
# ProCurve Secure Access 700wl Series Software Version 4.4.0.50 Update Guide

This document describes the process for updating the ProCurve Secure Access 700wl Series software from version 4.1.3.93 to version 4.4.0.50. It also provides information on some of the differences in functionality between these two versions, with information on how to reconfigure the system to take advantage of these changes.

Related 700wl Series publications include:

- *Software Version 4.4.0.50 Supplement to the ProCurve Secure Access 700wl Series Management and Configuration Guide*
- *ProCurve Secure Access 700wl Series Management and Configuration Guide*

ProCurve Networking periodically updates switch software and product manuals, and posts them on the world wide Web. For the latest software release and publications for your ProCurve networking product, visit **http://www.procurve.com**. Click on **Software updates** to check on the latest software releases. Click on **Technical support**, then **Product manuals (all)** to check on the latest publications.

### Publication Number

5991-3830
February, 2006

### Applicable Products

| | |
|---|---|
| ProCurve Access Controller 720wl | (J8153A) |
| ProCurve Access Controller xl Module | (J8162A) |
| ProCurve Access Control Server 740wl | (J8154A) |
| ProCurve Integrated Access Manager 760wl | (J8155A) |

### Trademark Credits

Microsoft®, Windows®, and Windows NT® are US registered trademarks of Microsoft Corporation.
Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

### Disclaimer

The information contained in this document is subject to change without notice.

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

### Warranty

See the Customer Support/Warranty booklet included with the product.

A copy of the specific warranty terms applicable to your Hewlett-Packard products and replacement parts can be obtained from your HP Sales and Service Office or authorized dealer.

Hewlett-Packard Company
8000 Foothills Boulevard, m/s 5551
Roseville, California 95747-5551
**http://www.procurve.com**

# Contents

# Introduction

This document describes how to update a ProCurve Secure Access 700wl Series system from version 4.1.3.93 to version 4.4.0.50, and discusses how to reconfigure your system if you were using port subnets under 4.1.3.93.

Version 4.4.0.50 provides a number of new features, including:

- Significantly enhanced support for multiple 802.1Q VLANs. This feature required significant changes to the underlying product structure, and therefore will require some reconfiguration if port subnets were configured under version 4.1.3.93. In addition, in support of this feature, the configuration of the network communication settings on the Access Controller 720wl and the Access Control Server 740wl has changed.
- Ability to act as a layer 2 entity and expose the actual MAC address for real IP clients on the uplink port.
- Support for traffic classification based on 802.1p, Differentiated Services (DiffServ), IP Precedence, and Type of Service (ToS) settings.
- A new Authentication Service for active 802.1X/WPA authentication.
- Specification of an external HTTP proxy server per Access Policy.
- Expanded definition of a Location, to include an individual client device identified by MAC address.
- Support for SSLv3 for the Login, Logout and Stop pages. SSLv3 is enabled by default.
- Clock synchronization for connected Access Controller 720wls uses the Access Control Server 740wl as the synchronization source.

See the *Software Version 4.4.0.50 Supplement to the ProCurve Secure Access 700wl Series Management and Configuration Guide* (December 2005) for a more detailed description of these features.

See the *ProCurve Secure Access 700wl Series Management and Configuration Guide* (December 2005) for instructions on using these features.

The enhanced support for 802.1Q VLANs is discussed in this document, as customers using port subnetting will need to reconfigure their system to use VLANs and subnets under the new software.

**Caution**

Because of the significant changes in the way subnets and VLANs are handled in release 4.4.0.50, it is not backward compatible with software version 4.1.3.93. However, to support a downgrade from 4.4.0.50 to 4.1.3.93, an intermediate release, version 4.1.4.4, must be used. The update process requires upgrading first from 4.1.3.93 to 4.1.4.4, and then from 4.1.4.4 to 4.4.0.50.

# Updating the 700wl Series

To update from version 4.1.3.93 to 4.4.0.50, the following steps are required.

1. If you have port subnets configured as part of the port configuration on your Access Controllers, and if you have VLAN tags associated with those subnets, make sure you record the relevant information. You will need to recreate these subnets as uplink VLANs under software version 4.4.0.50.

   Port subnet configurations can be viewed by selecting the Network icon on the Navigation Toolbar, then the Access Controller you want to view. Select the Interfaces tab, then the Subnet sub-tab to see the port subnet configurations for the Access Controller.

   This tab does not exist in the 4.4.0.50 software version, and these settings will be lost upon the update to 4.4.0.50.

2. Back up your Access Control Server 740wl.

   The backup can be performed from the Backup & Restore tab under the Maintenance function (the Maint icon on the Navigation Toolbar). See information in the *ProCurve Secure Access 700wl Series Management and Configuration Guide*, Chapter 8, for more detailed instructions.

   *This step is critical if at a future time you need to downgrade the system to 4.1.3.93.*

3. From the Access Control Server, update each connected Access Controller or Access Controller xl Module, updating each one first to 4.1.4.4, rebooting, then updating to 4.4.0.50.

4. Update the Access Control Server system to software version 4.1.4.4. The Update... function is found under Maintenance, on the main Software Setup page. This will lead you through steps for obtaining and installing the version 4.1.4.4 software. An update key will be required. Note that any Access Controller or Access Controller xl Module running 4.4.0.50 is not recognized until version 4.4.0.50 is installed in the Access Control Server.

   Follow the instructions in the *ProCurve Secure Access 700wl Series Management and Configuration Guide*, Chapter 8 to perform the update.

5. Reboot the Access Control Server to the new version, 4.1.4.4.

6. Running under 4.1.4.4, update the Access Control Server system to version 4.4.0.50. Reboot the system to 4.4.0.50. You should now have 4.4.0.50 installed as the Current Software, and 4.1.4.4 installed as the Alternate Software

The update process will migrate all your system configuration settings (except the port subnet configuration) to the new software. However, the configuration of the Network Setup pages will appear differently.

## Network Setup Differences

After you have updated to 4.4.0.50, the tabs and information under the Network area will be changed. There are some key differences in how network configuration is done under 4.4.0.50.

- Configuration settings for the DHCP server, domain name, DNS and WINS server addresses, are now configured on a Global Subnet Group basis on the Access Control Server, rather than per individual Access Controller. These settings, as previously defined for the Access Controllers in your system, are automatically transferred and the corresponding Global Subnet Groups are created as part of the update process.

- Each Access Controller may have multiple tagged VLANs and subnets defined as uplink subnets, in addition to a default, untagged subnet.

  Upon update, the Access Controller's previously-configured subnet (and default gateway) becomes the untagged default subnet for the Access Controller. Additional subnets can be defined individually on an Access Controller, or can be defined on the Access Control Server as Global Subnets, and then associated with VLAN tags on individual Access Controllers.

There are now two tabs in place of the former Network Setup tab: Network configuration is now divided into Global Network settings and Local Networks settings.

The Global Network page provides a picture of the entire set of network subnets present on the uplink ports of all the Access Controllers in the 700wl Series system, organized into Subnet Groups. The Global Network page centralizes the view of these subnets and the subnet groups of which they are members.

Under the Global Network tab, after the update, you should see one global subnet group for each Access Controller in your system. By default they are named with the base IP address of the Access Controller—for example, **AutoGroup_192.168.200.5**. The group is configured with the settings from the old Network Setup page for the Access Controller.

A global subnet is associated with each Subnet Group, also automatically created for each Access Controller. The global subnet defines the subnet itself—the subnet base address, subnet mask, and gateway, and is also named with the IP address of the Access Controller—for example, **AutoSubnet_92.168.200.5**.

With the auto-creation of these subnets and subnet groups, communication from the 700wl Series systems to the network can occur via the untagged subnets on the Access Controllers in the same way communication occurred in the previous version of the system.

However, if you were using port subnets configured on downlink ports, and the VLAN tag handling through Access Policies to designate traffic for specific subnets, you may need to configure uplink subnets and VLANs to accomplish the same results. Port-based subnets are no longer supported on downlink ports—and the Subnets sub-tab under the Interfaces tab no longer exists.

Under software version 4.1.3.93, you could use port subnetting to designate traffic for uplink subnets in the following way:

1. Define a subnet for a port that matches the upstream subnet. This will cause clients connecting through this port that want a real (non-NAT) IP address, to get an address in the desired subnet.
2. Create a Location defined as that specific port, and use that Location to define a port-specific Connection Profile. You could filter for specific VLAN traffic in the Connection Profile, so that only traffic from a specific VLAN would match the Connection Profile.

3. Use the Connection Profile in the Rights Table such that traffic that matched the Connection Profile would be associated with an Access Policy that would ensure that an appropriate VLAN tag would mark traffic for the desired subnet.

One of the obvious disadvantages of port subnets is that traffic must connect to the system through a specific downlink port in order to get properly designated for the correct subnet.

In the 4.4.0.50 software, subnets and VLANs are defined on the uplink side, through the Global Network and Local Networks pages. In this system you would do the following:

1. Configure a Global Subnet and Global Subnet Group that matches the upstream subnet.
2. On each Access Controller, define the appropriate VLAN using the Global Subnet you just defined, or define a VLAN and subnet directly on the Access Controller.
3. Create an Access Policy that ensures that the appropriate VLAN tag is applied to designate traffic for the desired subnet.

   The VLAN tag defined in the Access Policy is also used to determine what subnet the DHCP request should specify for clients that should get a real (non-NAT) IP address.
4. Create rows in the Rights Table that associate these Access Policies with the appropriate authenticated clients.

In this way, authenticated clients can be associated with the appropriate Access Policy (and thus VLAN and subnet) through a variety of criteria, such as identity and group membership, without having to specify the port or Access Controller through which the connection is made.

The next section discusses an example of how to configure the 700wl Series system to use upstream VLANs/subnets.

# Configuring Uplink Subnets

The simplified network topology shown in Figure 1 will illustrate how upstream subnets are handled in software version 4.4.0.50.

Under version 4.1.3.93, to ensure that a given client has access to a specific subnet, the client would need to enter the 720wl on a specific downlink port. In the scenario in Figure 1, the Access Point the client connects through would determine the subnet to which the client is assigned. If a client gets associated to the wrong AP, his traffic will arrive at the wrong port, and regardless of client identity or any other factors, that traffic will not reach the correct subnet.

Under version 4.4.0.50, subnets are much more flexible. The uplink port on the 720wl can be configured as a tagged member of each of the upstream VLANs, and those same VLAN could be configured on the uplink port of multiple 720wls, though none are shown in this figure. The Access Policy still determines the VLAN tag to be associated with a specific client's traffic, but the client can be matched to the Access Policy based on its Identity Profile, with no restrictions on where it entered the 700wl Series system.

Further, there are fewer restrictions in terms of the subnets themselves, as each subnet may have its own configuration of gateway, DHCP server, DNS services and so on (via the Global Subnet Group) rather than being restricted to a single configuration determined by the Access Controller through which the client is connected.

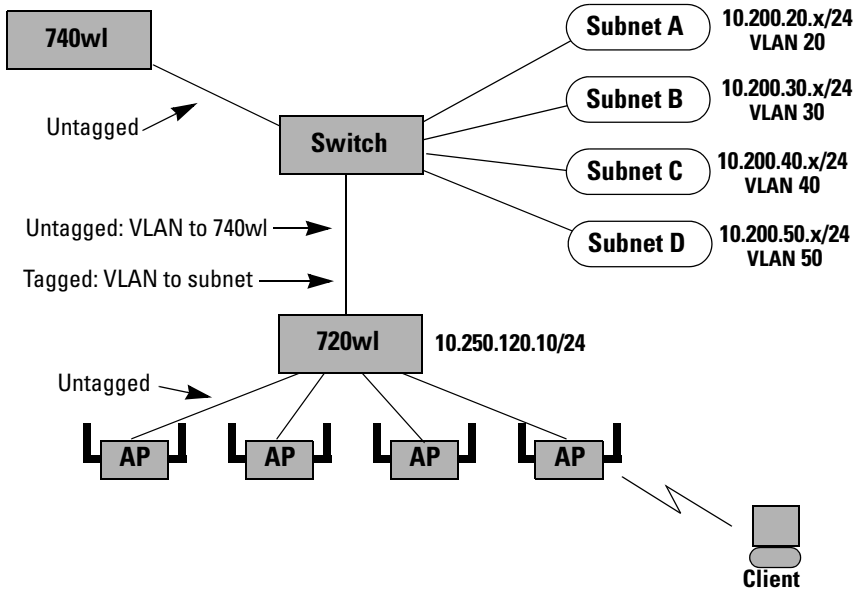


**Figure 1. Network topology with multiple upstream VLANs/subnets**

Under 4.4.0.50, configuring VLANs and subnets involves the following steps:

1. The 720wl uplink port should be configured with the untagged default VLAN **AutoSubnet_10.250.120.10**, which is a member of the global subnet group **AutoGroup_10.250.120.10**. This VLAN is used to communicate with the 740wl, and to send any untagged traffic onto the network. The setting for the subnet and subnet group should match those configured on the 720wl under version 4.1.3.93.

2. Under the Local Networks tab, with the 720wl selected, add the four upstream VLANs/subnets to the uplink.
   - Click New VLAN to add a new empty row to the VLAN table.
   - For each VLAN, you must provide the VLAN tag, base subnet IP address, subnet mask and the default gateway.

     For example, to configure subnet 10.200.20.x, you would enter the VLAN tag 20, the starting IP address and the /24 subnet mask, and the default gateway for this subnet (e.g. 10.200.20.1).
   - When you save the VLAN configuration, a new Global Subnet Group is created automatically (for example, **AutoGroup_10.200.20.4**). If DHCP was selected, and the DHCP server is appropriately configured, the other information such as DNS addresses and domain can be provided by the DHCP server.

     If you do not select DHCP or the DHCP server cannot provide the needed information, you must go to the Global Network page and configure the relevant information for this subnet group.
   - The new AutoSubnet and AutoGroup now appear under the Global Network tab. This allows the subnet to be configured on another 720wl simply by selecting it from the drop-down list of available subnets when creating a new VLAN row.

   After completing this step, you should have four VLANs configured on the 720wl—VLANs 20, 30, 40, and 50, configured for their respective subnets.

3. Create an Access Policy for each of the 4 upstream VLANs. The Access Policy must ensure that the correct client tag is applied to the traffic that is forwarded under that Access Policy. Since the traffic enters the system untagged (as shown in Figure 1) the Access Policy must add the correct tag.

   For example, for the Access Policy to be associated with VLAN 20, you would select the option **Apply this VLAN tag:** and enter 20. The VLAN Identifier settings appear under the Settings tab on the New Access Policy or Edit Access Policy page.

4. Add a set of rows to the Rights Table such that when a client is authenticated, he will be matched to the appropriate Access Policy for the subnet to which he should have access.

   For example, you might have a set of Identity Profiles defined that match the group Identity information returned with a successful RADIUS authentication—Accounting, Engineering, and so on. You could create a set of rows in the Rights Table that associate each Identity Profile with the Access Policy for the subnet in which an authenticated client should be placed:

| Row | Identity Profile | Connection Profile | Access Policy |
|---|---|---|---|
| 2 | Accounting | Any | Subnet A access |
| 3 | Engineering | Any | Subnet B access |
| | | and so on... | |

Now, when clients connect to the system, they are placed into the appropriate subnet based on their Identity Profile. The location through which the connection is made is not relevant in this case.

If you were using Connection Profiles to filter on incoming VLAN tags under 4.1.3.93, you can still do this in 4.4.0.50. However, the Connection Profiles would no longer need to have a 1-to-1 correspondence to a downlink port—the Connection Profile could use the default Location **Everywhere**, but filter so only traffic with the correct VLAN tag would match the Connection Profile. To duplicate the functionality of version 4.1.3.93, you might add rows to the Rights Table as follows:

| Row | Identity Profile | Connection Profile | Access Policy |
|---|---|---|---|
| 2 | Authenticated | VLAN 20 traffic | Subnet A access |
| 3 | Authenticated | VLAN 30 traffic | Subnet B access |
| | | and so on... | |

In this case, the VLAN tag associated with the incoming traffic determines what subnet a client is directed to, but the dependency on entering via a specific port is removed.

# Downgrading to the Previous Release

If for any reason you need to downgrade your systems to re-install the 4.1.3.93 software, you will need to perform several downgrade steps. Any changes you have made since upgrading will be lost. If you did not follow the update procedure specified above, by first installing version 4.1.4.4, then version 4.4.0.50, you will not be able to downgrade to version 4.1.3.93.

To downgrade to 4.1.3.93, follow these steps:

1. Do a Factory Reset.
2. Reboot your system to the Alternate partition that is running the 4.1.4.4 software version. The partition running 4.4.0.50 now becomes the Alternate Partition.
3. Re-install the 4.1.3.93 software into the alternate partition where the 4.4.0.50 software is installed. This will replace 4.4.0.50 with 4.1.3.93.
4. Reboot to the Alternate Partition running 4.1.3.93.
5. Restore the 4.1.3.93 backup that you made before you updated to 4.4.0.50.




February, 2006
Manual Part Number
5991-3830