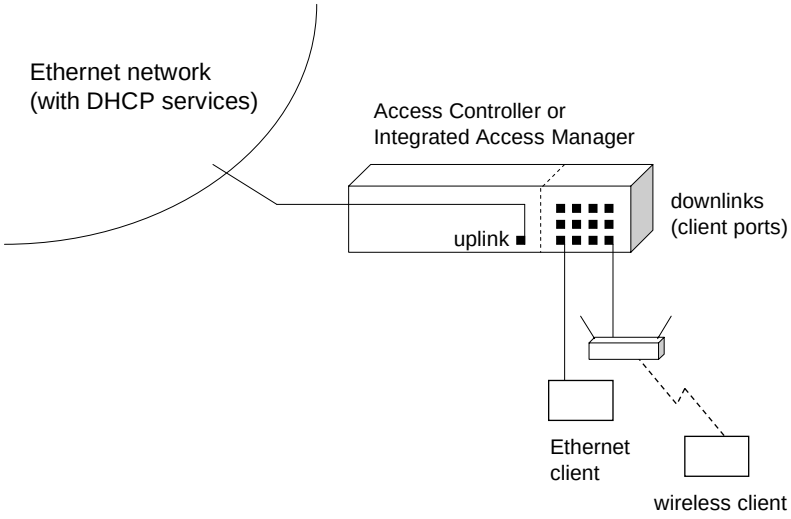
Initial Configuration

HP ProCurve Secure Mobility Solutions:

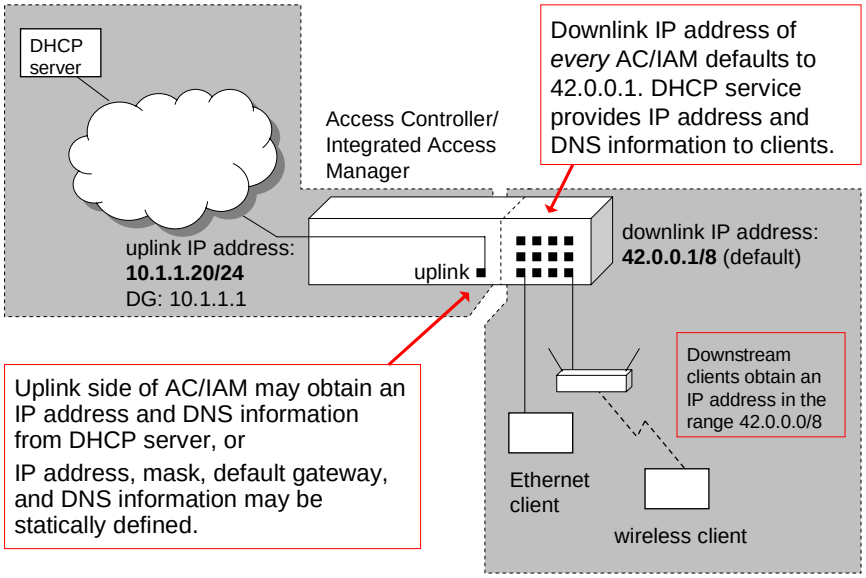
Ralf Krause

Initial Connections: AC or IAM



Rev. 3.31 2

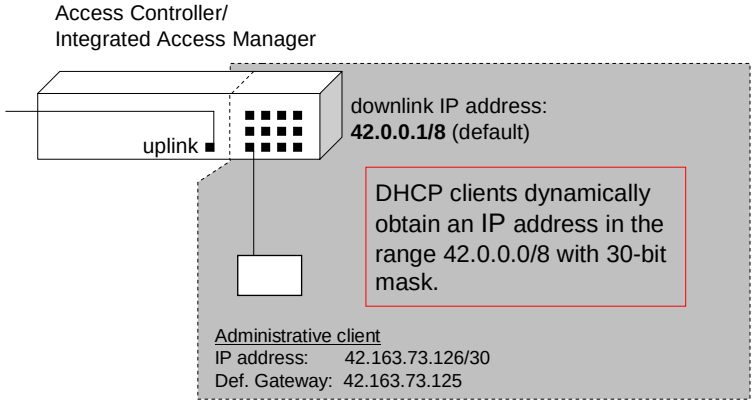
AC or IAM IP Addresses



Rev. 3.31 3

Connecting Through a Downlink Port

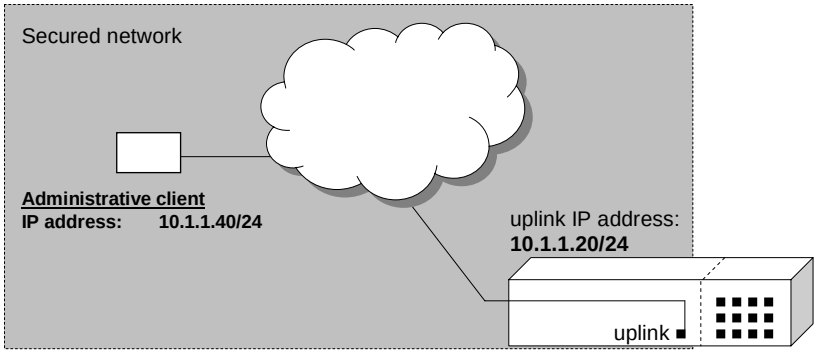
Initial connection to the AC or IAM is most easily accomplished through a downlink port.



Rev. 3.31 4

Connecting Through an Uplink Port

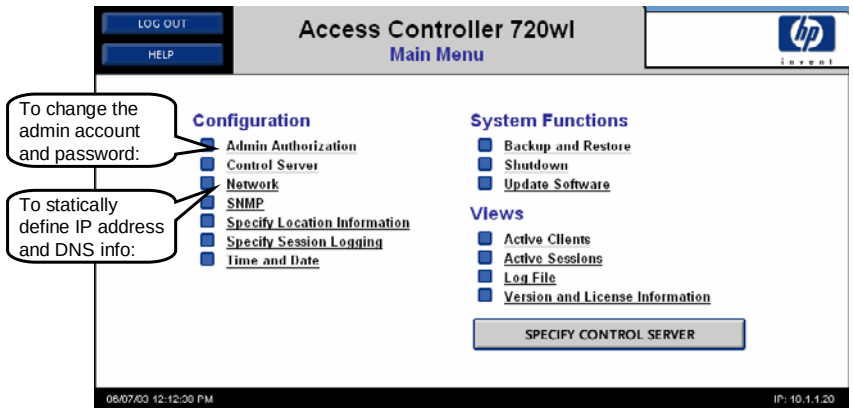
If the Secure Access device has an IP address, initial connection to may also be accomplished through an uplink port.



downlink IP address:
42.0.0.1/8 (default)

Rev. 3.31 5

Access Controller Main Menu

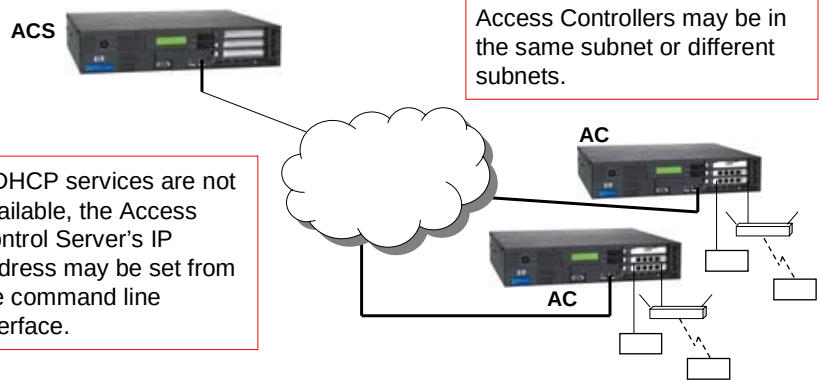


Rev. 3.31 6

Initial Connections: Access Control Server

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

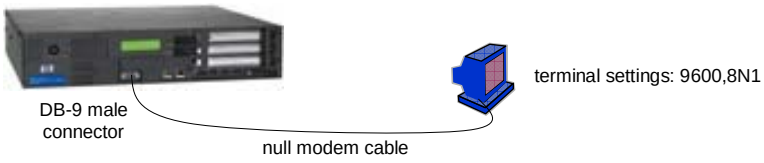
Access Control Server and Access Controllers may be in the same subnet or different subnets.



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

Rev. 3.31 7

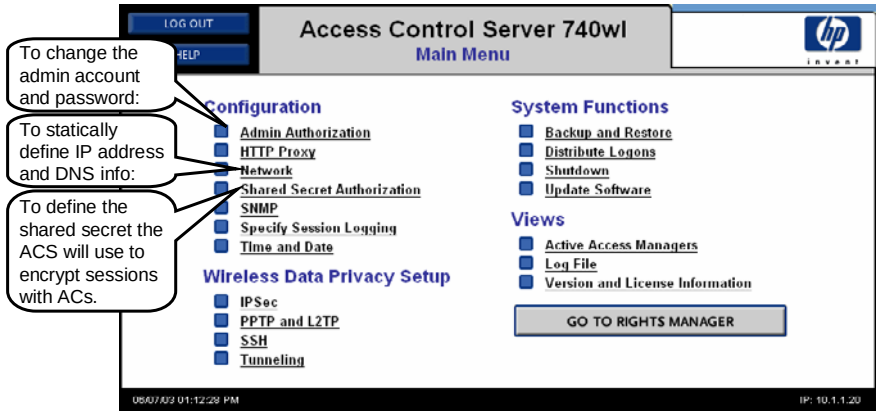
Setting IP address from CLI



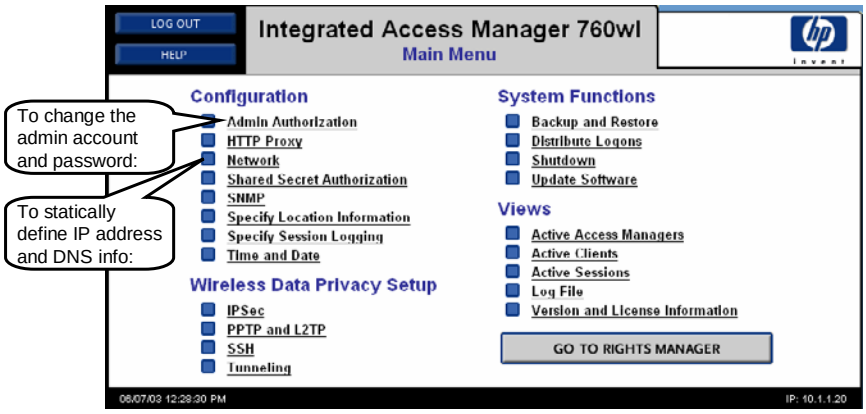

```
HP 700wl Series@[42.0.0.1]: set ip 10.1.1.20/24
HP 700wl Series@[10.1.1.20]: set gateway 10.1.1.1
HP 700wl Series@[10.1.1.20]: show ip
    Hostname:
    Domain Name:
    IP address:       10.1.1.20/24
    DHCP enabled:     No
    Default gateway:  10.1.1.1
    DHCP server:      None configured
 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

Rev. 3.31 8

Access Control Server Main Menu



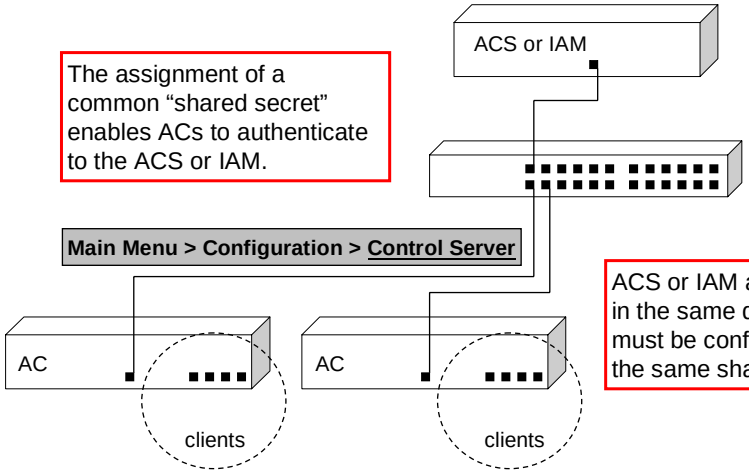
Integrated Access Manager Main Menu



Encrypted sessions between ACS/IAM and AC

Main Menu > Configuration > Shared Secret Authorization

The assignment of a common “shared secret” enables ACs to authenticate to the ACS or IAM.



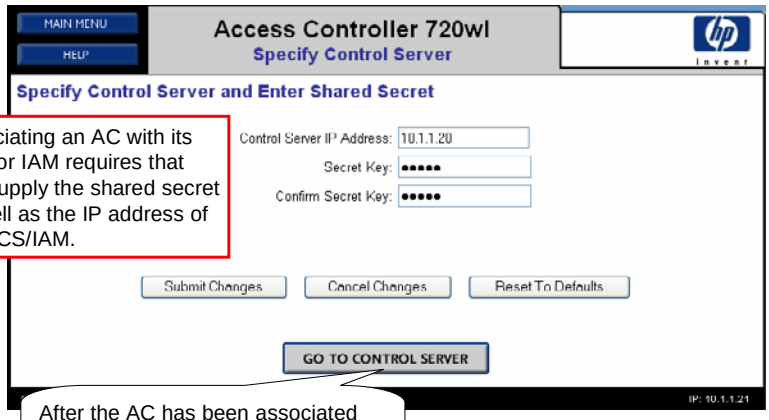
ACS or IAM and all ACs in the same domain must be configured with the same shared secret.

Rev. 3.31 11

Associating an AC with its ACS/IAM

Main Menu > Configuration > Control Server

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.



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

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

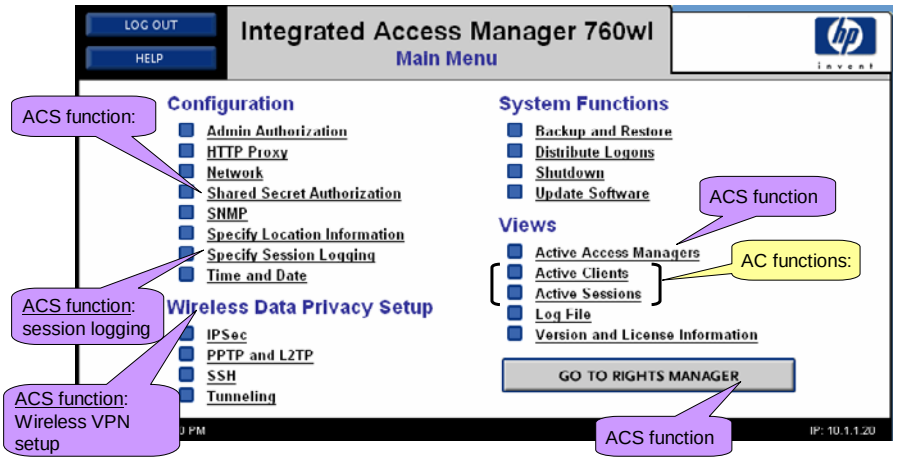
- contacts ACS or IAM for rights information on behalf of users, and
- performs Network Address Translation (NAT) and maintains sessions with downstream clients.

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

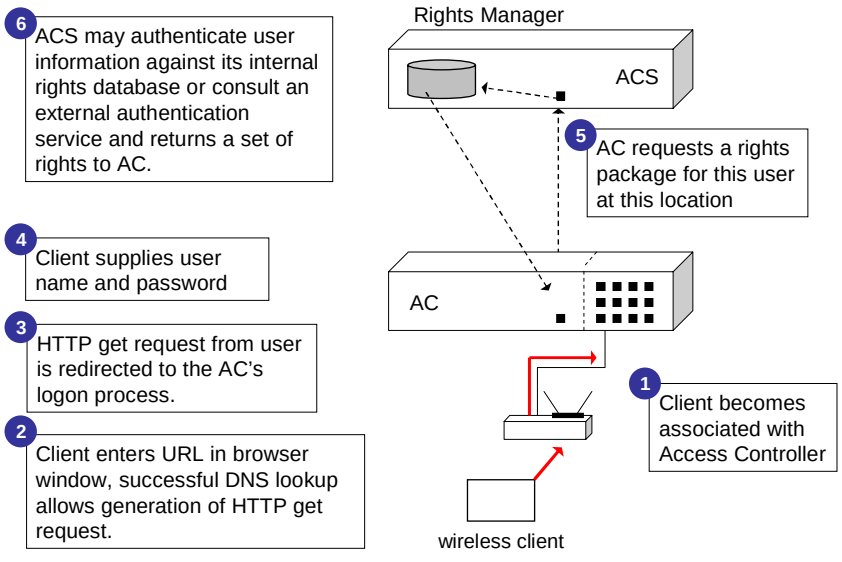
Authenticated Network Access

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 GO TO RIGHTS MANAGER button on the ACS or IAM Main Menu.
- Select the “Users” button on the Rights Manager menu bar.

Rev. 3.31 17

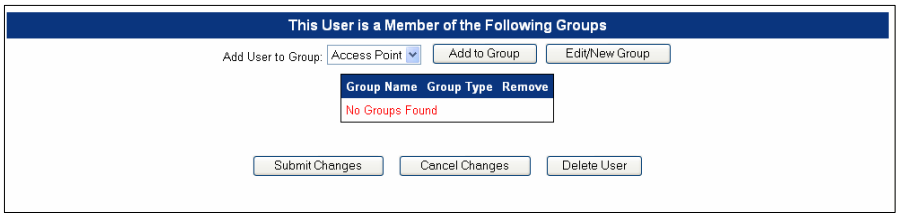
The User Editor

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.”



- 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

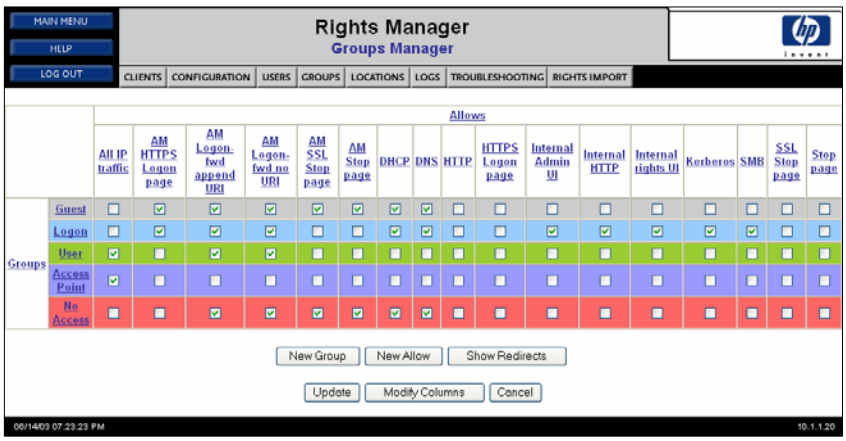
"Who" and "What" intersection

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

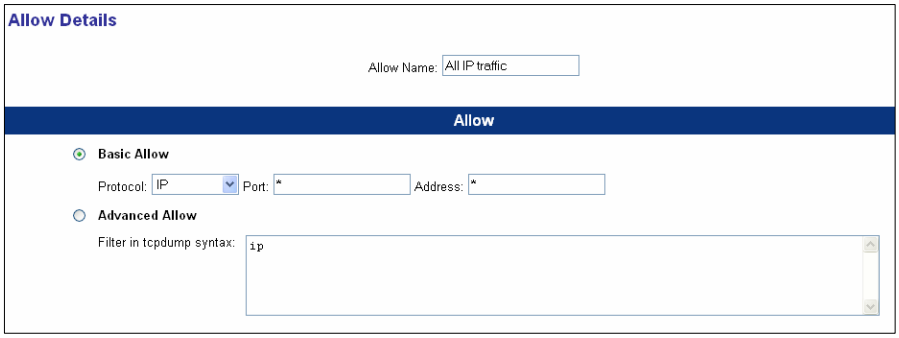


- Each of the five default Groups is initially given a a unique set of Allows.
- To view details on a specific Allow, follow the link that represents its name.

Rev. 3.31 22

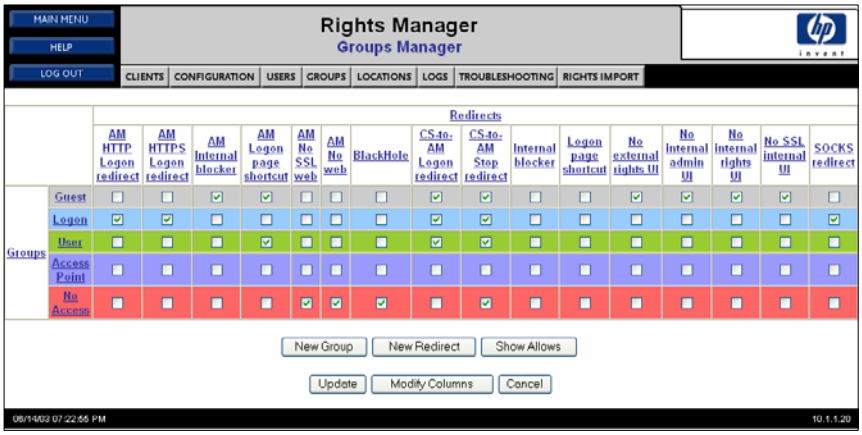
Allow “All IP traffic” for the “User” Group

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



Rev. 3.31 23

System-defined Redirects

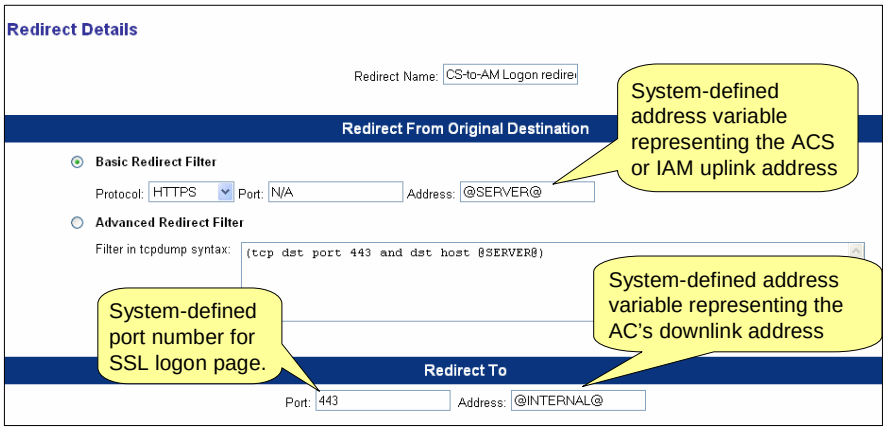


- Each of the five default Groups is initially given a a unique set of Redirects.
- To view details on a specific Redirect, follow the link that represents its name.

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.



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.

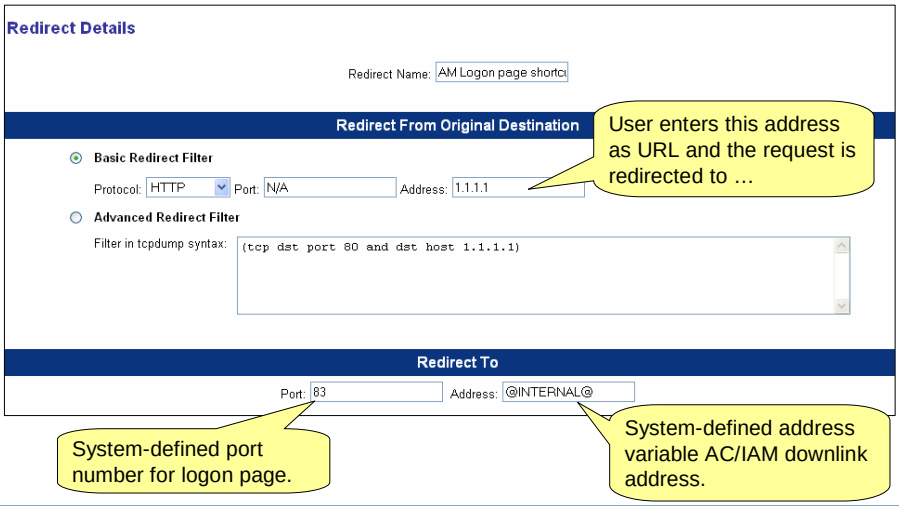
Built-in Ports

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

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



Rev. 3.31 27

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

- 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.

Rev. 3.31 28

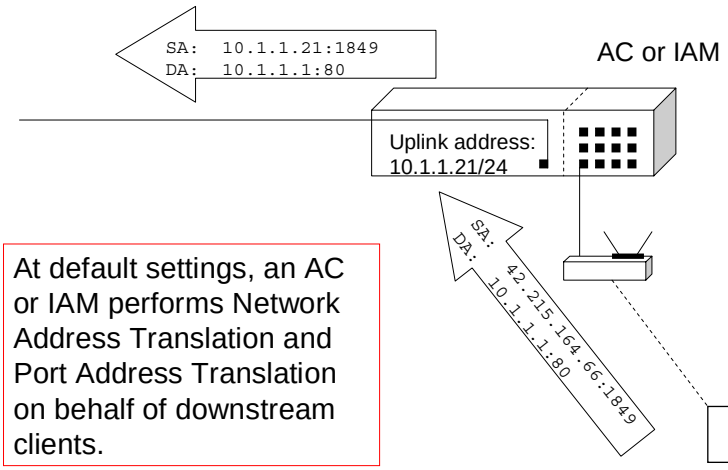
IP Addresses for Downstream Clients

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)



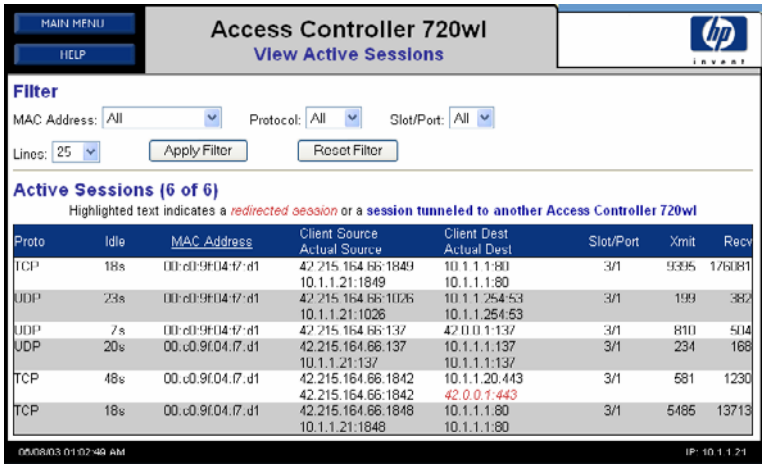
At default settings, an AC or IAM performs Network Address Translation and Port Address Translation on behalf of downstream clients.

IP address: 42.215.164.66/30
def. gateway: 42.215.164.65

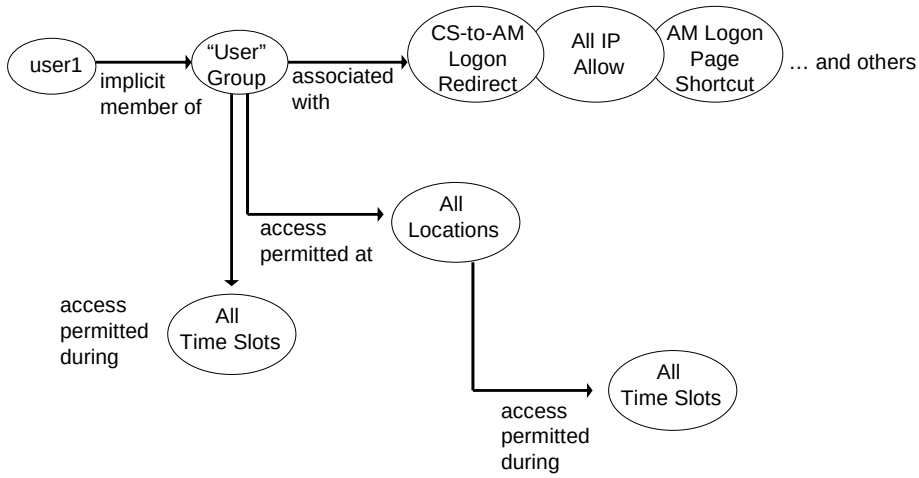
Rev. 3.31 30

View Active Sessions

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

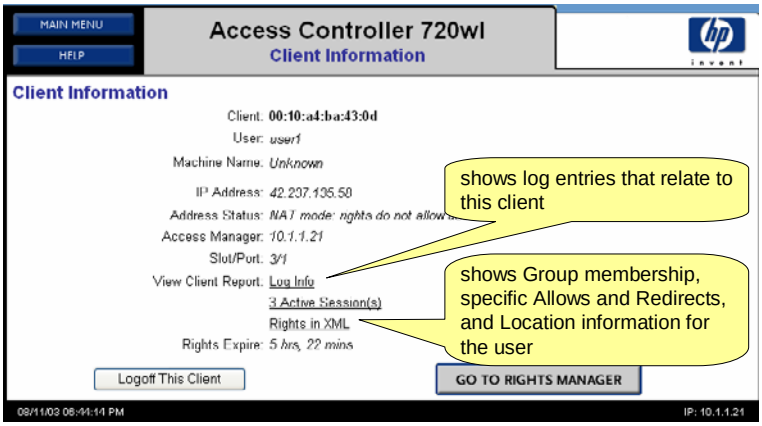


Inherited Rights of New User



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.



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.


Questions
?