Technical Guide

CAPWAP Tunnel Configuration

Released: 2016-10-28
Doc Rev No: R1
# TABLE OF CONTENTS

1. Introduction ........................................................................... 2
2. Established CAPWAP Channels ........................................... 3
3. Complete Tunnel ..................................................................... 4
4. Split Tunnel ........................................................................... 5
5. Application ............................................................................. 6
6. Standard Operating Procedures ............................................. 7
   6.1 Configure CAPWAP Settings on the Controller ...................... 7
   6.2 Configure Template for Remote AP Configuration ................ 7
   6.3 Pre-deployment or On-site Configuration ............................... 10
   6.4 AP List for managing APs .................................................. 10
7. Remarks ................................................................................... 12
1. Introduction

There are several benefits of using Wide Area AP Management on a Controller. Main Benefits of Wide Area AP Management:

- Cross Layer 3 IP network management
- Centralized traffic forwarding for distributed remote AP sites.
- Graphical Map utility for easy reference and deployment planning.
- Traffic transmit statistics for 3rd party AP devices.
- CAPWAP supported, complete tunnel and split tunnel.

CAPWAP is a standard interoperable protocol that enables a Controller to manage a collection of wireless access points. Two tunneling options are available: complete tunnel and split tunnel.

The following figure illustrates the centralized management of a remote network utilizing CAPWAP and its security protocol, Datagram Transport Layer Security **DTLS** Tunnel establishment.
2. Established CAPWAP Channels

The information between the remote Controller and the remote Access Points are divided into two channels; the Control Channel and the Data Channel. The Control Channel includes the management and authentication traffic while the Data Channel includes the data traffic.

What makes the WAPM feature impressive is its ability to pass though Network Address Translations, NAT’s, to manage remote Access Points with a private IP address such as 192.168.10.1. This is possible due to the two channels and the ports they utilize.

Other than separating the types of data transferred between the Controller and Access Point, the Control Channel uses the UDP port 5246 and the Data Channel uses the UDP port 5247 allowing remote management in layer 3 networks.

Businesses and organization with multiple branches or remote offices are able to apply this Remote Management Technology to monitor individual networks from a centralized interface such as the Controller.
3. Complete Tunnel

**Complete Tunnel** uses the CAPWAP protocol to communicate with an Access Point so that all management traffic, authentication traffic and data traffic from the service area Access Point provided are transmitted back to the Controller, before forwarding data traffic to the internet. The Controller is able to implement role-based policies over Layer 3 networks, with user access control available in the remote sites. This feature allows the Controller to fully support centralized Access Point management and user management.
4. Split Tunnel

For Split tunnel, only user authentication related traffic will be directed back to the controller. For authenticated users, data traffic will go to the Internet through the local network directly. The user data can be transmitted with a shorter path and the network load of the controller can also be reduced.

Internet Traffic going through the local ISP without having to re-route back to the centralized server provides an effective solution to bottle-necking and bandwidth congestion. Allowing user data traffic to exit locally means there are several limitations on the application and usage of Split Tunnel.

Split tunnel limitations to the network topology and user management:

- Tag-Based mode only
- WAN1 support only
- Policy Enforcement (Firewall, QoS, Specific Route) not supported
- Privilege List (IP Privilege, MAC Privilege) not supported
- Tunnel Port Location Mapping not supported

Statuses of users authenticated through established Split tunnels are updated periodically by the Controller through Accounting Traffic’s interim updates. User Access Controls such as Idle Timeout and kicking off users are in effect through the Controller.
5. Application

Controller proposes the latest solution to networks requiring centralized authentication across multiple remote branches. Split Tunnel allows users to be authenticated by the Controller located at your main site. There are many market sectors that value and prioritize high-performance and reliability. An example of split tunnel utilized in a network scenario for an educational institution at different sites is illustrated below.

The Bring Your Own Device (BYOD) trend has been the major factor in a need to improve network performance. With thousands of students and staffs accessing online content, a single server such as the built-in internal authentication server on the Controller or an external RADIUS server can be utilized to authenticate users from institutions located in different cities. Split Tunnel provides additional benefits in reducing cost and maintenance efforts.

Split tunnel Benefits:

- Reduced CapEx and OpEx
- Reduced bandwidth and bottle-necking
- Centralized interface for monitoring and maintenance
6. Standard Operating Procedures

6.1 Configure CAPWAP Settings on the Controller

Step 1. Enable **CAPWAP Status** under CAPWAP Tab in WAPM

Note: **Certificate** field can be modified with uploaded certificate if required.
Note: Not recommended to modify **IP Address** and **Netmask** for **Control Channel**.

![CAPWAP Configuration](image)

Main › Device Management › Wide Area AP Management › CAPWAP

6.2 Configure Template for Remote AP Configuration

![Template AP Setting](image)

Step 1. Confirm the specifications of the AP before configuring the Template.

Step 2. Configure **Template**.

Step 3. Configure **General Settings**.

Step 4. Confirm selected **Bands** is supported on both **RF Card A & B**.
Step 5. Click Apply and return to Template page.

Step 6. Configure VAP Configuration.

Step 7. Enable VAP.

Step 8. Fill in a Profile Name and ESSID.

Step 9. Configure VAPs with Complete Tunnel or Split Tunnel.

Note: Examples for configuring both CAPWAP tunnels types are provided in Steps 10 & 11.
Step 10. Complete Tunnel Configuration Example.
   a. Select **Complete Tunnel** under **CAPWAP Tunnel Interface**.
   b. Select **Service Zone** for AP to be managed and Apply.

Step 11. Split Tunnel Configuration Example.
   a. Select **Split Tunnel** under **CAPWAP Tunnel Interface**.
   b. Select **Service Zone** and Apply.

Note: VLAN configured in Split Tunnel is different from Complete Tunnel as its VLAN is solely based on the local router instead of the Controller.
6.3 Pre-deployment or On-site Configuration

Step 1. Enable **CAPWAP** on AP’s WMI.
Step 2. Enable only **Static Discovery**.
Step 3. Enter and Apply **AC’s WAN IP Address into field**.
Step 4. Reboot as required.

**Note:** Static discovery is the most recommended discovery method since it is intuitive to implement without any pre-settings to complete in advance. Simply enable the function and type in the IP address of the Controller that will manage this AP.

6.4 AP List for managing APs

Step 1. Confirm remote AP added has CAPWAP tunnel established.
Step 2. Go to AP Admin Web’s **System Overview**.
Step 3. Confirm CAPWAP’s Status field is RUN (WAN IP)
Step 4. Apply the configured Template to your added Access Points.

Successful CAPWAP joining will lead to the Access Point being listed in the managed AP list, as illustrated below:

CAPWAP column will display a ‘RUN’ status, and the tunnel status will show a clickable ‘Edit’ button in black if a VAP is configured to be tunneled back to the controller.
The Access Point’s WMI will show the VAP enabled, the VAP’s tunnel status with a green checkmark and the CAPWAP status on the System Overview page:

On the Access Point side, a successful CAPWAP will display the Status as Run and followed by the AC’s IP Address. The Data Channel as Active indicates both Control and Data Channels are successfully established.
7. Remarks
For more information, please contact our Technical Support team.

NOTE
1. Access Point tunnels will be established automatically when the CAPWAP template has selected VAP to be enabled and tunneled back to a SZ.
2. If the CAPWAP discovery process fails, please check the certificate settings used on the Controller and the certificate uploaded into the AP.
3. Controllers CAPWAP Log may be referenced during trouble shooting process.