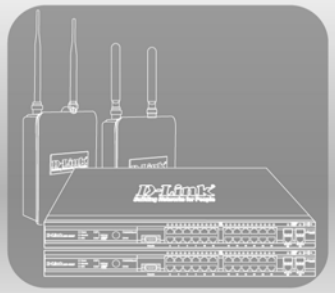


Unified Wired & Wireless Access System

Deployment Guide

Product Model: DWS-3000 Series, DWL-3500AP/8500AP

Version 1.0

Introduction

This document is to provide an overview of the variety of ways in which D-Link's wireless solution can be deployed by customers. It would also point out a few pointers to be kept in mind either as limitations or cautions to be taken while deploying the solution in a customer environment.

There are 3 unique features that D-Link's solution has which can be taken advantage of while proposing our solution in competition to other vendors based on the unique needs a customer's network may have.

1. Our solution can be deployed either as an Overlay Device (also called a Wireless Controller) or as an Edge Device that can leverage all the traditional wired functionality built into our switch.

2. Support for Peer Switches – Up to 4 Peer Switches can be supported in the same Wireless Domain with each of the Switches capable of managing 48 Access Points effectively enabling the network scale to a maximum of 192 APs. This Unified Access System can manage up to 2000 wireless clients simultaneously making it suitable for large-scale deployments.

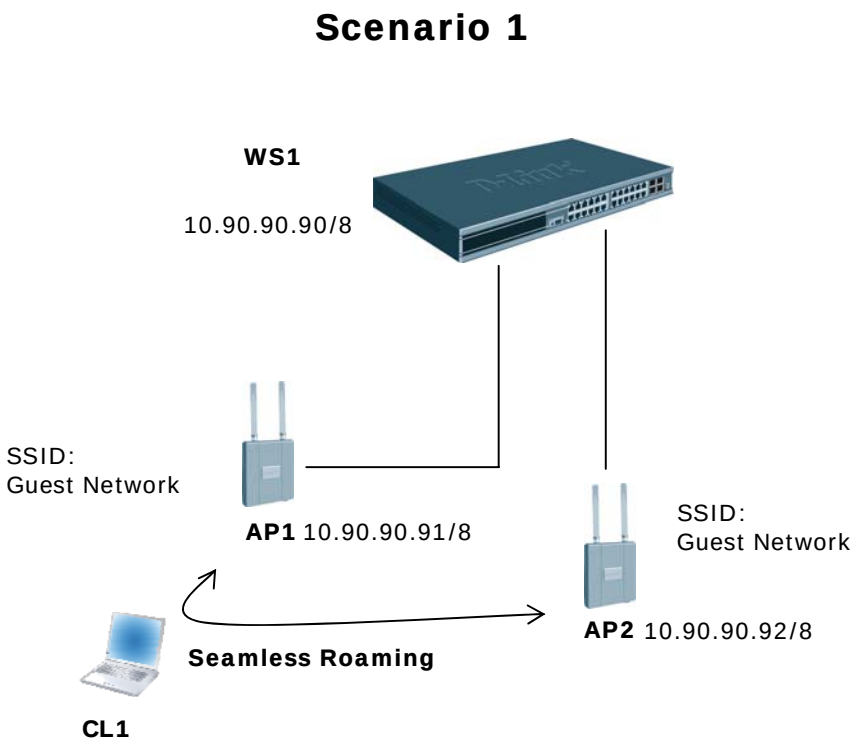
3. When the Access Points are in different IP subnets, the clients can still roam seamlessly across the access points with a feature called L3 Fast Roaming. This feature is mainly intended for Wireless VoIP communication using wi-fi phones and other such devices which require the clients to maintain their IP addresses even as they roam within the wireless domain. This is accomplished by the *Tunneled Data Forwarding* mode that is supported by the solution.

Deployment Scenarios

Given below are some of the typical deployments -

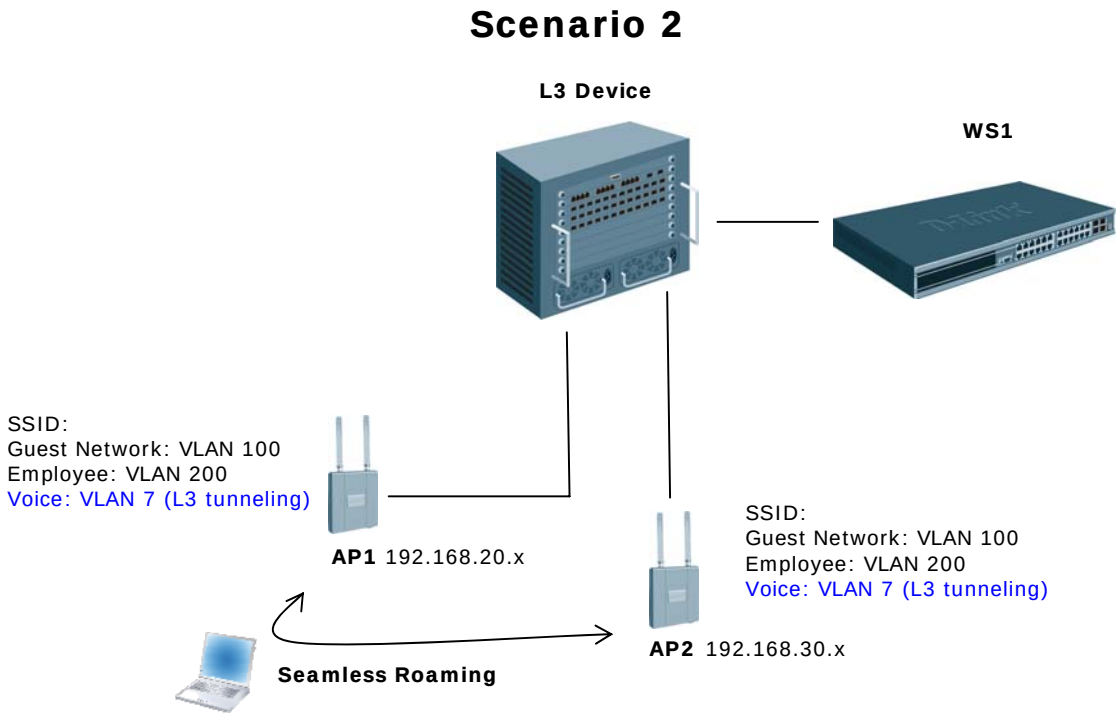
Deployment Scenario 1 – WS and AP are in the same subnet:

This deployment may consist of a single or multiple WLAN Switches at the edge connected together in the same VLAN (subnet), and the APs are either directly connected or connected over a unmanaged switch. In other words, there are no subnet boundaries to cross between the APs and between the APs and WSs. This configuration does not require L3 tunneling to accomplish seamless roaming. Each "service" (or VAP) is separated by VLANs and can have different security configurations. In this configuration, the "network" management interface address can be used as the only IP address on the switch and is used as the WLAN component IP address. Therefore static address can be used on the APs on the same subnet as the "network" IP. If DHCP is used, ensure that the APs have a route to the network IP address of the WLAN Switch.



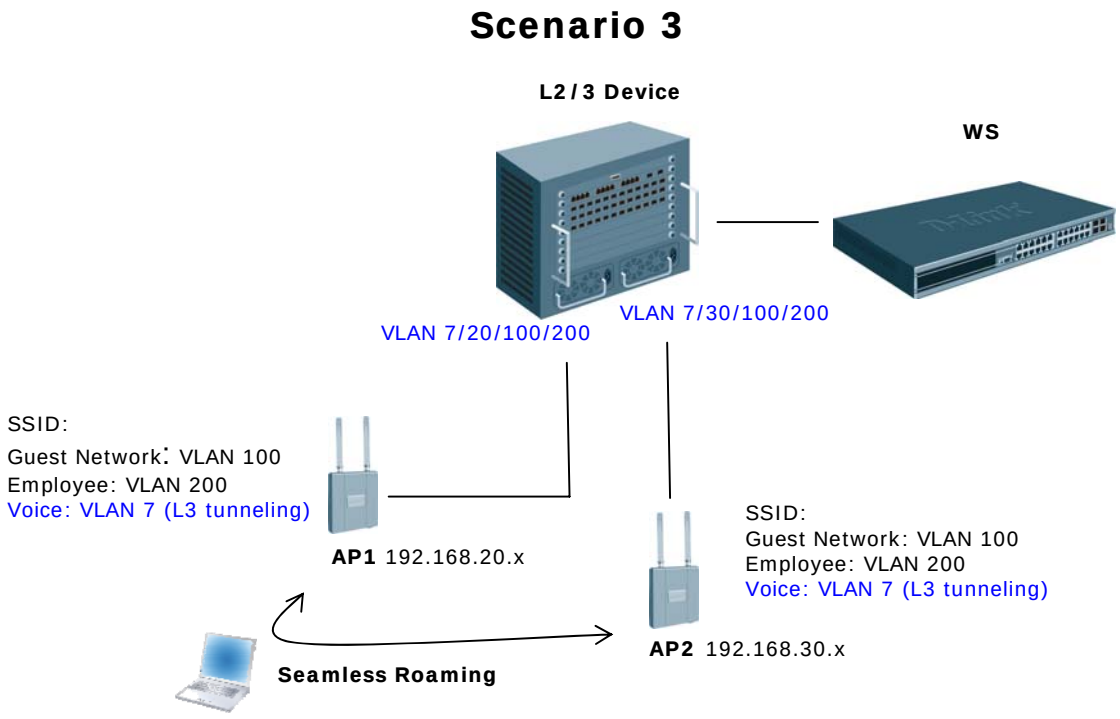
Deployment Scenario 2 - WS and AP are in different subnets (port-based routing):

This deployment consists of a single WLAN switch connected to a L3 device (router). APs are connected to the core with port-based routing. This configuration does require L3 tunneling to accomplish seamless roaming across APs connected to different L3 only ports on the core. Consider the MTU issue, services that require fast L3 roaming will need to be configured as L3 Tunneled VAPs to allow subnet roaming – these services will be affected by the MTU issue in that either the MTU configuration of the physical interfaces between the APs and the WLAN Switch must be increased by 20 bytes (or the client MTU decreased by 20 bytes), or the service must be expected to transmit "smaller" sized packets. Services that do not require fast roaming across L3 boundaries can be configured to non-Tunneling in which case the MTU issue is not observed for those services. If all devices in the network support increasing the MTU size, and this are feasible to do, then all of the services can be configured for Tunneling without any problems and fast roaming will be possible for all services.



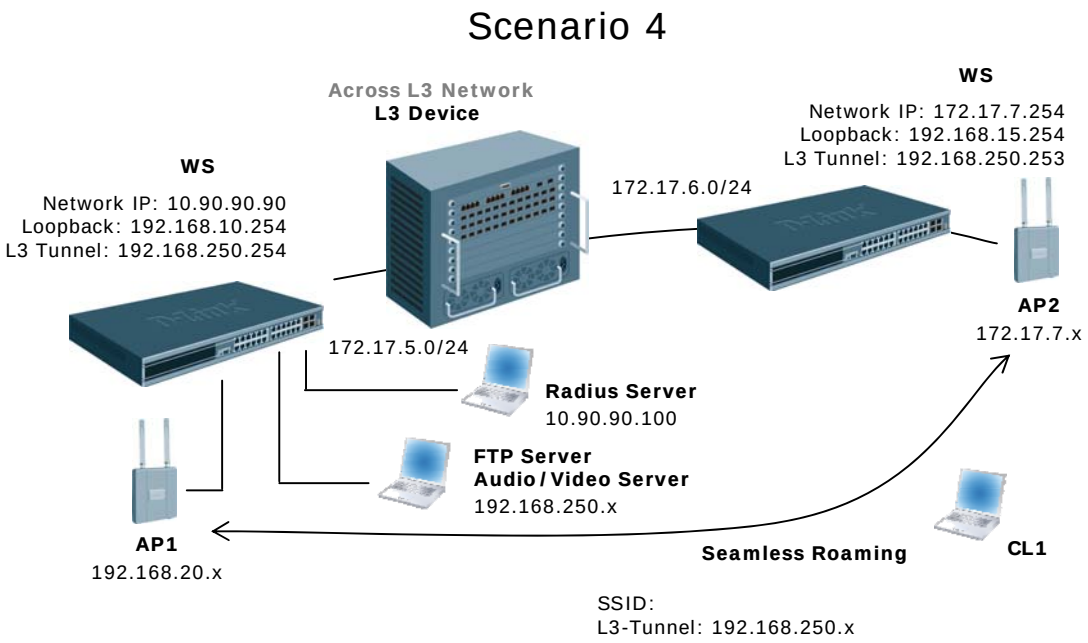
Deployment Scenario 3 - WS and AP are in different subnets (vlan-based routing):

This deployment consists of a single WLAN switch connected to a L2/3 device, and APs are connected to the core with VLAN-based routing (ensure that VLANs are properly set). This configuration does not require L3 tunneling to accomplish seamless roaming If the 802.1Q VLAN has been configured in customer's environment. In other words, through using VLAN Routing, you can spread VLANs across the network such that each VLAN has a path between each of the APs in the network.



Deployment Scenario 4 - L3 Edge Peers:

This deployment consists of multiple WLAN switches connected to a L3 core. APs are either directly connected to the WLAN switch or over a L2 or L3 device. This configuration does require L3 tunneling to accomplish seamless roaming. When Tunneling is used, an extra 20 bytes are added in the headers for encapsulation. To support these larger frames, you can increase the MTU size on all intermediate ports and WLAN switch ports. However, if you use tunneling only for IP telephony, or if the MTU size on all wireless clients can be set to 1480, you do not need to increase the MTU size in the network.



Notes:

1. **Where to place the WS & AP?** The Access Points need not be directly connected to the Switch to be managed by it; besides, the wireless switches need not be directly connected to each other to form a peer network. However, it is necessary that all the Switches and the Access Points are a part of the same Local Area Network. In other words, the Wireless Switch can not manage APs located across a Public Wide Area Network (internet), especially across a NAT device.

2. **About WPA2 Enterprise Authentication:** The solution also supports authenticated fast roaming using WPA2 Enterprise authentication in addition to other mechanisms. But, this is not currently supported by most of the wireless voice clients which only support WEP. Moreover, the newer versions of Windows XP Clients do support WPA2 but demonstrating L3 Fast Roaming with Windows Clients is not recommended to highlight seamless roaming as Windows Clients are inherently slow in managing hand-offs.

   The *Configuration Guide* indicates demonstrating roaming between the APs by powering down one of the APs thus forcing the clients to “roam” to the second AP. However, it must be noted that this is really a “*fail-over*” and not really roaming. In particular, when using WPA2 Enterprise for authentication, when an AP is powered down and brought back again, it loses the dynamic key information previously received from the switch causing the client who roams to that switch to re-authenticate itself from the Radius server. Although, none of these induced delays are more than a few milli-seconds and users would only see the loss of one ping, it must be pointed out that in real roaming under these delays would not exist. In the lab testing, we have recorded clients roaming with a hand-off time of 23 milli-seconds which is too quick to be noticed by a user.