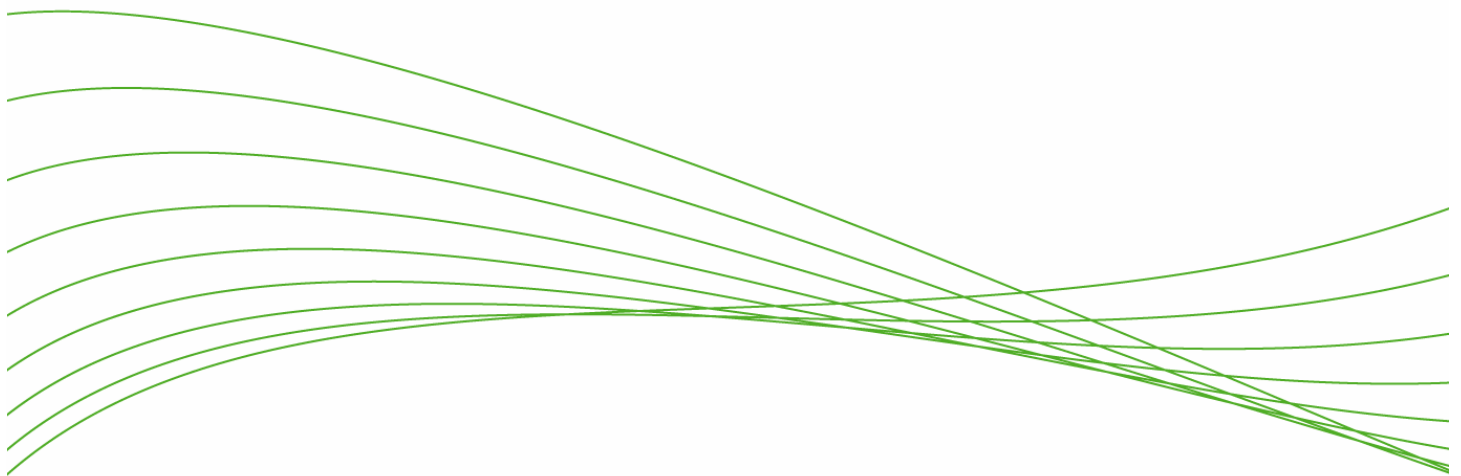


ProCurve Secure Access 700wl Series Wireless Clients: Connection Without Reconfiguration Technical Brief



Wireless Clients: Connection without Reconfiguration	2
What is a Misconfigured Client?	3
Misconfigured IP Configuration	3
Misconfigured Network Services	3
Mismatched HTTP Proxy Configuration.....	3
How the ProCurve 700wl Series Handles Misconfigured Clients	3
IP Address Configuration Problems	3
Network Services Configuration Problems	3
HTTP Proxy Configuration Problems	5
Summary.....	7
For more information.....	8

Wireless Clients: Connection without Reconfiguration

In discussions about wireless network access, the topic of access control – authentication and authorization of network users – is typically the main focus. However, this presupposes that the user is able to connect to the network – i.e. that the client can actually send packets to the network and receive packets in response. In reality, the ability to connect at all to a network using a wireless connection is not a foregone conclusion.

Mobile users who use their mobile device outside their corporate network face the challenge of matching their system's network settings to different network environments. A mobile user may connect via a hotspot in a coffee shop or the airport, or connect to a network at a customer's location, and need to change their network settings to match those environments. When this user returns to his office network, those changed network settings now prevent him from getting access. Most often this results in a support call to the IT staff.

In a corporate network, there is also the problem of providing network connections for visiting guests, to allow Internet access, or to allow access to selected Intranet sites set up for demonstrations, product information, etc. In the past this typically required the services of IT to help the visitor configure the proper settings or simply not permit "non-employee" access to network resources.

The ProCurve Secure Access 700wl series addresses this problem by translating the network settings on the client device to ones that are compatible with the corporate network, without requiring configuration changes on the client. Therefore, an employee who had changed her configuration to access another network can still get access her home network without reconfiguration of the mobile device. A visitor can connect to the host's network, without disrupting access to his own network when he returns to his office. (Note that being able to connect successfully does not mean that the visitor can access any network resources – the ProCurve 700wl still requires that users be authenticated in some way, such as through the Guest login feature.)

For example, the account manager at ABC Company occasionally brings customers into the corporate office for business meetings, product training and demonstration, facility tours, etc. These guests often bring their own laptops and want to gain access to the Internet to check their own corporate web sites and email services while visiting the conference and demonstration rooms at ABC corporate headquarters. Further, the account managers themselves often come from satellite offices that use their own networks separate from the main corporate network.

There are several issues ABC Company must address in allowing network access for both visitors and for employees from remote locations:

- The first problem is client adaptation – how to enable the visitor's (or account manager's) mobile computer, which is undoubtedly configured for his own network, to connect successfully. The visitor's device may have settings for services such as DNS, WINS, or Web proxy, that only work in the visitor's home corporate network. If ABC Company's IT staff reconfigures these settings, the visitor's device will no longer work on his home network unless IT restores the original settings before the visitor leaves.
- The second problem is how to allow an unknown user – one who does not have a user account on the corporate network - access to a limited set of resources (e.g. Internet/Intranet access only) without compromising the security of ABC's network and its resources.

ABC Company's goal is to enable an account manager and his or her customer to be in the same conference room, connected through the same wireless access point, and know that each will get the appropriate set of rights on the network. ABC wants this to occur without having to involve IT every time.

The ProCurve Secure Access 700wl series addresses both these problems.

The problem of granting a limited set of access rights on the network to an unauthenticated user is addressed through the Guest logon feature provided by the ProCurve 700wl series' Rights Manager. The ProCurve 700wl's implementation of access control, and how it determines the appropriate policies for individual users, is discussed in the "ProCurve Secure Access 700wl series: User Authentication and Authorization Technical Brief."

This paper describes how the ProCurve 700wl series handles the problems involved in client adaptation.

What is a Misconfigured Client?

The term “misconfigured” applies to a client device that is not configured correctly for the current network environment in which it is attempting to operate. What is misconfigured in one environment may be correctly configured for another environment. This configuration mismatch can take several forms:

Misconfigured IP Configuration

The elements of the client device’s IP configuration (IP address, network mask, and the default Gateway address) may be configured incorrectly for the current network. If these are statically configured with addresses that don’t exist in the network the client is attempting to connect to, the client will not be able to access the network.

Misconfigured Network Services

The IP address of a network service such as DNS (identified by address and well-known port number) is incorrect for the current network environment. This may apply to any IP service that can be identified by port number – for example, DNS (port 53), SMB (port 137, 138 or 139), or SMTP (port 25).

Mismatched HTTP Proxy Configuration

A mismatch may occur if the client and network settings do not agree – for example, the client is configured for a proxy server and the network does not use a proxy server, or the client uses a proxy server configuration that does not match that of the current network proxy configuration.

How the ProCurve 700wl Series Handles Misconfigured Clients

The ProCurve 700wl series can address and work around all of these types of configuration issues, without requiring changes on the client device. The following sections explain how the 700wl series handles each type of configuration problem.

IP Address Configuration Problems

The ProCurve 700wl series has the ability to determine if a client uses DHCP for IP address configuration or if it is statically configured. If the client device does not use the correct IP settings for the current network (i.e. the client has a static configuration with a specific IP address), the 700wl series will automatically use Network Address Translation (NAT) to allow the client’s existing static IP configuration to work on the current network. Additionally, if the network mask and gateway are incorrect for the current network, the 700wl series will work around these problems.

Network Services Configuration Problems

TCP/IP networks rely on “services” to perform many necessary functions. In fact, there are a set of “well-known services” consistently used in relation to TCP/IP networks, such as Domain Name Services (DNS), Simple Mail Transport Protocol (SMTP), or File Transfer Protocol (FTP) that use predefined TCP or UDP ports (“well-known ports”) that all TCP/IP implementations adhere to. For example, DNS uses UDP and TCP ports 53. Because of the concept of identifying well-known ports as services, the ProCurve 700wl series can be configured to listen on a particular port, regardless of the IP address, and then send that traffic to a different IP address to fulfill the service needs.

In addition, the ProCurve 700wl series can be configured to listen for any specific IP address plus port, and provide the same type of redirection service. To accomplish this, the 700wl series rewrites the destination address of the packet before sending it onto the network. This enables the 700wl series to intercept and redirect traffic destined for any arbitrary destination, identified either by port, by IP address, or both. For network services such as DNS, WINS, SMTP etc. the 700wl series can listen for the well-known port and then rewrite the IP address with the correct address for the current network’s DNS, WINS, or SMTP server as appropriate.

The following example shows how the 700wl series handles misconfigured DNS requests from ABC Company visitor’s mobile device:

- The ProCurve Switch 5300xl with Switch xl Access Controller Module listens to all requests going to port 53, (the well-known port for DNS), for requests that are destined to incorrect IP
- When the Switch xl Access Controller Module detects an incorrect destination, the Access Controller Module rewrites the packet with the correct DNS server IP and then sends the packet to the DNS server
- The DNS server replies to 700wl series with the answer
- In turn the Switch xl Access Controller Module rewrites the packet and sends the completed request back to the client device.

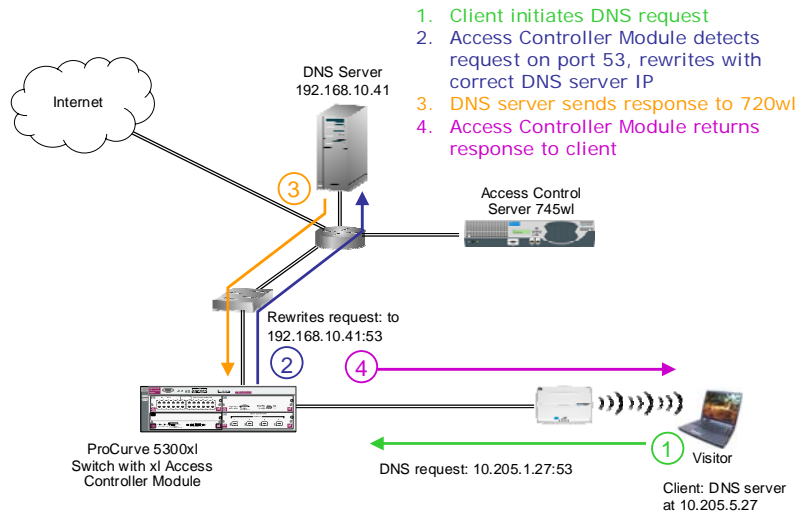


Figure 1: Handling a misconfigured network service request

HTTP Proxy Configuration Problems

For HTTP proxy configuration problems, the 700wl series can detect the client's proxy server settings and manage them appropriately in respect to the network proxy configuration. As with network services, the 700wl series listens for HTTP requests on a specific set of ports, and then redirects the requests as appropriate. However, as there several types of mismatched configurations that can occur, the 700wl series must be able to handle each combination appropriately.

Table 1 shows the configuration combinations that are possible, and briefly how the 700wl series handles each combination.

	Client has proxy server settings configured	Client does not have proxy server settings configured
Network uses proxy server	Listen for specific, well-known proxy port numbers and redirect to the network proxy server's IP address and port number.	Listen for port 80 traffic and redirect to the network proxy server's IP address and port number.
Network does not use proxy server	Listen for specific, well-known proxy port numbers and forward directly to the URL in the HTTP Get Request.	Do nothing.

Table 1: Automatic HTTP Proxy Support

For example, suppose ABC's visitor's laptop is configured to use a proxy server, but ABC Company does not use one. Normally this would require the visitor to reconfigure the browser to not use a proxy. However, the ProCurve700wl series makes this unnecessary. When the user points his browser to a web site, the Switch xl Access Controller Module detects the request on one of the well-known ports used for proxy servers (usually port 8080 or 3128). Because ABC Company does not use a proxy server, the 700wl series extracts the actual destination URL from the HTTP GET request, and forwards the request to that URL. In this case, the 700wl series acts as the proxy server for the client, without requiring any changes on the client's part. This process is shown in Figure 2.

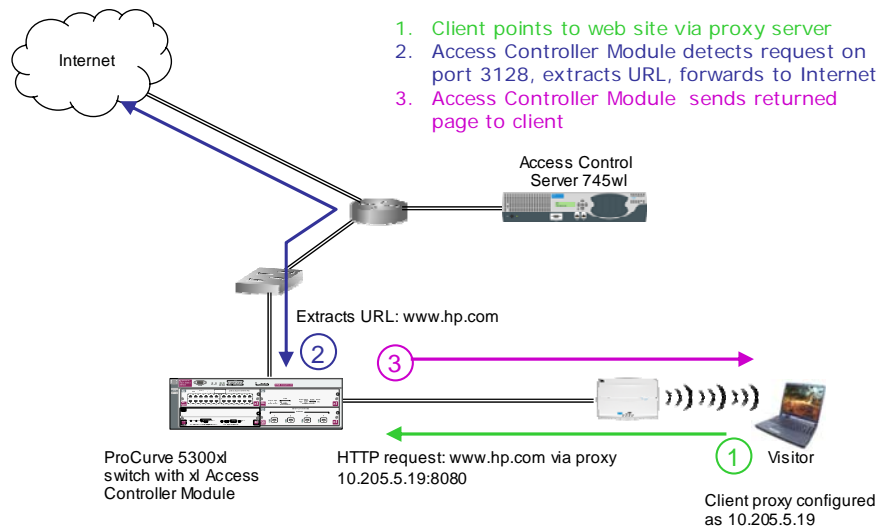


Figure 2: Client configured for a proxy server on a network with no proxy

If ABC Company did have a proxy server in place, then it would still listen for requests on the well-known ports, but instead of extracting the URL, it would rewrite the IP address and port number of the packet to use ABC's proxy server. Then ABC's proxy server would handle the request. Figure 3 illustrates how the 700wl series handles a client that is not configured to use a proxy server when the network requires one.

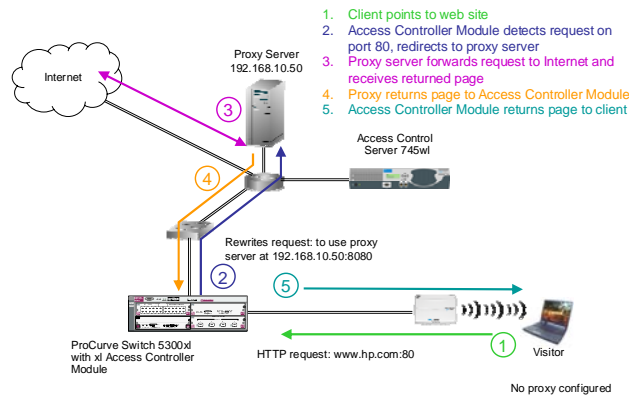


Figure 3: Client configured for no proxy, network uses a proxy server

The 700wl series' automatic HTTP proxy feature also enables an organization to selectively allow HTTP access to some destinations and not others. For example, ABC Company might want to prevent visitors from accessing sites on its own intranet that would otherwise be accessible to anyone with network access. The automatic HTTP proxy feature can be configured to allow or deny HTTP access to specific web sites by IP address, host name, domain name, or subnet. This means that ABC Company can enable HTTP access for its visitors without compromising the security of its own internal web sites.

Summary

The ProCurve Secure Access 700wl series provides features that allow wireless client devices to connect to a network without requiring reconfiguration of client settings such as IP addressing, HTTP proxy configuration, or network services configurations. By using Network Address Translation (NAT) the 700wl series can work around IP address configuration problems. The 700wl series' ability to recognize and redirect network service requests to the correct network-specific destination can work around address configuration problems concerning network services such as DNS, FTP and so on. Finally, the automatic HTTP Proxy feature addresses mismatches in HTTP proxy configurations. These features combine to make it easy to provide guest access to visitors, for example, without IT involvement and expense and the resultant user inconvenience and frustration.

For more information

For more information on ProCurve Networking products and solutions, visit www.procurve.com.

To find out more about
ProCurve Networking
products and solutions,
visit our web site at

www.procurve.com



© 2006 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for 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.

5982-8266EN, Revision 1, 6/2005