Free the RADIUS

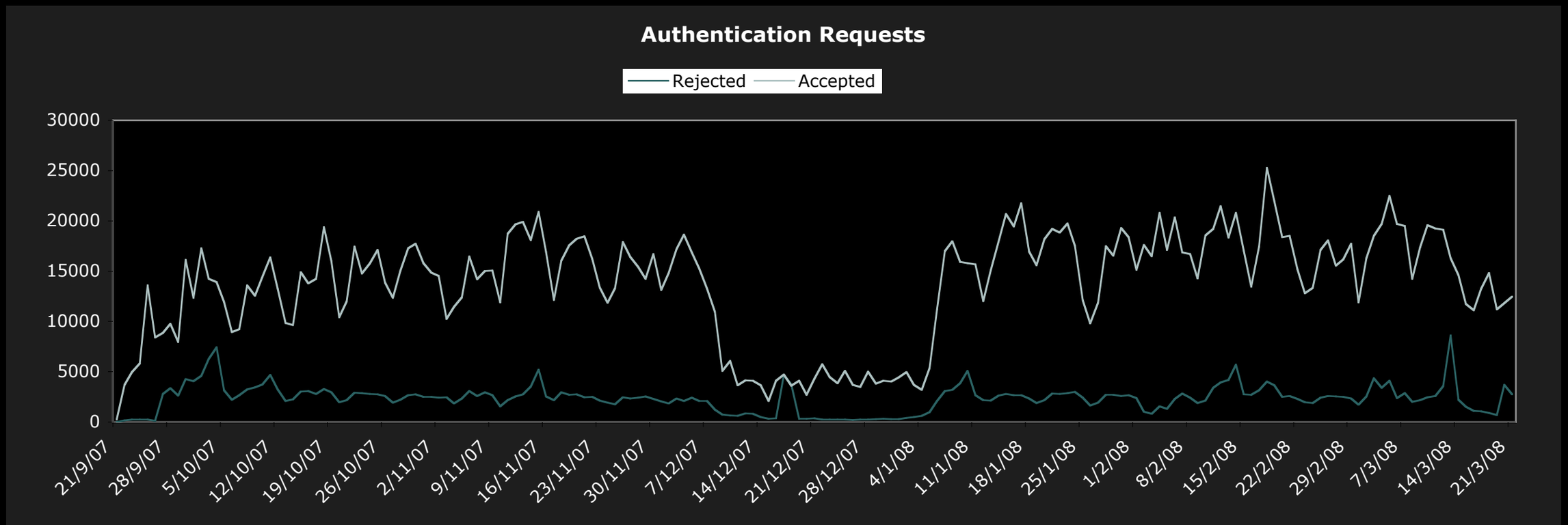
Expanding 802.1X beyond the niche network

Arran Cudbard-Bell
University of Sussex

Free the RADIUS
Design

Free the RADIUS - Design - It really can run on a 486 !

Expanding 802.1X beyond the niche network



Servers

- 2 x Apple XServe Dual 2.3Ghz G5 (Averaging < 5% CPU load) *free*RADIUS
- 1 x Sun E450 (MySQL)
- 6 x Apple Xserve LDAP Cluster nodes

Core & Zone

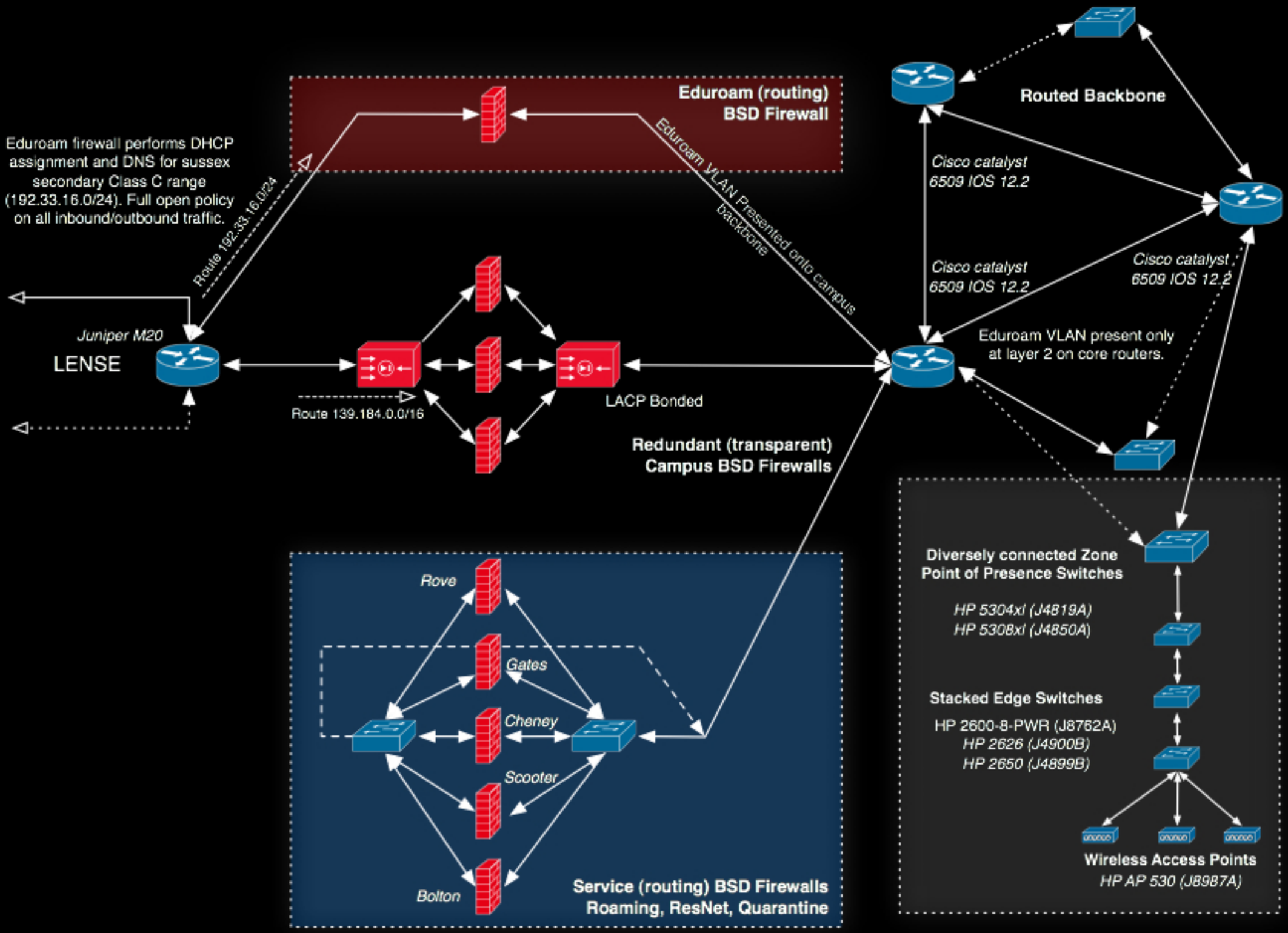
- 3 x Cisco Catalyst 6509 IOS 12.2 core routers
- 25 x 5300 Series HP ProCurve Point of Presence Switches

Edge

- 34 x HP 530 Wireless Access Points (more in 08/09)
- 90 x Apple Airport / Airport Extreme Base Stations (retiring 08/09/10)
- 358 x 2626/2650 HP ProCurve Edge Switches
- 184 x 2524 HP ProCurve Edge Switches (retiring 08/09/10)

Free the RADIUS - Design - Network Components

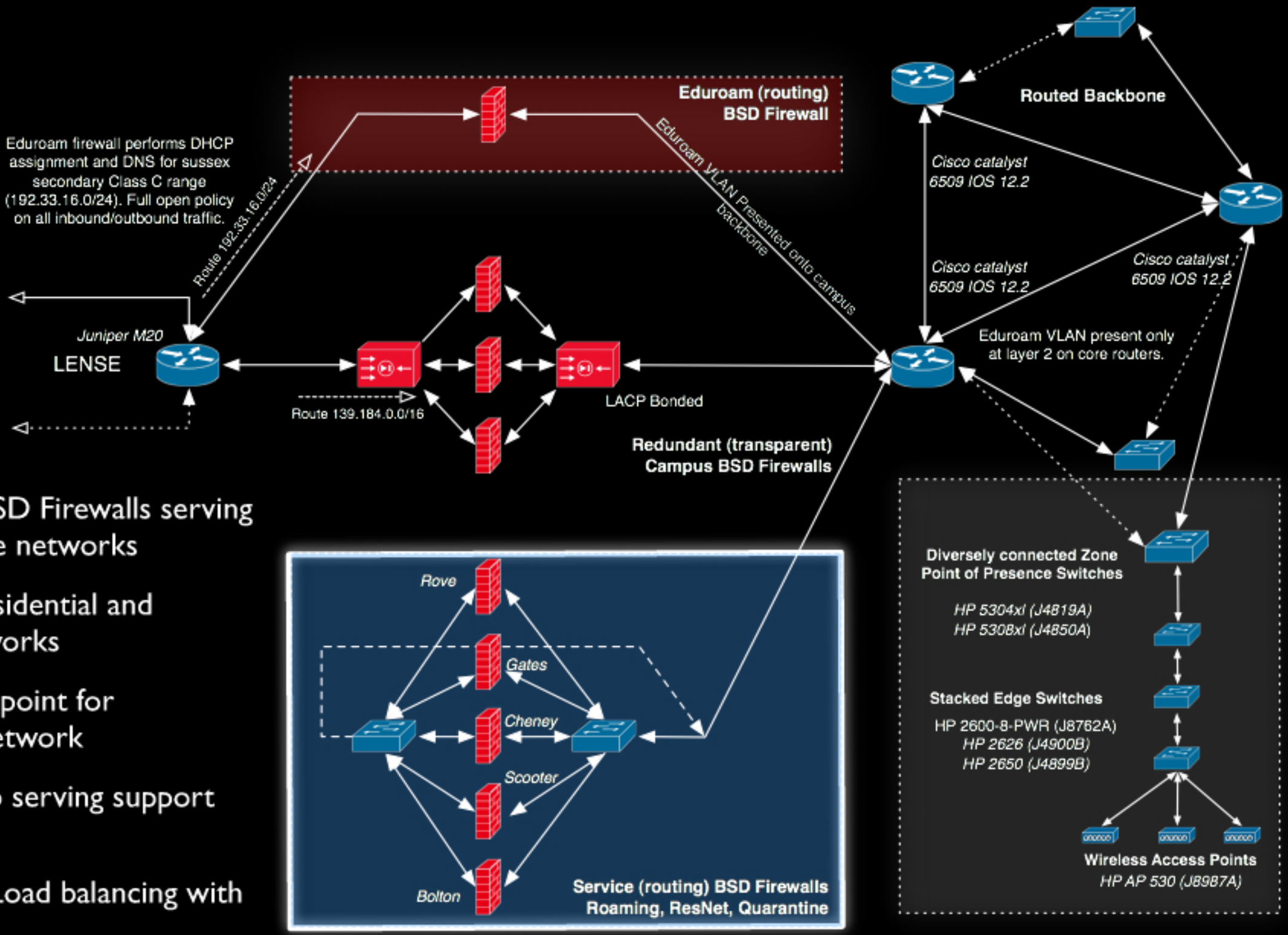
Expanding 802.1X beyond the niche network



Free the RADIUS - Design - Network Components

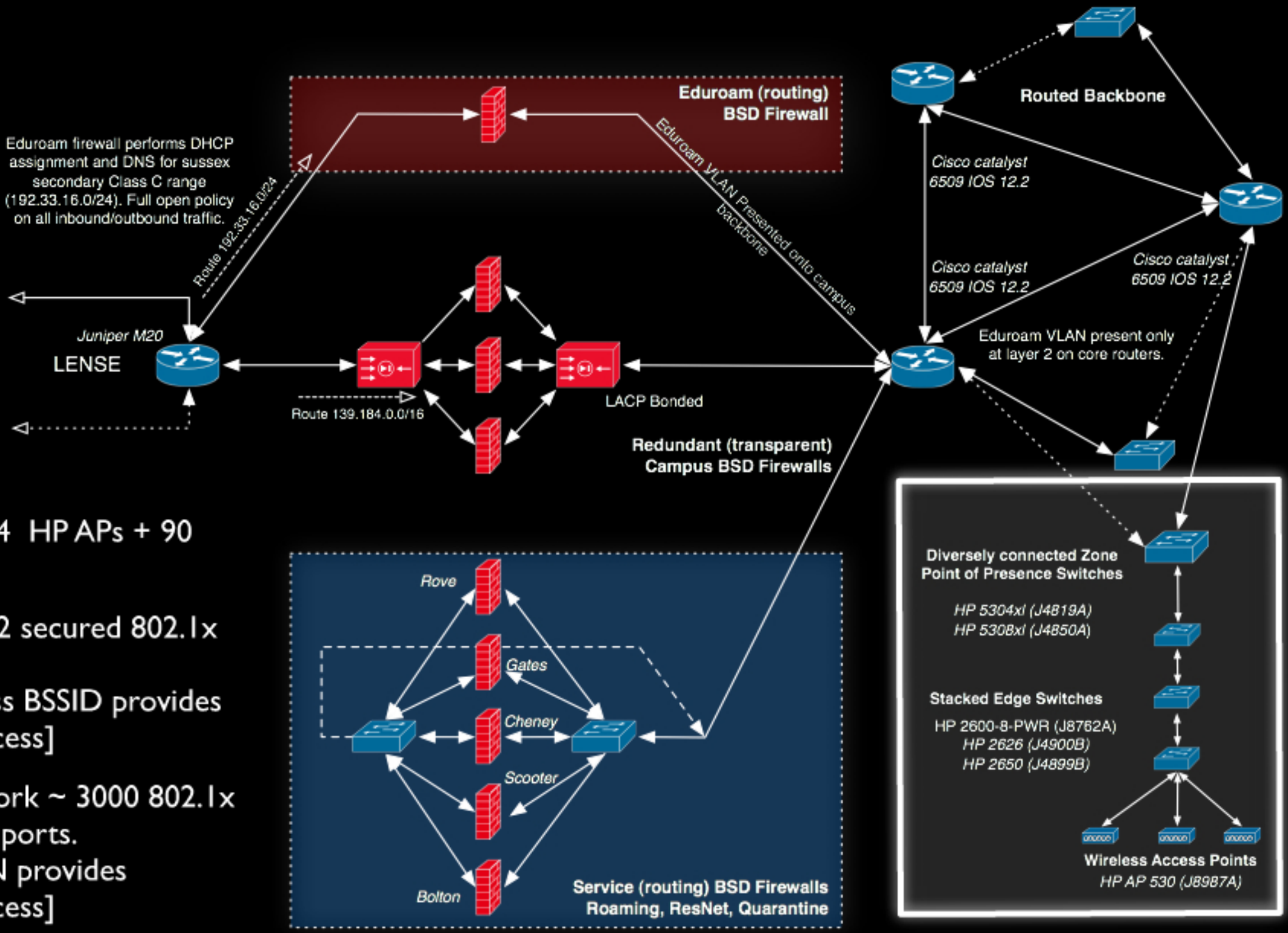
Expanding 802.1X beyond the niche network

- 5 Routing BSD Firewalls serving private service networks
- NAT for Residential and Roaming networks
- Termination point for Quarantine network
- BAMP Setup serving support pages
- Poor Mans Load balancing with DHCP



Free the RADIUS - Design - Network Components

Expanding 802.1X beyond the niche network

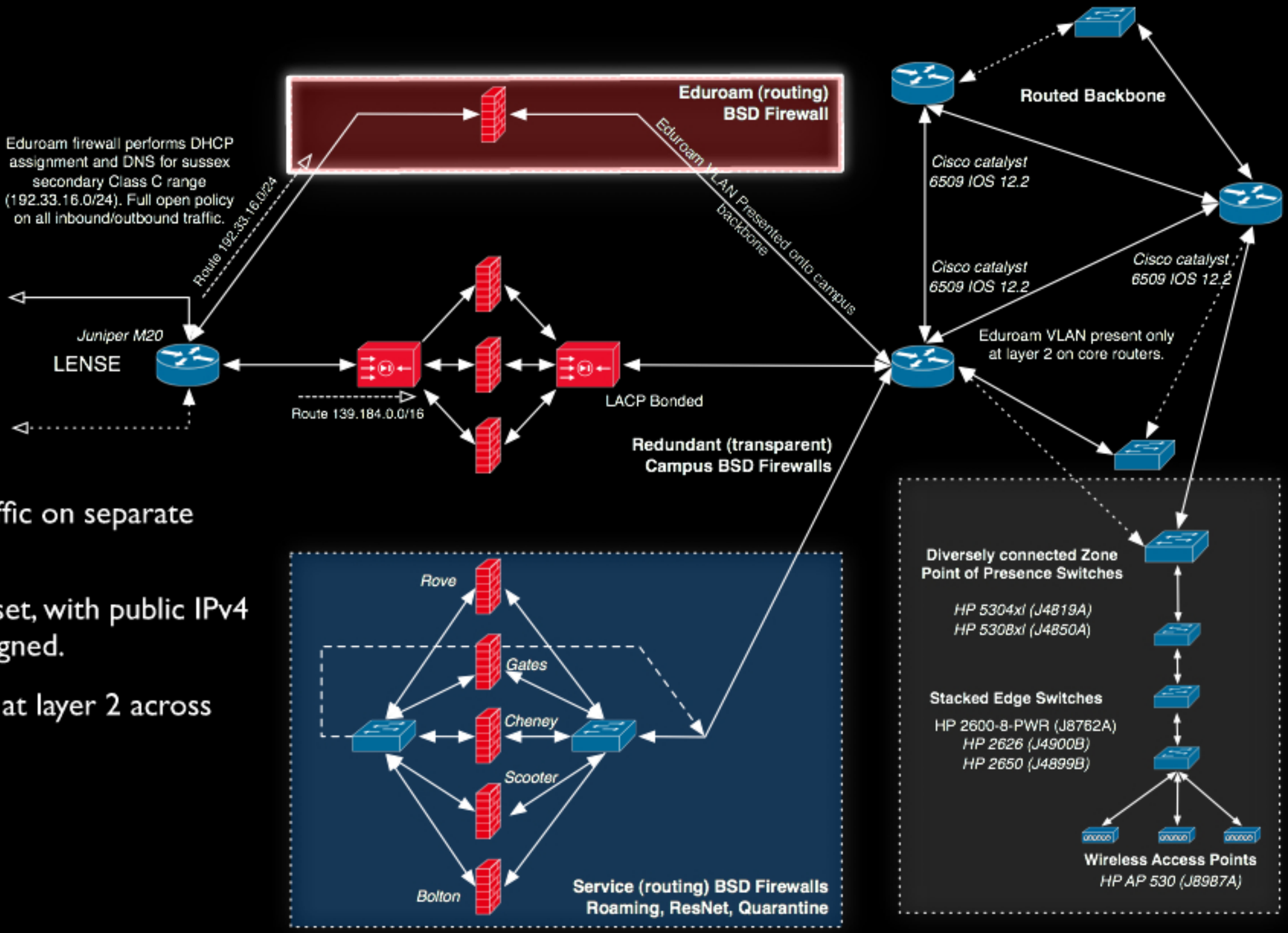


- Wireless - 34 HP APs + 90 legacy.
- WPA / WPA2 secured 802.1x authenticated.
  [Open wireless BSSID provides quarantine access]
- Wired network ~ 3000 802.1x authenticated ports.
  [Unauth VLAN provides quarantine access]

Free the RADIUS - Design - Network Components

Expanding 802.1X beyond the niche network

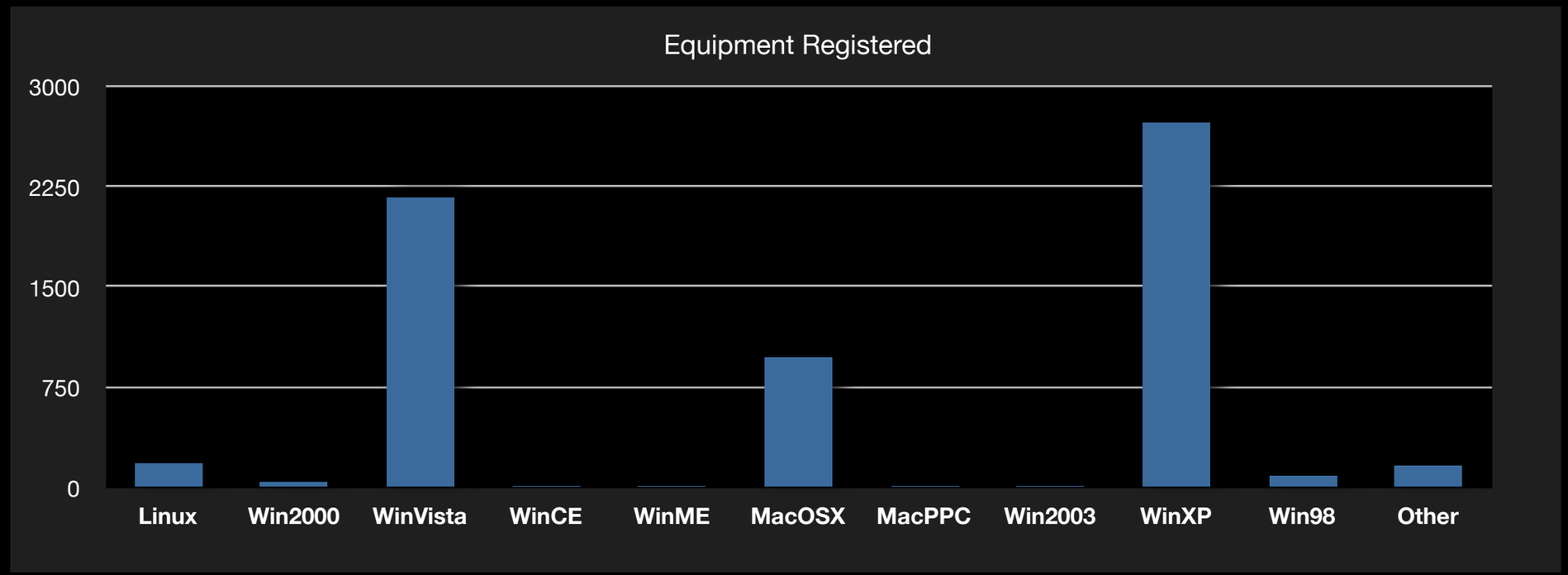
- Eduroam traffic on separate Class C.
- Minimal ruleset, with public IPv4 Addresses assigned.
- Present only at layer 2 across core network



Free the RADIUS - Design - Going native

Expanding 802.1X beyond the niche network

OS	Registered
Linux	180
Win2000	40
WinVista	2173
WinCE	15
WinME	2
MacOSX	975
MacPPC	4
Win2003	3
WinXP	2741
Win98	100
Other	175



Native Supplicant :

- Windows Mobile, 2000, XP, 2003, Vista (No 95/98/ME support)
- Mac OSX 10.3-10.5
- Symbian OS

WPA Supplicant :

- Linux (Ubuntu)

Secure W2 :

- Problem Cases (Windows 2000, XP, Vista)

Free the RADIUS

Problem Solving

Free the RADIUS - Problem Solving - Reducing Help Desk Hassles

Expanding 802.1X beyond the niche network

ResNet sussexroam eduroam

University of Sussex

Sussex Network Services

Arran Cudbard-Bell (ac221)

Hello Arran, welcome to the Sussex Network Services support site. Your account has been registered since the 21st September 2007.

To register new computers for access to sussex network services, please click the **Register »** button:

Register a computer Register »

You currently have the following computers registered for the roaming network.
To change a computer registration or any mac addresses associated with it, click the **Change Computer »** button.

Name	Type	Os	Comment	Mac Addresses	
PocketLoox720	PDA	WinCE	Windows CE 2003/Pocket Loox 720	003005922ba1	Change Computer »
Parallels Virtual 98	Desktop	Win98		001c42a87386	Change Computer »

Your status

Account Enabled

Computer Enabled (PocketLoox720) [Help] [Setup guide]

Computer Enabled (Parallels Virtual 98) [Help] [Setup guide]

Recent Events

Today at 03:40pm : ac221 Authenticated as manager on NAS hp-e-sb-3-sw3

16:45 23/03/08 : Authentication failed please check credentials and service entitlement.

16:45 23/03/08 : Authentication failed please check credentials and service entitlement.

16:45 23/03/08 : ac221 Authenticated as manager on NAS hp-e-engg1-1-sw1

12:10 23/03/08 : ac221 Authenticated as manager on NAS hp-e-sb-1-sw2

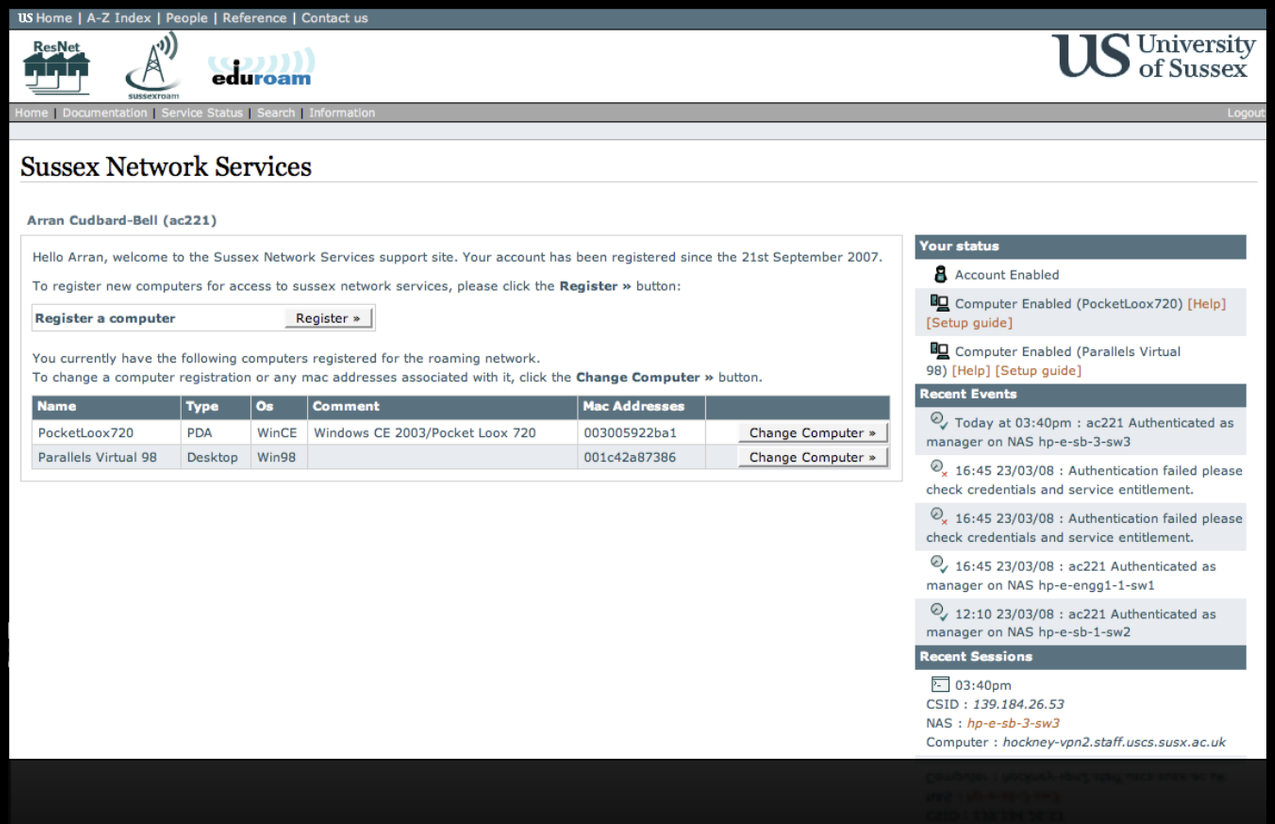
Recent Sessions

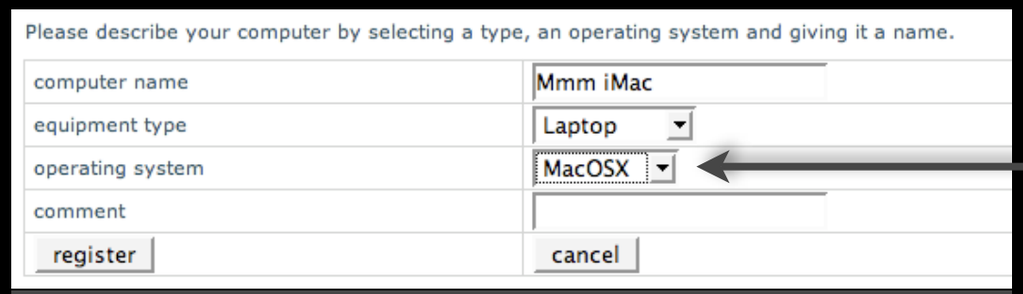
03:40pm
CSID : *139.184.26.53*
NAS : *hp-e-sb-3-sw3*
Computer : *hockney-vpn2.staff.uscs.susx.ac.uk*

Free the RADIUS - Problem Solving - Reducing Help Desk Hassles

Expanding 802.1X beyond the niche network

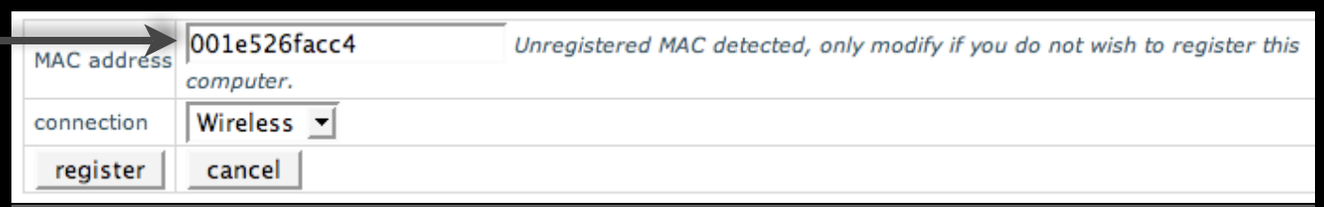
Registration site served from 'Quarantine' VLAN firewalls with automatic HTTP redirection.





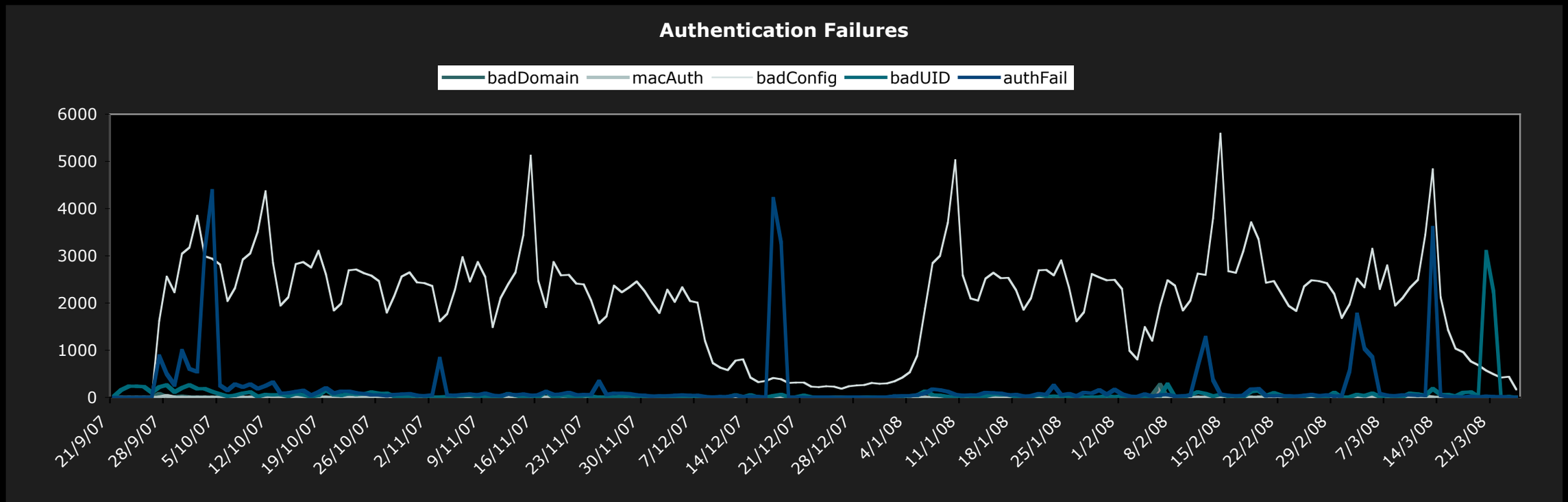
Automatic OS detection simplifies registration process, and allows for passive data collection.

Web server and client on the same Layer 2 segment. Unregistered MAC Addresses can be gleaned from servers ARP cache.



Free the RADIUS - Problem Solving - It looks bad but ...

Expanding 802.1X beyond the niche network



Authentication Failures

- During Advertised 'service at risk' periods
- Inappropriate DB locking
- Peaks in Authentication requests
- Hash Synchronisation
- Accounting DOS

Misconfigured Supplicant

- Initial Presentation onto network (2000, XP, Vista)
- Strange unexplainable authentication attempts on service start/ stop.

What's wrong with standard LLL DB Based accounting mechanisms ?

- Ties up finite resources processing Accounting data, where Authentication requests should always have priority
- Accounting request 'DOS' after widespread power loss
- Buggy NAS can easily overwhelm DB
- Accounting data lost during DB outages
- Accounting data lost during Home Server outages when proxying
- Doesn't scale easily

Increasing reliability and performance

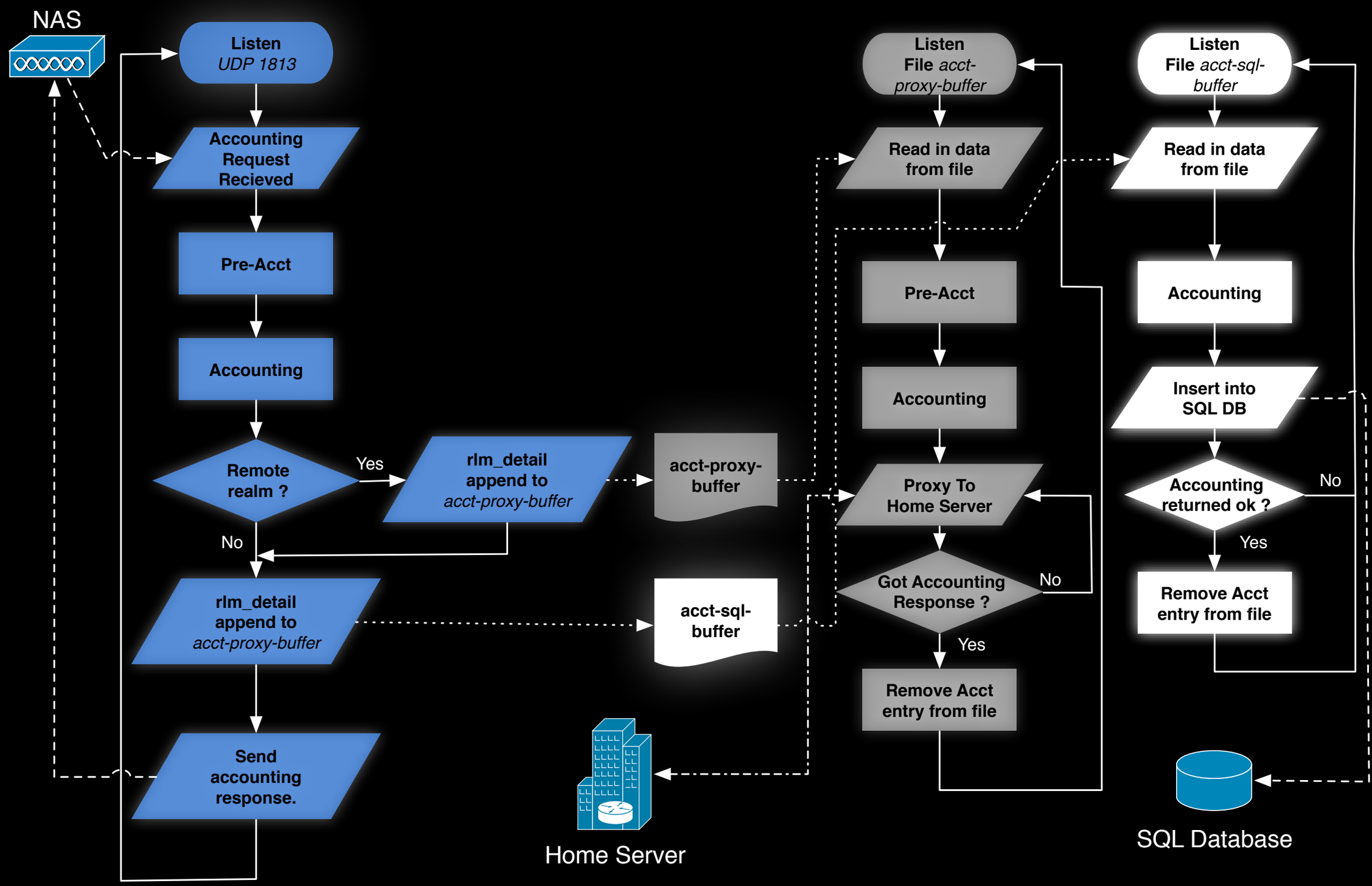
- InnoDB **not** MyISAM (if using MySQL)
- Separate pools of database connections for authentication and authorisation requests
- Load balance stanza to balance requests between SQL processing nodes
- File Based Buffers
  - FR < v2.0.3 RAD Relay / SQL Relay (File based Buffers)
  - FR >= v2.0.3 RAD Relay features integrated into server core as Virtual-Server option

File Based Buffers in FR 2.0.3

- Accounting Data not removed until operation has succeeded
- Server Auto-Throttles based on the time taken to process previous request and system load
- Buffer grows during peak load freeing up resources for authentication
- Requests processed in serial fashion, though parallel processing may be coming in the near future.

Free the RADIUS - Problem Solving - Bigger Buffers

Expanding 802.1X beyond the niche network



Free the RADIUS

Looking Forward

Why is Open VLAN a bad thing ?

- To prevent banned users being placed in the Open VLAN you may have to break RFC 3749 2.6.3
- No records regarding point of connection onto the 'unauth' VLAN
- No way to *easily* disconnect users
- One 'unauth' VLAN for all
- Can't use GVRP to distribute the 'unauth' VLAN
- It's a hack, and not a pretty one

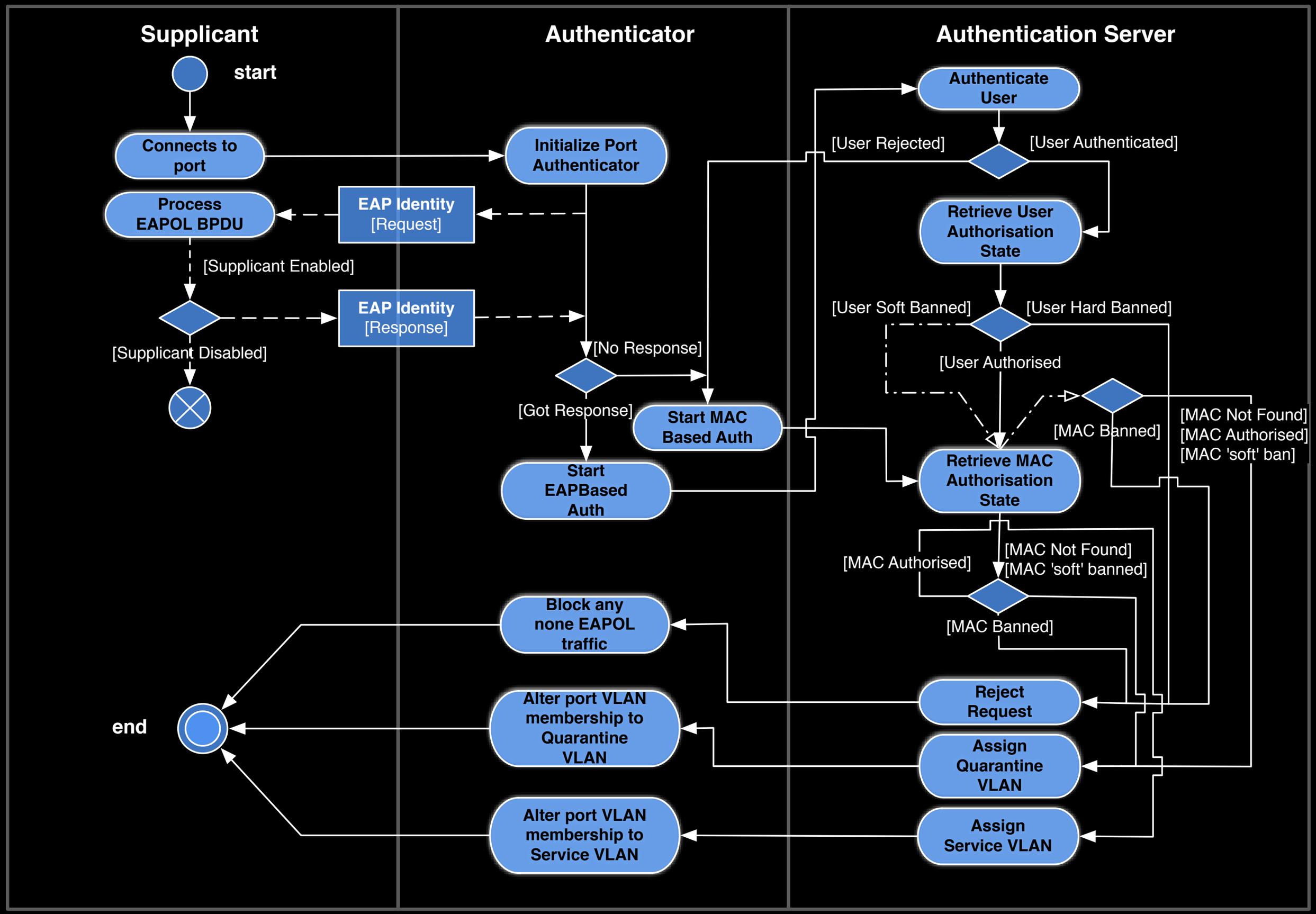
Benefits of multi-tiered authentication

- Hosts can be blocked at the edge
- Support for legacy hosts (Non Dot1x compliant devices can still use the network)
- Authentication records generated for every connection onto the network:
  - Allows context sensitive support pages
  - Reliable inventory of hosts connected to the network
  - Allows SNMP Based analysis of connected hosts (where supported)
  - Dynamic service changes via SNMP (no need for CoA support if not proxying)
  - and more...

- Different 'un-authorised' VLANs depending on host (concept of resting VLANs for workstations)
- Truly centralised VLAN assignment (part of a homogenous edge environment)

Free the RADIUS - Looking Forward - Twice the authentication of the next leading Vendor

Expanding 802.1X beyond the niche network



What the heck is GVRP (Generic VLAN Registration Protocol)?

- Defined in 802.1D as an implementation of GARP (Generic Attribute Registration Protocol)
- Allows registration of arbitrary attributes with ports of an 802.1D MAC Bridge
- Allows propagation of VLAN information from multiple GVRP advertisement roots
- Allows creation of dynamic on demand VLAN paths
- Follows spanning tree

Why hasn't it been widely used ?

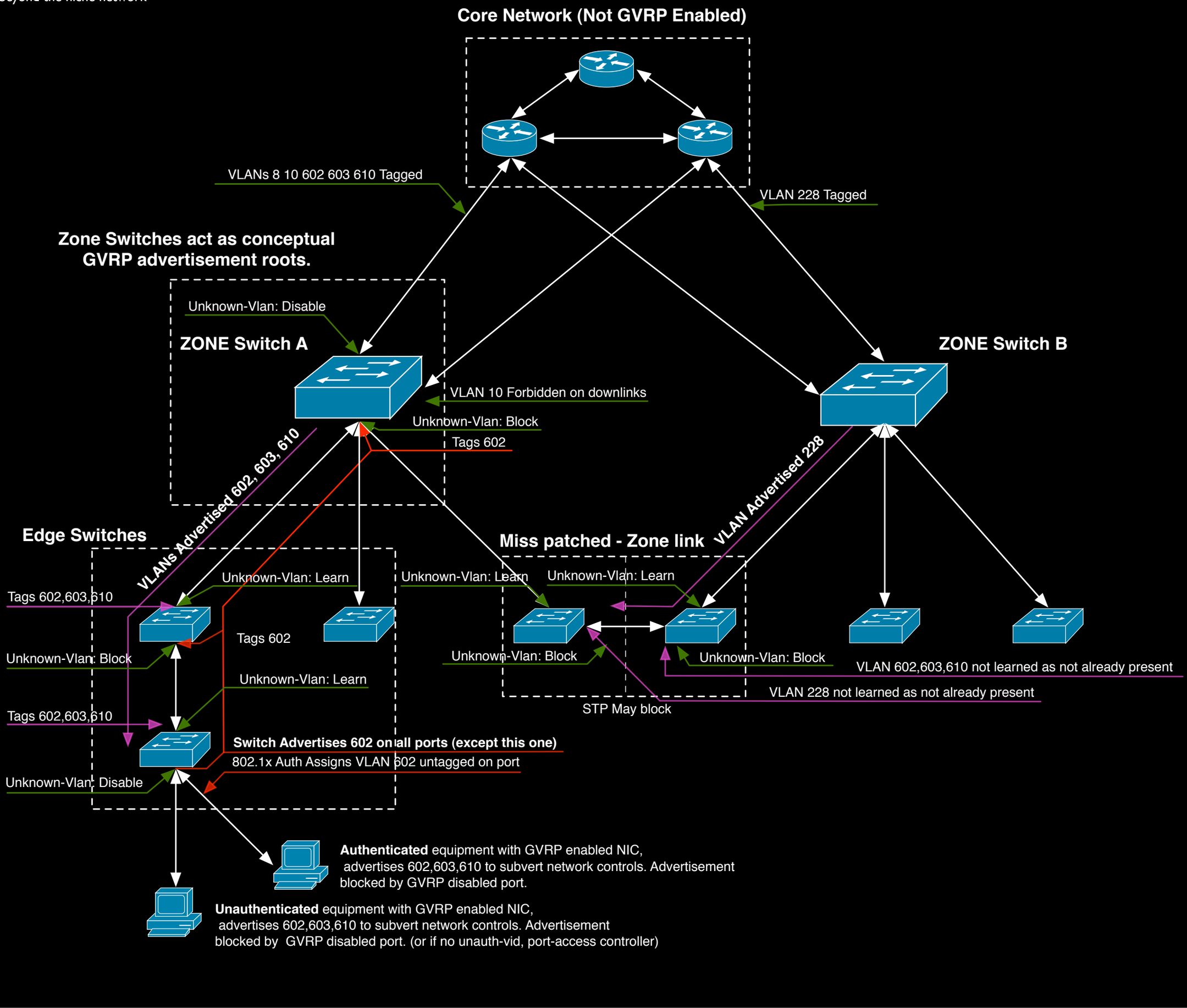
- Requires NIC support for VLAN advertisements - not much use for general hosts
- Inherently insecure in it's base form
- VLAN configuration largely static on edge switches

(GVRP && 802.1x) ? awesome : less-awesome

- Every VLAN on every switch VLAN everywhere
- VLANS assigned via 802.1x and paths created via GVRP
- VLANS follow users or hosts around the network !
- 802.1x negates the need for GVRP enabled NIC
- GVRP disabled on 802.1x edge ports (no more security risk) !
- Truly centralised VLAN management (part of a homogenous edge environment)

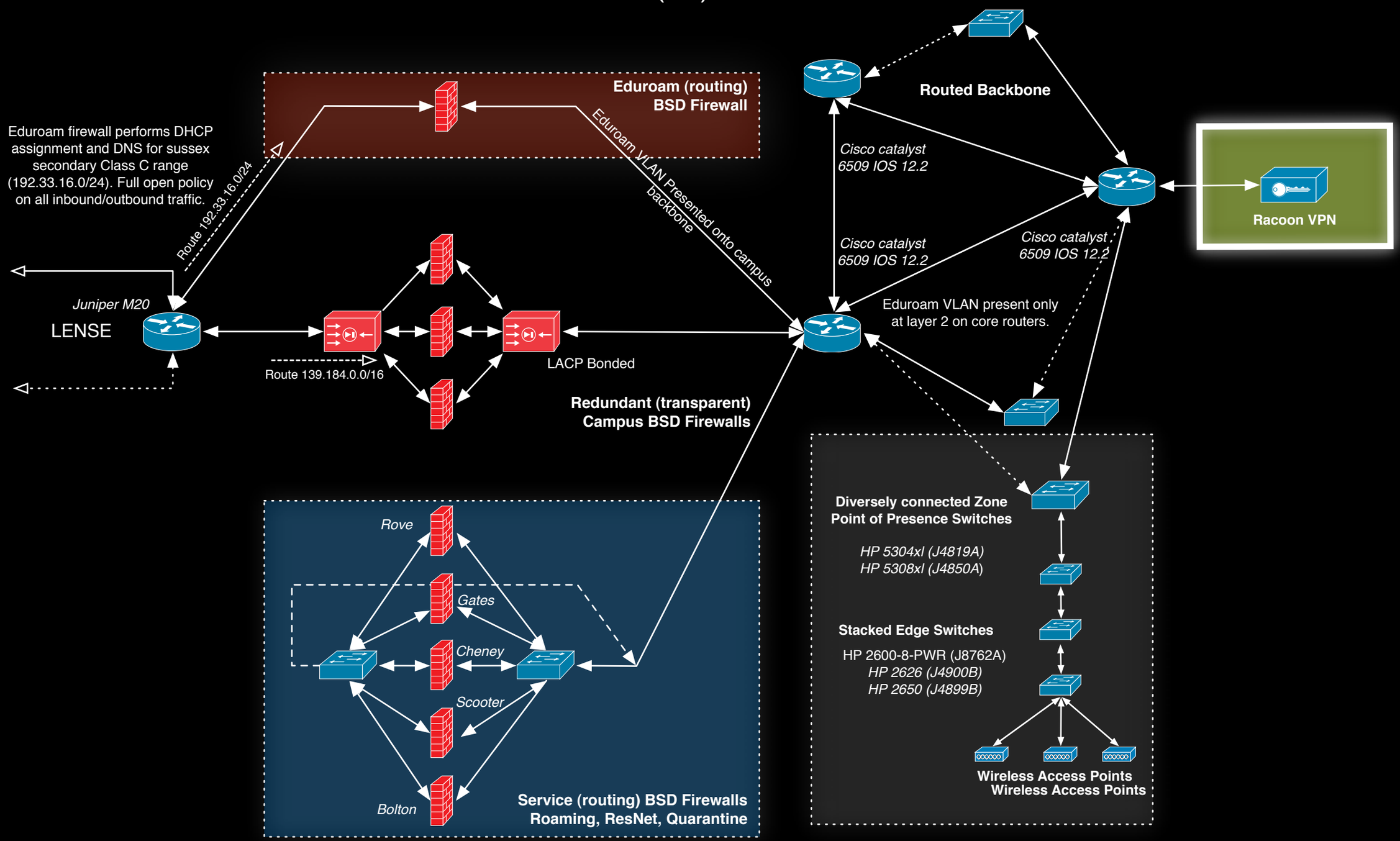
Free the RADIUS - Looking Forward - GVRP - For Example...

Expanding 802.1X beyond the niche network



FreeRADIUS += DHCP

All the flexibility of FreeRADIUS with DHCP
Very tight integration of 802.1x and DHCP lease assignment
Another piece of the support puzzle (Host registration, SNTP etc...)
User Based IP Assignment across PPP links and on Local Network
Mobile(ish) IPv4 / IPv6



Free the RADIUS

Question Time