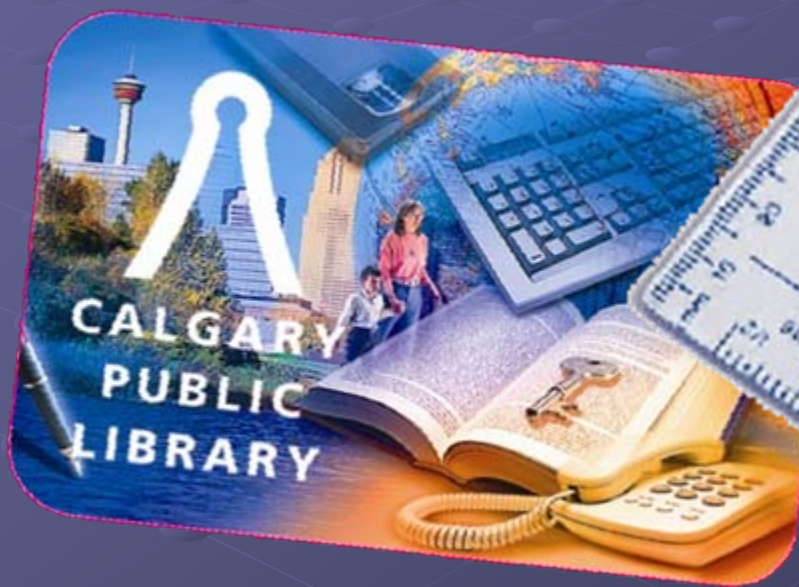


Calgary Public Library



Scott Stanley
Bonita Burchat
Marcin Skrzynski



Agenda

- Our Story
- Setup and operation considerations
- Equipment
- Demo
- Questions



Our Story – The Beginning

Wireless at CPL

- First implemented at CPL in 2001
- Early versions were older technology
 - Difficult to secure for Hotspots
- All branches have had wireless since 2004
 - Used for VOIP



Our Story – Our First Hotspot

Wireless City Pilot

- Partnership – Library, The City of Calgary, Calgary Technologies Inc
- 2003 – 2006
- Only at Central Branch
- Model for hotspot deployment
- Pilot ended



Our Story – Next Steps

Improving upon Wireless Hotspot model

- Looked for a technology that was:
 - A Secure Implementation
 - Easy to administer
 - Easy to deploy in multiple locations
 - Scalable



Our Story – Next Steps

Improving upon Wireless Hotspot model

● Policy and Procedure:

- Updated the Public Access Network Policy
- Developed Terms and Conditions for use of service
- Support Model
- Policy and Procedure will evolve



Our Story – Next Steps

Our Wireless Hotspots

● The roll out:

- Started at the Central Branch
- Rolled out to the branches
- No site survey – added access points as needed



Our Story – Next Steps

Our Wireless Hotspots

● The roll out:

- No initial Marketing
- Target marketing after all equipment deployed



Our Story – The Success

Wireless Hotspot

- More popular than we expected:
 - About 5000 uses in September
 - About 1400 unique users
 - Around 8% of our Internet use





Wireless Zone



Free with your library card!

Questions? Contact the info desk.

© 2006 Calgary Public Library

Process

- Governance
- Access Control
- Operations



Governance

- Board Policy
 - Public Access Network Policy
 - Sets out the framework to mitigate risk



Governance

- Board Policy
 - Access to the Network is governed by *Calgary Public Library Public Access Network Terms of Use*. The Library reserves the right to modify, limit services or stop services offered over the Network.



Governance

- Board Policy
 - Terms of Use are the key tool in mitigating risk
 - Gives library administration the framework to create and modify the Terms of Use



Governance

- Risk
 - Cover risks that are different from providing public access workstations



Governance

- Risk - stability of wireless transmission of data
 - Reduce the liability of the library by properly disclosing the risk to the user
 - any increased liability (as opposed to traditional workstations access) to the Library resulting from the provision of WiFi Access can be eliminated by proper disclosure



Governance

- Risk - security of wireless transmission of data
 - Reduce the liability of the library by properly disclosing the risk to the user
 - any increased liability (as opposed to traditional workstations access) to the Library resulting from the provision of WiFi Access can be eliminated by proper disclosure



Governance

● Terms of Use

- Customers must agree to the “Terms of Use” before gaining access to the Internet
- WiFi Access must not permit patrons to gain access to the Public Access Network except through one controlled entrance procedure.



Governance

- Terms of Use
 - a captive portal which intercepts and re-directs all access attempts to log-in / authentication page should be used





CALGARY PUBLIC LIBRARY
Wireless Network Authentication

Library Card Number:

Last 4 numbers of home phone or pin number:

As a vital community connection to a world of information and ideas, Calgary Public Library provides access to the Internet and its many useful information resources. In order to use the Public Access Network (the "Network") made available by the Calgary Public Library (the "Library"), you must agree to the Library's Public Access Network Terms of Use ("Terms of Use"). If you have not read the Terms Of Use, you can read them by clicking below. **Whether or not you have read the Terms of Use, by clicking on the "accept" button below, you agree to be bound by the Terms of Use.** If you do not agree to the Terms Of Use, do not click on the "accept" button, in which case you will not be granted access to the services available on the Network.

The Terms of Use is in effect since **July 24, 2006.**

Read Terms

Accept and Login

Decline



CALGARY PUBLIC LIBRARY

PUBLIC ACCESS NETWORK TERMS OF USE

- Basis of Access** The Calgary Public Library (the "Library") grants you the right to gain access through this public access network (the "Network") to the Internet and other electronic resources, on the following terms and conditions. Your use of this Network is subject to these terms and conditions, to which you agree. You agree that the Network is provided on an AS IS and AS AVAILABLE basis. The Library disclaims all responsibility and liability for the availability, timeliness, security or reliability of the Network. The Library also reserves the right to modify, suspend or discontinue your access to the Network with or without notice at any time and without any liability to you.
- Accuracy of Registration** You represent and warrant that (a) all of the information provided by you to the Library in order to log onto the Network is correct and current; and (b) you are not prohibited by any law, order or judgment (whether civil or criminal) from accessing the Internet.
- Internet Content** The Internet is an unregulated, global environment and should be used with care. Information found on the Internet may not be accurate, complete or current. Customers who use the Internet must carefully assess the information they receive from this medium. The Library does not control the information on the Internet and assumes no responsibility for any direct or indirect claims, damages or costs sought by users or third parties arising from the Library's provision of access to Internet services through this Network. The Library takes no responsibility for third party content (including, without limitation, any viruses or other disabling features), nor does the Library have any obligation to monitor such third party content.
- Public Use** Your access to the Library's Network is in public space, and you must not display materials on this Network which, in the opinion of any Library staff, are unlawful, obscene, abusive or otherwise objectionable. You will immediately comply with all directions from Library staff to stop accessing and displaying any such material. If you have accessed the Network through a public access terminal (the "Terminal"), to protect your privacy and security, and for the convenience of others, you agree to log/close out of any programs you have opened, before leaving the Terminal. The Library assumes no responsibility for the security or privacy of any on-line transactions you conduct.
- Privacy** Your use of this Network is subject to the Library's Confidentiality of User Records Policy. As a condition of use of this Network, you agree to the terms of that Policy as it may be updated from time to time. You agree that the Library may monitor, edit or disclose your personal information, including the material you have viewed or accessed through this Network, if required to do so in order to comply with any valid legal process or governmental request (such as a search warrant, subpoena, statute, or court order), or as otherwise provided in these Terms of Use.

Governance

- Terms of Use

- **Security** The Library does not provide encryption or other security measures to protect information you send or receive over the Internet. As with any Internet connection, there is no inherent security. We caution you to use prudence in your transmission of confidential or sensitive information over the Internet.



Governance

● Terms of Use

- **WiFi Hotspot service** If you are connecting to the Network through our WiFi Hotspot (wireless access service), be aware that wireless telecommunications connections are, by their very nature, more prone to loss of connection, due to the limited broadcast range of a hotspot, interference caused by physical structures and external interference (including interference with the radio signal through jamming, competing broadcasts on same frequency and temporary electromagnetic influences). This instability can result in the loss or corruption of data in transmission. In addition, any wireless transmission is capable of interception, even if you are sending data through a secure website (an “https” URL). The Library has no responsibility or liability to you resulting from any such loss or corruption of data, or from data interception or other consequences of your use of an unsecured wireless communications service.



Governance

- Terms of Use

- Accuracy of Registration You represent and warrant that (a) all of the information provided by you to the Library in order to log onto the Network is correct and current; and (b) you are not prohibited by any law, order or judgment (whether civil or criminal) from accessing the Internet.



Governance

- Terms of Use

- **Indemnification** You agree to hold harmless and indemnify the Library, its directors, officers, employees and agents, from and against all third party claims and legal proceedings of every kind whatsoever arising from or in any way related to your use of the Network, including all legal costs incurred by the Library in the defense of such claims and proceedings..



Governance

- Terms of Use Should Address
 - Internet Content
 - Access is in public space
 - Privacy
 - Limits on Privacy
 - Copyright



Governance

- Terms of Use
 - Time Limits and Reservations
 - Filtering Software
 - Breach of these Terms of Use



Governance

- Terms of Use
 - Law and Jurisdiction



Access Control

- Patrons seeking WiFi Access should log into a Library Public Access Network
 - captive portal technology
 - ILS database is used for authentication



Access Control

- Getting the captive portal talking to the ILS database was the most difficult part of our project
 - Would be easier if ILS systems supported LDAP or Radius Authentication
 - Creating a SIP authentication tool might needs to be investigated



Access Control

- The most important part of the authentication process is the acceptance of the Terms of Use before gaining access to the Internet
- This reduces the risk for the Library



Operations

● Connections

● Getting Connected

- Where service is available
 - Outside of building
 - Rental space (coffee shop)
- Hours of operation
- Length of time for use of service



Operations

● Connections

- User equipment - Support Model
 - No in depth user support – Info Sheet provided



Operations

● Coverage

- Placement of Access Points – built on previous models
 - Do not spend large amount of times on site survey

● Bandwidth

- Has not been an issue



Operations

- Space

- Furniture – seating space

- Power

- People want to plug in their laptops
- Not just a wireless issue



Operations

- Marketing

- Low Key

- In branch marketing



Goals of the technology

- Standards based implementation
- Improve data security features utilizing best practices
- A modular design with easy-to-add components and maximum flexibility
- Scalable
- Easy to administer



The Solution

Reviewed the Wireless Market:

- Looked at different ways of implementing captive portals
 - Free/shareware
 - Open source
 - Commercial products



The Solution

Reviewed the Wireless Market:

- Looked at market leaders
- Info-Tech Research Group identified Cisco and Aruba Networks as the segment leaders
- Talked to other public sector users of wireless technology



The Solution

Reviewed the Wireless Market:

- The Aruba solution was chosen
- Used by other public sector groups
- Ease of administration
- Captive portal technologies
- Ease of securing wireless traffic
- Worked with wireless VOIP



The Solution Traditional Wireless

- Traditional models for wireless access points gain access to the network at the switch
- The network needs to be secured from the switch to the exit point
- This is traditionally done by creating separate VLAN
- The administration of this model is complex



The Thin Client Solution

- The thin access points can only connect to the controller
- Traffic is securely contained in a GRE tunnel from the access point the controller. This means separate vlans do not have to be created in the WAN
- Traffic is securely separated from the library network

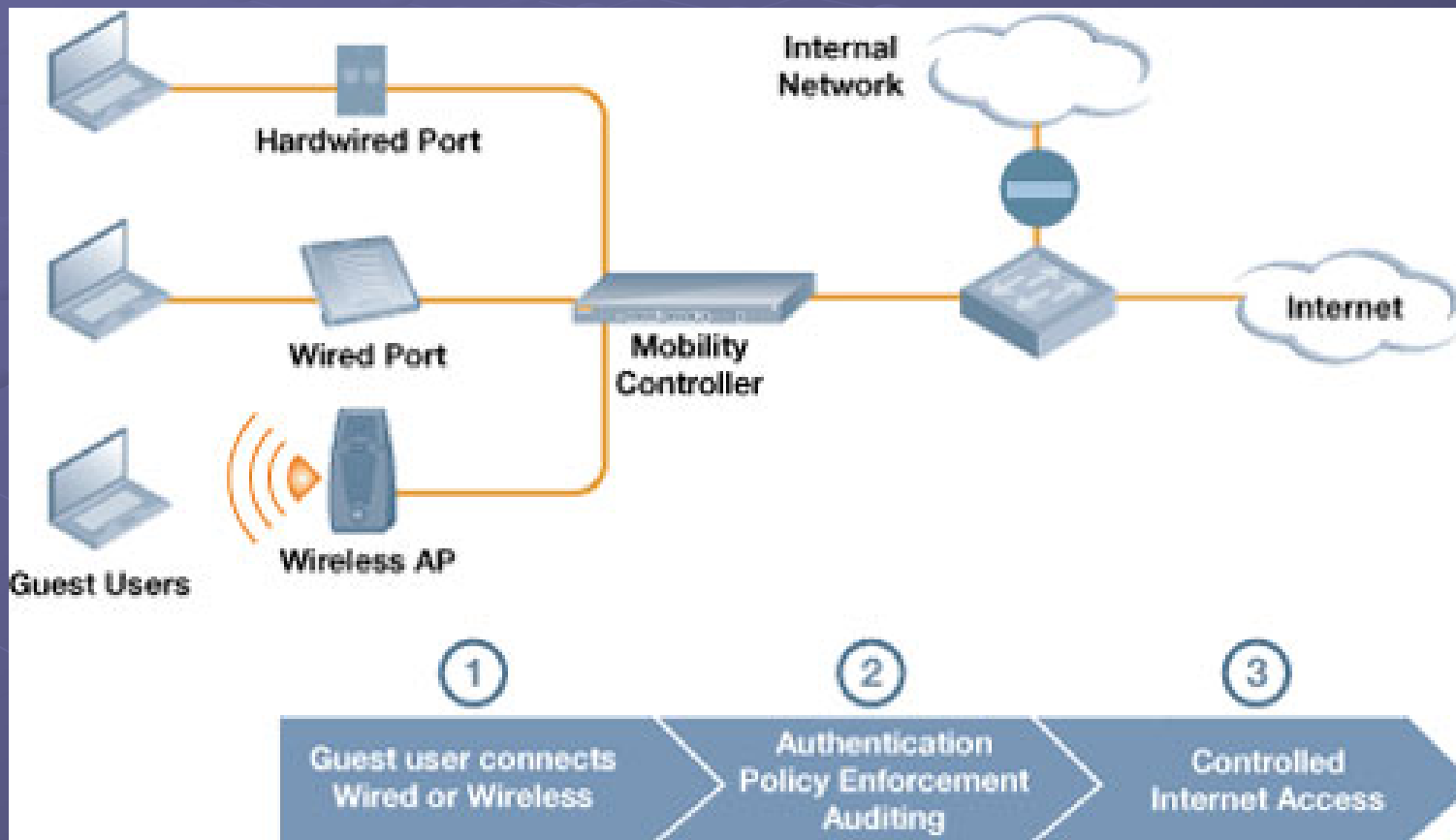


The Solution

- Administration takes place at the controller
- The controller is a role based firewall
- All wireless traffic goes through this firewall before entering the library network



The Solution



The Solution

- Policies are controlled in one place
- New access points can be added quickly and securely
- Existing VLANS can be used. New VLAN do not need to be added.



The Solution

- System upgrades are done to the controller reducing the amount of time to upgrade
- If the firmware needs to be updated on the access point it is done from the controller





- Network**
- Network Summary
- All WLAN Controllers
- All Access Points
- All Air Monitors
- All Wired Access Points
- Global Events
- Controller**
- Controller Summary
- Access Points
- Wired Access Points
- Wired Mux Ports
- Air Monitors
- Clients
- Blacklist Clients
- Firewall Hits
- External Services Interface
- Ports
- Inventory
- Local Events
- WLAN**
- library-private-02
- LibraryWiFiHotSpot

Network Summary

WLAN Network Status				
	Total	Total	IPSEC	IPSEC
	Up	Down	Up	Down
WLAN Controllers	1	0		
Access Points	66	0	0	0
Air Monitors	0	0	0	0
Wired Access Points	1	0	0	0
Unprovisioned Access Points	1			
Duplicate AP Name	0			
RADIUS Servers	2	0		
LDAP Servers	0	0		

WLAN Performance Summary			
	Last 5 Min	Last Hour	All
Load Balancing Events	0	0	0
Interference Events	0	0	0
Bandwidth Exceeded	0	0	0
Error Threshold Exceeded	0	0	0

Rogue AP Classification Summary			
	Last 5 Min	Last Hour	All
Rogue APs Detected	0	0	0
Rogue APs Disabled	0	0	0
Suspected Rogue APs	0	0	0
Interfering APs Detected	28	95	122
Known Interfering APs	0	0	0



- Network**
- Network Summary
- All WLAN Controllers
- All Access Points
- All Air Monitors
- All Wired Access Points
- Global Events
- Controller**
- Controller Summary
- Access Points
- Wired Access Points
- Wired Mux Ports
- Air Monitors
- Clients**
- Blacklist Clients
- Firewall Hits
- External Services Interface
- Ports
- Inventory
- Local Events
- WLAN**
- library-private-02
- LibraryWiFiHotSpot

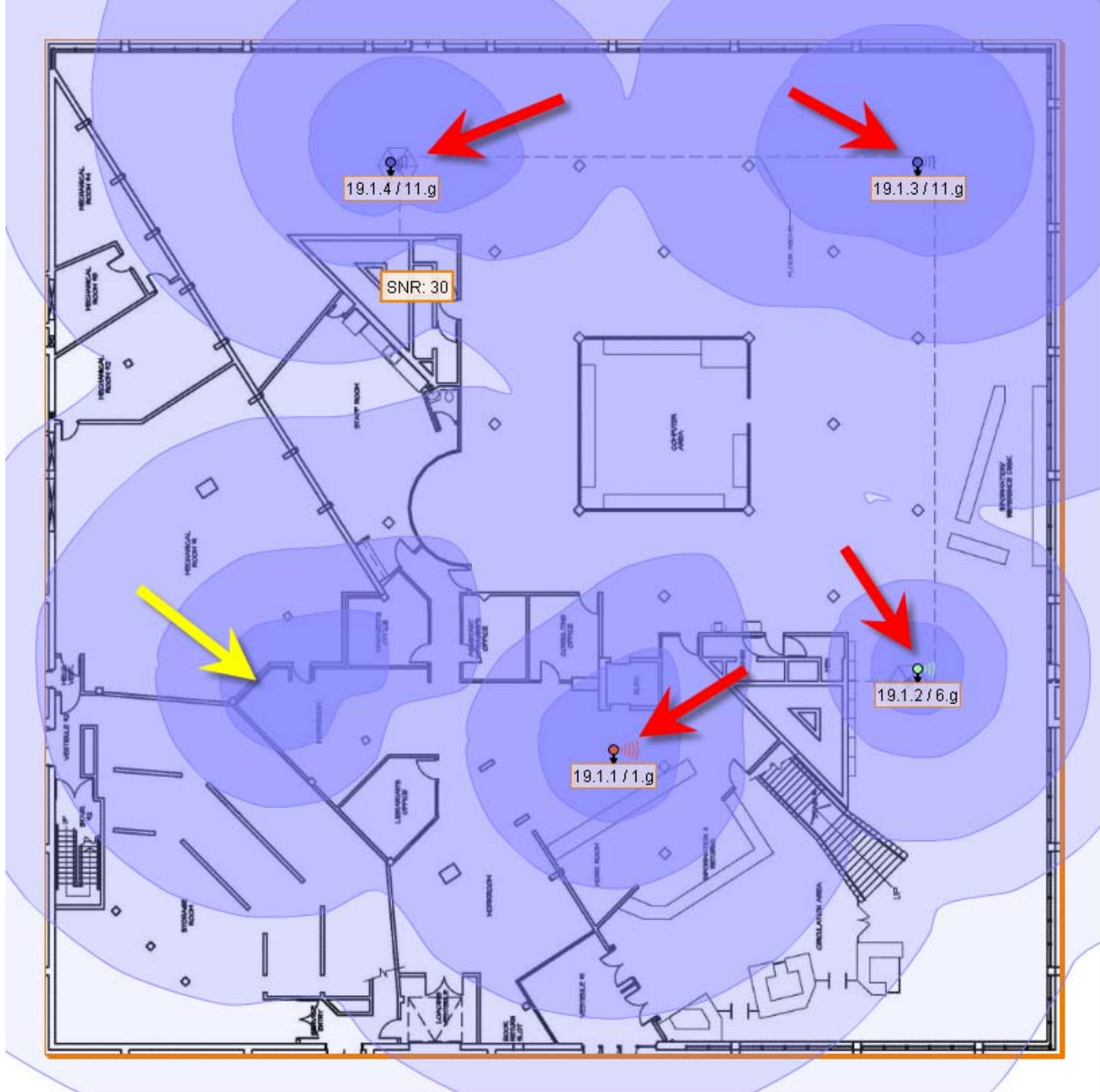
Controller > **Clients**

Search Results

	User Name	MAC address	Client IP	User Role	Authentication Method	ESSID	BSSID	Age
<input type="radio"/>	phone38	00:19:30:2f:35:c7	10.5.16.46	ip-phone	802.1x	library-private-02	00:0b:86:28:f5:c0	9 days 23 hrs 20 mins
<input type="radio"/>	phone10	00:14:a8:a7:8a:04	10.5.16.59	ip-phone	802.1x	library-private-02	00:0b:86:28:d0:60	6 days 22 hrs 35 mins
<input type="radio"/>		00:1c:26:0f:3f:14	172.16.2.75	cplpatron		LibraryWiFiHotSpot	00:0b:86:28:f8:11	1 mins
<input type="radio"/>		00:13:ce:dc:6c:81	172.16.2.62	Pre-CPLpatron		LibraryWiFiHotSpot	00:0b:86:aa:4c:f1	3 mins
<input type="radio"/>		00:15:00:3d:43:c3	172.16.3.23	Pre-CPLpatron		LibraryWiFiHotSpot	00:0b:86:28:d0:a1	53 mins
<input type="radio"/>		00:1c:b3:b3:c9:aa	172.16.3.213	Pre-CPLpatron		LibraryWiFiHotSpot	00:0b:86:24:c4:61	8 mins

Previous 1 2 3 | 21-26 of 26 10 ▾

- Status
- Profile
- Client Activity
- Packet Capture
- Locate
- Debug
- Disconnect
- Blacklist
- Ping



19.1.4 / 11.g

19.1.3 / 11.g

SNR: 30

19.1.2 / 6.g

19.1.1 / 1.g

Demo



Post Implementation

● Support

● Dropped Connections

- Security settings
- AP coverage

● Time Limits



Questions?

