WiFi Service Control

Design & Case Studies

Simon Newstead
APAC Product Manager
snewstead@juniper.net

Juniper NETWORKS

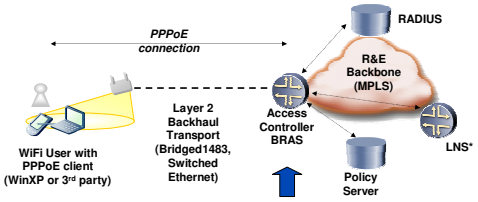
Agenda

- Comparing carrier and R&E WiFi requirements
- Overview of different access models
- Case studies
- Identifying user location and controlling the user
- Secure access options

Common WiFi service requirements

- Per user identification and service control (network policies)
- High scalability of # users, throughput – campus more so?
- Bill per user – volume, destination, time – and charge back to department / faculty, (or hotspot owner/ISP/user)
- Support "wholesale functions"
- Varying levels of security support – from unauthenticated insecure to full encryption end-end
- Support QoS for Voice over WLAN – WME now (802.11e next) - mapping to 802.1D (802.1p) / Diffserv
- *R&E deployments of WiFi now starting to adopt a carrier model – eg in Australia*

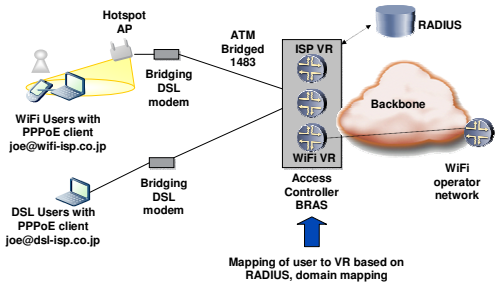
WiFi control - Access Models PPPoE



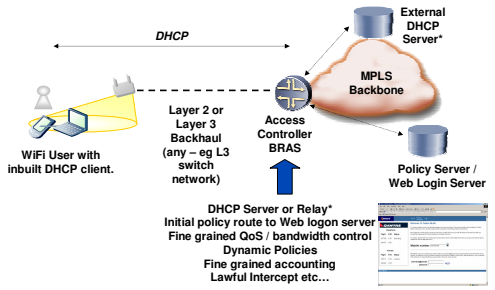
PPPoE access model - discussion

- **Pros:**
  - Full per user control with inbuilt PPP mechanisms (authentication, keepalives etc.)
  - Individual policy control per user simplified
  - Wholesale is simplified and possible at layer 2 and layer 3
  - Leverages the B-RAS model used in DSL – virtually no changes
- **Cons:**
  - Requires client software (maybe even with XP) – management issue for 1000s of end users.. Doesn't buy you security…
  - Only works in a bridged access environment; often not possible
  - Layer 3 access network requires use of native LAC client (BRAS acts as LNS or tunnel switch) – client support issues

PPPoE access model Case Study – Japanese Carrier



WiFi control - access models
DHCP model – Web Login



DHCP Web Login model - discussion

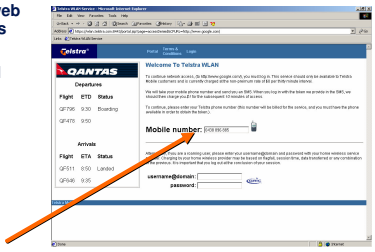
- **Pros**
  - No external client software – inbuilt DHCP – lower barriers greatly
  - Any access network – eg L3 switches, routing APs etc
  - Web Login provides extra options to provider (branding, location based content, time based content…)
- **Cons:**
  - Wholesale becomes more challenging eg. address allocation – NAT introduces complications (ALG support etc), no tunnelling with L2TP
  - Greater security / DoS implications – attack DHCP, Web server
  - No autologon by default (manual web login process) – unless unauthenticated ☺
- **Need to introduce mechanisms to enable per user control in DHCP environment (mimic PPP)**

DHCP / Web login example – Telstra Mobile

- Mobile centric service, launched in August 2003
  - Available in hotspot locations throughout Australia
  - Target of 600 hotspot locations in 2004 (Qantas, McDonalds, Hilton etc)
  - International roaming through the Wireless Broadband Alliance
  - Time based billing; hourly rate
  - Login via a password delivered by SMS to a Telstra mobile (credit card payment option for non-Telstra post-paid mobile customers)
- Lowered barriers to uptake
  - No special WLAN subscription needed – casual pay-per-use option
  - Captive portal logon using DHCP – no client software required

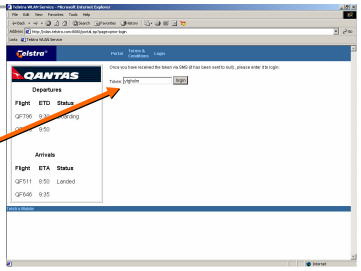
How it works - Step One

- User opens up web browser and tries to go to Google
- Session directed to captive portal on policy server
- Choice to enter mobile phone number or username and password
- Mobile phone number entered



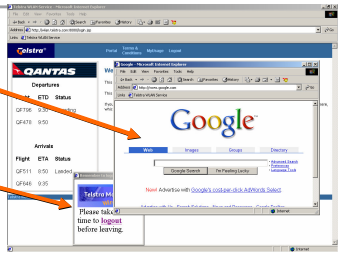
Step Two

- One-time password sent via SMS to user's mobile phone
- Received password entered into portal page



Step Three

- Upon successful authentication, captive portal is released and original web destination is loaded.
- Mini-logout window to facilitate signoff.
- Usage billed to user's mobile phone bill once finished

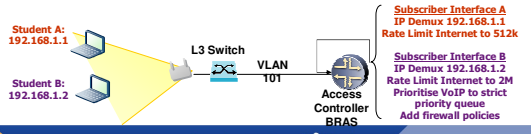


Dynamic Policies

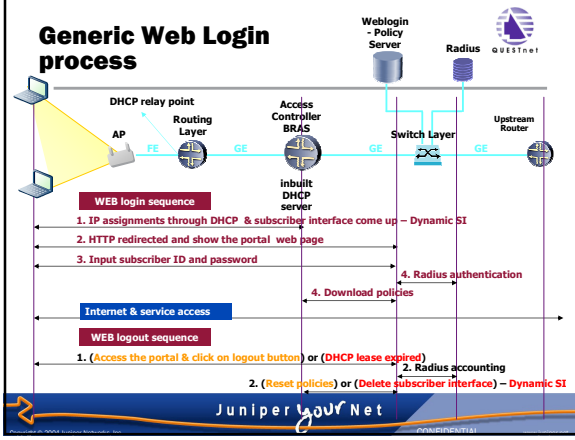
- Allow greater flexibility of services eg- prior to logon:
  - Free access to Internet for 15 mins without login… or
  - Internet access only, mail & p2p ports blocked…or
  - Location specific walled garden content only
- Bandwidth can be dynamically increased and restrictions removed on user authentication and login
- Also helps protect against abusive or Worm users (eg- dynamically limit users down on sliding window basis; consumed more than x MB in past 15 mins)
- => Individual Policies also enable fine grained accounting per user!

Per user control in a DHCP environment

- Objective - make an IP host on single aggregated interface appear like its own IP interface
  - Treat hosts as separate logical (demultixed) IP interfaces aka "Subscriber Interfaces"
  - Individual policy control on subscriber interface (linked to policy server) – eg filters, bandwidth control
  - Tie into DHCP dynamically. Use lease times as "keepalive"

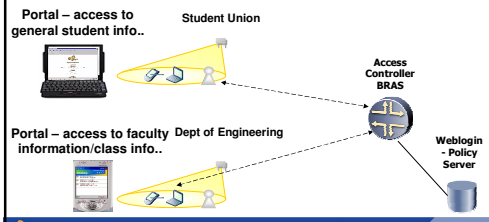


Generic Web Login process



Location / AP information – why??

- Generates portal pages based on hotspot location
- Enables targeted content dependent on the hotspot location, revenue sharing (charging models) etc…



Location information – how?

- PPPoE model
  - Easy – layer 2 circuit per hotspot to AC/BRAS
  - RADIUS will contain NAS Port ID etc…map back centrally
- DHCP model - rely on the relay to provide
  - Gateway address (GiAddr field)
  - Option 82 information, suboptions (ala RADIUS VSAs)
  - Or even layer 3 GRE tunnel back if access network can't provide info required (also simplifies routing)

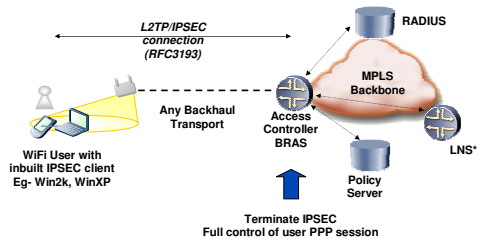
Quick point – routing back to WiFi user in DHCP environment

- Use location based info to allocate users from address pools; eg- pools per AP
  - Aggregate routes
  - Static, redistributed to IGP; simplified
- Central pools also possible but..
  - Require DHCP relay to store state - snoop address coming back from the server in DHCP offer / ACK, to be able to add the route
  - Also requires redistribution into IGP; scaling issues with that…

Secure access

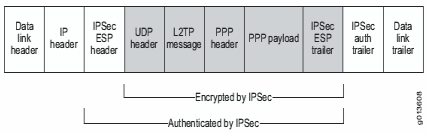
- Why?
  - Various access vulnerabilities in simple models
  - Session hijacking / spoofing, man in the middle
- Few main approaches:
  - IPSEC tunneling model
  - 802.1x/EAP approaches
  - SSL VPN access

WiFi secured access IPSEC option



Secure remote access Windows IPSEC – protocol stack

Figure 48: L2TP/IPSec-encapsulated data packet



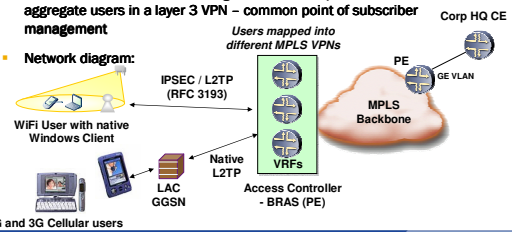
ESP Transport mode

IPSEC WiFi access

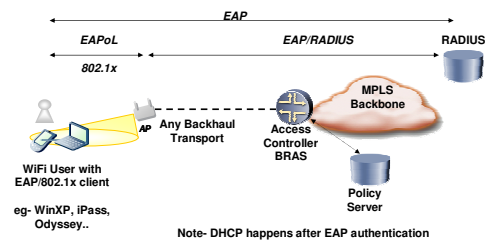
- **Pros**
  - No external client software – inbuilt into Windows
  - PPP model gives full per user control (eg- terminate IPSEC and tunnel on L2TP)
  - Integrates well into a VPN environment; user sessions terminated to MPLS VPNs at AC/BRAS (PE)
  - Can use digital certificates to ensure identity (server and maybe clients also)
- **Cons:**
  - Client issues – overhead, PDA support (eg- WinCE today only supports MSCHAPv2?)

IPSEC WiFi access Japan Case Study

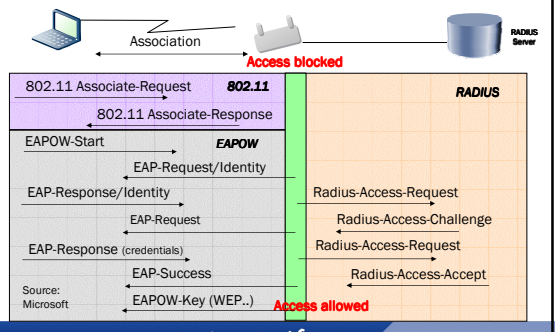
- **Integration of VPN access for mobile corporate users regardless of access type**
- **Outsource remote access management from corporates, and aggregate users in a layer 3 VPN – common point of subscriber management**
- **Network diagram:**



WiFi secured access 802.1/EAP option



Option - Authentication using 802.1X and EAP on 802.11 - overview



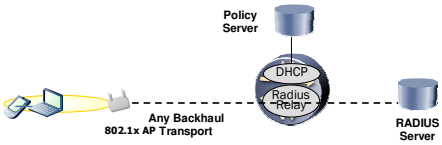
EAP/802.1x WiFi access

- **Pros**
  - EAP/802.1x built into WinXP
  - Flexible authentication architecture – many different EAP methods can be used eg- TLS, TTLS, GSM SIM using EAP/SIM, EAP-MD5, LEAP, Smartcards etc…
  - Can handle interAP roaming with 802.11f
- **Cons:**
  - Doesn't address core network / VPN portion, just secures access layer
  - Today uses session keys vs temporal (WPA, coming in 802.11i)
  - Need smarts to keep per user control in the network without double logon

Maintaining subscriber control when using 802.1x/EAP environment

"RADIUS relay" concept

- 802.1x access points have Radius client, EAP messages encapsulated in Radius messages
- Host MAC address in the calling-station-attribute
- Radius relay (BRAS) uses @domain name to forward Radius request to an external EAP capable Radius proxy or server
- BRAS relay stores Host MAC address (and maybe username passed back in access accept) and awaits authorization data (VR to use, IP pool/address to use, filters, etc)
- DHCP request, based on the host MAC address, creates subscriber interface in proper context allocates IP address, assign default policies. Policy server control with no Web login
- Access point creates Radius authentication and accounting (stop)



SSL approach for access

- **Rapidly emerging new secure access technique**
- **Pros**
  - Browser based access
  - No client required unlike IPSEC –thin client downloaded on demand
  - Able to restrict and control on per application basis – from restricted web access through to full IP network access (ultra skinny tunnel client PPP over SSL downloaded in real time via browser)
  - Works on any access – L2 or L3
- **Cons:**
  - Relatively new technology – today more enterprise focussed

Summary

- **Which access model?**
  - PPPoE is nice, but often not practical
  - DHCP – web login models now can provide good per user control, and location info etc
- **Where am I? Location information**
  - Useful in both carrier and R&E applications eg- generate content based on location (virtualised)
- **Security**
  - IPSEC is a proven end-end mechanism, integration with VPNs
  - EAP is flexible and useful in access, but needs to tie in with core network and per user control
  - SSL provides a flexible & lightweight technique – gaining favour
- **R&E requirements share many similarities with carrier model**

Thank you…!

Contact: snewstead@juniper.net