

LanWarden - LDAP driven 802.1x and DHCP

Alexander Clouter <ac56@soas.ac.uk>

Information Technology Department
School of Oriental and African Studies

JANET Networkshop 36, 2008



Outline

To give you lot an alternative to yet another barrage of Shibboleth presentations. . .

1 Motivation

- What SOAS Wanted
- Options Available To Us

2 Roll Yer Own

- How Does This All Work Then?
- FreeRADIUS and it's LDAP Queries
- Dependencies and the Rewards

Outline

1 Motivation

- What SOAS Wanted
- Options Available To Us

2 Roll Yer Own

- How Does This All Work Then?
- FreeRADIUS and it's LDAP Queries
- Dependencies and the Rewards

Clean and Shiny Network Management

aka 'Moon-on-a-Stick'

So what do we want? 802.1x... how though?

So we bought £250k of Cisco 3750's ... erm, what now?

- 802.1x used *everywhere* - link-layer neutrality
- no 'static' IP and go fully dynamic
- user self registration and service
- per host VLAN policing
- clean way for *users* to 'track' workstations
- *event* based logging
- accountability more important than prevention

Clean and Shiny Network Management

aka 'Moon-on-a-Stick'

So what do we want? **802.1x**... how though?

So we bought £250k of Cisco 3750's ... erm, what now?

- 802.1x used *everywhere* - link-layer neutrality
- no 'static' IP and go fully dynamic
- user self registration and service
- per host VLAN policing
- clean way for *users* to 'track' workstations
- *event* based logging
- accountability more important than prevention

Clean and Shiny Network Management

aka 'Moon-on-a-Stick'

So what do we want? **802.1x**... how though?

So we bought £250k of Cisco 3750's ... erm, what now?

- 802.1x used *everywhere* - link-layer neutrality
- no 'static' IP and go fully dynamic
- user self registration and service
- per host VLAN policing
- clean way for *users* to 'track' workstations
- *event* based logging
- accountability more important than prevention

Clean and Shiny Network Management

aka 'Moon-on-a-Stick'

So what do we want? **802.1x**... how though?

So we bought £250k of Cisco 3750's ... erm, what now?

- 802.1x used *everywhere* - link-layer neutrality
- no 'static' IP and go fully dynamic
- user self registration and service
- per host VLAN policing
- clean way for *users* to 'track' workstations
- *event* based logging
- accountability more important than prevention

Clean and Shiny Network Management

aka 'Moon-on-a-Stick'

So what do we want? **802.1x**... how though?

So we bought £250k of Cisco 3750's ... erm, what now?

- 802.1x used *everywhere* - link-layer neutrality
- no 'static' IP and go fully dynamic
- user self registration and service
- per host VLAN policing
- clean way for *users* to 'track' workstations
- *event* based logging
- accountability more important than prevention

Outline

- 1 Motivation
 - What SOAS Wanted
 - Options Available To Us
- 2 Roll Yer Own
 - How Does This All Work Then?
 - FreeRADIUS and it's LDAP Queries
 - Dependencies and the Rewards

Open Source Options

- NetReg

- only does L3 isolation
- introduced to MBSA¹

- PacketFence

- at the time only L3 isolation
- unclear if it really would support 802.1x
- L3 isolation trying to bolt on L2 - eek!
- missing a lot of needed functionality

- FreeNAC

- only free L2 based NAC - has roots in VMPS
- policy data in SQL
- heavily Cisco orientated²
- 802.1x support is ropey

¹Microsoft Baseline Security Analyser

²Cisco or HP switches at tender?

Open Source Options

- NetReg
 - only does L3 isolation
 - introduced to MBSA¹
- PacketFence
- FreeNAC

¹Microsoft Baseline Security Analyser

Open Source Options

- NetReg
 - only does L3 isolation
 - introduced to MBSA¹
- PacketFence
 - at the time only L3 isolation
 - unclear if it really would support 802.1x
 - L3 isolation trying to bolt on L2 - eek!
 - missing a lot of needed functionality
- FreeNAC

¹Microsoft Baseline Security Analyser

Open Source Options

- NetReg
 - only does L3 isolation
 - introduced to MBSA¹
- PacketFence
 - at the time only L3 isolation
 - unclear if it really would support 802.1x
 - L3 isolation trying to bolt on L2 - eek!
 - missing a lot of needed functionality
- FreeNAC
 - only free L2 based NAC - has roots in VMPS
 - policy data in SQL
 - heavily Cisco orientated²
 - 802.1x support is ropey

¹Microsoft Baseline Security Analyser

²Cisco or HP switches at tender?

Commercial Solutions

- Bradford Campus Manager:
 - 'hijacks' network port - no 802.1x and stateful
 - no LDAP or RADIUS authentication
 - no RADIUS accounting support
 - expensive
- Cisco NAC Appliance:
 - again not really 802.1x
 - rolls user and host authentication into one
 - 3rd party SW for functionality gaps (£££)
 - low user:server ratio ³
 - "Dear God, how much?!"

Shocked by the lack of choice

³"With five servers and one manager in a real-IP gateway configuration, the deployment supports 1700 users"



Commercial Solutions

- Bradford Campus Manager:
 - 'hijacks' network port - no 802.1x and stateful
 - no LDAP or RADIUS authentication
 - no RADIUS accounting support
 - expensive
- Cisco NAC Appliance:

Shocked by the lack of choice



Commercial Solutions

- Bradford Campus Manager:
 - 'hijacks' network port - no 802.1x and stateful
 - no LDAP or RADIUS authentication
 - no RADIUS accounting support
 - expensive
- Cisco NAC Appliance:
 - again not really 802.1x
 - rolls user and host authentication into one
 - 3rd party SW for functionality gaps (£££)
 - low user:server ratio ³
 - "Dear God, how much?!"

Shocked by the lack of choice

³"With five servers and one manager in a real-IP gateway configuration, the deployment supports 1700 users"



Commercial Solutions

- Bradford Campus Manager:
 - 'hijacks' network port - no 802.1x and stateful
 - no LDAP or RADIUS authentication
 - no RADIUS accounting support
 - expensive
- Cisco NAC Appliance:
 - again not really 802.1x
 - rolls user and host authentication into one
 - 3rd party SW for functionality gaps (£££)
 - low user:server ratio ³
 - "Dear God, how much?!"

Shocked by the lack of choice

³"With five servers and one manager in a real-IP gateway configuration, the deployment supports 1700 users"

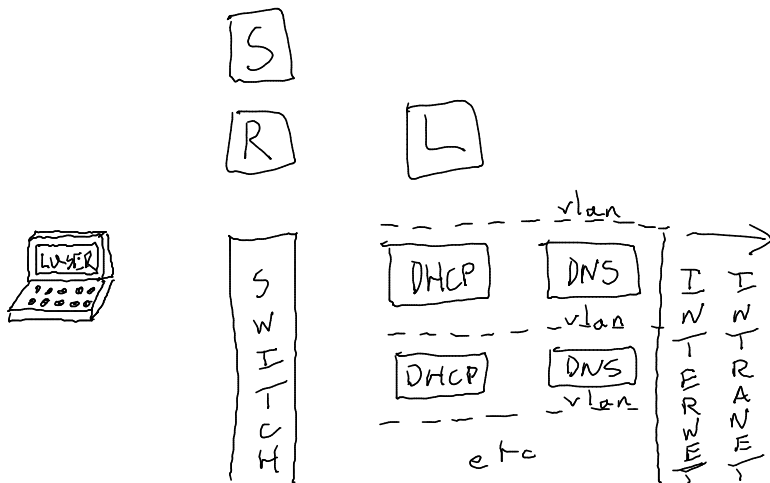


Outline

- 1 Motivation
 - What SOAS Wanted
 - Options Available To Us
- 2 Roll Yer Own
 - How Does This All Work Then?
 - FreeRADIUS and it's LDAP Queries
 - Dependencies and the Rewards

A Bird's Eye View

Brought to you by...



A Bird's Eye View

Brought to you by...

Roobarb



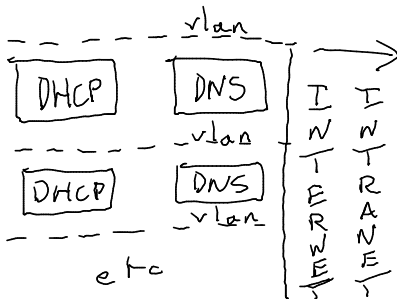
S

R

L



S
W
I
T
C
H

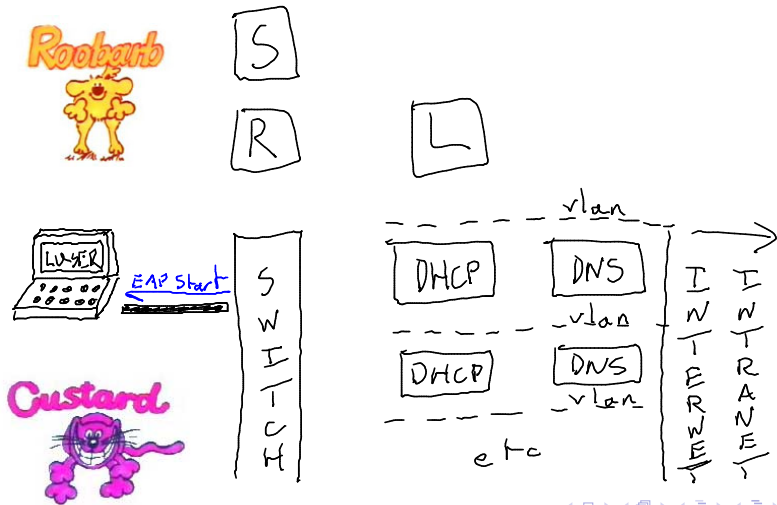


Custard



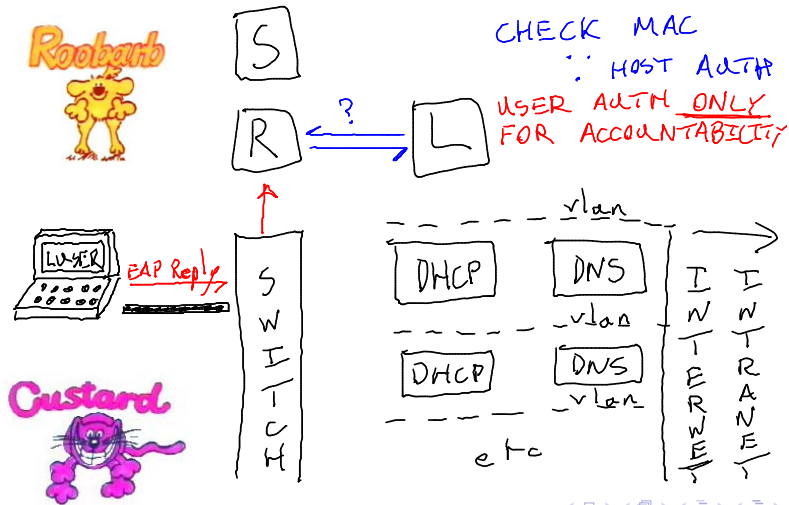
A Bird's Eye View

Brought to you by...



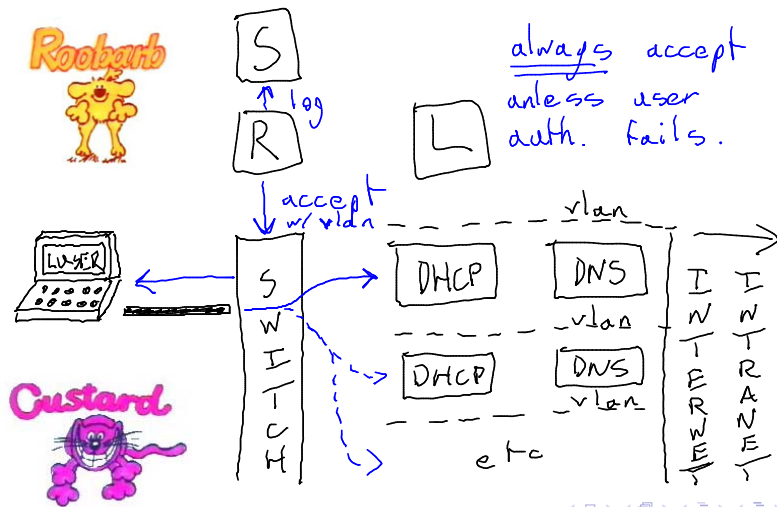
A Bird's Eye View

Brought to you by...



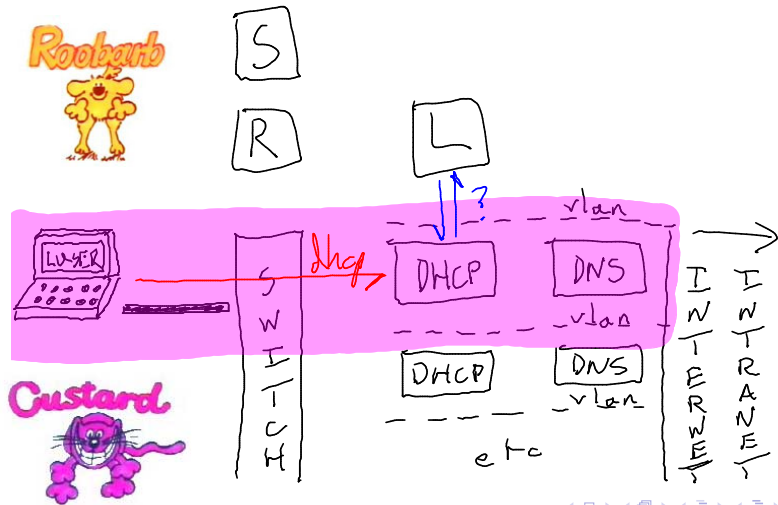
A Bird's Eye View

Brought to you by...



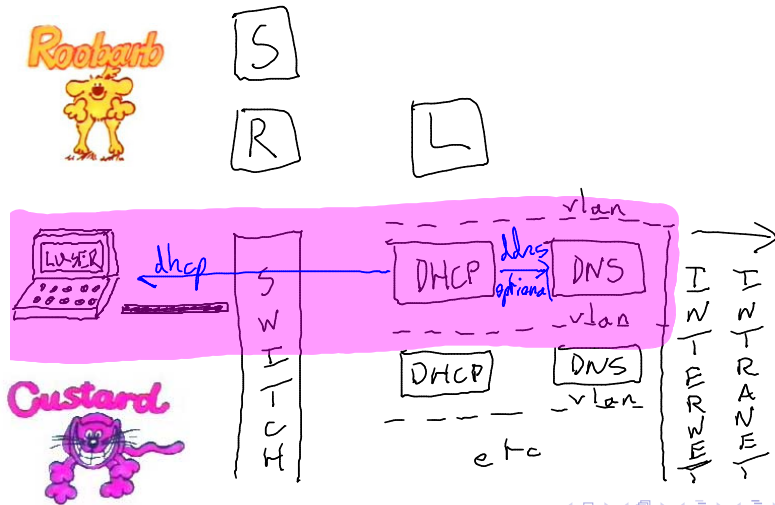
A Bird's Eye View

Brought to you by...



A Bird's Eye View

Brought to you by...

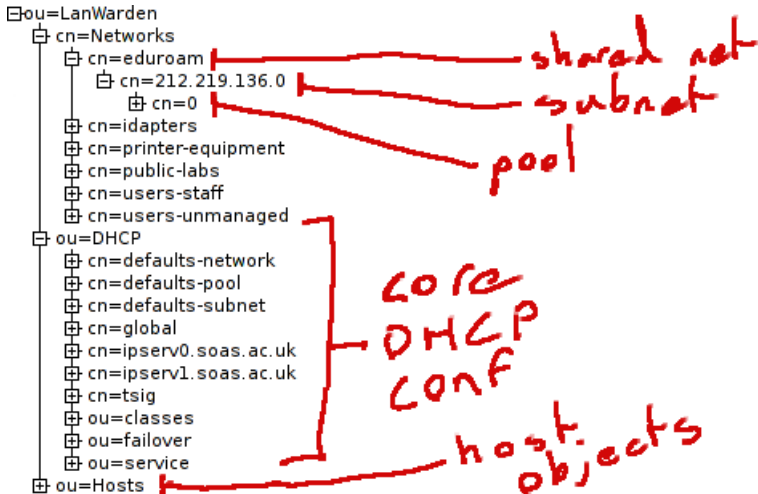


Outline

- 1 Motivation
 - What SOAS Wanted
 - Options Available To Us
- 2 Roll Yer Own
 - How Does This All Work Then?
 - **FreeRADIUS and it's LDAP Queries**
 - Dependencies and the Rewards

Gimme Some LDAP Lovin'

"At This Time of the Morning?"



802.1x Decisions via LDAP

Vanilla

Regular run of the mill 802.1x Auth and Autz
ie. EAP-TTLS, PEAP, EAP-TLS, and EAP-MD5⁴.

```
ldapsearch -b ou=Hosts,ou=LanWarden -s sub  
' (& (objectClass=lanwardenHost)  
  (! (lanwardenHostAuthenticateMethod=mac) )  
  (lanwardenHostState=enable)  
  (cn=Calling-Station-Id) )' dn
```

```
ldapsearch -b ou=Networks,ou=LanWarden -s one  
' (& (objectClass=lanwardenNetwork)  
  (member=Host-DN)  
  (member=Ldap-UserDn) )' cn
```

⁴well not quite for EAP-TLS/MD5...

802.1x Decisions via LDAP

MAC Based

For non-802.1x aware hosts

ie. switch 'spoofs' request with host's MAC address

```
ldapsearch -b ou=Hosts,ou=LanWarden -s sub  
' (&      (objectClass=lanwardenHost)  
          (lanwardenHostAuthenticateMethod=mac)  
          (lanwardenHostState=enable)  
          (cn=Calling-Station-Id) )' dn
```

```
ldapsearch -b ou=Networks,ou=LanWarden -s one  
' (&      (objectClass=lanwardenNetwork)  
          (member=Host-DN)      )' cn
```



Outcome Table

When Dumped into the 'unauthorised' VLAN

auth type	known?	mac-auth?	state	meaning
MAC	no	n/a	n/a	need 802.1x
	yes	no	-	need 802.1x
	yes	yes	disable	restricted
	yes	yes	enable	ERROR
802.1x	no	n/a	n/a	register
	yes	yes	-	TBA :)
	yes	no	disable	restricted
	yes	no	enable	ERROR

Outline

- 1 Motivation
 - What SOAS Wanted
 - Options Available To Us
- 2 Roll Yer Own
 - How Does This All Work Then?
 - FreeRADIUS and it's LDAP Queries
 - Dependencies and the Rewards

Further Dependencies

ISC DHCP LDAP patch with enabled OMAPI and patched OMAPI::DHCP

SQL server logging of RADIUS events

Secure L2/L3 force DHCP, ARP/IP anti-spoofing protection, one MAC per port

misc quarantine/registration - DNS hijacking/transparent proxy

DNS DDNS (*optional*) allows users to register custom FQDN

What Do I Get For My Sweat and Tears

- solid open standards foundation to bolt functionality to
- *event* triggered realtime logging
- graceful handling of 'power' events - stateless
- bulk imports and simple to identify and remove stale data
- simple backups - LDIF dumps and can use diff/RCS
- single 'unified' switch port configuration
- nice migration path, paced by *you*, to a life of 802.1x
- log of accountable 'person' to MAC with accounting data

Summary

- LanWarden is a blueprint for a network design
- you need to have OSI L2 and L3 secured
- Net::LanWarden assists in frontend/middleware design
- **LDAP + DHCP** + 802.1x + FreeRADIUS == Good Thing™

- TODO List - order of importance
 - EAP-MD5 - better printer, VoIP, etc support
 - develop code to control 802.1x state-machine via SNMP
 - a lot more frontend/middleware apps needed
 - DHCP leases into SQL db - tailing log?
 - LDAP group memberships get *large* - problem?

For Further Reading I



A. Clouter (aka 'me').

LanWarden Website.

<http://lanwarden.code.digriz.org.uk/>



B. Masney.

LDAP Patch for ISC DHCPv3.

<http://home.ntelos.net/~masneyb/>



E. Vyncke.

Layer 2 Security.

http://www.cisco.com/web/DK/assets/docs/security2006/Security2006_Eric_Vyncke_2.pdf
(or <http://tinyurl.com/29ern4>)

For Further Reading II



A. Williams.

LDAP and OpenLDAP (on the Linux Platform).

<http://www.whitemiceconsulting.com/node/30>
(or [google://'ldapv3.pdf'](http://google://ldapv3.pdf) for original 500 page tomb)

The Host LDAP Object

lanwardenHost - 1.3.6.1.4.1.26371.32768.2.10

```
dn: cn=001122334455,ou=Hosts,ou=LanWarden
objectClass: top
objectClass: device
objectClass: dhcpHost
objectClass: lanwardenHost
cn: 00122334455
```

```
owner: dn of 'responsible' user
ou: free text field, ie department?
o: free text field, ie organisation?
l: free text field, ie location?
serialNumber: free text field
description: free text field
```



The Host LDAP Object *cont.*

lanwardenHost - 1.3.6.1.4.1.26371.32768.2.10

`dhcpHWAddress: ethernet 00:11:22:33:44:55`

`dhcpStatements: as per dhcpd.conf`

`lanwardenHostAuthenticateMethod: (mac|x509|none)`

`lanwardenHostRegisteredTime: YYYYMMDDHHMMSSZ`

`lanwardenHostRegisteredTC: T&C's and AUP's`

`lanwardenHostState: (enable|disable)`

`lanwardenHostNotes: YYYYMMDDHHMMSSZ - type - msg`

`lanwardenHostRegisteredBy: dn of registrar`

`userCertificate: if 'x509' authentication`



The Network LDAP Object

lanwardenNetwork - 1.3.6.1.4.1.26371.32768.2.20

```
dn: cn=staff,cn=Networks,ou=LanWarden
objectClass: top
objectClass: dhcpSharedNetwork
objectClass: lanwardenNetwork
cn: staff
```

```
o: VLAN domain - unused
ou: VLAN number ID of network
```

```
description: free text field
member: dn of user's and host's
```



Typical 802.1x Cisco Example I

```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop \
  group radius
aaa session-id common
```

```
dot1x system-auth-control
```

```
errdisable recovery interval 300
errdisable recovery cause arp-inspection
errdisable recovery cause security-violation
errdisable recovery cause dhcp-rate-limit
```



Typical 802.1x Cisco Example II

```
errdisable recovery cause psecure-violation  
errdisable recovery cause bpduguard
```

```
ip dhcp snooping database flash:dhcp-snoop.db  
ip dhcp snooping vlan <VLANS-TO-SNOOP>  
ip dhcp snooping  
no ip dhcp snooping information option  
ip dhcp snooping verify mac-address  
ip arp inspection vlan <VLANS-TO-SNOOP>  
ip arp inspection log-buffer entries 1024  
ip arp inspection log-buffer logs 1024 interval 10  
ip arp inspection validate src-mac ip  
ip arp inspection validate dst-mac src-mac ip
```

Typical 802.1x Cisco Example III

```
! your edge ports
interface range FastEthernet1/0/1 - 48
  switchport port-security
  switchport port-security maximum 1
  switchport port-security violation restrict
  ! if you do not set this to 1440 you get a
  ! complete 802.1X reauth every five minutes
  switchport port-security aging time 1440
  switchport port-security aging type inactivity
  no ip arp inspection trust
  ip arp inspection limit rate 15
  no ip dhcp snooping trust
  ip dhcp snooping limit rate 10
  ip verify source
```

Typical 802.1x Cisco Example IV

```
ip verify source port-security

dot1x mac-auth-bypass
dot1x pae authenticator
dot1x port-control auto
dot1x control-direction in
dot1x timeout quiet-period 3
dot1x timeout server-timeout 10
dot1x timeout reauth-period server
dot1x timeout tx-period 5
dot1x timeout supp-timeout 5
dot1x reauthentication
no cdp enable
```

Typical 802.1x Cisco Example V

```
spanning-tree portfast  
spanning-tree bpduguard enable
```

```
! your trunk links  
int range Po1 - 2  
  ip dhcp snooping trust  
  ip arp inspection trust
```

```
radius-server host <DETAILS>  
radius-server source-ports 1645-1646  
radius-server unique-ident 4  
radius-server vsa send accounting  
radius-server vsa send authentication
```

