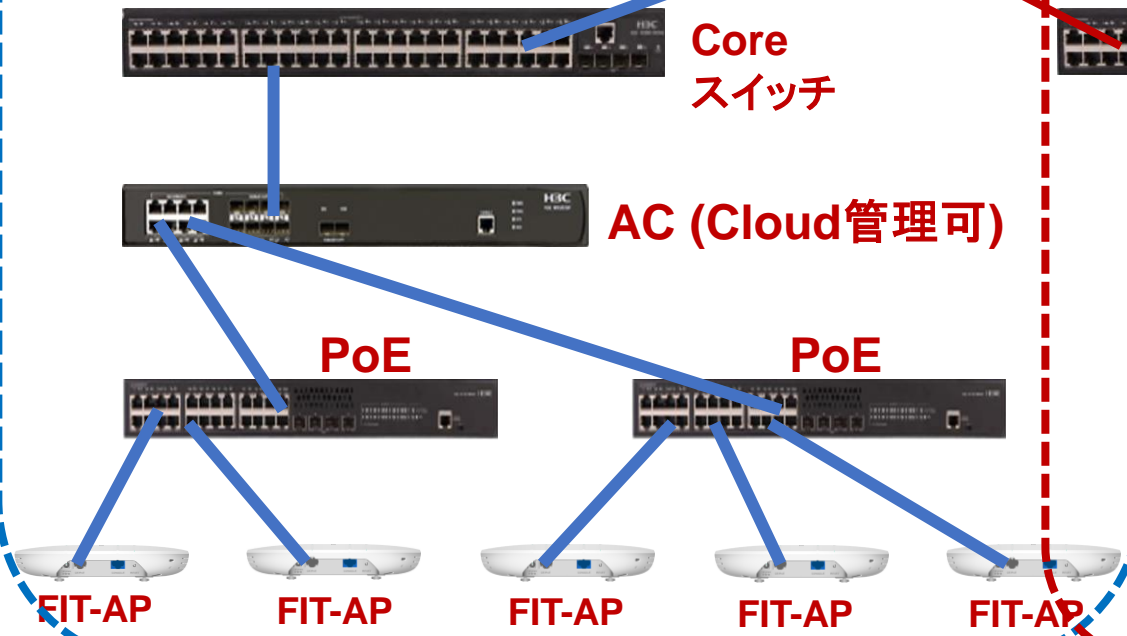
- 01 アクセスポイントをAnchor-acに設定する
- 02 Anchor-acをゲストモードにする
- 03 動作確認
- 04 完成した設定のコマンド
- 05 オプション:クライアントのAP接続の最適化
- 06 トラブルシューティング
- 07 アップリンクにある装置へのアクセス制限
- 08 マニュアルについて

アクセスポイントの動作モードの違い

アクセスポイントの動作モードには **FIT**、**Cloud**、**Anchor-ac**の3通りがあります。

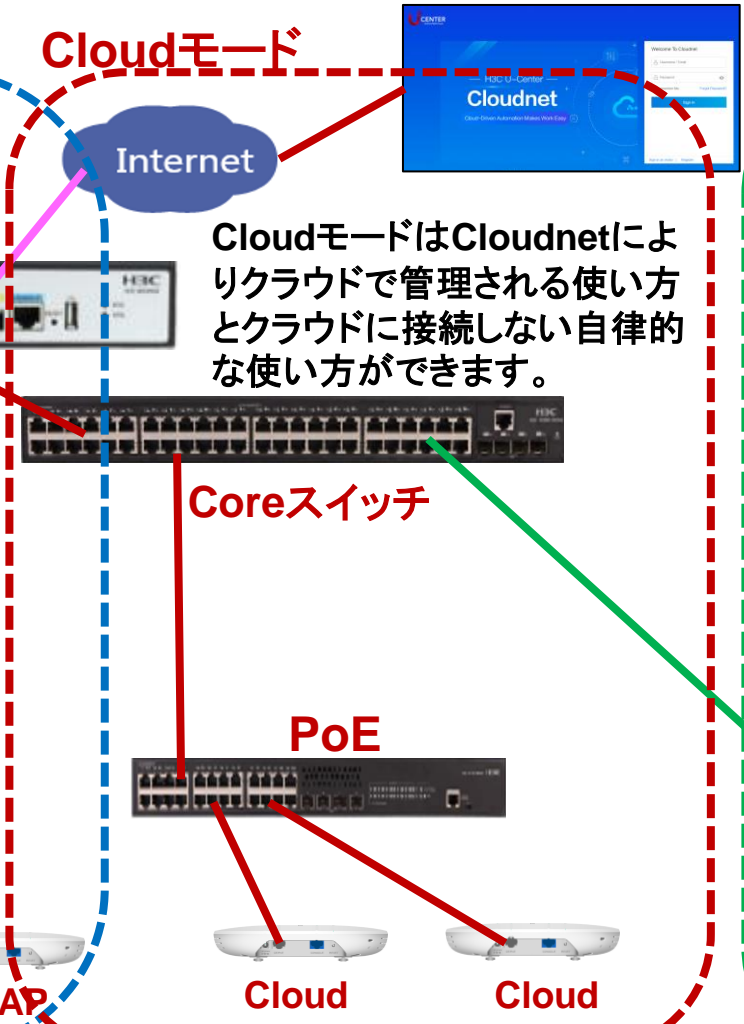
FITモード

FIT-APはACのGUI又はCLIで管理するので、**FIT-APを単体でGUI又はCLIで管理することはできません**。またFIT-APはACとの接続が切れると**ACを探してリブートを繰り返します**。



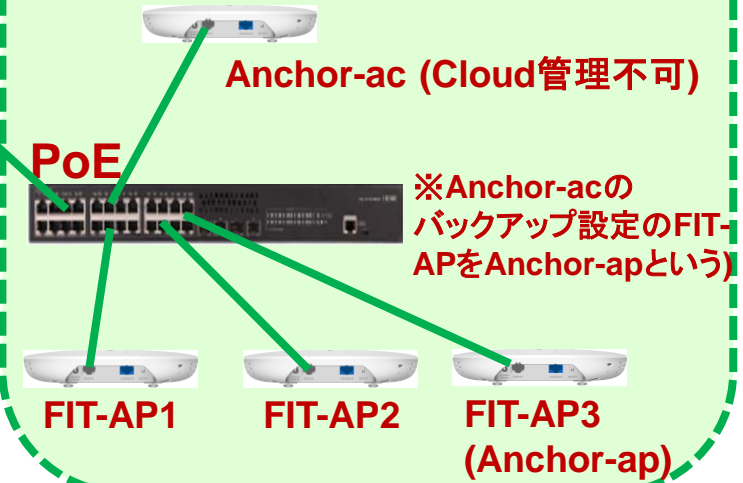
Cloudモード

CloudモードはCloudnetによりクラウドで管理される使い方とクラウドに接続しない自律的な使い方ができます。



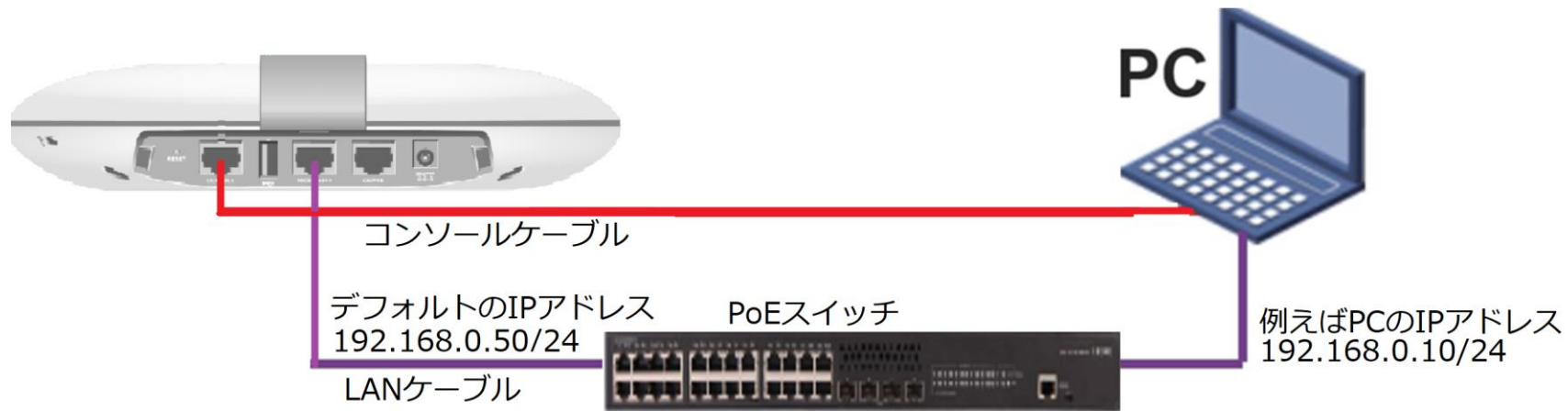
Anchor-acモード

Anchor-ACは簡易的なACの機能を持ち複数のFIT-APを管理することができます。Anchor-ACは複数台設定すると1台がmasterとなり、他のAPはバックアップとしてmasterが正常なうちはAnchor-APとして働き、masterに障害が発生するとAnchor-ACとなります。



動作モード変更はコマンドで行います

- RS-232規格のコンソールケーブルを用意し、図のようにWA6638の左端のRJ-45のジャックに挿入します。使用するボーレートは次ページを参照ください。
- WA6638はDC電源またはPoEスイッチで稼働しますので、PoEスイッチを用意して頂き、PoEスイッチを介してPCのLANポートに接続します。WA6638の真ん中のRJ-45ポートは100M/1G/10Gの自動認識になります。



アクセスポイントの動作モードのコマンドによる変更

手順: 現在の動作モードの確認 -> 動作モードの変更 -> 変更されたかどうかの確認

#現在のモードを確認(工場出荷状態ではFITモード)

<H3C> **display wlan device role**

Current running mode: FIT AP.

system-viewにてap-modeコマンドでAnchor-acモードに変更

<H3C> **system-view**

System View: return to User View with Ctrl+Z.

[H3C] **ap-mode anchor-ac**

Changing working mode will reboot system. Continue? [Y/N]:y

注: APモードには以下の3つのモードが選択できます。

ap-mode { anchor-ac | cloud | fit }

#モード変更のためにAPIは自動的にrebootします。

System is starting...

Press Ctrl+D to access BASIC-BOOTWARE MENU...

Booting Normal Extended BootWare

リブート中メッセージ省略

Image file flash:/wa6600-boot.bin is self-decompressing.....

.....Done.

System image is starting...

Line con0 is available.

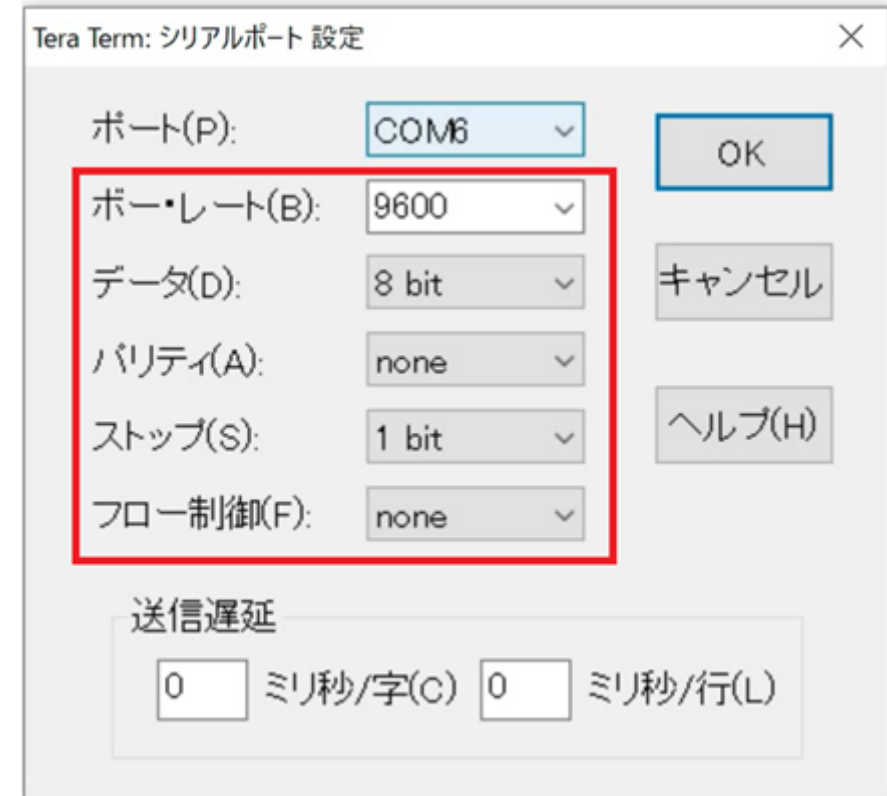
Press ENTER to get started.

#起動後Cloudモードになったことを確認します。

<H3C> **display wlan device role**

Current running mode: Anchor AC.

<H3C> **save force**



コンソール接続の通信設定は、9600ボー、データ8ビット、パリティなし、ストップビット1、フロー制御なし



- 01 アクセスポイントをAnchor-acに設定する
- 02 Anchor-acをゲストモードにする
- 03 動作確認
- 04 完成した設定のコマンド
- 05 オプション:クライアントのAP接続の最適化
- 06 トラブルシューティング
- 07 アップリンクにある装置へのアクセス制限
- 08 マニュアルについて

ゲストモード設定手順

手順 1 : SSID(guest)を作成します

手順 2 : クライアントがアクセスするためのVlan100を作成します
 手順 3 : クライアントにIPを割り当てるためにDHCP機能を有効にします

手順 4 : DHCPのIPプール、ゲートウェイアドレスを設定します

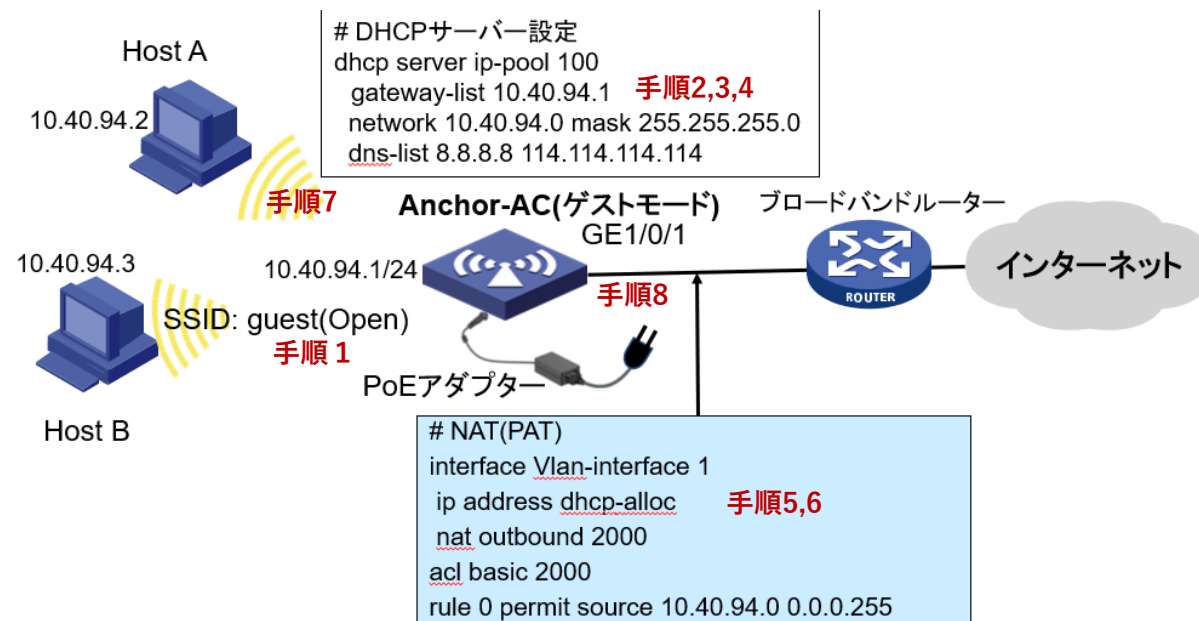
手順 5 : NATでインターネットにアクセスするIPの制限のためのACLを作成します

手順 6 : Vlan1にACLで制限されたNAT(PAT)を設定します

手順 7 : APの電波を有効にします

手順 8 : Vlan1のアドレスをデフォルトからDHCPで取得するように変更

手順 9 : 完成した設定を保存します



GUIでログインします <http://192.168.0.50/>
User: admin , Password: h3capadmin

H3C WLAN Management Platform

WA6320-JP

Remember username

English ▾

Login

Internet Explorer 10, Firefox 30.0.0.5269, Chrome 35.0.1916.114, Safari 5.1, and their higher versions are supported.

初期パスワード(h3capadmin)を変更します

Change Password

The default password is not secure. A qualified password must meet the following requirements: It must contain a minimum of 10 characters. It must contain a minimum of 2 types, and a minimum of 1 characters for each type. It can't contain the username or the reversed letters of the username.

Old Password
New Password
Confirm Password

Remember username English ▾

Internet Explorer 10, Firefox 30.0.0.5269, Chrome 35.0.1916.114, Safari 5.1, and their higher versions are supported.

ログインするとダッシュボードが表示されます

Actions | All Networks > Dashboard

System Logs

- Emergency: 0
- Critical: 4
- Warning: 10
- Informational: 23

APs

1 Online

System usage

- CPU: 0%
- Memory: 72%

Serial ID: 219801A2YF821BE00059
Hardware: Ver.A
Boot ROM: 7.18
Software: 7.1.064, Release 2453P01

Wireless services

guest

Clients

0

client number

← **メニュー**

ビューの切換え [System View | Network View]

System View **Network View**

Access Points: 1 Online, 0 Offline, 10 Warning, 23 Informational
Clients: 0
Event Logs: 0 Critical, 4 Warning, 10 Informational, 23 Debug

GUIのメニュー一覧

• Network view

Actions
Dashboard
Quick Start >
Monitoring >
Wireless Configuration >
Network Security >
System >
Tools >
Reporting >

Dashboard
Quick Start
 Add New AP
 Add New SSID
 Add New User
Monitoring
 Wireless Network
 Clients
 Wireless Security
 Client Proximity Sensor
 Application Monitoring
Wireless Configuration
 Wireless Networks
 AP Management
 Wireless QoS
Wireless Security
 WIPS
 Allowlist and denylist
Radio Management
 802.11n/802.11ax settings ,transmission distance
Applications
 Mesh, Multicast

Network Security
 Packet Filter
Traffic Policy
 Qos Policies, Priority Mapping
Access Control
 802.1x
Authentication
 RADIUS
 User Management
Access Control
 MAC Authentication
 Port Security
 Portal
System
Resource
 ACL, Time Range
 Cloud Platform
Tools
 Debug
Reporting
 Client Statistics
 Wireless Service Statistics

System View

Network View

GUIのメニュー一覧

• System view

Actions
Dashboard
Network Configuration >
Network Security >
System >
Tools >

Dashboard Network Configuration

Network Interfaces

VLAN

Network Routing

Routing table

Static Routing

Network Services

IP services

DHCP/DNS

Multicast

ARP

ND(Neighbor Discovery)

NAT

Network Security

Packet Filter

Traffic Policy

Access Control

802.1x

Authentication

RADIUS

User Management

Local users

System

Event Logs

Resource

ACL

Administrators

Management

Configuration save, import

Upgrade

Reboot

Tools

Debug

System View

Network View

手順1 : SSID(guest:オープン)を作成します

Actions All Networks > Quick Start > Add Services > Add Services

Dashboard Add Services

Quick Start **1**

Add AP

Add Services **2**

Add User

Monitoring >

Wireless Configuration >

Network Security >

System >

Tools >

Reporting >

5 Apply and Configure Advanced Settings Apply

Basic settings

Wireless service name * service (1-63 chars)

SSID * guest (1-32 chars)

Description (1-64 chars)

Wireless Service ON OFF **3**

Default VLAN 100 (1-4094, 1 by default)

Hide SSID Yes No

User Isolation Yes No

Forwarding type Centralized Local

Authentication settings

Authentication mode **4** Open (no authentication)

Static PSK

802.1X

802.1X (clear)

Static WEP

MAC Authentication

IPv4 Portal Authentication

IPv6 Portal Authentication

Authenticator AC

AP

Management Frame ON OFF

Protection

SSIDをAPのどの電波から出るかを関連付けします

Actions All Networks > Quick Start > Add Services > Add Services > Advanced Settings(service)

WLAN Authentication Authorization Intrusion Protection Key Management **Binding** Access control

Bind to APs

Candidate	Selected
<input type="text" value="Search for"/>	<input type="text" value="Search for"/>
→→	←←
<div style="border: 2px solid red; padding: 5px;">① ②</div>	00dd-b6b1-7ca0 (Radio1 5G) 00dd-b6b1-7ca0 (Radio2 2.4G)

Apply

③ Cancel

手順2: クライアントのアクセスするVlan 100を作成します

System > Network Configuration > VLAN > VLAN

VLAN MAC STP

2

3

4

VLAN	Untagged Port List	Tagged Port List	IP address of the VLAN interface	Description	Actions
1	↑ 1	0	10.10.11.22/255.255.255.0	VLAN 0001	✎

Total 2 entries, 1 matched. Page 1 / 1.

1

System View

Network View

Access Points Clients Event Logs

1 0 0 1 0 4 5 64

作成するVlanの番号(100)を設定します

System > Network Configuration > VLAN > VLAN

VLAN MAC STP

VLAN

VLAN	Untagged Port List	Tagged Port List	IP address of the VLAN interface	Description	Actions
1	↑ 1		55.0	VLAN 0001	

Create VLAN list

VLAN list * **1** (2-4094, e.g. 3,5,10-100)

2

Total 2 entries, 1 matched. Page 1 / 1.



Vlan100にIPアドレスを割り当てます

- Actions
- Dashboard
- Network Configuration
- Network Interfaces
- VLAN**
- Network Routing
- Network Services
- IP Services
- DHCP/DNS
- Multicast
- ARP
- ND
- NAT
- Management Protocols
- Network Security

System > Network Configuration > VLAN > VLAN

VLAN | MAC | STP

VLAN

VLAN	Untagged Port List	Tagged Port List	IP address of the VLAN interface	Description	Actions
1	↑ 1	0	10.10.11.22/255.255.255.0	VLAN 0001	
100	0	0	--	VLAN 0100	1 

Total 3 entries, 2 matched. Page 1 / 1.

クライアントのアクセスするVlan100のアドレスを10.40.94.1/24に設定

Actions

Dashboard

Network Configuration

Network Interfaces

VLAN

Network Routing

Network Services

Management Protocols

Network Security

System

Tools

System > Network Configuration > VLAN > VLAN > Edit VLAN

VLAN ID: 100

Description: VLAN 0100 (1-255 chars)

Untagged port list

Candidate	Selected
Search for	Search for
→→	←←
GE1/0/1	

Tagged port list

Candidate	Selected
Search for	Search for
→→	←←
GE1/0/1	

IP address of the VLAN interface **1**

Create VLAN interface

IPv4 address/mask: 10.40.94.1 **2** / 255.255.255.0

3 Apply Cancel

手順3: クライアントのためにDHCPサーバーを有効にします

System > Network Configuration > Network Services > DHCP/DNS > DHCP

Dashboard

Network Configuration

Network Interfaces

VLAN

Network Routing

Network Services

IP Services

DHCP/DNS

Multicast

ARP

ND

NAT

Management Protocols

Network Security

DHCP IPv4 DNS IPv6 DNS

1 DHCP

The Dynamic Host Configuration Protocol(DHCP) provides a framework to assign configuration information to network devices.

Enable DHCP 4

2

3

System View Network View

Access Points Clients Event Logs

Access Points	Clients	Event Logs
1 0 0	0	0 8 14 43

手順4: クライアントの割り当てるIPのためにDHCPサーバーを設定します

System > Network Configuration > Network Services > DHCP/DNS > DHCP

Dashboard

Network Configuration

Network Interfaces

VLAN

Network Routing

Network Services

IP Services

DHCP/DNS

Multicast

ARP

ND

NAT

Management Protocols

Network Security

DHCP IPv4 DNS IPv6 DNS

DHCP

The Dynamic Host Configuration Protocol(DHCP) provides a framework to assign configuration information to network devices.

Service **Address pool** Relay agent

1

Search

Interface	DHCP Service	Relay Server
Vlan1	DHCP server	
Vlan100	DHCP server	

Apply Cancel

アドレスプールの名前を入力します

Network Configuration

System > Network Configuration > Network Services > DHCP/DNS > DHCP

Network Interfaces

VLAN

Network Routing

Network Services

IP Services

DHCP/DNS

Multicast

ARP

ND

NAT

Management Protocols

Network Security

System

Tools

DHCP

The Dynamic Host Configuration Protocol(DHCP) provides a framework to assign configuration information to network devices.

Add Address Pool

①

Assigned Address DHCP Options IP In Use

Apply

New DHCP Server Address Pool

Address pool name * (1-63 chars)

②

③

Apply

Cancel

System View

Network View

Access Points

1 0 0 0

Clients

0

Event Logs

0 8 14 45

割り当てるアドレスセグメントを指定します(10.40.94.0)

Network Configuration

System > Network Configuration > Network Services > DHCP/DNS > DHCP

Network Interfaces

VLAN

Network Routing

Network Services

IP Services

DHCP/DNS

Multicast

ARP

ND

NAT

Management Protocols

Network Security

System

Tools

DHCP

The Dynamic Host Configuration Protocol(DHCP) provides a framework to assign configuration information to network devices.

Service

Address pool

Relay agent



100

Delete

Add Address Pool

Assigned Address

DHCP Options

IP In Use

Dynamic assignment

①

10.40.94.0

/ 255.255.255.0

(Network address/mask)

IPv4 address Range

X.X.X.X

- X.X.X.X

Static assignment

IP Address

Mask

Type

Hardware Address/Client ID

X.X.X.X

Ethernet

Mask length must be in the range of 1 to 30.

Hardware Address should be a string of 4-39 characters.

Apply

System View

Network View

Access Points

1 0 0 0

Clients

0

Event Logs

0 8 14 46

DHCPで伝えるゲートウェイのアドレス(Vlan100のアドレス)を設定します

System > Network Configuration > Network Services > DHCP/DNS > DHCP

ip-pool [Delete] [Add Address Pool]

Assigned Address **1** DHCP Options IP In Use

Lease duration Unlimited
 1 days 0 hours 0 minutes 0 seconds

Client domain name (1-50 chars)

Gateways **2**

DNS servers

WINS servers

NetBIOS node type

DHCP options

Option Code	Type	Option Content
2 - 254	Hex	1 - 256 chars.

DHCP Option should be a number of 2-254, but 50-54, 56, 58, 59, 61 and 82.
When the DHCP option type is Hex, the option content must be a hexadecimal string with a length of an even number in the range of 2 to 256.

[Apply] **3**

手順5: NATを利用して外部にアクセスできるアドレスをACLで制限します

System > Network Security > Packet Filter > Packet Filter

Packet Filter

Interface

Network Security

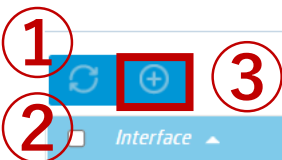
Packet Filter

Interface

Interface	Direction	Filter	ACL	State	Counting	Actions
-----------	-----------	--------	-----	-------	----------	---------

Total 0 entries, 0 matched, 0 selected. Page 1 / 1.

Delete



手順6: NATを適用するVlan1用にACLを作成します

Actions

Dashboard

Network Configuration >

Network Security >

Packet Filter

Traffic Policy

Access Control

Authentication

User Management

System >

Tools >

System > Network Security > Packet Filter > Packet Filter

Interface *

Vlan1

①

Direction *

 Inbound Outbound

Packet filter *

 IPv4 ACL IPv6 ACL Ethernet frame header ACL User defined ACL Default action

ACL *

+

②

Apply

Cancel

New ACL

ACL type

- IPv4 ACL
- IPv6 ACL
- Ethernet frame header ACL
- User-defined ACL

③

Apply

Cancel

basic ACLで番号は2000で最初のルールを作成します

Actions

Dashboard

Network Configuration >

Network Security >

Packet Filter

Traffic Policy

Access Control

Authentication

User Management

System >

Tools >

System > Network Security > Packet Filter > Packet Filter

Interface * Vlan1

Direction * Inbound Outbound

Packet filter * IPv4 ACL IPv6 ACL Ethernet frame header ACL User defined ACL Default action

ACL *

Apply Cancel

New IPv4 ACL

ACL Category * Basic Advanced

ACL * **1** (2000-2999 or 1-63 chars)

Rule match order Config Auto

Rule numbering step **2** (1-20)

Description (1-127 chars)

3 Continue to add rule

4

System View Network View

Access Points 1 0 0 0 Clients 0 Event Logs 0 8 14 47

クライアントがDHCPで割り当てられたIPセグメントからのみ許可

Actions

Dashboard

Network Configuration >

Network Security >

Packet Filter

Traffic Policy

Access Control

Authentication

User Management

System >

Tools >

System > Network Security > Packet Filter > Packet Filter

Interface *

Vlan1

Direction *

 Inbound Outbound

Packet filter *

 IPv4

ACL *

2000

Apply

Cancel

New Rule For IPv4 Basic ACL

ACL

2000

(2000-2999 or 1-63 chars)

Rule ID *

(0-65534) Auto numbered

Description

(1-127 chars)

Action

 Permit Deny

Match criterion

 Source IP address/wildcard mask

10.40.94.0 / 0.0.0.255

Time range

Fragments

 Only apply to non-first fragments

Logging

 Log matching packets

Counting

 Count the number of times this rule has been matched Continue to add next rule

4

Apply

Cancel

Vlan1のアクセスにACLで制限されたNATを設定します

Actions System > Network Configuration > Network Services > NAT > NAT

Dashboard

Network Configuration

Network Interfaces

VLAN

Network Routing

Network Services

IP Services

DHCP/DNS

Multicast

ARP

ND

NAT

Management Protocols

Network Security

NAT

Dynamic NAT Static NAT NAT Server Dynamic NAT444 Static NAT444

Search

Interface	Interface Description	ACL	Address Group	Address Group N...	VRF	Translation Mode...	Reversible	Port Preservatio...	State	Actions
-----------	-----------------------	-----	---------------	--------------------	-----	---------------------	------------	---------------------	-------	---------

Total 0 entries, 0 matched, 0 selected. Page 1 / 1.

Vlan1にACL2000を適用したnat(PAT)を設定します

System > Network Configuration > Network Services > NAT > NAT > Edit Dynamic NAT Rule

Interface *
Vlan1: Vlan-interface1 Interface

ACL
1 2000 +

Address group
○ Address Group
2 ● Easy IP

VRF
Public network

Translation mode
● PAT

Port preservation
 Try to preserve port number for PAT

Enable
 Enable this rule

3 Apply Cancel

Actions

Dashboard

Network Configuration

Network Interfaces

VLAN

Network Routing

Network Services

IP Services

DHCP/DNS

Multicast

ARP

ND

NAT

Management Protocols

Network Security

手順7: APの電波を有効にします

Actions


All Networks > Wireless Configuration > AP Management > AP

AP | AP Groups | AP Global Settings

AP Groups

Search

- AP Groups
- default-group (1)

Name	Installation Da...	Description	AP Group	Type	Model	Serial ID	MAC Address	Radios	Status	Actions
00dd-b6b1-7...	2022-05-24		default-group	Manual AP ...	WA6320-JP	219801A2YF8...	00-DD-B6-B1-7C-A0	802.11ax(5GH...	Online	

Total 1 entries, 1 matched, 0 selected. Page 1 / 1.

System View | **Network View**

Access Points: 1 Online, 0 Offline, 0 Disabled, 0 Unknown
Clients: 0
Event Logs: 0 Info, 8 Warning, 14 Error, 35 Critical

① ② ③ ④

5G(電波1)と2.4G(電波2)をONにします

Actions

All Networks > Wireless Configuration > AP Management > AP > Edit AP (00dd-b6b1-7ca0)

Dashboard

Quick Start >

Monitoring >

Wireless Configuration ▾

Wireless Networks

AP Management

Wireless QoS

Wireless Security >

Radio Management

Applications

Network Security >

System >

Tools >

Reporting >


Installation position (city/district/county)


Installation position (street)


Detail Installation position


AP description

Remarks

LED mode  Normal(Inherit) ✕ ▾

Map File  Select... ▾


AP connection priority  4(Inherit) (0-7, Inherit by default)


CAPWAP tunnel keepalive Echo interval  10(Inherit) seconds (0,5-255, Inherit by default)


Request retransmission Interval 5(Inherit) seconds (3-8, Inherit by default)

Retransmission attempts 3(Inherit) (2-5, Inherit by default)

Statistics report interval 50(Inherit) seconds (0-240, Inherit by default)

AC Election  ON OFF

CAPWAP tunnel encryption  Enable Disable Inherit (Disabled)

Firmware upgrade  Enable Disable Inherit (Enabled)

5GHz(1) radio ON OFF Inherit(Disabled)

2.4GHz(2) radio ON OFF Inherit(Disabled)

Apply

Cancel

System View Network View

Access Points 1 0 1 0 0 Clients 0 Event Logs 1 0 8 14 35

手順8: Vlan 1のIPアドレスを固定からDHCPへ変更します

Actions System > Network Configuration > Network Interfaces > Interfaces

Dashboard

Network Configuration **Network Interfaces**

VLAN

Network Routing

Network Services >

Management Protocols

Network Security >

System >

Tools >

Interfaces Link Aggregation

Statistics

All interfaces Search

Interface	Status	IP Address	Speed(Kbps)	Duplex	Description	Actions
<input type="checkbox"/> GE1/0/1	Up	--	1000000	Full	GigabitEthernet1/0/1 Interface	<input type="checkbox"/>
<input type="checkbox"/> InLoop0	Up	127.0.0.1/255.0.0.0	--	--	InLoopBack0 Interface	<input type="checkbox"/>
<input type="checkbox"/> NULL0	Up	--	--	--	NULL0 Interface	<input type="checkbox"/>
<input type="checkbox"/> Vlan1	Up	192.168.0.50/255.255.255.0	--	--	Vlan-interface1 Interface	<input checked="" type="checkbox"/>
<input type="checkbox"/> Vlan100	Down	10.40.94.1/255.255.255.0	--	--	Vlan-interface100 Interface	<input type="checkbox"/>
<input type="checkbox"/> WLAN-Radio1/0/1	Up	--	--	--	WLAN-Radio1/0/1 Interface	<input type="checkbox"/>
<input type="checkbox"/> WLAN-Radio1/0/2	Up	--	--	--	WLAN-Radio1/0/2 Interface	<input type="checkbox"/>

Total 7 entries, 7 matched, 0 selected. Page 1 / 1.

1

System View

Network View

> をクリックします

Actions System > Network Configuration > Network Interfaces > Interfaces > Edit Interface

Dashboard

Network Configuration >

Network Interfaces

VLAN

Network Routing

Network Services >


Management Protocols

Network Security >

System >



Tools >

Interface **Vlan-interface1** (Vlan1)


Status  up Shut down

Description (1-255 chars)

MAC address (HH-HH-HH-HH-HH-HH)

IP address IP address/Mask   192.168.0.50/255.255.255.0
IPv6 address/Prefix length >

Bandwidth (Current: 1000000kbit/s) (1-400000000)kbit/s

Link mode Bridge Route 

DHCPを利用する設定に変更します

Actions System > Network Configuration > Network Interfaces > Interfaces > Edit IP

Dashboard

Network Configuration

Network Interfaces

VLAN

Network Routing

Network Services

Management Protocols

Network Security

System

Tools

Interface **Vlan-interface1** (Vlan1)

Status **up**

Description Vlan-interface1 Interface

IP address Through DHCP **1**
 Manual assignment

MTU (Current: 1500)
 (46-1587)

TCP MSS (Current: 1460)
 (128-1547)

Apply **2** Cancel

H3C WLAN Management Platform

WA6320-JP

Remember username

English ▾

Login





Internet Explorer 10, Firefox 30.0.0.5269, Chrome 35.0.1916.114, Safari 5.1, and their higher versions are supported.

手順9: 設定が全て終わりましたので設定を保存(save)します

- Actions
- Dashboard
- Quick Start >
- Monitoring >
- Wireless Configuration >
- Network Security >
- System >
- Tools >
- Reporting >

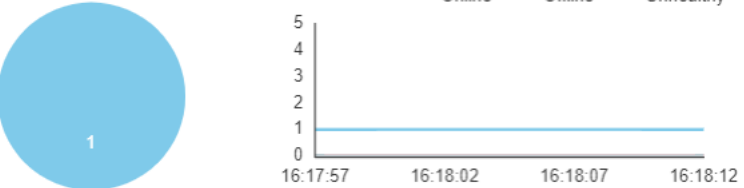
All Networks > Dashboard

System Logs

 0 Emergency	 4 Critical	 8 Warning	 23 Informational
--	---	--	---

APs

1 Online, 0 Offline, 0 Unhealthy



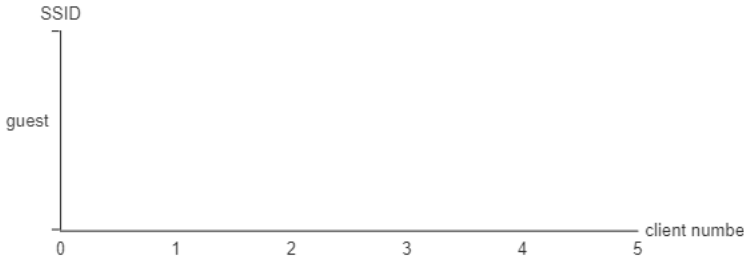
System usage

0% CPU, 72% Memory

Serial ID: 219801A2YF821BE00059
Hardware: Ver.A
Boot ROM: 7.18
Software: 7.1.064, Release 2453P01


Wireless services

guest SSID, 0 clients



Clients

0 clients



System View **Network View**

Access Points: 1 Online, 0 Offline, 0 Critical, 0 Warning, 0 Informational
Clients: 0
Event Logs: 0 Critical, 4 Warning, 8 Informational, 23 Informational

設定の上書き保存の確認にYesで答えます


Actions All Networks > Dashboard

System Logs

Emergency	0
Critical	4
Warning	8
Informational	23

APs

Online Offline Unhealthy



System usage

72% Memory

Serial ID: 219801A2YF821BE00059
Hardware: Ver.A
Boot ROM: 7.18
Software: 7.1.064, Release 2453P01

Wireless services

SSID: guest

client number

5GHz	0
2.4GHz	0

Clients

Quantity: 0

N/A

Confirm [X]

Are you sure you want to save the current configuration?

1 Yes No



- 01 アクセスポイントをAnchor-acに設定する
- 02 Anchor-acをゲストモードにする
- 03 **動作確認**
- 04 完成した設定のコマンド
- 05 オプション:クライアントのAP接続の最適化
- 06 トラブルシューティング
- 07 アップリンクにある装置へのアクセス制限
- 08 マニュアルについて

完成したゲストAPに接続して動作を確認します

オープン認証



接続したPC

```
Microsoft Windows [Version 10.0.22000.675]  
(c) Microsoft Corporation. All rights reserved.
```

```
C:¥Users¥H3C>ipconfig
```

```
Windows IP 構成
```

```
Wireless LAN adapter Wi-Fi:
```

```
接続固有の DNS サフィックス . . . . .:  
リンクローカル IPv6 アドレス. . . . .: fe80::35e8:d633:3383:d67%9  
IPv4 アドレス . . . . .: 10.40.94.2  
サブネット マスク . . . . .: 255.255.255.0  
デフォルト ゲートウェイ . . . . .: 10.40.94.1
```

```
C:¥Users¥weigu>ping www.google.com
```

```
www.google.com [142.251.42.164]に ping を送信しています 32 バイトのデータ:  
142.251.42.164 からの応答: バイト数 =32 時間 =7ms TTL=115  
142.251.42.164 からの応答: バイト数 =32 時間 =16ms TTL=115  
142.251.42.164 からの応答: バイト数 =32 時間 =14ms TTL=115  
142.251.42.164 からの応答: バイト数 =32 時間 =3ms TTL=115
```

```
142.251.42.164 の ping 統計:
```

```
パケット数: 送信 = 4、受信 = 4、損失 = 0 (0% の損失)、  
ラウンドトリップの概算時間 (ミリ秒):  
最小 = 3ms、最大 = 16ms、平均 = 10ms
```

```
C:¥Users¥H3C>
```



- 01 アクセスポイントをAnchor-acに設定する
- 02 Anchor-acをゲストモードにする
- 03 動作確認
- 04 **完成した設定のコマンド**
- 05 オプション:クライアントのAP接続の最適化
- 06 トラブルシューティング
- 07 アップリンクにある装置へのアクセス制限
- 08 マニュアルについて

完成した設定のCLIリストです

```
version 7.1.064, Release 2453P01
```

```
#
```

```
sysname H3C
```

```
#
```

```
wlan global-configuration
```

```
#
```

```
telnet server enable
```

```
#
```

```
port-security enable
```

```
#
```

```
dhcp enable
```

```
#
```

```
lldp global enable
```

```
lldp hold-multiplier 8
```

```
#
```

```
password-recovery enable
```

```
#
```

```
vlan 1
```

```
#
```

```
vlan 100
```

```
#
```

```
dhcp server ip-pool 100
```

```
gateway-list 10.40.94.1
```

```
network 10.40.94.0 mask 255.255.255.0
```

```
dns-list 8.8.8.8 114.114.114.114
```

```
#
```

```
wlan service-template service
```

```
ssid guest
```

```
vlan 100
```

```
user-isolation enable
```

```
service-template enable
```

```
#
```

```
interface NULL0
```

```
#
```

```
interface Vlan-interface1
```

```
ip address dhcp-alloc
```

```
nat outbound 2000
```

```
#
```

```
Interface Vlan-interface100
```

```
ip address 10.40.94.1 255.255.255.0
```

```
#
```

```
Interface GigabitEthernet1/0/1
```

```
#
```

```
Interface WLAN-Radio1/0/1
```

```
#
```

```
Interface WLAN-Radio1/0/2
```

```
#
```

```
scheduler logfile size 16
```

```
#
```

```
Line class console
```

```
user-role network-admin
```

```
#
```

```
Line class vty
```

```
user-role network-operator
```

```
#
```

```
Line con 0
```

```
user-role network-admin
```

```
#
```

```
Line vty 0 31
```

```
authentication-mode scheme
```

```
user-role network-operator
```

```
#
```

```
Line vty 32 63
```

```
user-role network-operator
```

```
#
```

```
acl basic 2000
```

```
step 1
```

```
rule 0 permit source 10.40.94.0 0.0.0.255
```

```
#
```

```
Domain system
```

```
#
```

```
domain default enable system
```

```
#
```

```
role name level-0
```

```
description Predefined level-0 role
```

```
途中のrole設定は省略
```

```
#
```

```
role name level-14
```

```
description Predefined level-14 role
```

```
#
```

```
user-group system
```

```
#
```

```
local-user admin class manage
```

```
password simple xxxxxxxxxxxxxx
```

```
service-type telnet http https
```

```
authorization-attribute user-role network-admin
```

```
#
```

```
ip http enable
```

```
ip https enable
```

```
#
```

```
undo attack-defense tcp fragment enable
```

```
#
```

```
wlan ap-group default-group
```

```
vlan 1
```

```
#
```

```
wlan ap xxxx-xxxx-001 model WA6320-JP
```

```
serial-id xxxxxxxxxxxxxxxxxxxxxx
```

```
mac-address xxxx-xxxx-0001
```

```
anchor-ap enable #デフォルトはdisableですが
```

```
# enableにすると障害復旧後master選挙に参加する
```

```
radio 1
```

```
radio enable
```

```
service-template service
```

```
radio 2
```

```
radio enable
```

```
service-template service
```

```
gigabitethernet 1
```

```
#
```

参考: Anchor-ACがFIT APを管理する場合以下のように設定します

```
version 7.1.064, Release 2453P01
#
sysname H3C
#
wlan global-configuration
#
telnet server enable
#
port-security enable
#
dhcp enable
#
lldp global enable
lldp hold-multiplier 8
#
password-recovery enable
#
vlan 1
#
vlan 100
#
dhcp server ip-pool 100
gateway-list 10.40.94.1
network 10.40.94.0 mask 255.255.255.0
dns-list 8.8.8.8 114.114.114.114
#
wlan service-template service
ssid guest
vlan 100
user-isolation enable
service-template enable
#
interface NULL0
#
interface Vlan-interface1
ip address dhcp-alloc
nat outbound 2000
#
```

```
Interface Vlan-interface100
ip address 10.40.94.1 255.255.255.0
#
Interface GigabitEthernet1/0/1
#
Interface WLAN-Radio1/0/1
#
Interface WLAN-Radio1/0/2
#
scheduler logfile size 16
#
Line class console
user-role network-admin
#
Line class vty
user-role network-operator
#
Line con 0
user-role network-admin
#
Line vty 0 31
authentication-mode scheme
user-role network-operator
#
Line vty 32 63
user-role network-operator
#
acl basic 2000
step 1
rule 0 permit source 10.40.94.0 0.0.0.255
#
Domain system
#
domain default enable system
#
role name level-0
description Predefined level-0 role
```

```
途中のrole設定は省略
#
user-group system
#
local-user admin class manage
password simple xxxxxxxxxxxxxx
service-type telnet http https
authorization-attribute user-role network-admin
#
ip http enable
ip https enable
#
undo attack-defense tcp fragment enable
#
wlan auto-ap enable
wlan auto-persistent enable
wlan anchor-ap persistent-mode ac
#
wlan ap-group default-group
ap-model WA6320-JP
vlan 1
radio 1
radio enable
service-template service
radio 2
radio enable
service-template service
#
#以下はAnchor-AC(メイン)
#
wlan ap xxxx-xxxx-001 model WA6320-JP
serial-id xxxxxxxxxxxxxxxxxxxxxx
mac-address xxxx-xxxx-0001
anchor-ap enable
radio 1
radio 2
gigabitethernet 1
#
```

```
#
#以下はAnchor-AP(バックアップ)
#
wlan ap xxxx-xxxx-0002 model WA6320-JP
serial-id xxxxxxxxxxxxxxxxxxxxxx
mac-address xxxx-xxxx-0002
anchor-ap enable
radio 1
radio 2
gigabitethernet 1
#
#以下はFIT APが連なる
#
wlan ap xxxx-xxxx-0003 model WA6320-JP
serial-id xxxxxxxxxxxxxxxxxxxxxx
mac-address xxxx-xxxx-003
radio 1
radio 2
gigabitethernet 1
#
wlan ap xxxx-xxxx-0004 model WA6320-JP
serial-id xxxxxxxxxxxxxxxxxxxxxx
mac-address xxxx-xxxx-0004
radio 1
radio 2
gigabitethernet 1
#
return
```




- 01 アクセスポイントをAnchor-acに設定する
- 02 Anchor-acをゲストモードにする
- 03 動作確認
- 04 完成した設定のコマンド
- 05 オプション:クライアントのAP接続の最適化
- 06 トラブルシューティング
- 07 アップリンクにある装置へのアクセス制限
- 08 マニュアルについて

クライアントのAP接続の最適化

チャンネル使用の有効化(DFS: calibrate-channel self-decisive)

WLANの動作チャンネルは限られています。チャンネルのオーバーラップは非常に簡単に発生します。さらに、レーダーや電子レンジなどの他の無線ソースがAPの動作を妨げる可能性があります。動的周波数選択 (DFS) は、これらの問題を解決できます。DFSを使用すると、ACは各APに最適なチャンネルをリアルタイムで選択して、同一チャンネル干渉や他の無線ソースからの干渉を回避します。

次の条件によってDFSが決まります。

- ・エラーコード率-物理層のエラーコードとCRCエラー。
- ・干渉-ワイヤレスサービスに対する802.11および非802.11ワイヤレス信号の影響。
- ・再送信：APは、ACからACKメッセージを受信しない場合にデータを再送信します。
- ・動作チャンネルで検出されたレーダー信号-ACは、動作チャンネルを変更するようにAPにただちに通知します。

最初の3つの条件が満たされると、ACは新しいチャンネルを選択します。APは、新しいチャンネルと古いチャンネルのチャンネル品質の差が許容レベルを超えるまで、新しいチャンネルを使用しません。

送信電力制御(TPC: calibrate-power self-decisive)

TPCを使用すると、ACはリアルタイムのWLAN条件に基づいてアクセスポイントの送信電力を動的に制御できます。無線間のチャンネル干渉を回避しながら、必要なRFカバレッジを実現できます。

ACは、関連付けられたAP上の各無線のネイバーレポートを維持して、この無線によって検出された他の無線に関する情報を記録します。ACは、それに関連付けられた無線のみを管理できます。

帯域幅使用の有効化(calibrate-bandwidth self-decisive)

自動帯域幅調整を有効にすると、ACは、自動帯域幅調整間隔に達するとチャンネル品質検出を開始し、帯域幅調整を実行するかどうかを決定します。無線の隣接無線の数が多い場合は、無線の帯域幅を減らして干渉を減らし、数が少ない場合は帯域幅を増やして伝送速度を上げます。このコマンドは、5GHz無線でのみ有効です。

クライアントのAP接続の最適化

Actions

All Networks > Wireless Configuration > Radio Management > Radio Configuration

Dashboard

Quick Start >

Monitoring >

Wireless Configuration ▾

Wireless Networks

AP Management

Wireless QoS

Wireless Security >

Radio Management

Applications

Network Security >

System >

Tools >

Reporting >

Radio Configuration | RRM | Load Balancing | Band Navigation

Radios of all AP models

AP Group	AP Model	Radio	Radio Type	Bandwidth(MHz)	Channel	Max Power(dBm)	Status
----------	----------	-------	------------	----------------	---------	----------------	--------

0/0

Radios of all APs

AP Name	Radio	Radio Type	Bandwidth(MHz)	Working Channel	Specified Channel	Max Power(dBm)	Administrative Stat...	Running State	Channel Usage	Clients
00dd-b6b1-4540	5GHz(1)	802.11ax(5GHz)	80	116	Auto unlock(Inherit	20	ON	ON	0%	0
00dd-b6b1-4540	2.4GHz(2)	802.11ax(2.4GHz)	20	1	Auto unlock(Inherit	21	ON	ON	16%	1
00dd-b6b1-7ca0	5GHz(1)	802.11ax(5GHz)	80	-	Auto unlock(Inherit	20	ON	-	-	0
00dd-b6b1-7ca0	2.4GHz(2)	802.11ax(2.4GHz)	20	-	Auto unlock(Inherit	21	ON	-	-	0
5ca7-21f3-67e0	5GHz(1)	802.11ax(5GHz)	80	-	Auto unlock(Inherit	20	OFF	OFF	0%	0
5ca7-21f3-67e0	2.4GHz(2)	802.11ax(2.4GHz)	20	-	Auto unlock(Inherit	21	OFF	OFF	0%	0

1/1

System View

Network View

Access Points

2 - 1 0

Clients

1

Event Logs

0 11 13 79

Real-time adjustment

Global Channel Optimization - **DFS**

wlan global-configuration
calibrate-channel self-decisive enable all

Global Power Optimization - **TPC**

wlan global-configuration
calibrate-power self-decisive enable all

Global Bandwidth Adjustment - **bandwidth**

wlan global-configuration
calibrate-bandwidth self-decisive enable

Optimize Channel

Optimize Power

AP configuration

AP Name	Radio	Auto DFS	Auto TPC	Auto Bandwidth Adj.
00dd-b6b1-4540	5GHz(1)	Inherited	Inherited	Inherited
00dd-b6b1-4540	2.4GHz(2)	Inherited	Inherited	Inherited
00dd-b6b1-7ca0	5GHz(1)	Inherited	Inherited	Inherited
00dd-b6b1-7ca0	2.4GHz(2)	Inherited	Inherited	Inherited
5ca7-21f3-67e0	5GHz(1)	Inherited	Inherited	Inherited
5ca7-21f3-67e0	2.4GHz(2)	Inherited	Inherited	Inherited

AP group configuration

AP Group	AP Model	Radio	Auto DFS	Auto TPC	Auto Bandwidth ...
----------	----------	-------	----------	----------	--------------------

RRM history information

AP Name	Radio	BSSID	Adjustment Count
---------	-------	-------	------------------

The screenshot displays the H3C WA6320-JP network management interface. The main navigation menu on the left includes sections like Actions, Dashboard, Quick Start, Monitoring, Wireless Configuration, and Radio Management. The current view is 'Radio Management > RRM'. A 'Calibration Interval' dialog box is open, allowing configuration of three intervals: DFS interval (23 minutes), TPC interval (11 minutes), and Bandwidth Adjustment interval (13 minutes). The 'Apply' button in the dialog is highlighted with a red box. In the background, the 'Real-time adjustment' section has three items: Global Channel Optimization, Global Power Optimization, and Global Bandwidth Adjustment, each with a red arrow pointing to the dialog box. The 'AP configuration' table below shows a list of APs with their names and radio types. The bottom status bar shows 'Access Points' (2 green, 1 red, 0 blue), 'Clients' (1), and 'Event Logs' (0 red, 11 blue, 14 yellow, 83 green).

H3C WA6320-JP Save Roadmap | admin

All Networks > Wireless Configuration > Radio Management > RRM

Radio Configuration **RRM** Load Balancing Band Navigation

Real-time adjustment

- Global Channel Optimization
- Global Power Optimization
- Global Bandwidth Adjustment

Calibration Interval

- DFS interval: 23 minutes(3-1440, 23 by default)
- TPC interval: 11 minutes(3-180, 11 by default)
- Bandwidth Adjustment interval: 13 minutes(3-1440, 13 by default)

Apply Cancel

AP configuration

AP Name	Radio
00dd-b6b1-4540	5GHz(1)
00dd-b6b1-4540	2.4GHz(2)
00dd-b6b1-7ca0	5GHz(1)
00dd-b6b1-7ca0	2.4GHz(2)
5ca7-21f3-67e0	5GHz(1)
5ca7-21f3-67e0	2.4GHz(2)

1/1

0/0

RRM history information

System View **Network View**

Access Points: 2 (green), 1 (red), 0 (blue) | Clients: 1 | Event Logs: 0 (red), 11 (blue), 14 (yellow), 83 (green)

- Actions
- Dashboard
- Quick Start >
- Monitoring >
- Wireless Configuration ▾
- Wireless Networks
- AP Management
- Wireless QoS
- Wireless Security >
- Radio Management**
- Applications
- Network Security >
- System >
- Tools >
- Reporting >

All Networks > Wireless Configuration > Radio Management > RRM


Radio Configuration **RRM** Load Balancing Band Navigation

Real-time adjustment

Global Channel Optimization

Global Power Optimization

Global Bandwidth Adjustment

 **Optimize Channel**

 **Optimize Power**

AP configuration

AP Name	Radio	Auto DFS	Auto TPC	Auto Bandwidth Adj...
00dd-b6b1-4540	5GHz(1)	Inherited	Inherited	Inherited
00dd-b6b1-4540	2.4GHz(2)	Inherited	Inherited	Inherited
00dd-b6b1-7ca0	5GHz(1)	Inherited	Inherited	Inherited
00dd-b6b1-7ca0	2.4GHz(2)	Inherited	Inherited	Inherited
5ca7-21f3-67e0	5GHz(1)	Inherited	Inherited	Inherited
5ca7-21f3-67e0	2.4GHz(2)	Inherited	Inherited	Inherited

1/1

Navigation icons



AP group configuration

AP Group	AP Model	Radio	Auto DFS	Auto TPC	Auto Bandwidth ...
----------	----------	-------	----------	----------	--------------------

0/0

Navigation icons

RRM history information

AP Name	Radio	BSSID	Adjustment Count
---------	-------	-------	------------------

System View **Network View**

Access Points Clients Event Logs

2 1 0 1 0 9 11 75







クライアントのAP接続の最適化

Actions

All Networks > Wireless Configuration > Radio Management > RRM > Details

AP Configuration | AP Group Configuration | RRM History Information

Search

AP Name ▲	Radio	Auto DFS	Auto TPC	Auto Bandwidth Adjustment	Actions
00dd-b6b1-4540	5GHz(1)	Inherited	Inherited	Inherited	
00dd-b6b1-4540	2.4GHz(2)	Inherited	Inherited	Inherited	 ...
00dd-b6b1-7ca0	5GHz(1)	Inherited	Inherited	Inherited	 ...
00dd-b6b1-7ca0	2.4GHz(2)	Inherited	Inherited	Inherited	 ...
5ca7-21f3-67e0	5GHz(1)	Inherited	Inherited	Inherited	 ...
5ca7-21f3-67e0	2.4GHz(2)	Inherited	Inherited	Inherited	 ...

Total 6 entries, 6 matched. Page 1 / 1.

- Actions
- Dashboard
- Quick Start >
- Monitoring >
- Wireless Configuration ▾
- Wireless Networks
- AP Management
- Wireless QoS
- Wireless Security >
- Radio Management
- Applications
- Network Security >
- System >
- Tools >
- Reporting >

All Networks > Wireless Configuration > Radio Management > RRM > AP Configuration (00dd-b6b1-4540)

AP name
00dd-b6b1-4540

Radio
5GHz(1)

DFS configuration

Auto DFS  Enable **radio 1 rrm** Disable Inherit

Bandwidth adjustment configuration **calibrate-channel self-decisive enable**

Auto Bandwidth Adjustment Enable **radio 1 rrm** Disable Inherit

Apply

Cancel

TPC configuration

Auto TPC  Enable **radio 1 rrm** Disable Inherit

calibrate-bandwidth self-decisive enable

クライアントのAP接続の最適化

バンドナビゲーション

バンドナビゲーションにより、APは5 GHz無線でデュアルバンド（2.4GHzおよび5GHz）クライアントを受け入れることを選択できます。これは、2.4 GHz帯域が混雑していることが多く、ネットワーク全体のパフォーマンスが向上するためです。

バンドナビゲーションが有効になっている場合、APは次の原則に従って、クライアントを2.4GHzまたは5GHzの無線に誘導します。

- APは、2.4 GHz無線を数回拒否した後、2.4GHz無線で2.4GHzクライアントに関連付けられます。
- APは、デュアルバンドクライアントを5GHz無線に転送します。
- APは、5GHz無線で5GHzクライアントに関連付けられます。

APは、クライアントを5 GHz無線に転送する前に、デュアルバンドクライアントのRSSIをチェックします。RSSIがコマンドband-navigationrssi-thresholdで指定された値よりも低い場合、APはクライアントを5GHz帯域に誘導しません。5 GHz無線のクライアント数が上限に達し、5GHz無線のクライアント数と2.4GHz無線のクライアント数のギャップが上限に達した場合（2つのしきい値はコマンドで指定します）、APはクライアントの5 GHz無線への関連付けを拒否し、新しいクライアントが2.4GHz無線に関連付けることを許可します。クライアントが5GHz無線で最大時間（コマンドband-navigation balance access-denialで指定）を超えて拒否された場合、APは、クライアントが他のAPにアソシエートできないと見なし、5GHzを許可します。

- Actions
- Dashboard
- Quick Start >
- Monitoring >
- Wireless Configuration ▾
- Wireless Networks
- AP Management
- Wireless QoS
- Wireless Security >
- Radio Management**
- Applications
- Network Security >
- System >
- Tools >
- Reporting >

All Networks > Wireless Configuration > Radio Management > Band Navigation

Radio Configuration | RRM | Load Balancing | **Band Navigation**

Global settings

Status	OFF	Max denials	1
Session threshold		Client info aging time	180 s
Session gap threshold	4	RSSI threshold	15

APs

AP Name	Band Navigation
00dd-b6b1-4540	Inherit
00dd-b6b1-7ca0	Inherit
5ca7-21f3-67e0	Inherit

1/1

◀ ◁ ▷ ▶

AP groups

Group Name	Band Navigation
default-group	ON

1/1

◀ ◁ ▷ ▶

- Actions
- Dashboard
- Quick Start >
- Monitoring >
- Wireless Configuration ▾
- Wireless Networks
- AP Management
- Wireless QoS
- Wireless Security >
- Radio Management**
- Applications
- Network Security >
- System >
- Tools >
- Reporting >

All Networks > Wireless Configuration > Radio Management > Band Navigation

Radio Configuration | RRM | Load Balancing | **Band Navigation**

Global settings

Status	OFF	Max denials	1
Session threshold		Client info aging time	180 s
Session gap threshold	4	RSSI threshold	15



APs

AP Name	Band Navigation
00dd-b6b1-4540	Inherit
00dd-b6b1-7ca0	Inherit
5ca7-21f3-67e0	Inherit

1/1



AP groups

Group Name	Band Navigation
default-group	ON


1/1





- Actions
- Dashboard
- Quick Start >
- Monitoring >
- Wireless Configuration ▾
- Wireless Networks
- AP Management
- Wireless QoS
- Wireless Security >
- Radio Management**
- Applications
- Network Security >
- System >
- Tools >
- Reporting >


All Networks > Wireless Configuration > Radio Management > Band Navigation > Details

Global settings | **AP Configuration** | AP Group Configuration


Band navigation  ON OFF **wlan global-configuration
wlan band-navigation enable**

Client info aging time  s (10-600, 180 by default)

Max denials  (1-10)

Load balancing  Session threshold (2-255)

Session gap (1-8, 4 by default)

RSSI threshold  dB (5-100, 15 by default)




クライアントのAP接続の最適化

H3C WA6320-JP Save Roadmap | admin

Actions

All Networks > Wireless Configuration > Radio Management > Band Navigation > Details

Global settings **AP Configuration** AP Group Configuration

<input type="checkbox"/> AP Name ▲	Band Navigation status
<input type="checkbox"/> 00dd-b6b1-4540	Inherit
<input type="checkbox"/> 00dd-b6b1-7ca0	Inherit
<input type="checkbox"/> 5ca7-21f3-67e0	Inherit

Total 3 entries, 3 matched, 0 selected. Page 1 / 1.

System View **Network View**

Access Points: 2 (green), 1 (blue), 0 (red) | Clients: 1 | Event Logs: 0 (red), 15 (red), 25 (yellow), 109 (blue)

クライアントのAP接続の最適化

- Actions
- Dashboard
- Quick Start >
- Monitoring >
- Wireless Configuration ▾
- Wireless Networks
- AP Management
- Wireless QoS
- Wireless Security >
- Radio Management**
- Applications
- Network Security >
- System >
- Tools >
- Reporting >

All Networks > Wireless Configuration > Radio Management > Band Navigation > Details

Global settings **AP Configuration** AP Group Configuration



Search



<input type="checkbox"/> AP Name ▲		Band Navigation status	
<input checked="" type="checkbox"/> 00dd-b6b1-4540	wlan ap XXXX-XXXX-XXXX model WA6320-JP serial-id XXXXXXXXXXXXXXXXXXXX mac-address 00dd-b6b1-4540 band-navigation enable	Inherit	
<input type="checkbox"/> 00dd-b6b1-7ca0		Inherit	
<input type="checkbox"/> 5ca7-21f3-67e0		Inherit	

Total 3 entries, 3 matched, 1 selected. Page 1 / 1.



- ON**
- OFF
- Inherit

System View

Network View

Access Points

2 1 0

Clients

1

Event Logs

0 15 25 109

クライアントのAP接続の最適化

ロードバランス

WLANロードバランシングは、無線間でクライアントを動的にロードバランシングして、高密度WLANのクライアントにワイヤレスサービス品質と適切な帯域幅を確保します。特定のAP間でWLANロードバランシングを設定するには、APを同じACで管理する必要があり、クライアントはAPを検出できます。

動作メカニズム

次の条件が満たされた場合、デバイスはロードバランシングを実行します。

- ・無線の負荷がしきい値に達しました。
- ・無線機と最も負荷の軽い無線機との間の負荷ギャップが負荷ギャップしきい値に達します。

無線の負荷と負荷ギャップがそれぞれのしきい値に達すると、無線はクライアントの関連付け要求を拒否します。無線がクライアントを拒否する回数が、アソシエーション要求に対して指定された最大拒否数に達すると、無線はクライアントのアソシエーション要求を受け入れません。

負荷分散モード

このデバイスは、セッションモード、トラフィックモード、および帯域幅モードのロードバランシングをサポートしています。次の条件が満たされた場合に、特定のモードの負荷分散を実行します。

- ・指定されたセッション/トラフィック/帯域幅のしきい値に達しました。
- ・指定されたセッション/トラフィック/帯域幅ギャップのしきい値に達しました。

負荷分散の種類

デバイスは、次の負荷分散タイプをサポートしています。

- ・無線ベース—デバイスは、受信したネイバーレポートに基づいて、ロードバランシングに参加する無線を決定します。無線のネイバーレポートは、無線によって検出された各クライアントのMACアドレスとRSSI値を記録します。デバイスは、次のいずれかの条件が満たされたときに、無線がロードバランシングに参加することを決定します。

- クライアントが無線との関連付けを要求します。
- 無線は、クライアントのRSSIがRSSIしきい値に達したことを検出しますが、クライアントは無線との関連付けを要求しません。
- ・ロードバランシンググループベース：目的のAPの無線をロードバランシンググループに追加します。デバイスは、このロードバランシンググループの無線でのみロードバランシングを実行します。

- Actions
- Dashboard
- Quick Start >
- Monitoring >
- Wireless Configuration ▾
- Wireless Networks
- AP Management
- Wireless QoS
- Wireless Security >
- Radio Management**
- Applications
- Network Security >
- System >
- Tools >
- Reporting >

All Networks > Wireless Configuration > Radio Management > Load Balancing

Radio Configuration RRM **Load Balancing** Band Navigation

Global settings

Status	OFF	Session threshold	20
Mode	Session-mode	Session gap threshold	4
Max denials	10		
RSSI threshold	25		

Loadbalancing groups

Group ID	Description	Radios
0/0		

System View **Network View**

Access Points: 2 (green), 1 (grey), 0 (red) Clients: 1 Event Logs: 0 (red), 15 (red), 23 (yellow), 108 (blue)

Actions

All Networks > Wireless Configuration > Radio Management > Load Balancing > Details

Global settings

Load Balancing Groups

**wlan global-configuration
wlan load-balance enable**

Load balancing

 ON OFF

Mode

 Session Traffic Bandwidth

Session threshold

 (1-120,20 by default)

Session gap threshold

 (1-12,4 by default)

Max denials

 (2-10,10 by default)

RSSI threshold

 (5-100,25 by default)

Apply

Cancel

System View

Network View

Access Points

1 1 0

Clients

1

Event Logs

0 15 27 125

$RSSI = SNR$ (信号対雑音比: db) = $Signal(dbm) - \text{フロアノイズ}(-95dbm)$

RSSI(db)	dBm	評価
40以上	-55	非常に信頼性が高くリアルタイムの通信が可能な水準
25～40	-70～-55	信頼性が高くリアルタイムの通信の最低限の水準
15～25	-80～-70	遅いが信頼性の高い通信の最低限の水準
10～15	-85～-80	遅く信頼性の低い水準
10以下	-85	使用に耐えない

クライアントのAP接続の最適化

ローミングナビゲーション

802.11プロトコルはクライアントローミング制御メカニズムを提供せず、一部のクライアントは、より高い信号強度でAPにアクティブにローミングできません。

APのビーコンまたはプローブ応答の送信電力を減らして、クライアントがより高い信号強度でAPにローミングできるようにするには、次の作業を実行します。

ビーコンまたはプローブ応答の送信電力を設定した場合、システムはデフォルトの送信電力を使用して他のパケットを送信します。

```
[AC] wlan ap ap1 model WA6632-JP
```

```
[AC-wlan-ap-ap1] radio 1
```

```
[AC-wlan-ap-ap1-radio-1] option roam-navigation enable rssi 20 beacon-power 20 probe-response-power 20
```

```
[AC-wlan-ap-ap1-radio-1] quit
```

```
[AC-wlan-ap-ap1] radio 2
```

```
[AC-wlan-ap-ap1-radio-2] option roam-navigation enable rssi 20 beacon-power 20 probe-response-power 20
```

```
[AC-wlan-ap-ap1-radio-2] quit
```

```
[AC-wlan-ap-ap1]quit
```

クライアントのAP接続の最適化

スティッキークライアントの制御

クライアントの信号強度によるアクセス制限(信号の弱いクライアントのアソシエーションを制限します)

```
[AC] wlan ap ap1 model WA6632-JP
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] option client reject enable rssi 20
[AC-wlan-ap-ap1-radio-1] quit
[AC-wlan-ap-ap1] radio 2
[AC-wlan-ap-ap1-radio-2] option client reject enable rssi 20
[AC-wlan-ap-ap1-radio-2] quit
[AC-wlan-ap-ap1]quit
```



- 01 アクセスポイントをAnchor-acに設定する
- 02 Anchor-acをゲストモードにする
- 03 動作確認
- 04 完成した設定のコマンド
- 05 オプション:クライアントのAP接続の最適化
- 06 **トラブルシューティング**
- 07 アップリンクにある装置へのアクセス制限
- 08 マニュアルについて

Actions

System > Dashboard

Dashboard

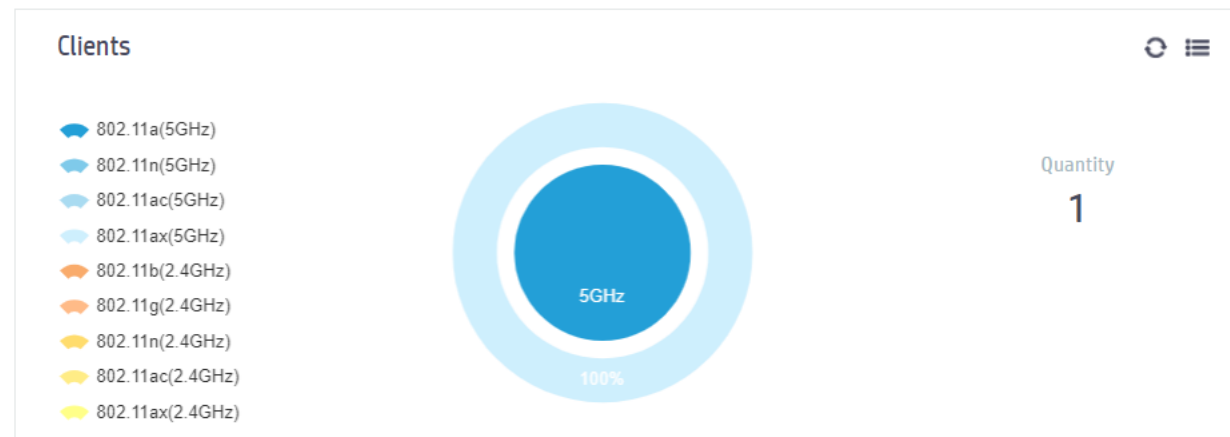
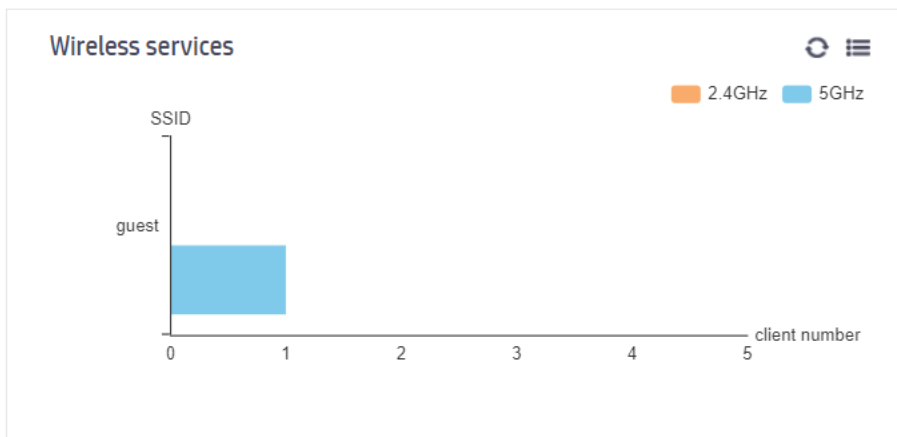
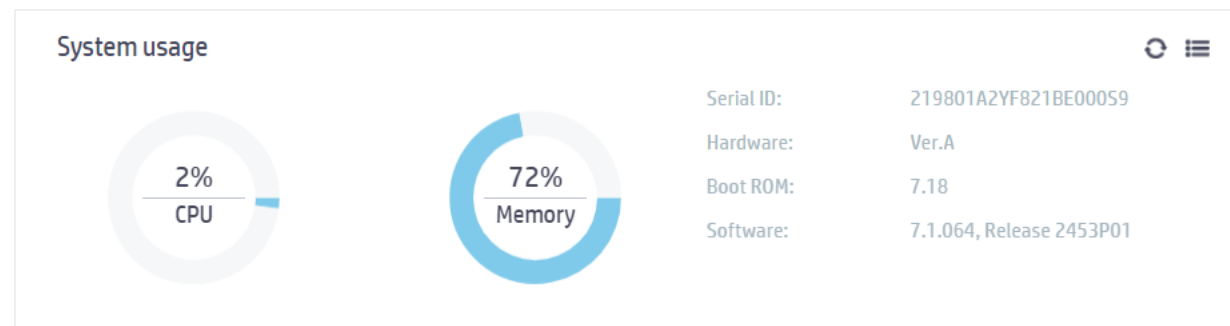
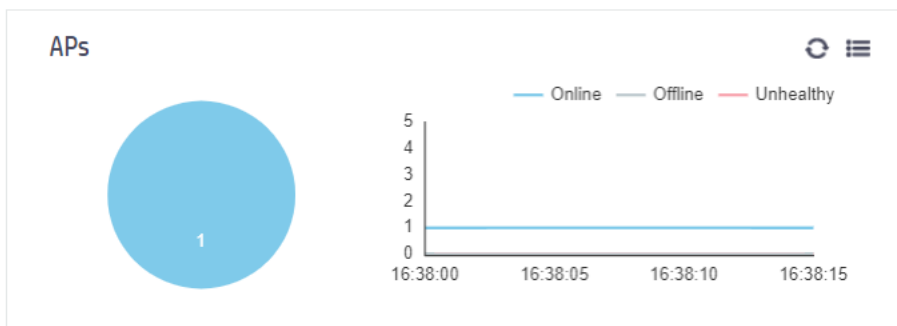
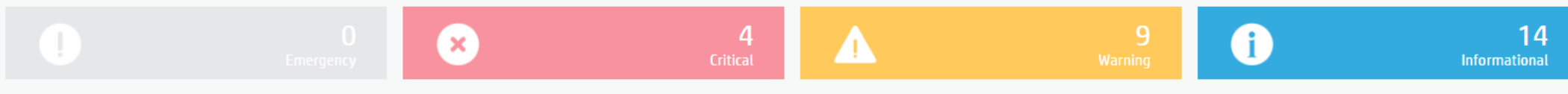
2 System Logs

Network Configuration >

Network Security >

System >

Tools >



System View

1 Network View

Access Points | Clients | Event Logs

1 0 0 1 | 1 0 4 9 14

- Actions
- Dashboard
- Quick Start >
- Monitoring **▼**
- Wireless Networks
- Access Points**
- Clients
- Wireless Security
- RF Monitoring
- Application Monitoring
- Wireless Configuration >
- Network Security >
- System >
- Tools >
- Reporting >

All Networks > Monitoring > Access Points > APs

APs | AP Groups

AP quantity

②

Online APs

✔ 1

Offline APs

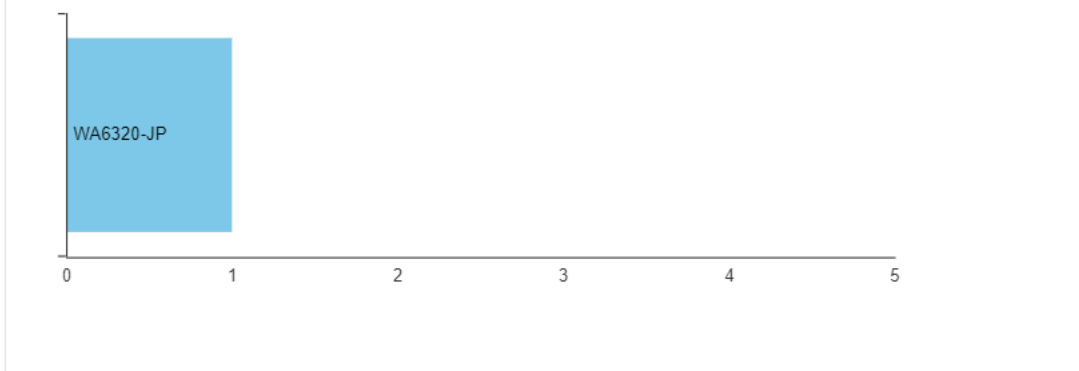
- 0

Unhealthy APs

! 0

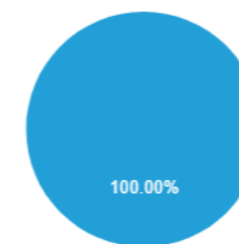
③

By AP model



By AP type

- Online manual APs
- Auto APs
- Offline manual APs
- Unauthenticated APs



System View

Network View

①

Access Points

✔ 1 - 0 ! 0

Clients

0

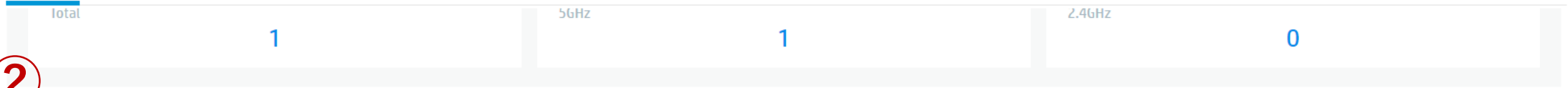
Event Logs

! 0 ✖ 4 ⚠ 7 ⓘ 5

- Actions
- Dashboard
- Quick Start >
- Monitoring **▼**
- Wireless Networks
- Access Points
- Clients**
- Wireless Security
- RF Monitoring
- Application Monitoring
- Wireless Configuration >
- Network Security >
- System >
- Tools >
- Reporting >

All Networks > Monitoring > Clients > Clients

Clients



2

By AP

AP Name	Clients(5GHz)	Clients(2.4GHz)
00dd-b6b1-7ca0	1	0

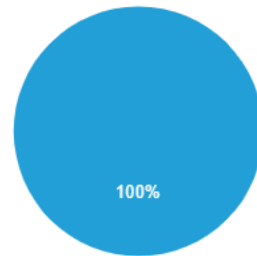
3

By SSID

SSID	Clients(5GHz)	Clients(2.4GHz)
guest	1	0

By Authentication Mode

- Open
- 802.1X
- MAC
- Portal
- MAC + Portal
- PSK + WEP



By radio type

- 802.11a(5GHz)
- 802.11n(5GHz)
- 802.11ac(5GHz)
- 802.11ax(5GHz)
- 802.11b(2.4GHz)
- 802.11g(2.4GHz)
- 802.11n(2.4GHz)
- 802.11ac(2.4GHz)



1

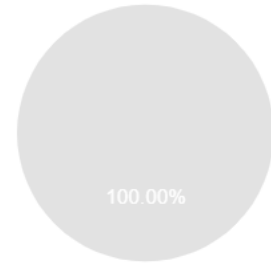
- Actions
- Dashboard
- Quick Start >
- Monitoring** v
- Wireless Networks
- Access Points
- Clients
- Wireless Security
- RF Monitoring**
- Application Monitoring
- Wireless Configuration >
- Network Security >
- System >
- Tools >
- Reporting >

All Networks > Monitoring > RF Monitoring > RRM

RRM

DFS 動的チャンネル選択

NO Calibration Information



TPC 動的送信パワー制御

AP Name	Radio	Date	Time
---------	-------	------	------

0/0

2

3

Bandwidth Adjustment 帯域幅調整

AP Name	Radio	Date	Time
00dd-b6b1-7ca0	5GHz(1)	2022-05-24	16:27:44

1/1

System View

Network View

1

Access Points | Clients | Event Logs

1 0 0 1 1 0 4 9 14

System > System > Event Logs > Event Logs

System Logs

Statistics ?

Search

Time	Level	Description	Actions
2022-05-24 15:47:50	Informational	System restarted -- H3C Comware Software.	...
2022-05-24 15:48:23	Error	Physical state on the interface WLAN-Radio1/0/1 changed to up.	...
2022-05-24 15:48:23	Error	Physical state on the interface WLAN-Radio1/0/2 changed to up.	...
2022-05-24 15:48:25	Informational	BSS 00dd-b6b1-7cb0 was created after service template service with SSID guest was bound to radio 2 on AP 00dd-b6b1-7ca0.	...
2022-05-24 15:48:25	Informational	BSS 00dd-b6b1-7ca0 was created after service template service with SSID guest was bound to radio 1 on AP 00dd-b6b1-7ca0.	...
2022-05-24 15:48:55	Notification	Line protocol state on the interface Vlan-interface1 changed to up.	...
2022-05-24 15:48:55	Error	Physical state on the interface Vlan-interface1 changed to up.	...
2022-05-24 15:48:55	Notification	Line protocol state on the interface GigabitEthernet1/0/1 changed to up.	...
2022-05-24 15:48:55	Error	Physical state on the interface GigabitEthernet1/0/1 changed to up.	...
2022-05-24 15:48:56	Informational	Nearest bridge agent neighbor created on port GigabitEthernet1/0/1 (IfIndex 1), neighbor's chassis ID is c4ca-d9a5-8ee9, port ID is GigabitEthernet1/0/2.	...
2022-05-24 16:04:49	Notification	Console logged in from con0.	...

Total 27 entries, 27 matched. Page 1 / 1.

エラーレベル	状況説明	重大度レベル
emergency(緊急)	システムは使用できません	重大度= 0
alert(アラート)	推奨アクションはすぐに実行する必要があります	重大度= 1
critical(クリティカル)	危機的な状態	重大度= 2
error(エラー)	エラー状態	重大度= 3
warning(警告)	警告条件	重大度= 4
notification(通知)	正常だが重大な状態	重大度= 5
informational(情報)	情報メッセージ	重大度= 6
debugging(デバッグ)	デバッグレベルのメッセージ	重大度= 7

Actions

Dashboard

Network Configuration

Network Interfaces

VLAN

Network Routing

Network Services

IP Services

DHCP/DNS

Multicast

ARP

ND

NAT

Management Protocols

Network Security

System > Network Configuration > Network Routing > Routing Table

Routing Table Static Routing

2 Routing Table

3

IPv4 routing table

13

>

4

IPv6 routing table

3

>

System View

1 Network View

Access Points Clients Event Logs

1 0 0 1 0 4 10 14

- Actions
- Dashboard
- Network Configuration ▾
- Network Interfaces
- VLAN
- Network Routing
- Network Services ▾
- IP Services
- DHCP/DNS
- Multicast
- ARP
- ND
- NAT
- Management Protocols
- Network Security >

System > Network Configuration > Network Routing > Routing Table

< IPv4 Routing Table

Statistics

2

3

Destination ▲	Mask Length	Protocol	Preference	Next Hop	Interface
0.0.0.0	0	Static	70	10.10.11.254	Vlan1
0.0.0.0	32	Direct	0	127.0.0.1	InLoop0
10.10.11.0	24	Direct	0	10.10.11.22	Vlan1
10.10.11.0	32	Direct	0	10.10.11.22	Vlan1
10.10.11.22	32	Direct	0	127.0.0.1	InLoop0
10.10.11.255	32	Direct	0	10.10.11.22	Vlan1
127.0.0.0	8	Direct	0	127.0.0.1	InLoop0
127.0.0.0	32	Direct	0	127.0.0.1	InLoop0
127.0.0.1	32	Direct	0	127.0.0.1	InLoop0
127.255.255.255	32	Direct	0	127.0.0.1	InLoop0
224.0.0.0	4	Direct	0	0.0.0.0	NULLO
224.0.0.0	24	Direct	0	0.0.0.0	NULLO
255.255.255.255	32	Direct	0	127.0.0.1	InLoop0

Total 13 entries, 13 matched. Page 1 / 1.

Navigation icons

System View

1

Access Points Clients Event Logs
✓ 1 ⊖ 0 ⊕ 0 1 ! 0 ✖ 4 ⚠ 10 i 14

Actions

System > Network Configuration > Network Services > ARP > ARP

Dashboard

Network Configuration

Network Interfaces

VLAN

Network Routing

Network Services

IP Services

DHCP/DNS

Multicast

ARP

ND

NAT

Management Protocols

Network Security

ARP

Address Resolution Protocol resolves IP addresses into MAC addresses on Ethernet networks.

IP Address	MAC Address	Type	VLAN	Interface	Actions
<input type="checkbox"/> 10.10.11.23	14-51-7E-CA-93-A2	Dynamic	1	GE1/0/1	
<input type="checkbox"/> 10.10.11.24	C8-E2-65-35-5D-0E	Dynamic	1	GE1/0/1	
<input type="checkbox"/> 10.10.11.25	5C-A7-21-F3-67-E0	Dynamic	1	GE1/0/1	
<input type="checkbox"/> 10.10.11.71	0C-DA-41-1D-EA-99	Dynamic	1	GE1/0/1	
<input type="checkbox"/> 10.10.11.72	0C-DA-41-1D-5A-4B	Dynamic	1	GE1/0/1	
<input type="checkbox"/> 10.10.11.73	0C-DA-41-1D-37-CC	Dynamic	1	GE1/0/1	
<input type="checkbox"/> 10.10.11.74	0C-DA-41-1D-B8-64	Dynamic	1	GE1/0/1	
<input type="checkbox"/> 10.10.11.75	0C-DA-41-1D-73-60	Dynamic	1	GE1/0/1	
<input type="checkbox"/> 10.10.11.76	0C-DA-41-1D-30-67	Dynamic	1	GE1/0/1	
<input type="checkbox"/> 10.10.11.77	0C-DA-41-1D-17-5E	Dynamic	1	GE1/0/1	
<input type="checkbox"/> 10.10.11.78	0C-DA-41-1D-DB-AB	Dynamic	1	GE1/0/1	

Total 14 entries, 14 matched, 0 selected. Page 1 / 1.

診断情報はSystem view > Tools > Debug > Collect > xxxx.tar.gz形式でPCへダウンロードされます 76
※Ciscoのshow tech support相当

H3C WA6320-JP Save Roadmap admin

System > Tools > Debug > Diagnostics

Actions

Dashboard

Network Configuration >

Network Security >

System >

Tools **2**

Debug **3**

Ping

Tracert

Diagnostics

Collect **4**

1 System View Network View

Access Points: 1 ✓ 0 0
Clients: 0
Event Logs: 0 4 4 6

診断情報は同時にAPのflashにも保存されますので、PCにダウンロードできます。

System > System > File Systems > File System Management

File System Management

flash:

Total: 115343360 bytes, Used: 100311040 bytes, Free: 15032320 bytes

1

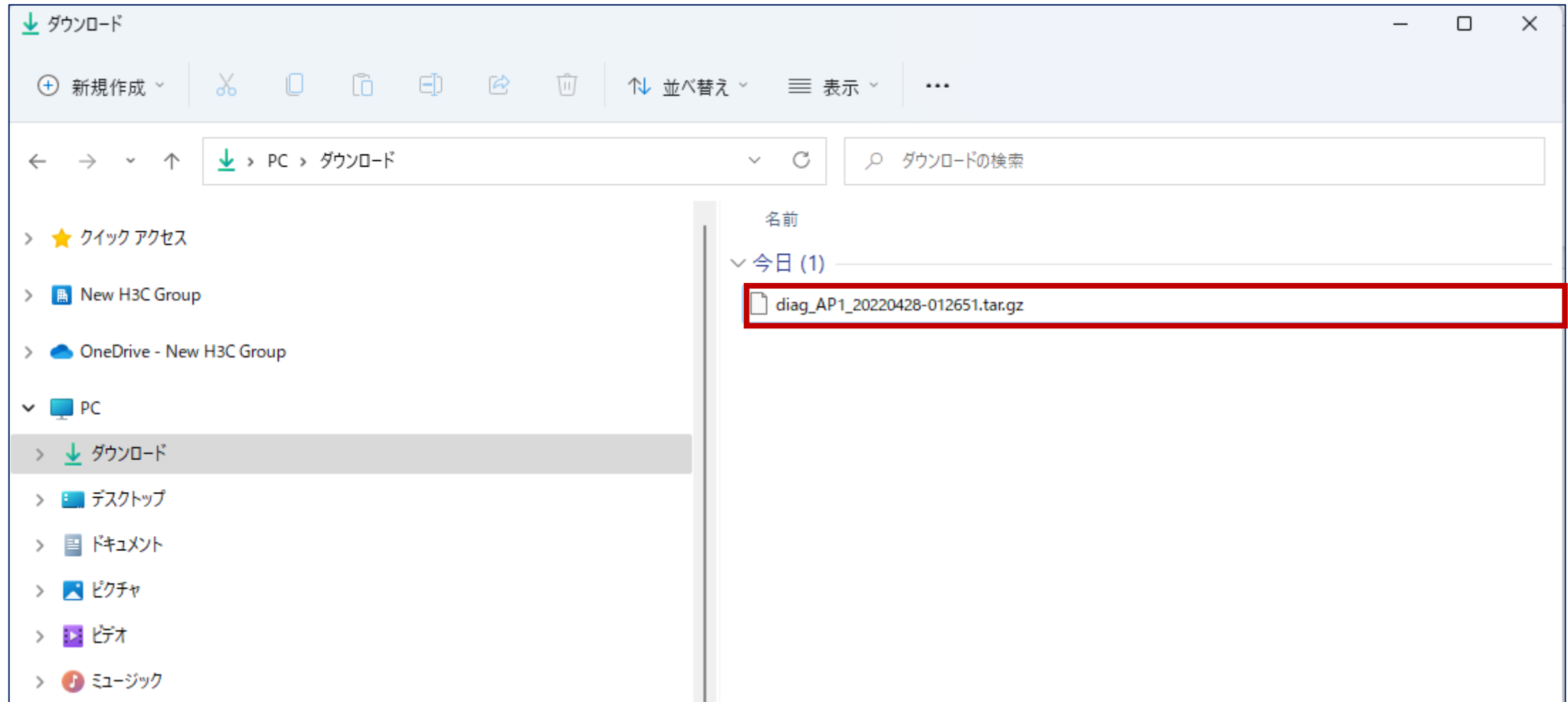
Name	Size(bytes)	Time	Directory	Actions
flash:/WA6300-CMW710-R2453P01.ipe	48091136	2022-02-22 12:03:48	No	
flash:/anchor-ac		2022-02-22 11:55:40	Yes	
2 flash:/anchor-ac/startup.cfg	3165	2022-05-24 20:20:05	No	
flash:/background-logon.jpg	133328	2022-04-14 15:39:18	No	
flash:/cloud		2022-05-10 04:33:23	Yes	
flash:/cloud/startup.cfg	17704	2022-05-24 07:06:54	No	
flash:/defaultfile.zip	260649	1970-01-01 00:00:20	No	
3 <input checked="" type="checkbox"/> flash:/diag_H3C_20220526-184506.tar.gz	105321	2022-05-24 16:02:00	No	
flash:/diagfile		2022-02-21 11:36:30	Yes	
flash:/dsakey	567	2022-05-24 07:06:14	No	

Total 27 entries, 27 matched, 1 selected. Page 1 / 1.

4

Delete Download

PCにダウンロードされたAPの診断ファイル



Actions

Dashboard

Network Configuration >

Network Security >

System **2**

Event Logs

Resource

File Systems

Administrators

Management **3**

Tools >

System > System > Management > Reboot

Settings Configuration Upgrade **Reboot 4**

Reboot Device 5

System View **1** Network View

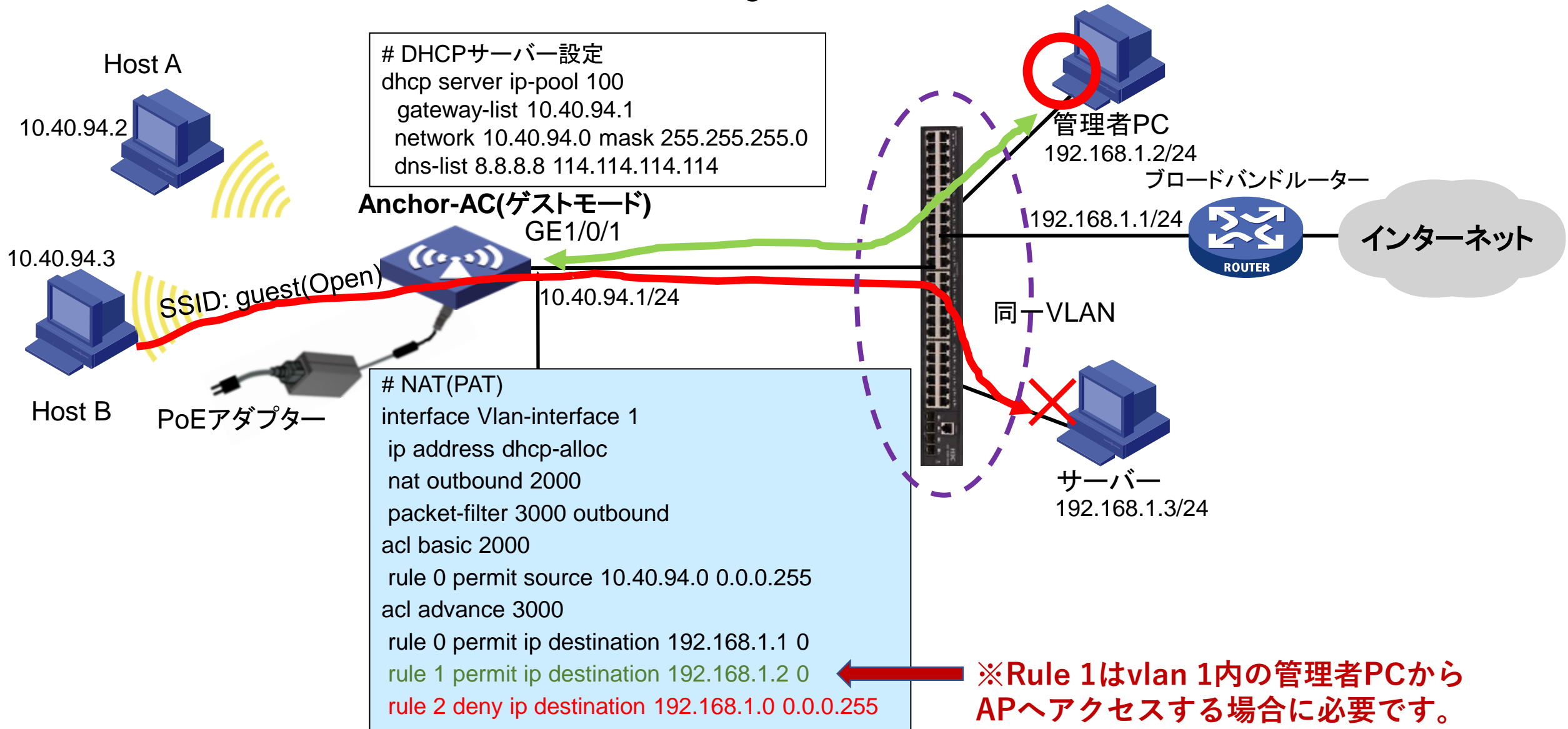
Access Points	Clients	Event Logs
✓ 1 - 0 ! 0	1	! 0 ✖ 4 ⚠ 10 i 14



- 01 アクセスポイントをAnchor-acに設定する
- 02 Anchor-acをゲストモードにする
- 03 動作確認
- 04 完成した設定のコマンド
- 05 オプション:クライアントのAP接続の最適化
- 06 トラブルシューティング
- 07 アップリンクにある装置へのアクセス制限
- 08 マニュアルについて

ゲスト(オープン認証)

Anchor-ACと同じVLANに属する社内のサーバーへguestに接続したクライアントにアクセスさせない方法



H3C WA6320-JP Save Roadmap | admin

System > System > Resource > IPv4 ACL

IPv4 ACL Layer 2 ACL Time Range

IPv4 ACLs

Search

<input type="checkbox"/> ACL Category ▲	ACL	Rules	Match Order	Step	Description	Actions
<input type="checkbox"/> advanced	default	2	Config	5		

Total 1 entries, 1 matched, 0 selected. Page 1 / 1.

System View Network View

Clients: 1 | Event Logs: 0 (info), 10 (error), 22 (warning), 83 (info)

応用ACLでACL番号を3000として作成

Actions

Dashboard

Network Configuration >

Network Security >

System ▾

Event Logs

Resource

Management

Tools >

System > System > Resource > IPv4 ACL > New IPv4 ACL

ACL Category *

ACL *

Rule match order

Rule numbering step

Description

Apply

Cancel

 Basic Advanced

3000

(3000-3999 or 1-63 chars)

 Config Auto

1

(1-20)

deny access to internal server

(1-127 chars)

 Continue to add rule

宛先IPアドレスに対してアクセス禁止のルールを作成(続けて別のルールを追加)

The screenshot shows the H3C WA6320-JP web interface for configuring an IPv4 ACL. The breadcrumb path is System > System > Resource > IPv4 ACL > New IPv4 ACL > New Rule For IPv4 Advanced ACL. The configuration form includes the following fields:

- ACL: 3000 (3000-3999 or 1-63 chars)
- Rule ID: (0-65535) Auto numbered
- Description: (1-127 chars)
- Action: Permit Deny
- IP protocol: 256 (0-256)
- Match criterion:
 - Source IP address/wildcard mask
 - Destination IP address/wildcard mask: 192.168.1.1 / 0.0.0.0
 - Source port in TCP/UDP packet
 - Destination port in TCP/UDP packet
 - Established TCP connection
 - TCP flag
 - ICMP message type
 - DSCP priority
 - IP precedence priority
 - TOS priority
- Time range: (empty)
- Fragments: Only apply to non-first fragments
- Logging: Log matching packets
- Counting: Count the number of times this rule has been matched
- Continue to add next rule

Buttons: Apply, Cancel

※permit ip destination 192.168.1.1 0に相当

宛先IPアドレスに対してアクセス禁止のルールを作成(続けて別のルールを追加)

The screenshot shows the H3C WA6320-JP configuration interface for creating a new IPv4 ACL rule. The breadcrumb path is System > System > Resource > IPv4 ACL > New IPv4 ACL > New Rule For IPv4 Advanced ACL. The interface includes a left sidebar with navigation options like Dashboard, Network Configuration, Network Security, System, Event Logs, Resource, Management, and Tools. The main configuration area is titled 'New Rule For IPv4 Advanced ACL' and contains the following fields and options:

- ACL:** 3000 (3000-3999 or 1-63 chars)
- Rule ID:** (0-65535) with the **Auto numbered** option selected.
- Description:** (1-127 chars)
- Action:** **Permit** / Deny
- IP protocol:** 256 (0-256)
- Match criterion:**
 - Source IP address/wildcard mask
 - Destination IP address/wildcard mask: 192.168.1.2 / 0.0.0.0
 - Source port in TCP/UDP packet
 - Destination port in TCP/UDP packet
 - Established TCP connection
 - TCP flag
 - ICMP message type
 - DSCP priority
 - IP precedence priority
 - TOS priority
- Time range:** (empty)
- Fragments:** Only apply to non-first fragments
- Logging:** Log matching packets
- Counting:** Count the number of times this rule has been matched
- Continue to add next rule

At the bottom, there are **Apply** and **Cancel** buttons. A red box highlights the 'Continue to add next rule' checkbox.

※permit ip destination 192.168.1.2 0に相当

宛先IPアドレスに対してアクセス禁止のルールを追加して完成

The screenshot shows the H3C WA6320-JP configuration interface for creating a new IPv4 ACL rule. The breadcrumb path is: System > System > Resource > IPv4 ACL > Edit IPv4 ACL > New Rule For IPv4 Advanced ACL.

Configuration details:

- ACL ID: 3000 (3000-3999 or 1-63 chars)
- Rule ID: (0-65535) Auto numbered
- Description: (1-127 chars)
- Action: Permit Deny
- IP protocol: 256 (0-256)
- Match criterion: Source IP address/wildcard mask Destination IP address/wildcard mask
- Destination IP address/wildcard mask: 192.168.1.0 / 0.0.0.255
- Other match criteria (all unchecked): Source port in TCP/UDP packet, Destination port in TCP/UDP packet, Established TCP connection, TCP flag, ICMP message type, DSCP priority, IP precedence priority, TOS priority, Only apply to non-first fragments, Log matching packets, Count the number of times this rule has been matched.
- Counting: Continue to add next rule

Buttons: Apply, Cancel

※deny ip destination 192.168.1.0 0.0.0.255に相当

ACLを適用するインタフェースを指定する

The screenshot displays the H3C WA6320-JP web management interface. The top navigation bar includes the H3C logo, the model number WA6320-JP, and user options for Save, Roadmap, and admin. The left sidebar contains a menu with 'Network Security' and 'Packet Filter' highlighted in red. The main content area shows the 'Packet Filter' configuration page, with a table header containing columns for Interface, Direction, Filter, ACL, State, Counting, and Actions. A red box highlights the '+' icon in the top-left corner of the table area. At the bottom, the 'Network View' tab is selected and highlighted in red. The bottom right corner shows system status indicators for Clients (1) and Event Logs (0 errors, 10 warnings, 26 info).

Actions

Dashboard

Quick Start >

Monitoring >

Wireless Configuration >

Network Security >

Packet Filter

Traffic Policy

Access Control

Authentication

User Management

Access Control

System >

Tools >

Reporting >

All Networks > Network Security > Packet Filter > Packet Filter

Packet Filter

Packet Filter

Interface

+

Search

Interface	Direction	Filter	ACL	State	Counting	Actions
-----------	-----------	--------	-----	-------	----------	---------

Total 0 entries, 0 matched, 0 selected. Page 1 / 1.

Delete

System View Network View

Clients 1

Event Logs 0 10 26 84

Vlan 1から出力する際にACL 3000のルールを適用する

Actions

All Networks > Network Security > Packet Filter > Packet Filter

Interface *
Vlan1

Direction *
 Inbound Outbound

Packet filter *
 IPv4 ACL IPv6 ACL Ethernet frame header ACL User defined ACL Default action

ACL *
3000

Apply Cancel

Dashboard

Quick Start >

Monitoring >

Wireless Configuration >

Network Security >

Packet Filter

Traffic Policy

Access Control

Authentication

User Management

Access Control

System >

Tools >

Reporting >

これまでの操作で生成されたコマンド

```
#  
interface Vlan-interface1  
 ip address dhcp-alloc  
 tcp mss 1400  
packet-filter 3000 outbound  
 nat outbound 2000  
#  
acl advanced 3000 match-order auto  
 description deny access to internal server  
 step 1  
rule 0 permit ip destination 192.168.1.1 0  
rule 1 permit ip destination 192.168.1.2 0  
rule 2 deny ip destination 192.168.1.0 0.0.0.255  
#
```



- 01 アクセスポイントをAnchor-acに設定する
- 02 Anchor-acをゲストモードにする
- 03 動作確認
- 04 完成した設定のコマンド
- 05 オプション:クライアントのAP接続の最適化
- 06 トラブルシューティング
- 07 アップリンクにある装置へのアクセス制限
- 08 マニュアルについて

マニュアルのダウンロードサイト

https://www.h3c.com/jp/



http://www.h3c.com/en/Support/Resource_Center/Technical_Documents/

ログイン 国/地域 検索

H3C 製品・技術 ソリューション サポート ① 研修・認定 パートナー企業 会社概要

サポート

すべて表示 >

リソースセンター

ソフトウェアのダウンロード
知識ベース

テクニカルドキュメント ②
テクニカルドキュメント

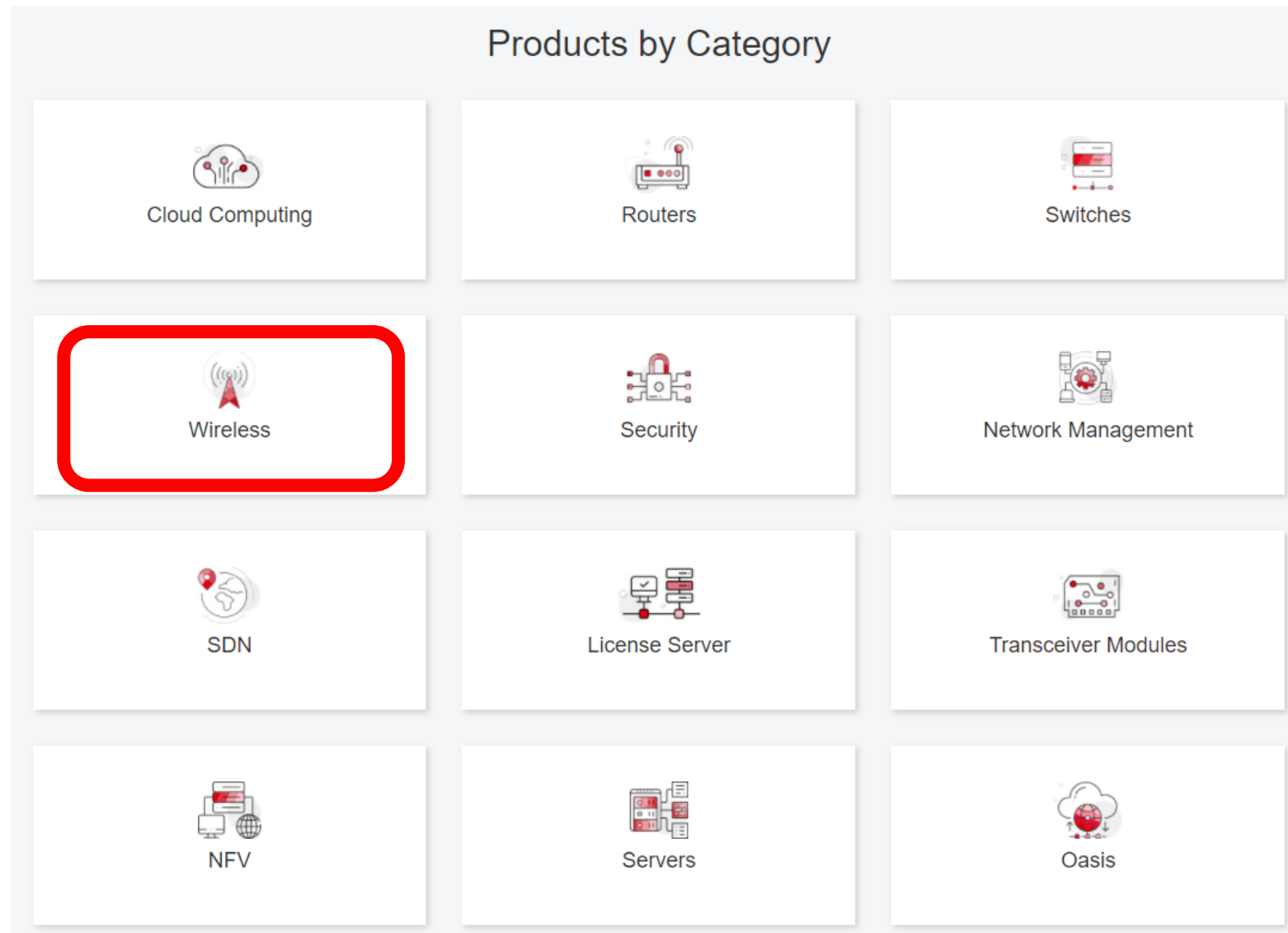
ポリシー

サービス掲示板
チャンネルサービス

製品ライフサイクル管理戦略
サービス・保証

オンラインヘルプ

製品カテゴリーの選択



個別製品の選択

H3C WX1800H Series Access Controllers

H3C WX1800H Series Access Controllers

[Learn More →](#)

H3C WX5800H Series Access Controllers

H3C WX5800H Series Access Controllers

[Learn More →](#)

H3C 802.11ax Series Access Points

H3C WA6638 Access Point

[Learn More →](#)

H3C WX3800H Series Access Controllers

H3C WX3800H Series Access Controllers

[Learn More →](#)

H3C 802.11ac Wave2 Series Access Points

H3C WA510H Access Point

[Learn More →](#)

H3C WA6636 Access Point

[Learn More →](#)

H3C WA530 Access Point

[Learn More →](#)

H3C WA6630X Access Point

[Learn More →](#)

H3C WA530X Access Point

[Learn More →](#)

H3C WA6628X Access Point

[Learn More →](#)

設置、コマンド、コンフィグ、保守マニュアル

[Products & Technology](#) ▾[Solutions](#) ▾[Support](#) ▾[Training & Certification](#) ▾[Partners](#) ▾[About](#)[Technical Documents](#)[Software Download](#)[Knowledge Base](#)

Technical Documents

[Trending](#)[Install](#)[Command](#) →[Configure](#)[Maintain](#)

Command References

Title	Date
H3C Access Controllers Command References(R5426P02)-6W103	10-12-2020
→ 00-About the H3C command references	
→ 01-License Management Command Reference	
→ 02-Fundamentals Command Reference	
→ 03-System Management Command Reference	
→ 04-Interface Command Reference	
→ 05-Network Connectivity	
→ 06-WLAN Access Command Reference	
→ 07-AP and WT Management Command Reference	
→ 08-WLAN Security Command Reference	

日本語資料、FAQなど準備中

https://h3cgroup-my.sharepoint.com/:f:/g/personal/gw_koshiromasahiro_h3c_com/EiBUlIdoWxFDnfFta80H7N4B6bQhI1dv263wp-SoMyJ36g?e=cmzjxu

 名前 ▾	更新日時 ▾	更新者 ▾	ファイルサイズ ▾
 Certification	4 日前	koshiromasahiro gw35...	1 個のアイテム
 common	3月17日	koshiromasahiro gw35...	5 個のアイテム
 firewall	3月17日	koshiromasahiro gw35...	9 個のアイテム
 Oasis	3月19日	koshiromasahiro gw35...	5 個のアイテム
 Switch	3月19日	koshiromasahiro gw35...	4 個のアイテム
 wireless	3月17日	koshiromasahiro gw35...	3 個のアイテム

Anchor-ACモードのデフォルトのコンフィグ (telnet/http/httpsでのアクセスが可能)

```

#
version 7.1.064, Release 2451
#
sysname H3C
#
wlan global-configuration
#
telnet server enable
#
port-security enable
#
lldp global enable
lldp hold-multiplier 8
#
password-recovery enable
#
vlan 1
#
interface NULL0
#
interface Vlan-interface1
ip address 192.168.0.50 255.255.255.0
#
interface GigabitEthernet1/0/1
#
interface WLAN-Radio1/0/1
#
interface WLAN-Radio1/0/2
#
scheduler logfile size 16
#

line class console
user-role network-admin
#
line class vty
user-role network-operator
#
line con 0
user-role network-admin
#
line vty 0 31
authentication-mode scheme
user-role network-operator
#
line vty 32 63
user-role network-operator
#
domain system
#
domain default enable system
#
role name level-0
description Predefined level-0 role
#
role name level-1
description Predefined level-1 role
#
role name level-2
description Predefined level-2 role
#
role name level-3
description Predefined level-3 role
#
role name level-4
description Predefined level-4 role
#
role name level-5
description Predefined level-5 role
#
role name level-6
description Predefined level-6 role
#
role name level-7
description Predefined level-7 role
#
role name level-8
description Predefined level-8 role
#
role name level-9
description Predefined level-9 role
#
role name level-10
description Predefined level-10 role
#
role name level-11
description Predefined level-11 role
#
role name level-12
description Predefined level-12 role
#
role name level-13
description Predefined level-13 role
#
role name level-14
description Predefined level-14 role
#
user-group system
#
local-user admin class manage
password simple h3capadmin
service-type telnet http https
authorization-attribute user-role network-admin
#
ip http enable
ip https enable
#
undo attack-defense tcp fragment enable
#
wlan ap-group default-group
vlan 1
#
wlan ap xxxx-xxxx-xxxx model WA6320-JP
serial-id xxxxxxxxxxxxxxxxxxxxxx
mac-address xxxx-xxxx-xxxx
anchor-ap disable
radio 1
radio 2
gigabitethernet 1
#
return

```

無線アクセスコントローラーとしての機能一覧

大項目	中項目	Anchor-AC
基本機能	デフォルト管理AP数	50(WA6638), 32(WA6320)
	ライセンスサイズ	—
	最大管理可能AP数	50(WA6638), 32(WA6320)
	最大同時ユーザー数	512
802.11MAC	802.11プロトコル	サポート
	マルチSSID(RF当たり)	16
	SSIDの非表示	サポート
	802.11G 保護	サポート
	802.11nオンリー	サポート
	ユーザー数の制限	SSIベース/RFベースをサポート
	キープアライブ	サポート
	アイドル	サポート
	複数の国コード割当て	サポート
	40MHzモードの20MHz/40MHzの自動スイッチ	サポート
	ローカル転送	デフォルトのローカル転送
CAPWAP	自動シリアル番号入力	サポート
	AC検出 (DHCPオプション43、DNS)	サポート
	IPv6トンネル	サポート
	Clock同期	サポート
	Jumbo frame転送	サポート
	ACを介してAPの基本的なNWパラメータを割り当てる	サポート: 静的IP、VLAN、接続されたACアドレス
	APとAC間のL2 / L3接続	サポート
	APとAC間のNATトラバース	非サポート

大項目	中項目	Anchor-AC
ローミング	AC内のAP間でのL2と3ローミング	サポート
G/W機能	NAT	サポート
	PPoE	非サポート
	DDNS	非サポート
	SSL-VPN	非サポート
	IPsec-VPN	非サポート
	RIP	非サポート
	GRE	非サポート
アクセス制御	オープンシステム シェアードキー	サポート
	WEP-64/128, 動的WEP	サポート
	WPA, WPA2	サポート
	TKIP	サポート
	CCMP	サポート(802.11nを推奨)
	SSH v1.5/v2.0	サポート
	ワイヤレスEAD (エンドポイントアクセスコントロール)	サポート
	ポータル認証	サポート: リモート認証、外部サーバー
	802.1x認証	EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-MD5, EAP-GTC
	ポータルページヘリダイレクション	サポート: SSIDベース、APポータルページ プッシュ
ローカル認証	802.1x、ポータル、MAC認証	

大項目	中項目	Anchor-AC
	ローカル認証	802.1x、ポータル、MAC認証
	LDAP認証	非サポート
	APロケーションベースのユーザーアクセス制御	サポート
	ゲストアクセス制御	サポート
	VIPチャンネル	サポート
	ARP攻撃検知	サポート:ワイヤレスSAVI
	SSIDなりすまし防御	SSIDとユーザー名をバインド
	SSID&ドメインでAAAサーバー選択	サポート
	AAAサーバーバックアップ	サポート
	ワイヤレスユーザー用のローカルAAAサーバー	サポート
	TACACS+	非サポート
QoS	プライオリティ マッピング	サポート
	L2-L4パケットフィルタリングとトラフィック分類	非サポート
	レート制限	非サポート
	802.11e/WMM	サポート:8Kbpsの粒度でサポート
	ユーザープロファイルに基づくアクセス制御	サポート
	インテリジェントな帯域幅制限(等帯域幅共有アルゴリズム)	非サポート
	インテリジェントな帯域幅制限	非サポート
	インテリジェントな帯域保証	非サポート

大項目	中項目	Anchor-AC
	SVPフォンへのQoS最適化	サポート
	コールアドミッション制御(CAC)	サポート: ユーザー数/帯域幅ベース
	End to End QoS	サポート
	APアップロード速度制限	サポート
RF管理	国コードロック	サポート
	静的なチャネルと電力の設定	サポート
	自動的なチャネルと電力設定	サポート
	自動的な伝送レート調整	サポート
	カバレッジホールの検出と修正	サポート
	ロードバランシング	サポート: トラフィック、 ユーザー
	インテリジェントロードバランシング	サポート
APロードバランシンググループ	サポート: 自動検出と柔軟な設定	
セキュリティ	静的ブラックリスト	サポート
	動的ブラックリスト	サポート
	不正APの検出	サポート: SSIDベース、BSSID、デバイスOUIなど
	不正AP対策	サポート
	フラッディング攻撃の検出	サポート
	なりすまし攻撃の検出	非サポート
	WeakIV攻撃の検出	サポート
WIPS	サポート: 7層モバイルセキュリティ	

大項目	中項目	Anchor-AC
レイヤ2プロトコル	ARP	サポート
	802.1p	サポート
	802.1q	サポート
	802.1x	サポート
	IPv4プロトコル	サポート
	Native IPv6	サポート
	IPv6 SAVI	非サポート
	IPv6 portal	サポート
マルチキャスト	MLD スヌーピング	サポート
	IGMP スヌーピング	サポート
	マルチキャストグループ	非サポート
	マルチキャストからユニキャストへ (IPv4、IPv6)	サポート:動作環境に基づいてユニキャスト制限を設定します
冗長性	AC間の1 + 1フェイルオーバー	非サポート
	AC間のインテリジェントAP共有	非サポート
	リモートAP	非サポート
	メッシュネットワーク	非サポート
管理と展開	ネットワーク管理	WEB、RMON等 SNMP v1/v2/v3
	ネットワーク展開	WEB、CLI、Telnet、FTPなど
WiFiロケーション	CUPIDロケーション	非サポート
グリーン機能	AP RFインターフェイスの スケジュールされたシャットダウン	サポート
	ワイヤレスサービス計画的なシャットダウン	サポート
	パケット毎の電力調整(PPC)	非サポート

大項目	中項目	Anchor-AC
LAN アプリケーション	RF Ping	サポート
	リモートプローブ分析	サポート
	リアルタイム スペクトラム・ガード	非サポート
	wIAA	非サポート
	パケット転送の公平性の調整	非サポート
	802.11nパケット転送抑制	非サポート
	アクセスベースのトラフィックシェーピング	非サポート
	Co-APチャンネル共有	非サポート
	Co-APチャンネルの再利用	非サポート
	RFインターフェースの 伝送速度調整アルゴリズム	非サポート
	信号が弱いワイヤレスパケット をドロップする	非サポート
	電波の弱いユーザーアクセスを 無効にする	非サポート
	マルチキャストパケットキャッシング を無効にする	非サポート
	ステータスの点滅	サポート
新機能	ポリシー転送	非サポート
	VLANプール	非サポート
	Bonjour gateway	サポート
	802.11w	サポート
	802.11k	サポート
	Hotspot2.0 (802.11u)	非サポート
	VPN	サポート

項目	WA6320-JP	WA6638-JP
メモリー	512M	1024M
Flash	128M	8M NOR+256M NAND
対応規格、 デュアル/トリプル帯域	802.11a/b/g/n/ac/ax (WiFi6)、デュアルバンド	802.11a/b/g/n/ac/ax (WiFi6)、トリプルバンド
MU-MIMO	ダウンリンク/MU-MIMO	ダウンリンク/アップリンク MU-MIMO
2.4GHz帯アンテナ数 /無線スループット	2x2/0.575Gbps	4x4/1.15Gbps
5GHz帯アンテナ数 /無線スループット	2x2/1.2Gbps	4x4 +4x4/2.4G+2.4Gbps

H3C

www.h3c.com