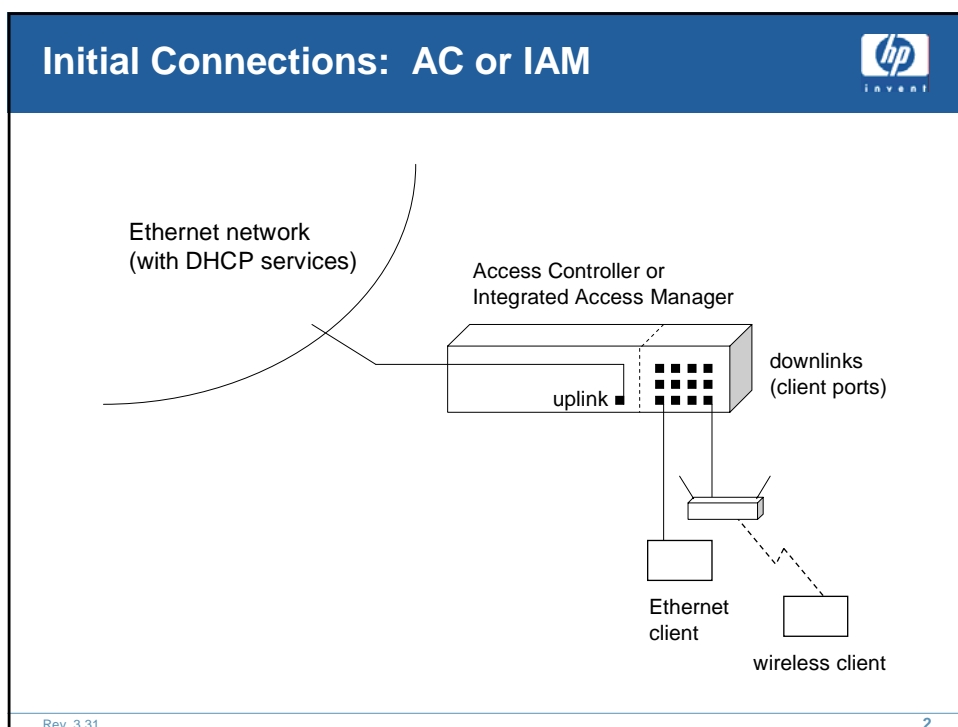
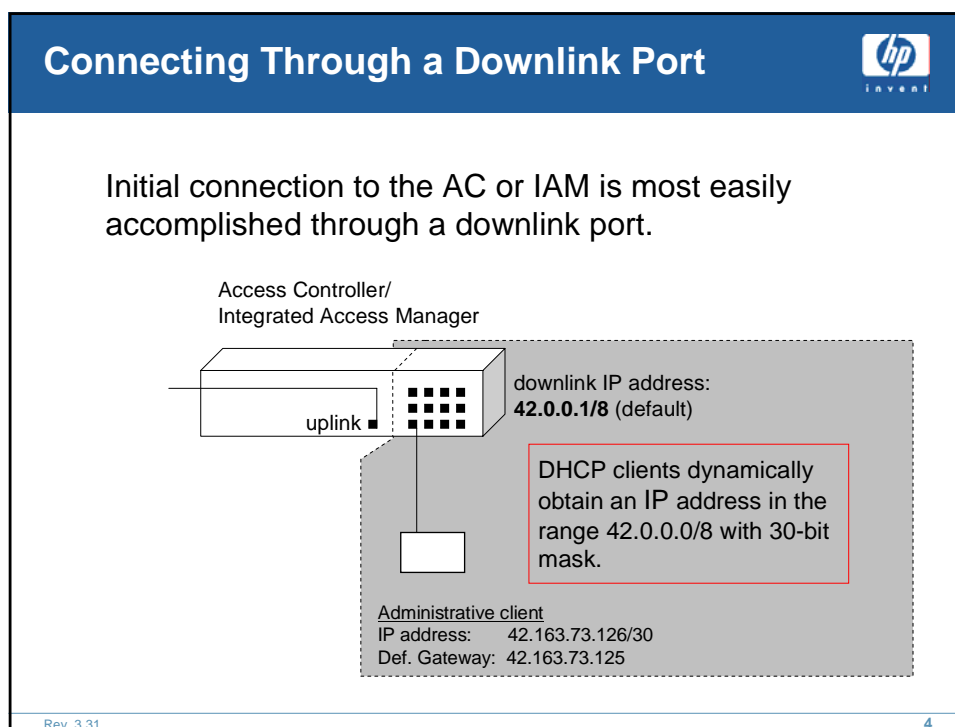
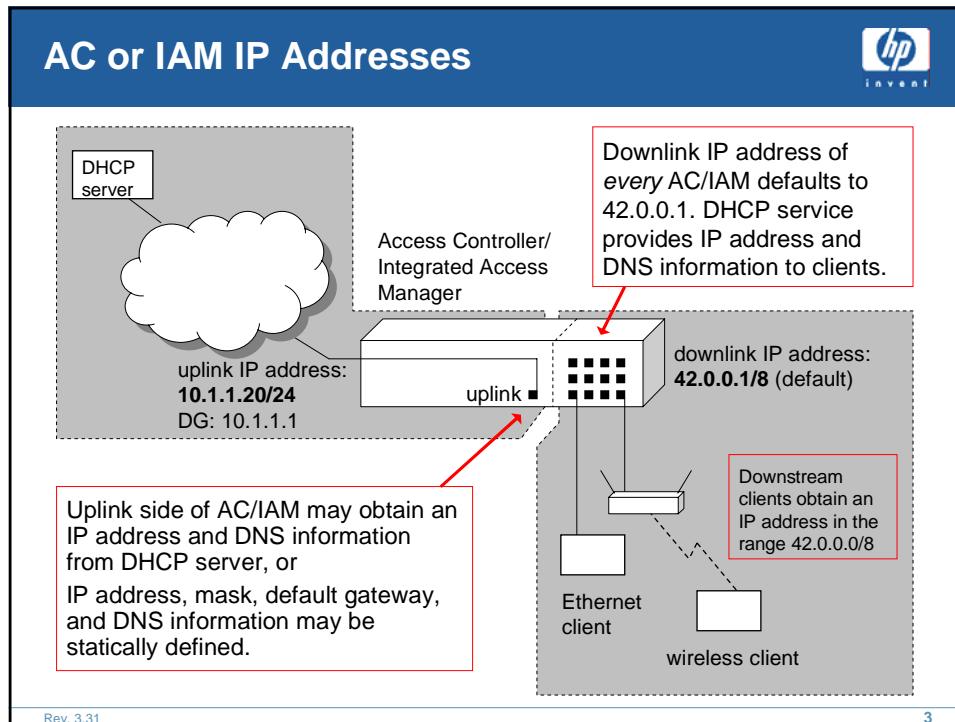


# Initial Configuration

HP ProCurve Secure Mobility Solutions:

Ralf Krause

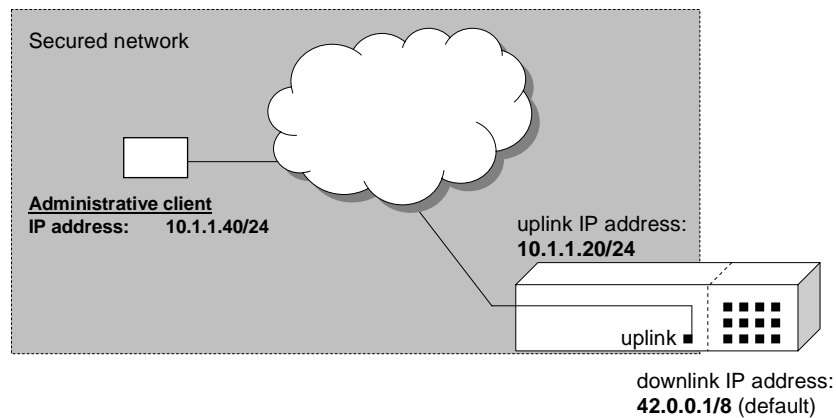




## Connecting Through an Uplink Port



If the Secure Access device has an IP address, initial connection to may also be accomplished through an uplink port.



Rev. 3.31

5

## Access Controller Main Menu



LOG OUT  
HELP

Access Controller 720wl  
Main Menu

**Configuration**

- ☐ Admin Authorization
- ☐ Control Server
- ☐ Network
- ☐ SNMP
- ☐ Specify Location Information
- ☐ Specify Session Logging
- ☐ Time and Date

**System Functions**

- ☐ Backup and Restore
- ☐ Shutdown
- ☐ Update Software

**Views**

- ☐ Active Clients
- ☐ Active Sessions
- ☐ Log File
- ☐ Version and License Information

SPECIFY CONTROL SERVER

To change the admin account and password:

To statically define IP address and DNS info:

06/07/03 12:12:30 PM IP: 10.1.1.20

Rev. 3.31

6

## Initial Connections: Access Control Server



Connection to the Access Control Server is most easily accomplished if it initially obtains a DHCP-assigned address.

ACS

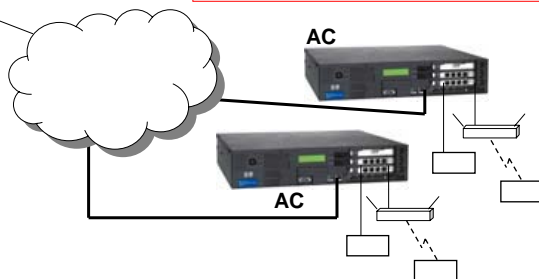


If DHCP services are not available, the Access Control Server's IP address may be set from the command line interface.

Access Control Server and Access Controllers may be in the same subnet or different subnets.

AC

AC



Rev. 3.31

7

## Setting IP address from CLI



DB-9 male connector



terminal settings: 9600,8N1


null modem cable

```
HP 700w1 Series@[42.0.0.1]: set ip 10.1.1.20/24
HP 700w1 Series@[10.1.1.20]: set gateway 10.1.1.1
HP 700w1 Series@[10.1.1.20]: show ip
Hostname:
Domain Name:
IP address:      10.1.1.20/24
DHCP enabled:    No
Default gateway: 10.1.1.1
DHCP server:     None configured
DNS servers:     None configured
WINS servers:    None configured
```

Rev. 3.31


8

## Access Control Server Main Menu



[LOG OUT](#)  
[HELP](#)

**Access Control Server 740w1**  
 Main Menu



**Configuration**

- [Admin Authorization](#)
- [HTTP Proxy](#)
- [Network](#)
- [Shared Secret Authorization](#)
- [SNMP](#)
- [Specify Session Logging](#)
- [Time and Date](#)

**Wireless Data Privacy Setup**

- [IPSec](#)
- [PPTP and L2TP](#)
- [SSH](#)
- [Tunneling](#)

**System Functions**

- [Backup and Restore](#)
- [Distribute Logons](#)
- [Shutdown](#)
- [Update Software](#)

**Views**

- [Active Access Managers](#)
- [Log File](#)
- [Version and License Information](#)

[GO TO RIGHTS MANAGER](#)

08/07/02 01:12:28 PM
IP: 10.1.1.20

Rev. 3.31
9

To change the admin account and password:

To statically define IP address and DNS info:


To define the shared secret the ACS will use to encrypt sessions with ACs.

## Integrated Access Manager Main Menu



[LOG OUT](#)  
[HELP](#)

**Integrated Access Manager 760w1**  
 Main Menu



**Configuration**

- [Admin Authorization](#)
- [HTTP Proxy](#)
- [Network](#)
- [Shared Secret Authorization](#)
- [SNMP](#)
- [Specify Location Information](#)
- [Specify Session Logging](#)
- [Time and Date](#)

**Wireless Data Privacy Setup**

- [IPSec](#)
- [PPTP and L2TP](#)
- [SSH](#)
- [Tunneling](#)

**System Functions**

- [Backup and Restore](#)
- [Distribute Logons](#)
- [Shutdown](#)
- [Update Software](#)

**Views**

- [Active Access Managers](#)
- [Active Clients](#)
- [Active Sessions](#)
- [Log File](#)
- [Version and License Information](#)

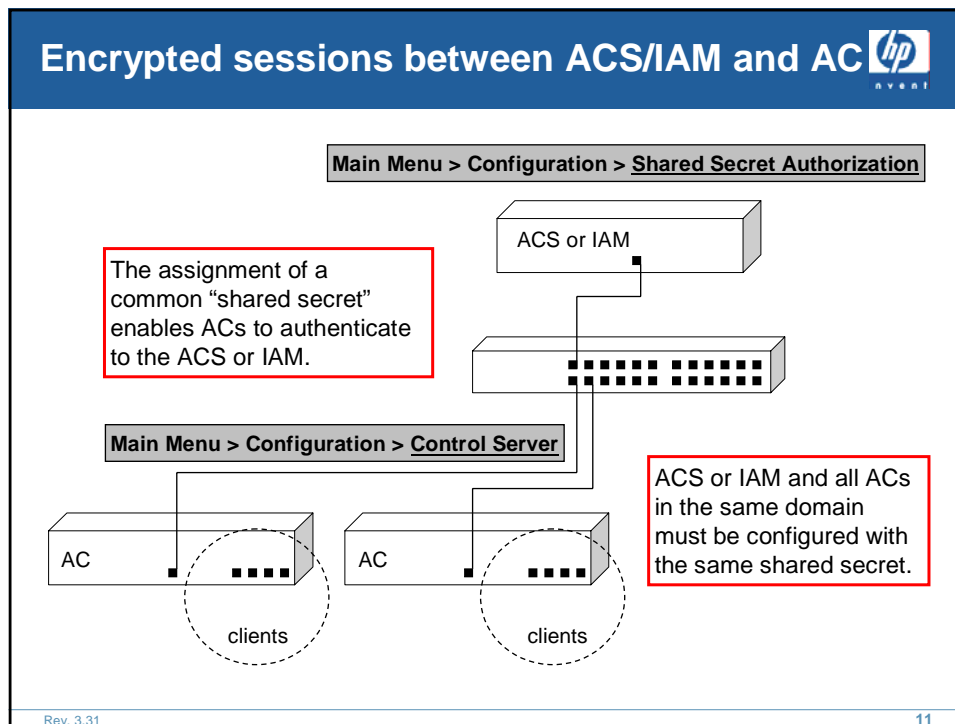
[GO TO RIGHTS MANAGER](#)

08/07/02 12:28:30 PM
IP: 10.1.1.20

Rev. 3.31
10

To change the admin account and password:

To statically define IP address and DNS info:



## Associating an AC with its ACS/IAM

**Main Menu > Configuration > Control Server**

**Access Controller 720wl**  
**Specify Control Server**

**Specify Control Server and Enter Shared Secret**

Associating an AC with its ACS or IAM requires that you supply the shared secret as well as the IP address of the ACS/IAM.

Control Server IP Address:

Secret Key:

Confirm Secret Key:

After the AC has been associated with the ACS, you can test the association by selecting this button.

IP: 10.1.1.21

Rev. 3.31 12

## Comparing ACS, AC, and IAM



### The Access Control Server

- maintains the rights database, handles authentication requests and supplies rights information to ACs within its domain, and
- maintains VPN protocol configuration information.

### The Access Controller

- contacts ACS or IAM for rights information on behalf of users, and
- performs Network Address Translation (NAT) and maintains sessions with downstream clients.

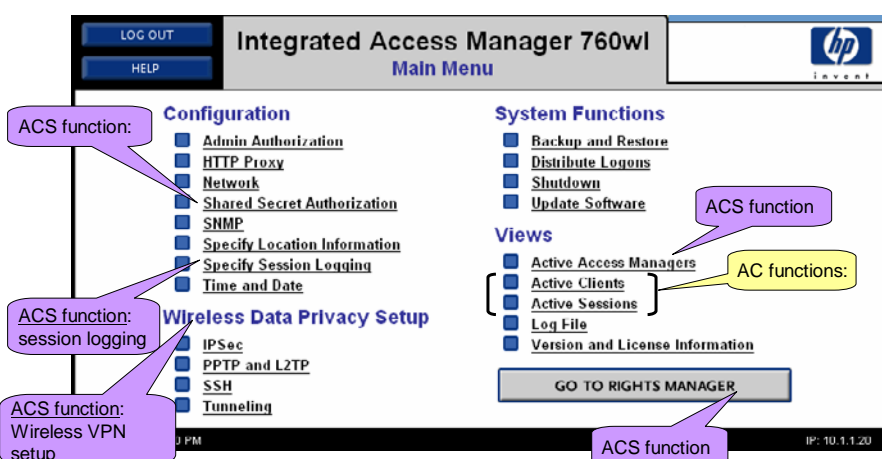
### The Integrated Access Manager

- maintains rights database, handles authentication requests for users connected to its integrated downlink ports as well as subordinate ACs,
- maintains VPN protocol configuration information, and
- performs NAT and maintains sessions on behalf of clients.

Rev. 3.31

13

## IAM Combines ACS and AC Features



Rev. 3.31

14

## Authenticated Network Access



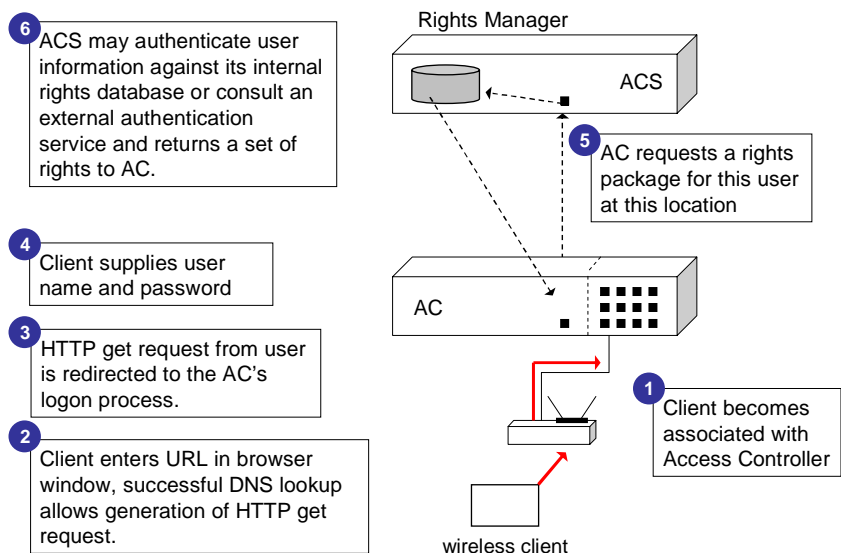
**There are several ways that a wireless user can gain access to the secured network.**

- Active authentication methods:
  - Browser-based: user provides name and password at a system-generated logon screen, and
  - VPN: user launches a VPN client application, provides name and password, and establishes an authenticated, encrypted tunnel using the Access Controller as a gateway.
- Passive authentication methods enable the Secure Access system to monitor authentication sessions and enable access when it detects successful authentication.
  - Windows NT/2000 domain monitored logon, and
  - IEEE 802.1X authentication (EAP-TLS or EAP-MD5) monitored logon.

Rev. 3.31

15

## Browser-based Logon



Rev. 3.31

16




## Defining User Accounts



**Only authenticated users can send network traffic *through* the AC or IAM into the secured network.**

- The downstream “admin” user can perform configuration and monitoring tasks, but it is not considered a system user.

- To define user accounts and their permissions, select the  button on the ACS or IAM Main Menu.

- Select the “Users” button on the Rights Manager menu bar.



Rev. 3.31

17

## The User Editor



By default, no users are defined. Select the “Go To the User Editor” link. This brings up the *User Editor*.

Rev. 3.31

18

## Group Membership



- The *User Editor* provides an opportunity to place the new user in an existing Group.
- Every “Normal” user is an implicit member of a default Group known as “User.”

This User is a Member of the Following Groups

Add User to Group:

Group Name	Group Type	Remove
No Groups Found		

- Select “Submit Changes” to create a new user with implied membership in the “User” Group.

Rev. 3.31

19

## Effective Rights



**Each user’s effective rights on the system is based on an intersection of:**

- “who” – Group membership,
- “what” – a set of “Redirect” and “Allow” statements that specify traffic that will be either redirected to some other destination or permitted to pass through the AC or IAM,
- “where” – the location of the downlink port through which the user is attempting network access, and
- “when” – the time of day and day of the week that the user is attempting network access.

Rev. 3.31

20

## “Who” and “What” intersection



### Groups are associated with Redirects and Allows in the Rights Manager's *Group Manager* page.

- A table in the *Groups Manager* represents Group names in rows and Redirects or Allows in columns.
- A Redirect defines characteristics of traffic that should be sent to a different IP address and/or port number.
- An Allow defines characteristics of traffic that should be permitted to pass through the system.
- Several system-defined Redirects and Allows are associated with system-defined Groups, such as “User.”
- To allow for flexible definition of permissions, the system supports user-defined Redirects and Allows.

Rev. 3.31

21

## System-defined Allows




MAIN MENU

HELP

LOG OUT

Rights Manager

Groups Manager



CLIENTS

CONFIGURATION

USERS

GROUPS

LOCATIONS

LOGS

TROUBLESHOOTING

RIGHTS IMPORT

Allows

	All IP traffic	AM HTTPS Logon page	AM Logon: fwd append URI	AM Logon: fwd no URI	AM SSL Stop page	AM Stop page	DHCP	DNS	HTTP	HTTPS Logon page	Internal Admin UI	Internal HTTP	Internal rights UI	Kerberos	SMB	SSL Stop page	Stop page
Groups	Guest	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Logon	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	User	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Access Point	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	No Access	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

New Group

New Allow

Show Redirects

Update

Modify Columns

Cancel

00/1403 07.23.23 PM

10.1.1.1

- Each of the five default Groups is initially given a unique set of Allows.
- To view details on a specific Allow, follow the link that represents its name.

Rev. 3.31

22

## Allow "All IP traffic" for the "User" Group



Authenticated members of the "User" Group, such as "user1," are allowed to send IP traffic to all destination addresses.

### Allow Details

Allow Name:

### Allow

#### ☒ Basic Allow

Protocol:  Port:  Address:

#### ☐ Advanced Allow

Filter in tcpdump syntax:

Rev. 3.31

23

## System-defined Redirects



MAIN MENU		Rights Manager														hp	
HELP		Groups Manager														invent	
LOG OUT		CLIENTS CONFIGURATION USERS GROUPS LOCATIONS LOGS TROUBLESHOOTING RIGHTS IMPORT															
		Redirects															
		AM HTTP Logon redirect	AM HTTPS Logon redirect	AM Internal blocker	AM Logon page shortcut	AM No SSL web	AM No web	BlackHole	CS.to. AM Logon redirect	CS.to. AM Stop redirect	Internal blocker	Logon page shortcut	No external rights UI	No internal admin UI	No internal rights UI	No SSL internal UI	SOCKS redirect
Groups	Guest	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Logon	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	User	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Access Point	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	No Access	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		<input type="button" value="New Group"/> <input type="button" value="New Redirect"/> <input type="button" value="Show Allows"/>															
		<input type="button" value="Update"/> <input type="button" value="Modify Columns"/> <input type="button" value="Cancel"/>															
08/14/03 07:22:55 PM																10.1.1.20	

- Each of the five default Groups is initially given a unique set of Redirects.
- To view details on a specific Redirect, follow the link that represents its name.

Rev. 3.31

24

## The “CS-to-AM Logon” Redirect



- In “distributed logon” mode Access Controllers handle logon procedures.
- Users that attempt a direct SSL logon to the ACS or IAM uplink address are redirected to the AC’s downlink address.

**Redirect Details**

Redirect Name: CS-to-AM Logon redirect

**Redirect From Original Destination**

☒ **Basic Redirect Filter**  
 Protocol: HTTPS Port: N/A Address: @SERVER@

☐ **Advanced Redirect Filter**  
 Filter in tcpdump syntax: {tcp dst port 443 and dst host @SERVER@}

**Redirect To**  
 Port: 443 Address: @INTERNAL@

System-defined address variable representing the ACS or IAM uplink address

System-defined port number for SSL logon page.

System-defined address variable representing the AC's downlink address

Rev. 3.31

25

## Default address variables and ports



Built-in Addresses	
Name	Address
@DNS@	127.0.0.1
@INTERNAL@	42.0.0.1
@INTRANET@	10.1.1.0/24
@SERVER@	10.1.1.20

The ACS or IAM derives the values of these address variables from its Network Configuration.

These are internal logical destinations (port numbers) that the ACS or IAM recognizes.

Built-in Ports	
Port Number	Description
81	Stop Page
82	Logon Page, preserving original destination url
83	Logon Page, dropping original destination url
443	SSL logon page
444	Rights manager admin pages
446	SSL stop page

Rev. 3.31

26

## The “AM Logon Page Shortcut” Redirect

hp  
invent

A very useful system-defined Redirect enables users to enter the URL “1.1.1.1” to bring up the logon/logoff page.

**Redirect Details**

Redirect Name:

---

**Redirect From Original Destination**

☒ **Basic Redirect Filter**

Protocol:  Port:  Address:

☐ **Advanced Redirect Filter**

Filter in tcpdump syntax:

---

**Redirect To**

Port:  Address:

User enters this address as URL and the request is redirected to ...

System-defined port number for logon page.

System-defined address variable AC/IAM downlink address.

Rev. 3.31 27

## Intersection of “Who,” “Where,” and “When”

hp  
invent

- Access to the network is explicitly permitted to specific Groups by associating them with Locations, which are associated with AC or IAM slot/port numbers.
- By default, the “User” Group is associated with a Location called “Everywhere Else” that includes all AC or IAM ports and a time slot that allows 24 x 7 access.

**Rights Manager**  
Locations Manager

MAIN MENU | HELP | LOG OUT | CLIENTS | CONFIGURATION | USERS | GROUPS | LOCATIONS | LOGS | TROUBLESHOOTING | RIGHTS IMPORT

		Groups				
		Guest	Logon	User	Access Point	No Access
Locations	Everywhere Else	✓	✓	✓	✓	✗

Rev. 3.31 28

## IP Addresses for Downstream Clients



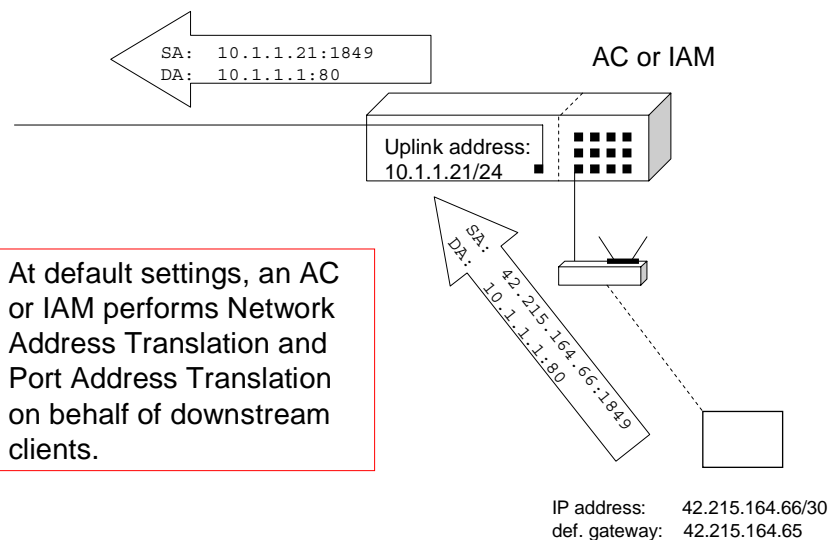
**Wireless clients connected to an AC or IAM obtain their IP addresses in one of the following ways:**

- Network Address Translation (NAT) mode – each AC or IAM has a pool of addresses (42.0.0.0/8) from which it dynamically distributes addresses to its clients.
- Non-NAT, static IP addresses – an IP address is statically defined on the client computer. This address is not translated by the AC.
- Non-NAT, dynamic IP addresses – the AC or IAM relays DHCP requests from the client to a DHCP server within the secured network. This address is not translated by the AC.

Rev. 3.31

29

## Network Address Translation (NAT)



Rev. 3.31

30

## View Active Sessions



- To view actual and translated addresses and port numbers, select the “View Active Sessions” link at the AC or IAM.

Access Controller 720wl  
View Active Sessions

Filter  
MAC Address: All Protocol: All Slot/Port: All  
Lines: 25 Apply Filter Reset Filter

Active Sessions (6 of 6)  
Highlighted text indicates a *redirected session* or a *session tunneled to another Access Controller 720wl*

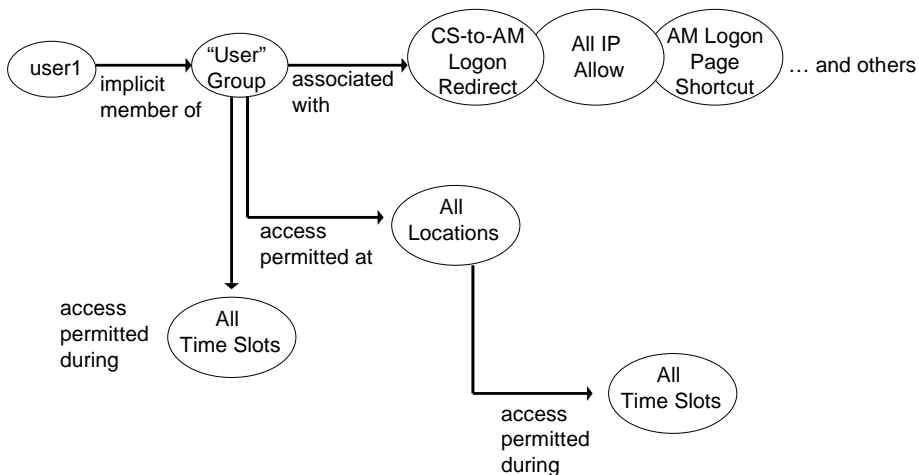
Proto	Idle	MAC Address	Client Source Actual Source	Client Dest Actual Dest	Slot/Port	Xmit	Recv
TCP	18s	00:d1:9f:04:17:d1	42.215.164.66:1849 10.1.1.21:1849	10.1.1.1:80 10.1.1.1:80	3/1	5335	176381
UDP	23s	00:d1:9f:04:17:d1	42.215.164.66:1106 10.1.1.21:1026	10.1.1.254:53 10.1.1.254:53	3/1	199	362
UDP	7s	00:d1:9f:04:17:d1	42.215.164.66:137 10.1.1.21:137	42.0.0.1:443 10.1.1.1:137	3/1	810	504
UDP	20s	00:c0:9f:04:17:d1	42.215.164.66:137 10.1.1.21:137	10.1.1.1:137 10.1.1.1:137	3/1	234	168
TCP	48s	00:c0:9f:04:17:d1	42.215.164.66:1842 42.215.164.66:1848	10.1.1.20:443 42.0.0.1:443	3/1	581	1230
TCP	18s	00:c0:9f:04:17:d1	42.215.164.66:1848 10.1.1.21:1848	10.1.1.1:80 10.1.1.1:80	3/1	5485	13713

09/08/03 01:02:49 AM IP: 10.1.1.21

Rev. 3.31

31

## Inherited Rights of New User



Rev. 3.31

32



## View Client information



- To view detailed information about logged on clients, select the client's name from the list that is displayed when you select Views > Active Clients from the AC or IAM Main Menu.

Client: 00:10:a4:ba:43:0d  
 User: user1  
 Machine Name: Unknown  
 IP Address: 42.237.135.50  
 Address Status: NAT mode: rights do not allow  
 Access Manager: 10.1.1.21  
 Slot/Port: 3/1  
 View Client Report: [Log Info](#)  
[3 Active Session\(s\)](#)  
 Rights in XML  
 Rights Expire: 5 hrs, 22 mins

Logoff This Client GO TO RIGHTS MANAGER

09/11/03 09:41:11 PM IP: 10.1.1.21

Rev. 3.31

33

## System Management and Maintenance



**The HP ProCurve Secure Access system provides management and maintenance tools that allow an administrator to:**

- reset the system to factory defaults,
- update system software,
- enable system level and Rights Manager events to be sent to a syslog server,
- backup and restore the system configuration, and
- gracefully shut down the system.

Rev. 3.31

34

