RADIUS Configuration Note

WINS™: Wireless Interoperability & Network Solutions

MERU NETWORKS
WINS PARTNER
WIRELESS INTEROPERABILITY
& NETWORK SOLUTIONS

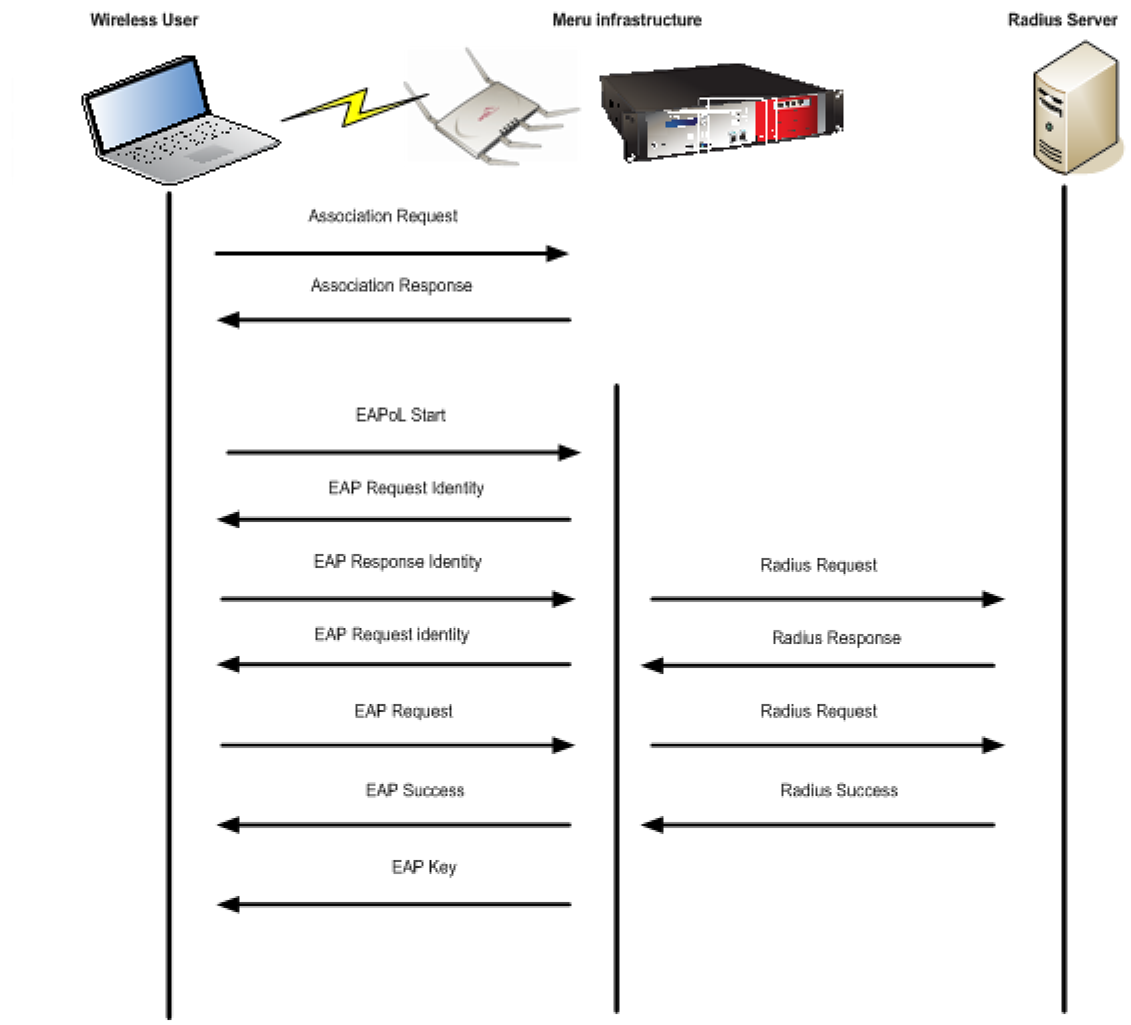
MERUNETWORKS.COM

February 2013

1. OVERVIEW

RADIUS is a protocol that provides centralized authentication, accounting & authorization (AAA) management for user laptops/computers to gain access to a network. Meru Controller as a Radius client sends user credentials and connection parameter information in the form of a RADIUS messages to a RADIUS server. The RADIUS server authenticates and authorizes the RADIUS client requests, and sends back a RADIUS message response. Meru supports various EAP types such as EAP-TLS, TTLS, PEAP etc associated to 802.1 x using RADIUS. While not getting in to the low level details, the real intention of this document is to make the reader understand basic and optional configuration on Meru controllers/RADIUS Servers, Failover mechanism defined and some other Meru specific aspects.

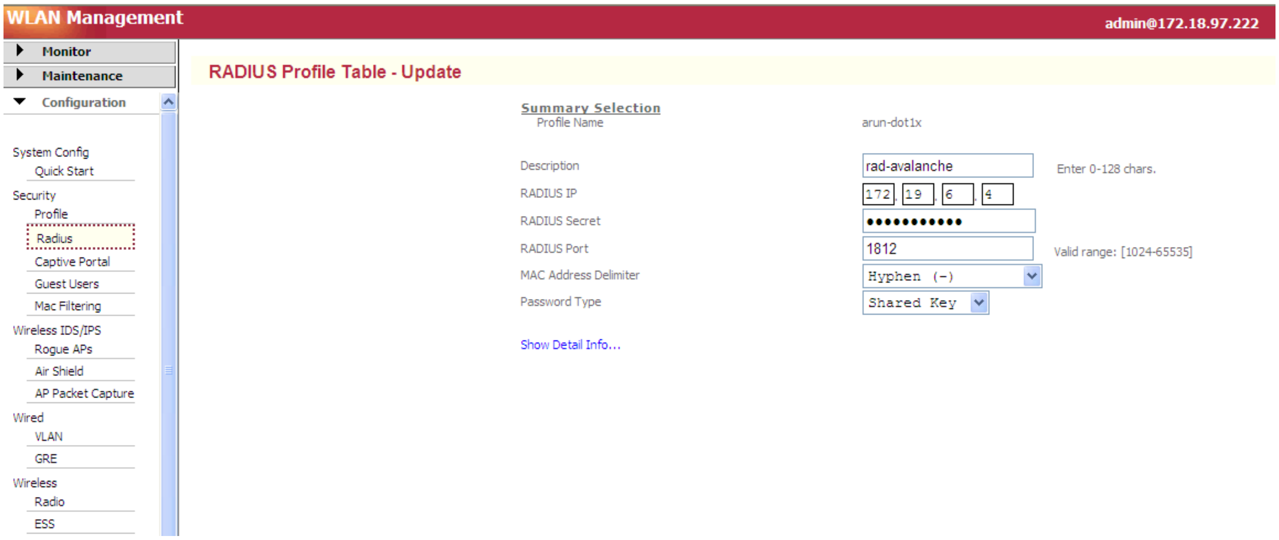
EAP exchanges during 802.1 x authentication



2. AUTHENTICATION AND ACCOUNTING

If there are any specific software requirements in the controller to support a particular client model as suggested in Meru documents, the same should be installed in the controller accordingly. The client devices used in the test bed for this documentation are generic and supported by standard software releases. Below procedure explains how to create RADIUS authentication and accounting profiles and map it to the ESS profiles in a Meru Controller.

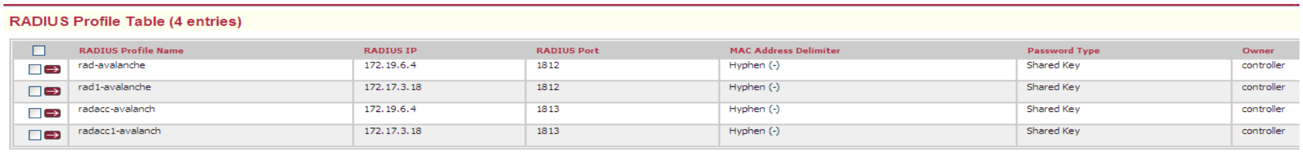
Global RADIUS Authentication and Accounting Profile



RADIUS Profile Table - Update

Summary Selection

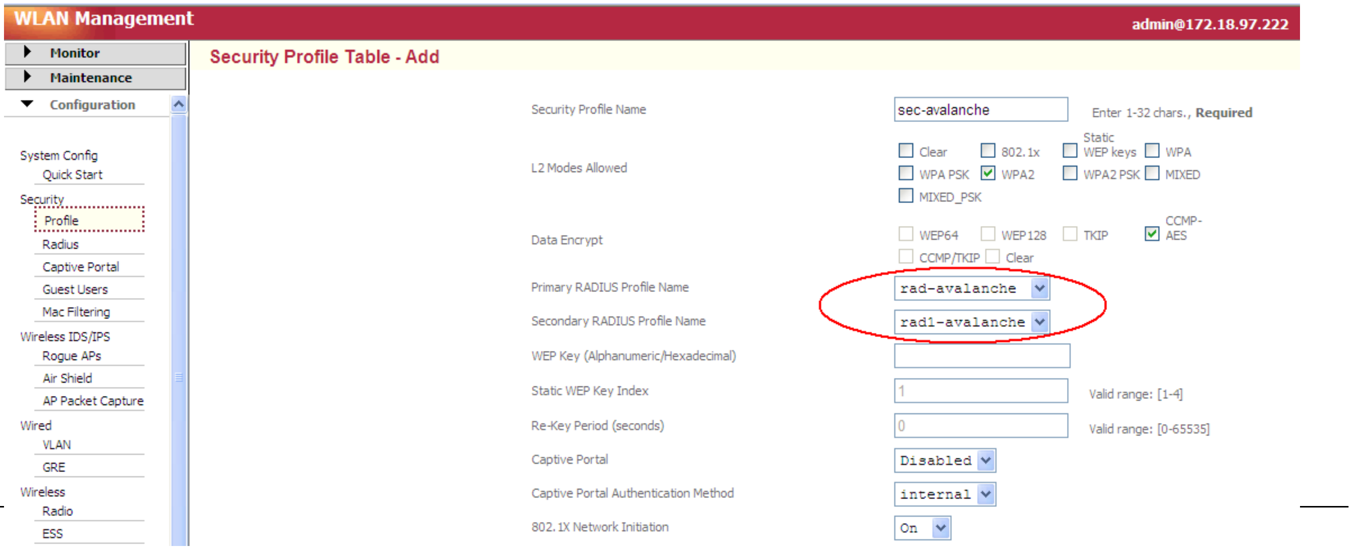
Profile Name	arun-dot1x	
Description	rad-avalanche	Enter 0-128 chars.
RADIUS IP	172 . 19 . 6 . 4	
RADIUS Secret	●●●●●●●●●●●	
RADIUS Port	1812	Valid range: [1024-65535]
MAC Address Delimiter	Hyphen (-)	
Password Type	Shared Key	



RADIUS Profile Table (4 entries)

□	RADIUS Profile Name	RADIUS IP	RADIUS Port	MAC Address Delimiter	Password Type	Owner
□	rad-avalanche	172.19.6.4	1812	Hyphen (-)	Shared Key	controller
□	rad1-avalanche	172.17.3.18	1812	Hyphen (-)	Shared Key	controller
□	radacc-avalanch	172.19.6.4	1813	Hyphen (-)	Shared Key	controller
□	radacc1-avalanch	172.17.3.18	1813	Hyphen (-)	Shared Key	controller

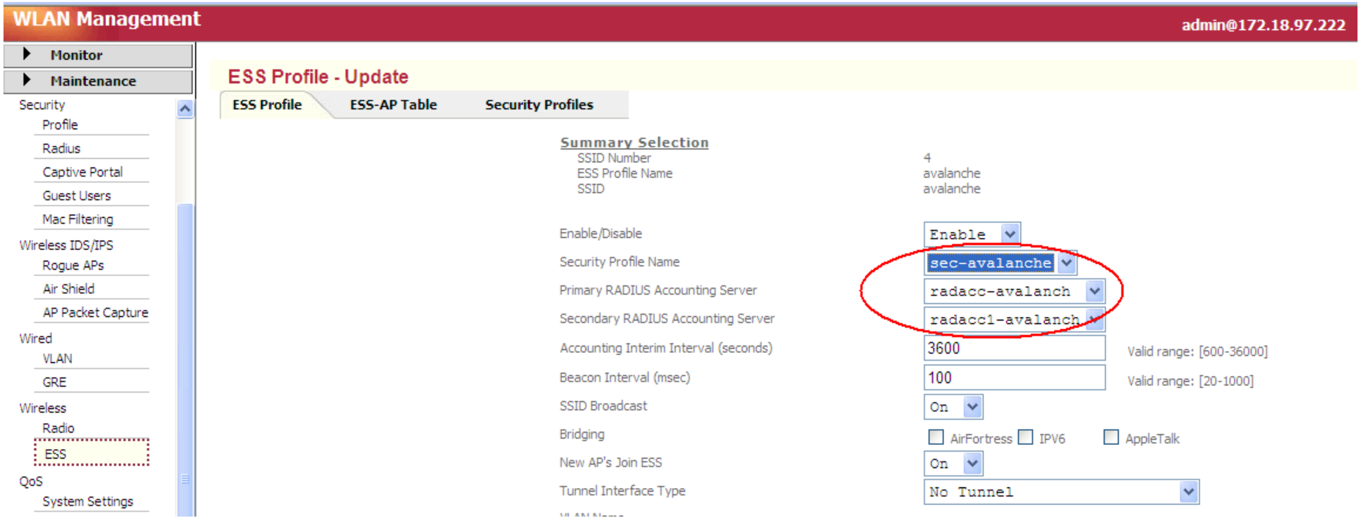
Mapping the RADIUS authentication profile to a Security profile



Security Profile Table - Add

Security Profile Name	sec-avalanche	Enter 1-32 chars., **Required**
L2 Modes Allowed	□ Clear □ 802.1x □ Static WEP keys □ WPA □ WPA PSK ☑ WPA2 □ WPA2 PSK □ MIXED □ MIXED_PSK	
Data Encrypt	□ WEP64 □ WEP128 □ TKIP ☑ CCMP-AES □ CCMP/TKIP □ Clear	
Primary RADIUS Profile Name	rad-avalanche	
Secondary RADIUS Profile Name	rad1-avalanche	
WEP Key (Alphanumeric/Hexadecimal)		
Static WEP Key Index	1	Valid range: [1-4]
Re-Key Period (seconds)	0	Valid range: [0-65535]
Captive Portal	Disabled	
Captive Portal Authentication Method	internal	
802.1X Network Initiation	On	

Mapping the RADIUS accounting profile to ESS profile



ESS Profile - Update

Summary Selection

SSID Number	4
ESS Profile Name	avalanche
SSID	avalanche

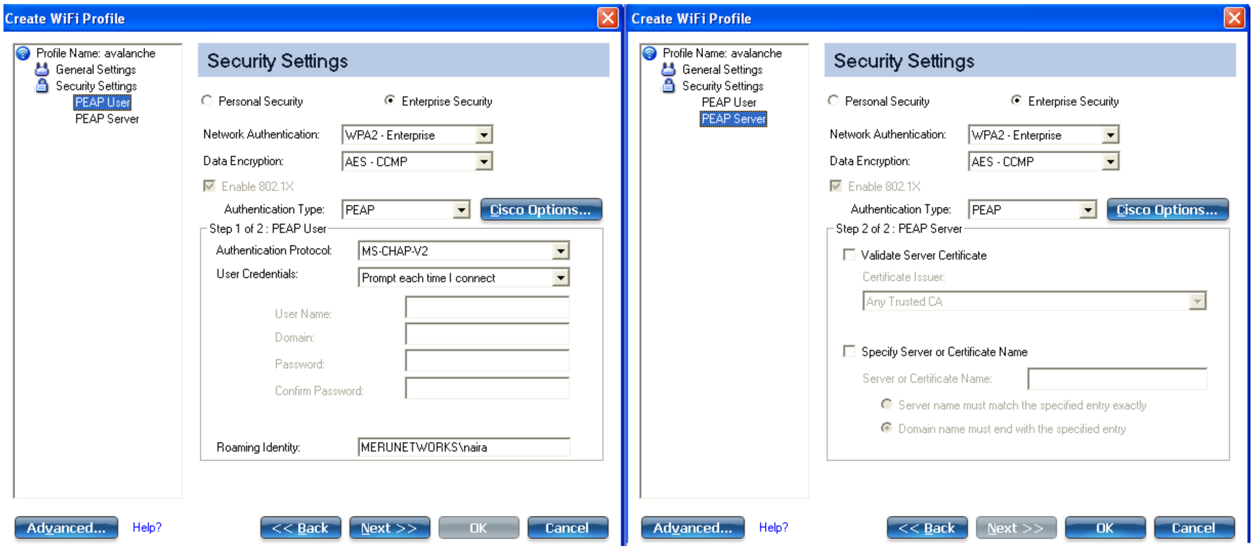
Enable/Disable	Enable	
Security Profile Name	sec-avalanche	
Primary RADIUS Accounting Server	radacc-avalanch	
Secondary RADIUS Accounting Server	radacc1-avalanch	
Accounting Interim Interval (seconds)	3600	Valid range: [600-36000]
Beacon Interval (msec)	100	Valid range: [20-1000]
SSID Broadcast	On	
Bridging	□ AirFortress □ IPV6 □ AppleTalk	
New AP's Join ESS	On	
Tunnel Interface Type	No Tunnel	

3. 802.1X, CAPTIVE PORTAL AND MAC-FILTERING

3.1 802.1x

802.1X is an IEEE standard for authenticated network access to wired Ethernet networks and wireless 802.11 networks. IEEE 802.1X enhances security and deployment by providing support for centralized user identification, authentication, dynamic key management, and accounting. The support that 802.1X provides for Extensible Authentication Protocol (EAP) types such as, EAP, EAP-TLS, EAP-MS-CHAP v2, and PEAP allows you to choose several authentication methods for wireless clients and servers. Meru controllers and APs are transparent to the EAP types as no special configuration is required to enforce any of it. However the wireless client supplicants and RADIUS Server should be appropriately configured to support a specific EAP type. Below screen shots explains the configuration requirement in Intel client supplicant and Network Policy Server running in windows 2008 Server to support PEAP.

Sample configuration with Intel Utility to support PEAP



Create WiFi Profile

Profile Name: avalanche
General Settings
Security Settings
PEAP User
PEAP Server

Security Settings

○ Personal Security ● Enterprise Security

Network Authentication: WPA2 - Enterprise
Data Encryption: AES - CCMP
☑ Enable 802.1X
Authentication Type: PEAP

Step 1 of 2 : PEAP User
Authentication Protocol: MS-CHAP-V2
User Credentials: Prompt each time I connect
User Name:
Domain:
Password:
Confirm Password:
Roaming Identity: MERUNETWORKS\naira

Create WiFi Profile

Profile Name: avalanche
General Settings
Security Settings
PEAP User
PEAP Server

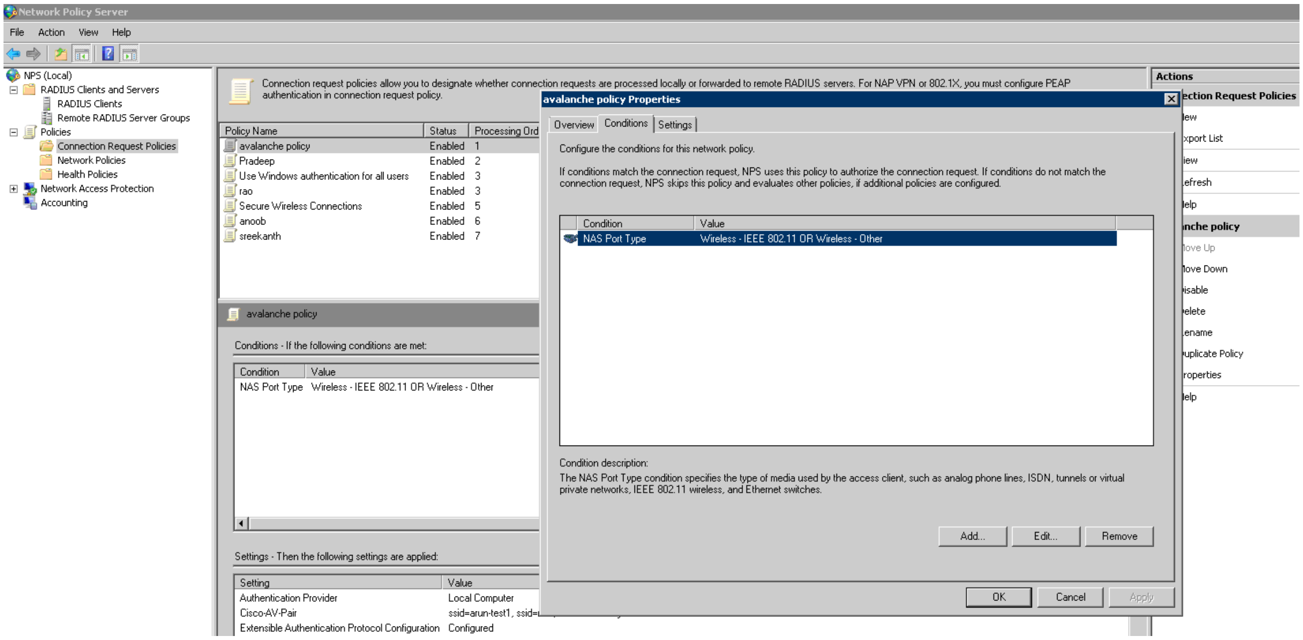
Security Settings

○ Personal Security ● Enterprise Security

Network Authentication: WPA2 - Enterprise
Data Encryption: AES - CCMP
☑ Enable 802.1X
Authentication Type: PEAP

Step 2 of 2 : PEAP Server
□ Validate Server Certificate
Certificate Issuer:
Any Trusted CA
□ Specify Server or Certificate Name
Server or Certificate Name:
○ Server name must match the specified entry exactly
● Domain name must end with the specified entry

Windows NPS configuration. Meru controller already added to the RADIUS client list



Connection request policies allow you to designate whether connection requests are processed locally or forwarded to remote RADIUS servers. For NAP VPN or 802.1X, you must configure PEAP authentication in connection request policy.

Policy Name	Status	Processing Ord
avalanche policy	Enabled	1
Pradeep	Enabled	2
Use Windows authentication for all users	Enabled	3
rao	Enabled	3
Secure Wireless Connections	Enabled	5
anoob	Enabled	6
sreekanth	Enabled	7

avalanche policy

Conditions - If the following conditions are met:

Condition	Value
NAS Port Type	Wireless - IEEE 802.11 OR Wireless - Other

Settings - Then the following settings are applied:

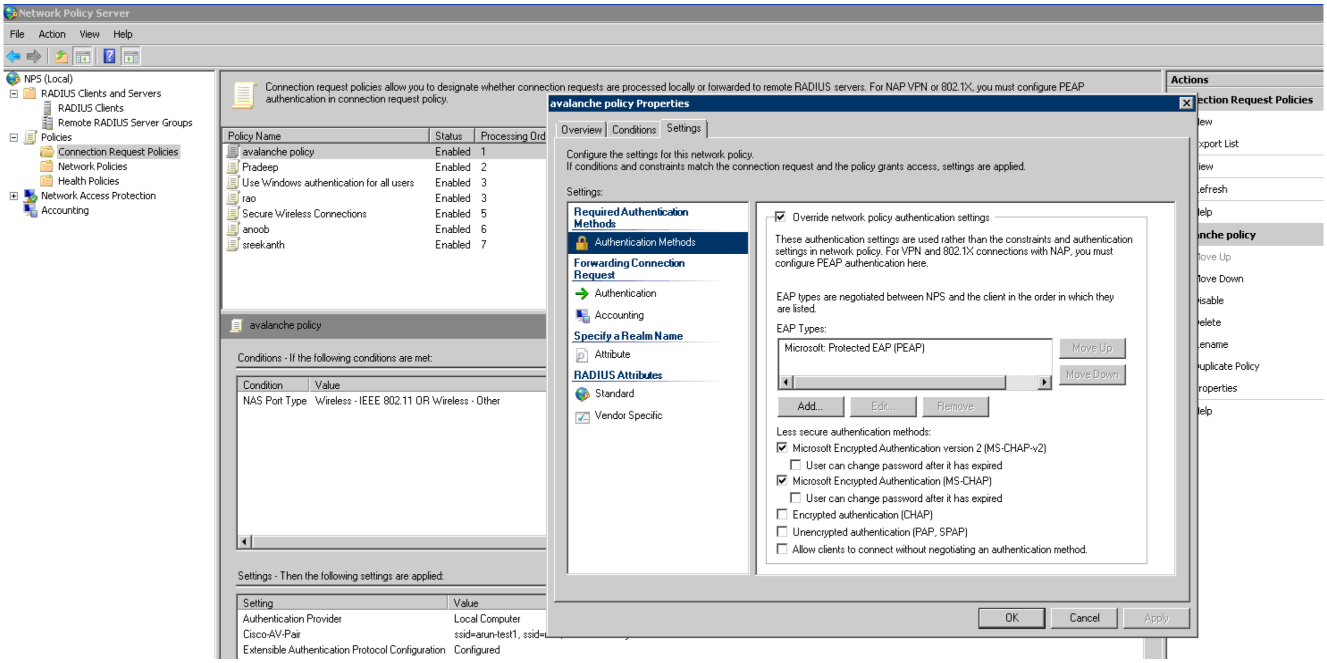
Setting	Value
Authentication Provider	Local Computer
Cisco-AV-Pair	ssid=arun-test1, ssid=
Extensible Authentication Protocol Configuration	Configured

Configure the conditions for this network policy.

If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.

Condition	Value
NAS Port Type	Wireless - IEEE 802.11 OR Wireless - Other

Condition description:
The NAS Port Type condition specifies the type of media used by the access client, such as analog phone lines, ISDN, tunnels or virtual private networks, IEEE 802.11 wireless, and Ethernet switches.



Connection request policies allow you to designate whether connection requests are processed locally or forwarded to remote RADIUS servers. For NAP VPN or 802.1X, you must configure PEAP authentication in connection request policy.

Policy Name	Status	Processing Ord
avalanche policy	Enabled	1
Pradeep	Enabled	2
Use Windows authentication for all users	Enabled	3
rao	Enabled	3
Secure Wireless Connections	Enabled	5
anoob	Enabled	6
sreekanth	Enabled	7

avalanche policy

Conditions - If the following conditions are met:

Condition	Value
NAS Port Type	Wireless - IEEE 802.11 OR Wireless - Other

Settings - Then the following settings are applied:

Setting	Value
Authentication Provider	Local Computer
Cisco-AV-Pair	ssid=arun-test1, ssid=
Extensible Authentication Protocol Configuration	Configured

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

☑ Override network policy authentication settings

These authentication settings are used rather than the constraints and authentication settings in network policy. For VPN and 802.1X connections with NAP, you must configure PEAP authentication here.

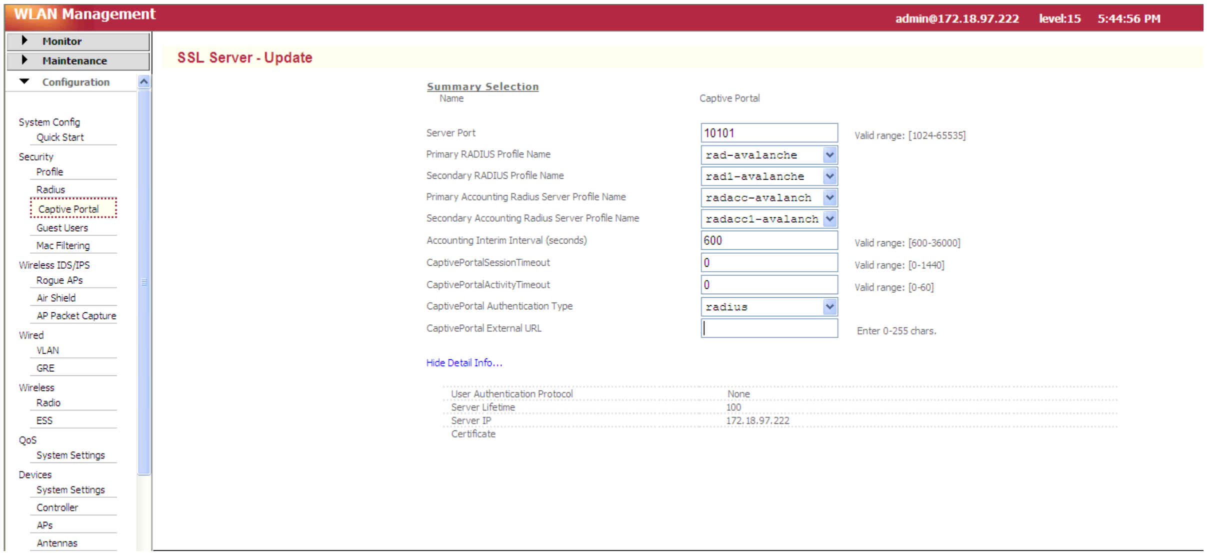
EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:
Microsoft: Protected EAP (PEAP)

Less secure authentication methods:
- ☑ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
  - ☐ User can change password after it has expired
- ☑ Microsoft Encrypted Authentication (MS-CHAP)
  - ☐ User can change password after it has expired
- ☐ Encrypted authentication (CHAP)
- ☐ Unencrypted authentication (PAP, SPAP)
- ☐ Allow clients to connect without negotiating an authentication method.

3.1 Captive Portal Authentication with RADIUS

Captive Portal is a feature designed to isolate temporary users on a network, for example guests in a company or students using a library. If Captive Portal is enabled, the HTTP protocol over Secure Socket Layer (SSL, also known as HTTPS) provides an encrypted login interchange with the RADIUS server until the user is authenticated and authorized.(Captive Portal feature also supports local authentication). During this interchange, all traffic with the Client station except DHCP, ARP, and DNS packets are dropped until access is granted. If access is not granted, the user will not be able to leave the Captive Portal login page. If access is granted, the user is released from the Captive Portal page and is redirected to the originally requested URL/Website as the user now gain full access to WLAN. This section provides instructions to implement Captive Portal in Meru controllers by using RADIUS Server to authenticate the users.



SSL Server - Update

Summary Selection

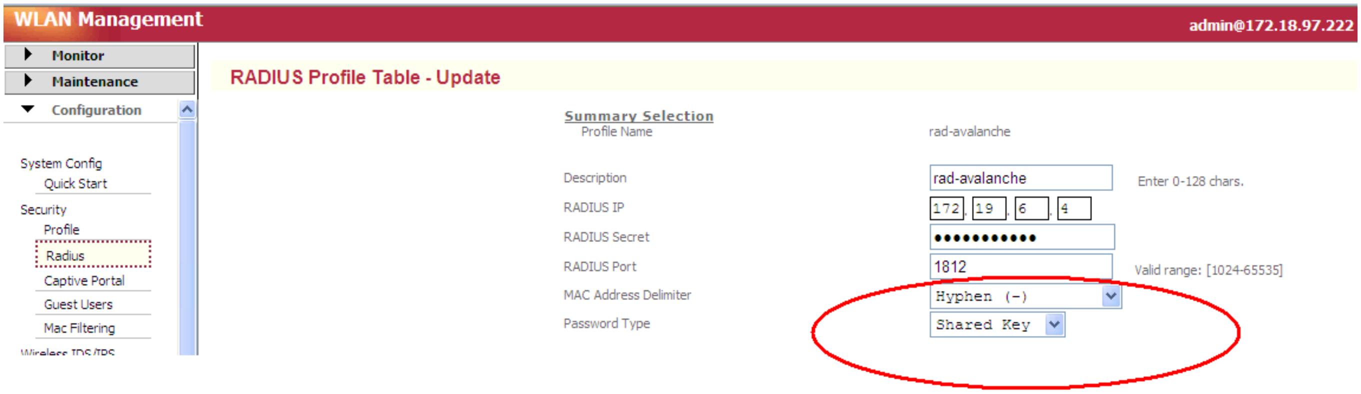
Name	Captive Portal	
Server Port	10101	Valid range: [1024-65535]
Primary RADIUS Profile Name	rad-avalanche	
Secondary RADIUS Profile Name	rad1-avalanche	
Primary Accounting Radius Server Profile Name	radacc-avalanch	
Secondary Accounting Radius Server Profile Name	radacc1-avalanch	
Accounting Interim Interval (seconds)	600	Valid range: [600-36000]
CaptivePortalSessionTimeout	0	Valid range: [0-1440]
CaptivePortalActivityTimeout	0	Valid range: [0-60]
CaptivePortal Authentication Type	radius	
CaptivePortal External URL		Enter 0-255 chars.

User Authentication Protocol	None
Server Lifetime	100
Server IP	172.18.97.222
Certificate	

The back-end authentication between RADIUS server and controller uses PAP, in other words the user credentials are sent in clear text. Also if an external captive portal server is used, the authentication happens between External Captive portal server and RADIUS server directly (the external captive portal server is the RADIUS client).

3.2 MAC-filtering

MAC-filtering is a global configuration that can be used in the system to control access by enabling a permit or deny list, based on the MAC-address of users. Similar to captive portal, the user database can reside in the controller locally also can be in an external database authenticated using a RADIUS server. As explained in the sequential screen shots below, MAC-filtering procedure involves 3 steps; **a)** to configure a RADIUS profile, **b)** to enable ACL globally, **c)** enabling the “MAC-filtering flag” in a security profile. Note the delimiter type defined in RADIUS profile will be the format used by Controller to send the MAC address (user name) to the RADIUS Server. Also the password can be same MAC-address or RADIUS secret/shared key by itself which needs to be configured in the directory server accordingly.

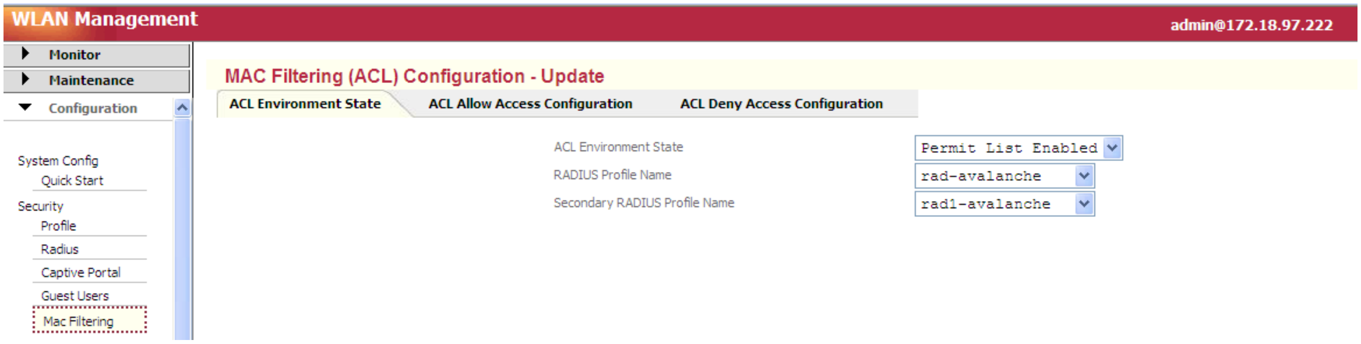


RADIUS Profile Table - Update

Summary Selection

Profile Name	rad-avalanche	
Description	rad-avalanche	Enter 0-128 chars.
RADIUS IP	172 . 19 . 6 . 4	
RADIUS Secret	●●●●●●●●●●●	
RADIUS Port	1812	Valid range: [1024-65535]
MAC Address Delimiter	Hyphen (-)	
Password Type	Shared Key	

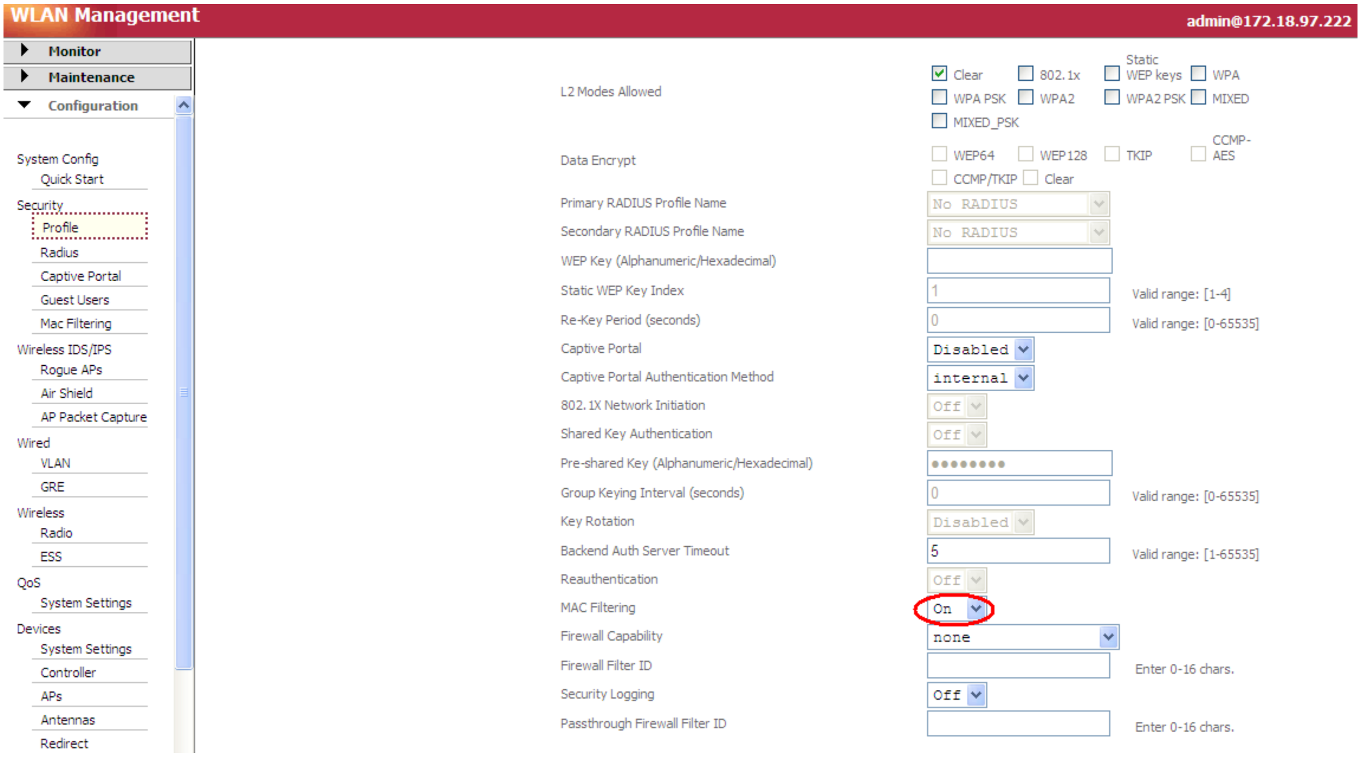
To configure MAC-filtering



MAC Filtering (ACL) Configuration - Update

ACL Environment State	Permit List Enabled
RADIUS Profile Name	rad-avalanche
Secondary RADIUS Profile Name	rad1-avalanche

Enable MAC-filtering in a specific Security Profile



L2 Modes Allowed	☑ Clear □ 802.1x □ Static WEP keys □ WPA □ WPA PSK □ WPA2 □ WPA2 PSK □ MIXED □ MIXED_PSK	
Data Encrypt	□ WEP64 □ WEP128 □ TKIP □ CCMP-AES □ CCMP/TKIP □ Clear	
Primary RADIUS Profile Name	No RADIUS	
Secondary RADIUS Profile Name	No RADIUS	
WEP Key (Alphanumeric/Hexadecimal)		
Static WEP Key Index	1	Valid range: [1-4]
Re-Key Period (seconds)	0	Valid range: [0-65535]
Captive Portal	Disabled	
Captive Portal Authentication Method	internal	
802.1X Network Initiation	Off	
Shared Key Authentication	Off	
Pre-shared Key (Alphanumeric/Hexadecimal)	●●●●●●●●	
Group Keying Interval (seconds)	0	Valid range: [0-65535]
Key Rotation	Disabled	
Backend Auth Server Timeout	5	Valid range: [1-65535]
Reauthentication	Off	
MAC Filtering	On	
Firewall Capability	none	
Firewall Filter ID		Enter 0-16 chars.
Security Logging	Off	
Passthrough Firewall Filter ID		Enter 0-16 chars.

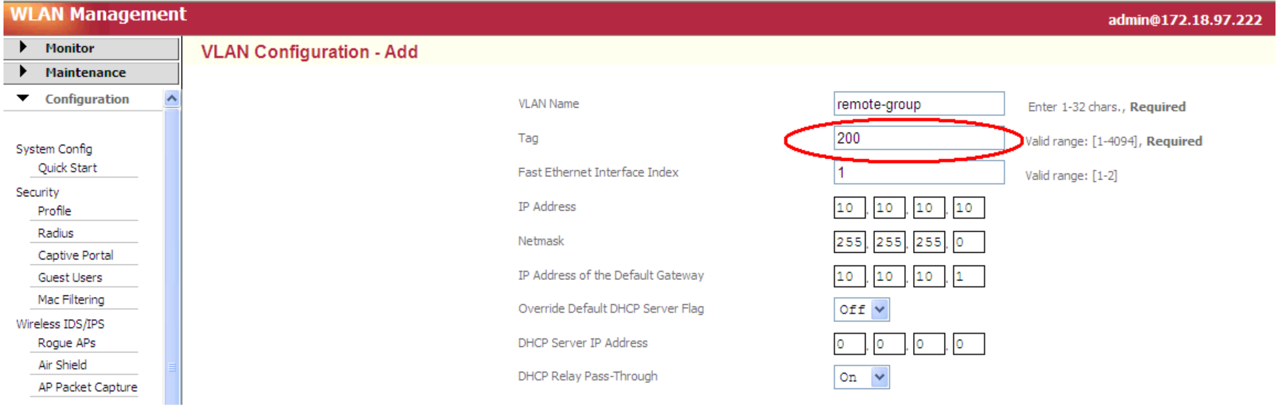
4. COMMONLY USED RADIUS FEATURES

4.1 Dynamic VLAN assignments:

Each WLAN has a static network policy that applies to all clients associated with a Service Set Identifier (SSID). Clients are required to associate with different SSIDs in order to inherit different QoS and security policies depending to the subnet they belong. Dynamic VLAN assignment is a feature to help overcome such a situation which places a wireless user into a specific VLAN, based on the credentials supplied by the user.

All supported VLANs should be configured in the controller and mapped to the correct controller interfaces to allow segmentation of traffic once a VLAN-id is returned by the RADIUS server upon a successful user authentication. Also the uplink switch ports where controller is connected should be tagged with the same VLANs to forward traffic. Following snap shots explains how dynamic VLAN assignment works in Meru Infrastructure using windows 2008 NPS.

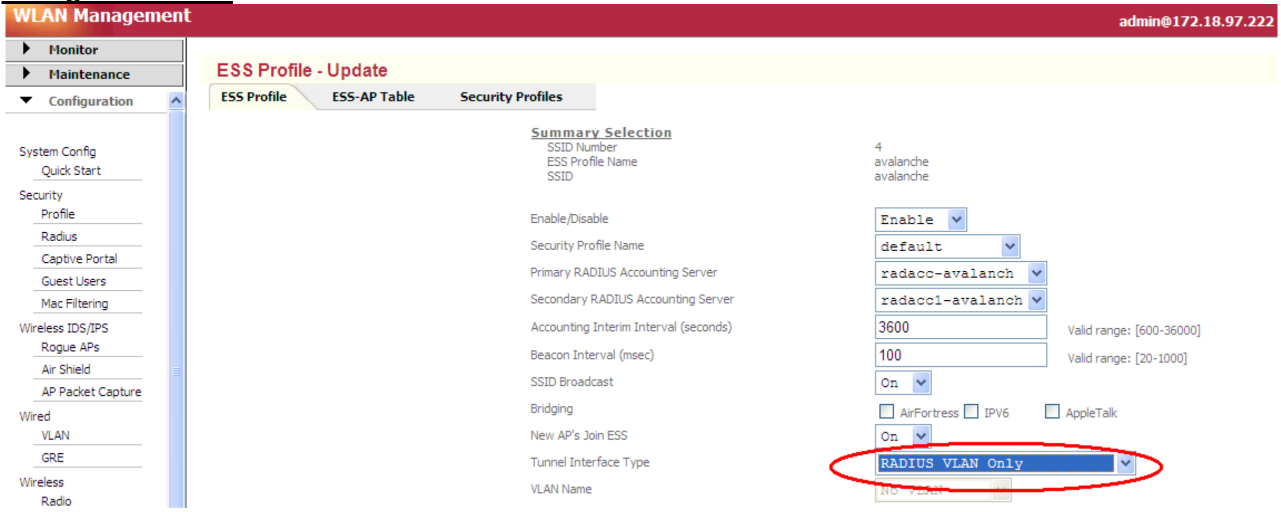
Add a VLAN profile in the controller



VLAN Configuration - Add

VLAN Name: remote-group — Enter 1-32 chars., **Required**
Tag: 200 — Valid range: [1-4094], **Required**
Fast Ethernet Interface Index: 1 — Valid range: [1-2]
IP Address: 10 . 10 . 10 . 10
Netmask: 255 . 255 . 255 . 0
IP Address of the Default Gateway: 10 . 10 . 10 . 1
Override Default DHCP Server Flag: Off
DHCP Server IP Address: 0 . 0 . 0 . 0
DHCP Relay Pass-Through: On

Select tunnel interface type in an ESS-configuration to "RADIUS VLAN only or RADIUS and configured VLAN"

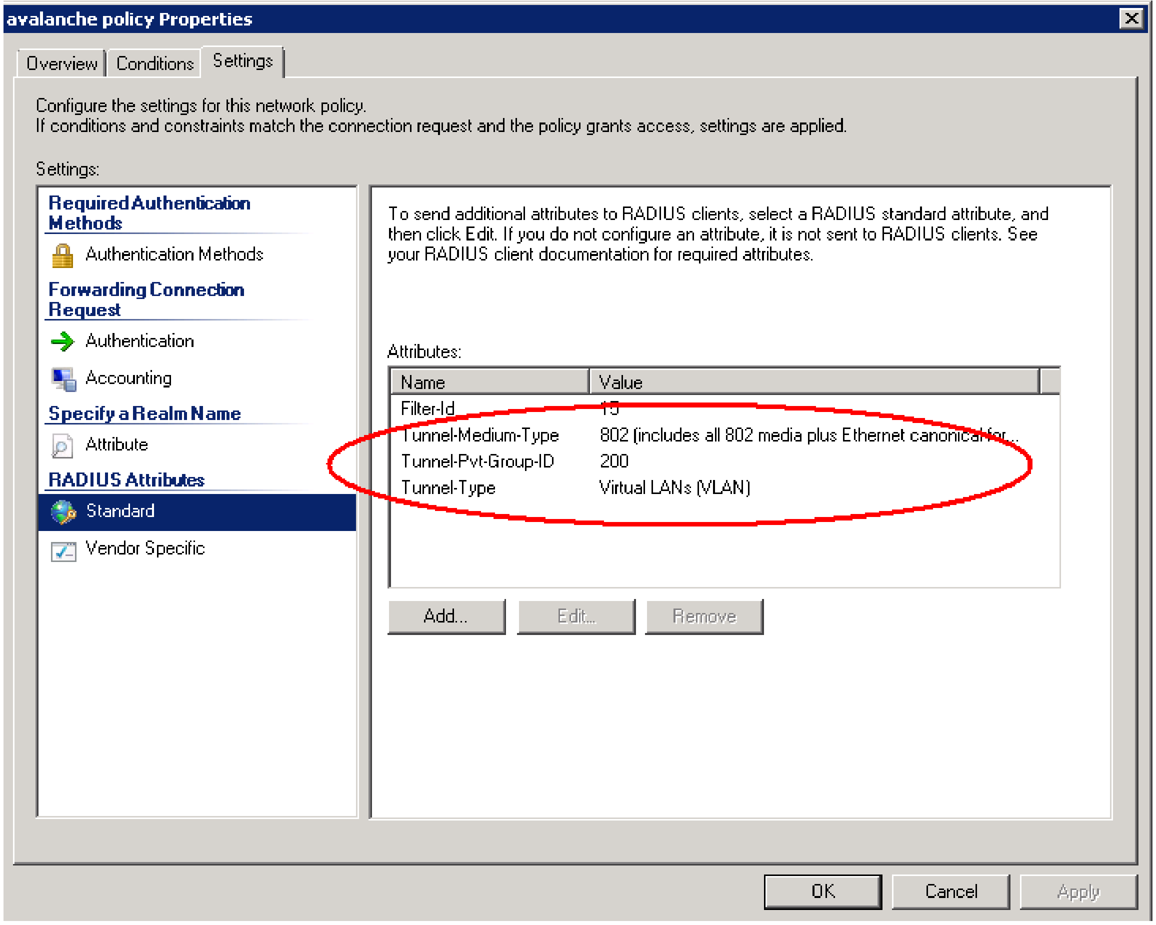


ESS Profile - Update

Summary Selection
SSID Number: 4
ESS Profile Name: avalanche
SSID: avalanche

Enable/Disable: Enable
Security Profile Name: default
Primary RADIUS Accounting Server: radacc-avalanch
Secondary RADIUS Accounting Server: radacc1-avalanch
Accounting Interim Interval (seconds): 3600 — Valid range: [600-36000]
Beacon Interval (msec): 100 — Valid range: [20-1000]
SSID Broadcast: On
Bridging: □ AirFortress □ IPV6 □ AppleTalk
New AP's Join ESS: On
Tunnel Interface Type: RADIUS VLAN Only
VLAN Name: NO VLAN

Add a VLAN attribute in the connection request policy of NPS



Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

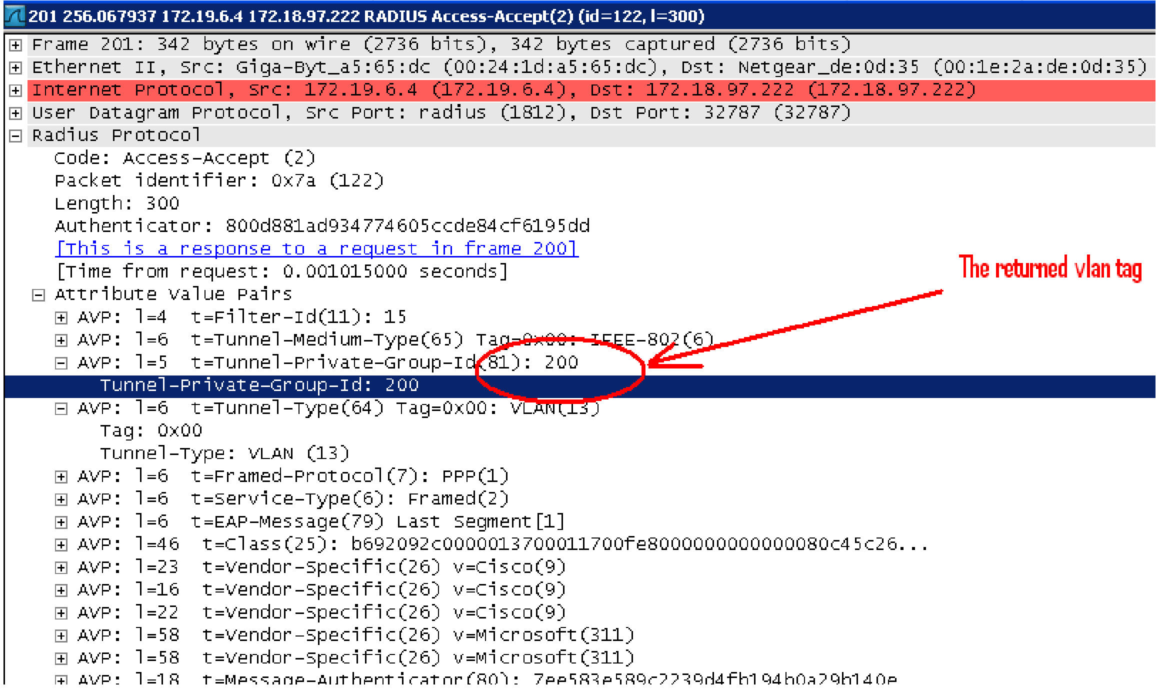
Settings:

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Value
Filter-Id	15
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical for...
Tunnel-Pvt-Group-ID	200
Tunnel-Type	Virtual LANs (VLAN)

Packet inspection made using a Sniffer. RADIUS-ACCEPT returning the VLAN tag



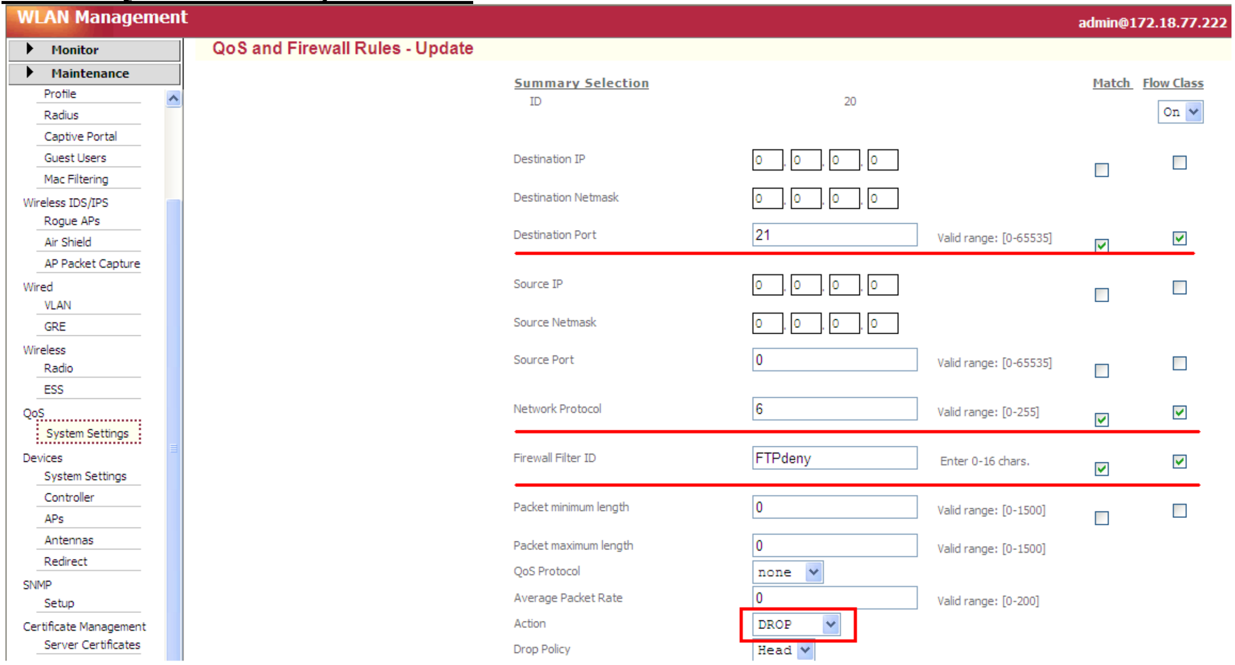
```
201 256.067937 172.19.6.4 172.18.97.222 RADIUS Access-Accept(2) (id=122, l=300)
⊞ Frame 201: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
⊞ Ethernet II, Src: Giga-Byt_a5:65:dc (00:24:1d:a5:65:dc), Dst: Netgear_de:0d:35 (00:1e:2a:de:0d:35)
⊞ Internet Protocol, Src: 172.19.6.4 (172.19.6.4), Dst: 172.18.97.222 (172.18.97.222)
⊞ User Datagram Protocol, Src Port: radius (1812), Dst Port: 32787 (32787)
⊟ Radius Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x7a (122)
    Length: 300
    Authenticator: 800d881ad934774605ccde84cf6195dd
    [This is a response to a request in frame 200]
    [Time from request: 0.001015000 seconds]
  ⊟ Attribute Value Pairs
    ⊞ AVP: l=4  t=Filter-Id(11): 15
    ⊞ AVP: l=6  t=Tunnel-Medium-Type(65) Tag=0x00: IEEE-802(6)
    ⊟ AVP: l=5  t=Tunnel-Private-Group-Id(81): 200
        Tunnel-Private-Group-Id: 200
    ⊟ AVP: l=6  t=Tunnel-Type(64) Tag=0x00: VLAN(13)
        Tag: 0x00
        Tunnel-Type: VLAN (13)
    ⊞ AVP: l=6  t=Framed-Protocol(7): PPP(1)
    ⊞ AVP: l=6  t=Service-Type(6): Framed(2)
    ⊞ AVP: l=6  t=EAP-Message(79) Last Segment[1]
    ⊞ AVP: l=46  t=Class(25): b692092c0000013700011700fe8000000000000080c45c26...
    ⊞ AVP: l=23  t=Vendor-Specific(26) v=Cisco(9)
    ⊞ AVP: l=16  t=Vendor-Specific(26) v=Cisco(9)
    ⊞ AVP: l=22  t=Vendor-Specific(26) v=Cisco(9)
    ⊞ AVP: l=58  t=Vendor-Specific(26) v=Microsoft(311)
    ⊞ AVP: l=58  t=Vendor-Specific(26) v=Microsoft(311)
    ⊞ AVP: l=18  t=Message-Authenticator(80): 7ee583e589c2239d4fb194b0a29b140e
```

The returned vlan tag

4.2 Personal Firewall:

RADIUS-configured filter-id provides a policy firewall after successful 802.1X authentication of the user. This feature requires the RADIUS server to return a firewall filter-id upon a successful user authentication and a matching QoS rule configured in controller. A PEF license also should be installed in the controller for the policy enforcement. The below example demonstrates a test case to deny the FTP usage for a set of users.

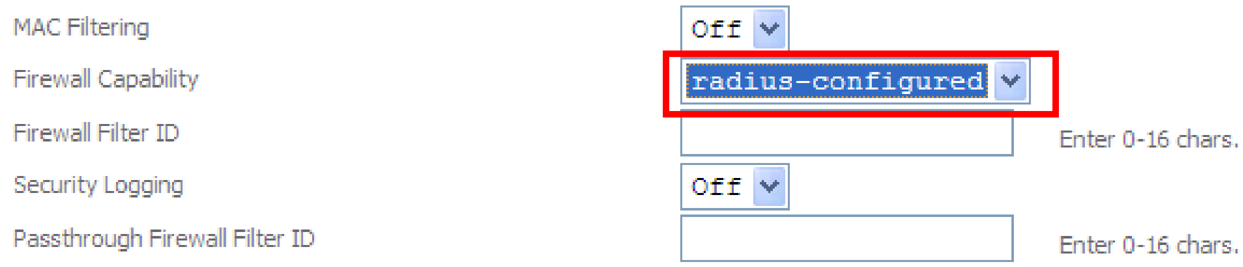
Create a Qos Rule to deny FTP traffic



QoS and Firewall Rules - Update

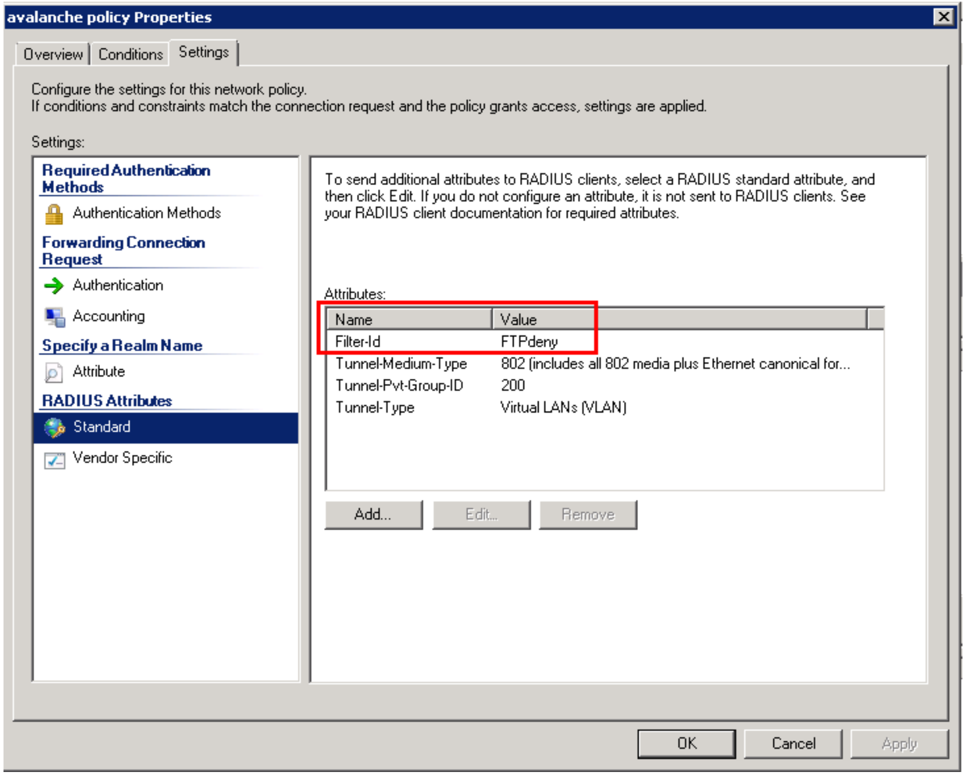
Summary Selection			Match	Flow Class
ID	20			On
Destination IP	0 . 0 . 0 . 0		□	□
Destination Netmask	0 . 0 . 0 . 0			
Destination Port	21	Valid range: [0-65535]	☑	☑
Source IP	0 . 0 . 0 . 0		□	□
Source Netmask	0 . 0 . 0 . 0			
Source Port	0	Valid range: [0-65535]	□	□
Network Protocol	6	Valid range: [0-255]	☑	☑
Firewall Filter ID	FTPdeny	Enter 0-16 chars.	☑	☑
Packet minimum length	0	Valid range: [0-1500]	□	□
Packet maximum length	0	Valid range: [0-1500]		
QoS Protocol	none			
Average Packet Rate	0	Valid range: [0-200]		
Action	DROP			
Drop Policy	Head			

Turn ON RADIUS-configured firewall capability in the Security Profile



MAC Filtering	Off	
Firewall Capability	radius-configured	
Firewall Filter ID		Enter 0-16 chars.
Security Logging	Off	
Passthrough Firewall Filter ID		Enter 0-16 chars.

Add the attribute to the RADIUS server policy



Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

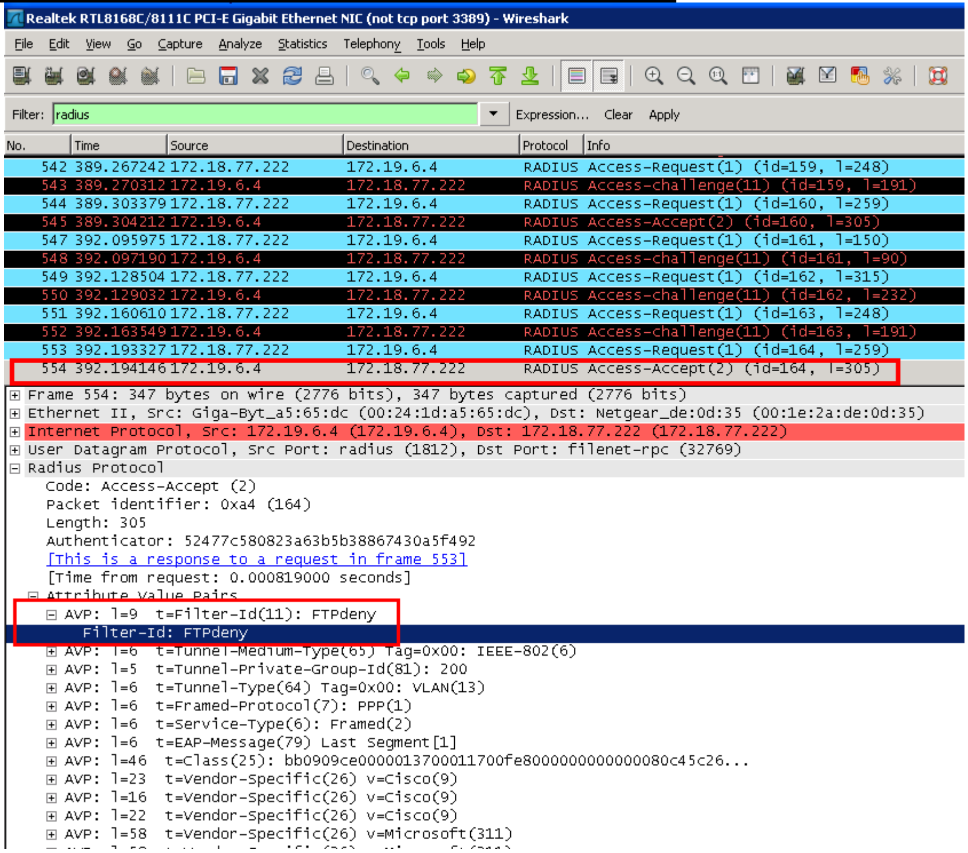
Settings:

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Value
Filter-Id	FTPdeny
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical for...
Tunnel-Pvt-Group-ID	200
Tunnel-Type	Virtual LANs (VLAN)

Verify the filter-id returned by RADIUS from a capture


Realtek RTL8168C/8111C PCI-E Gigabit Ethernet NIC (not tcp port 3389) - Wireshark
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Tools
Help
Expression...
Clear
Apply

Filter: radius

```
No.   Time       Source        Destination   Protocol Info
  542 389.267242 172.18.77.222 172.19.6.4    RADIUS   Access-Request(1) (id=159, l=248)
  543 389.270312 172.19.6.4    172.18.77.222 RADIUS   Access-challenge(11) (id=159, l=191)
  544 389.303379 172.18.77.222 172.19.6.4    RADIUS   Access-Request(1) (id=160, l=259)
  545 389.304212 172.19.6.4    172.18.77.222 RADIUS   Access-Accept(2) (id=160, l=305)
  547 392.095975 172.18.77.222 172.19.6.4    RADIUS   Access-Request(1) (id=161, l=150)
  548 392.097190 172.19.6.4    172.18.77.222 RADIUS   Access-challenge(11) (id=161, l=90)
  549 392.128504 172.18.77.222 172.19.6.4    RADIUS   Access-Request(1) (id=162, l=315)
  550 392.129032 172.19.6.4    172.18.77.222 RADIUS   Access-challenge(11) (id=162, l=232)
  551 392.160610 172.18.77.222 172.19.6.4    RADIUS   Access-Request(1) (id=163, l=248)
  552 392.163549 172.19.6.4    172.18.77.222 RADIUS   Access-challenge(11) (id=163, l=191)
  553 392.193327 172.18.77.222 172.19.6.4    RADIUS   Access-Request(1) (id=164, l=259)
  554 392.194146 172.19.6.4    172.18.77.222 RADIUS   Access-Accept(2) (id=164, l=305)
```

```
⊞ Frame 554: 347 bytes on wire (2776 bits), 347 bytes captured (2776 bits)
⊞ Ethernet II, Src: Giga-Byt_a5:65:dc (00:24:1d:a5:65:dc), Dst: Netgear_de:0d:35 (00:1e:2a:de:0d:35)
⊞ Internet Protocol, Src: 172.19.6.4 (172.19.6.4), Dst: 172.18.77.222 (172.18.77.222)
⊞ User Datagram Protocol, Src Port: radius (1812), Dst Port: filenet-rpc (32769)
⊟ Radius Protocol
    Code: Access-Accept (2)
    Packet identifier: 0xa4 (164)
    Length: 305
    Authenticator: 52477c580823a63b5b38867430a5f492
    [This is a response to a request in frame 553]
    [Time from request: 0.000819000 seconds]
  ⊟ Attribute Value Pairs
    ⊟ AVP: l=9  t=Filter-Id(11): FTPdeny
        Filter-Id: FTPdeny
    ⊞ AVP: l=6  t=Tunnel-Medium-Type(65) Tag=0x00: IEEE-802(6)
    ⊞ AVP: l=5  t=Tunnel-Private-Group-Id(81): 200
    ⊞ AVP: l=6  t=Tunnel-Type(64) Tag=0x00: VLAN(13)
    ⊞ AVP: l=6  t=Framed-Protocol(7): PPP(1)
    ⊞ AVP: l=6  t=Service-Type(6): Framed(2)
    ⊞ AVP: l=6  t=EAP-Message(79) Last Segment[1]
    ⊞ AVP: l=46  t=Class(25): bb0909ce0000013700011700fe8000000000000080c45c26...
    ⊞ AVP: l=23  t=Vendor-Specific(26) v=Cisco(9)
    ⊞ AVP: l=16  t=Vendor-Specific(26) v=Cisco(9)
    ⊞ AVP: l=22  t=Vendor-Specific(26) v=Cisco(9)
    ⊞ AVP: l=58  t=Vendor-Specific(26) v=Microsoft(311)
```

4.3 Restricted SSID

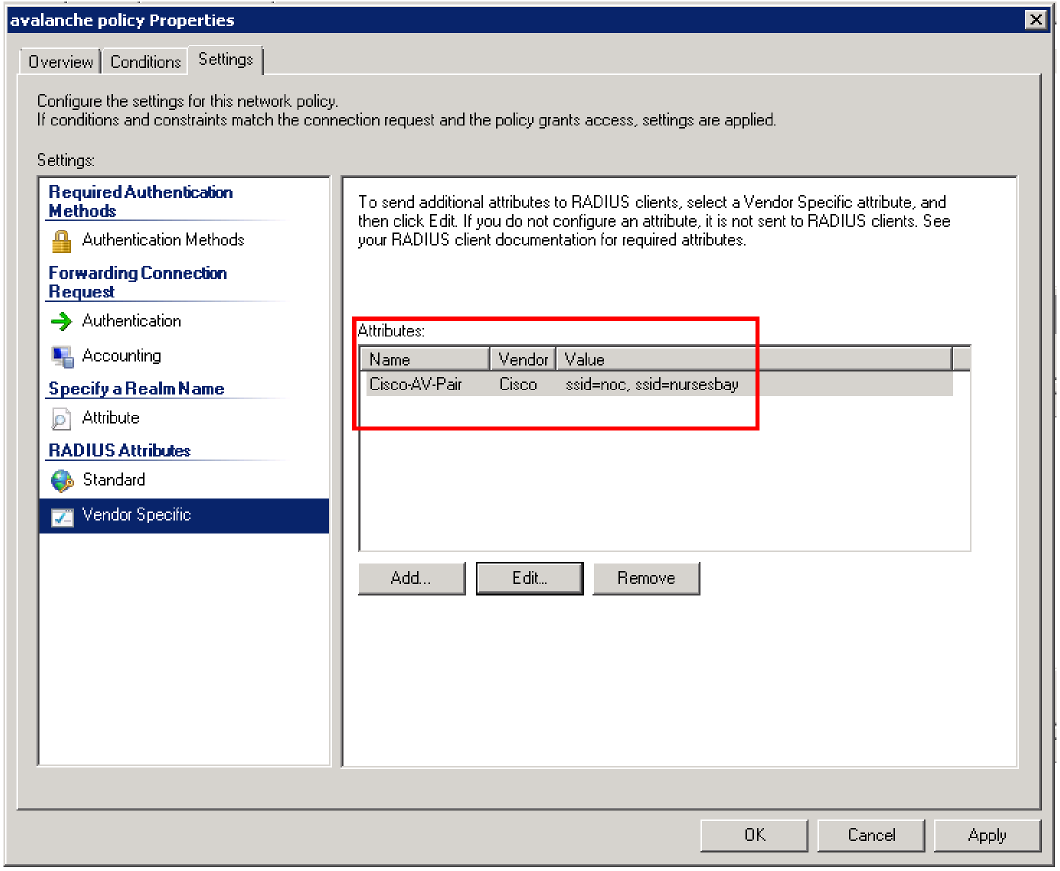
RADIUS-Based ESS Profile Restriction is a feature that gives a controller the capability to restrict wireless clients attempting connection through multiple ESS profiles which uses same RADIUS profiles in the backend to authenticate users. The clients can connect only to certain SSIDs which will be mentioned in a RADIUS Accept message. In absence of the RSSID feature, all wireless clients provisioned in the RADIUS Server have access to all ESS profiles and hence all associated VLANS. With SSID restriction, the RADIUS server can be configured for each wireless client specifying the SSIDs they can connect with. You can use a RADIUS server to restrict SSID connection using VSA in the RADIUS Accept message.

There are three possible conditions for an SSID

RADIUS Server is sending	Results in
No list of acceptable SSIDs	Connection is accepted
A list of acceptable SSIDs that includes the ID	Connection is accepted
A list of acceptable SSIDs that does not include the ID	Connection is not accepted

The RADIUS server should return the allowed SSID(s) in a Vendor-specific attribute (VSA) with Vendor code 9 and attribute number 1 in the Access-Accept message. The attribute value should be string format. The string should say ssid=<ssid-string> where <ssid-string> is replaced by the actual SSID (also known as the ESSID). If a list of multiple allowed SSIDs is used, put each SSID in a separate instance of the attribute. The order of the attributes does not matter. If the SSID to which the station is trying to connect is not among the SSIDs returned by the RADIUS server, the station access will be denied. This feature has no CLI or Web UI commands associated with it. If the RADIUS responds with a list of allowed SSIDs, the list is used to process and limit the user.

Adding attribute in RADIUS Server



avalanche policy Properties

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

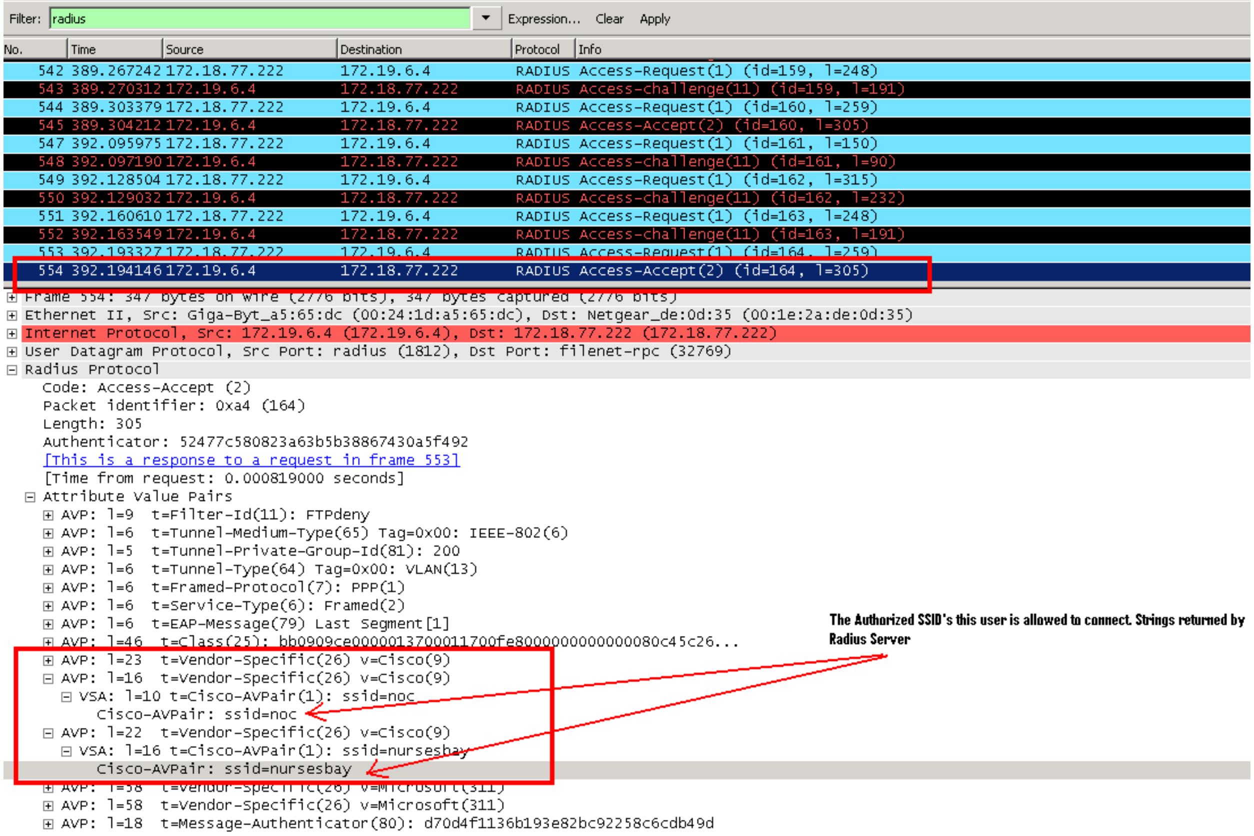
Settings:

To send additional attributes to RADIUS clients, select a Vendor Specific attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Vendor	Value
Cisco-AV-Pair	Cisco	ssid=noc, ssid=nursesbay

Verifying using a capture



```
No.  Time       Source         Destination    Protocol Info
 542 389.267242 172.18.77.222  172.19.6.4     RADIUS Access-Request(1) (id=159, l=248)
 543 389.270312 172.19.6.4     172.18.77.222  RADIUS Access-challenge(11) (id=159, l=191)
 544 389.303379 172.18.77.222  172.19.6.4     RADIUS Access-Request(1) (id=160, l=259)
 545 389.304212 172.19.6.4     172.18.77.222  RADIUS Access-Accept(2) (id=160, l=305)
 547 392.095975 172.18.77.222  172.19.6.4     RADIUS Access-Request(1) (id=161, l=150)
 548 392.097190 172.19.6.4     172.18.77.222  RADIUS Access-challenge(11) (id=161, l=90)
 549 392.128504 172.18.77.222  172.19.6.4     RADIUS Access-Request(1) (id=162, l=315)
 550 392.129032 172.19.6.4     172.18.77.222  RADIUS Access-challenge(11) (id=162, l=232)
 551 392.160610 172.18.77.222  172.19.6.4     RADIUS Access-Request(1) (id=163, l=248)
 552 392.163549 172.19.6.4     172.18.77.222  RADIUS Access-challenge(11) (id=163, l=191)
 553 392.193327 172.18.77.222  172.19.6.4     RADIUS Access-Request(1) (id=164, l=259)
 554 392.194146 172.19.6.4     172.18.77.222  RADIUS Access-Accept(2) (id=164, l=305)

⊞ Frame 554: 347 bytes on wire (2776 bits), 347 bytes captured (2776 bits)
⊞ Ethernet II, Src: Giga-Byt_a5:65:dc (00:24:1d:a5:65:dc), Dst: Netgear_de:0d:35 (00:1e:2a:de:0d:35)
⊞ Internet Protocol, Src: 172.19.6.4 (172.19.6.4), Dst: 172.18.77.222 (172.18.77.222)
⊞ User Datagram Protocol, Src Port: radius (1812), Dst Port: filenet-rpc (32769)
⊟ Radius Protocol
    Code: Access-Accept (2)
    Packet identifier: 0xa4 (164)
    Length: 305
    Authenticator: 52477c580823a63b5b38867430a5f492
    [This is a response to a request in frame 553]
    [Time from request: 0.000819000 seconds]
  ⊟ Attribute Value Pairs
    ⊞ AVP: l=9  t=Filter-Id(11): FTPdeny
    ⊞ AVP: l=6  t=Tunnel-Medium-Type(65) Tag=0x00: IEEE-802(6)
    ⊞ AVP: l=5  t=Tunnel-Private-Group-Id(81): 200
    ⊞ AVP: l=6  t=Tunnel-Type(64) Tag=0x00: VLAN(13)
    ⊞ AVP: l=6  t=Framed-Protocol(7): PPP(1)
    ⊞ AVP: l=6  t=Service-Type(6): Framed(2)
    ⊞ AVP: l=6  t=EAP-Message(79) Last Segment[1]
    ⊞ AVP: l=46  t=Class(25): bb0909ce0000013700011700fe8000000000000080c45c26...
    ⊞ AVP: l=23  t=Vendor-Specific(26) v=Cisco(9)
    ⊟ AVP: l=16  t=Vendor-Specific(26) v=Cisco(9)
      ⊟ VSA: l=10 t=Cisco-AVPair(1): ssid=noc
          Cisco-AVPair: ssid=noc
    ⊟ AVP: l=22  t=Vendor-Specific(26) v=Cisco(9)
      ⊟ VSA: l=16 t=Cisco-AVPair(1): ssid=nursesbay
          Cisco-AVPair: ssid=nursesbay
    ⊞ AVP: l=58  t=Vendor-Specific(26) v=Microsoft(311)
    ⊞ AVP: l=58  t=Vendor-Specific(26) v=Microsoft(311)
    ⊞ AVP: l=18  t=Message-Authenticator(80): d70d4f1136b193e82bc92258c6cdb49d
```

The Authorized SSID's this user is allowed to connect. Strings returned by Radius Server

The RADIUS Server authenticates the user, but the controller can drop the user if the RSSID string is not matching the SSID to which user connection was attempted. The reason for disconnect, as of today will be printed as a “back end authentication failure” in the station logs ,but more detailed information can be gathered from security traces with flags 800009 enabled. Below is example of an extract of traces collected when a user trying to establish a connection and there is a mismatch in the SSID.

```
[08/28 23:38:03.982] SEC: RSSID ===> ESSID Name : avalanche SSID : avalanche and Len : 9
[08/28 23:38:03.982] SEC: ********** Cisco attribute : attr id : 8
[08/28 23:38:03.982] SEC: cisco_attr: subattributeID 1 subattribute_len 10
[08/28 23:38:03.982] SEC: rad_ssid : avalanche attribute is : noc
[08/28 23:38:03.982] SEC: ********** Cisco attribute : attr id : 9
[08/28 23:38:03.982] SEC: cisco_attr: subattributeID 1 subattribute_len 16
[08/28 23:38:03.982] SEC: rad_ssid : avalanche attribute is : nursesbay
[08/28 23:38:03.982] SEC: Restrict SSID 1
[08/28 23:38:03.982] SEC: RADIUS message: code=2 (Access-Accept) identifier=231
length=345, attr_used=3840
[08/28 23:38:03.982] SEC:    Attribute 11 (?Unknown?) length=9
[08/28 23:38:03.982] SEC:    Attribute 65 (Tunnel-Medium-Type) length=6
[08/28 23:38:03.982] SEC:       Value: 6
[08/28 23:38:03.982] SEC:    Attribute 81 (Tunnel-Private-Group-ID) length=5
[08/28 23:38:03.982] SEC:       Value: '200'
[08/28 23:38:03.982] SEC:    Attribute 64 (Tunnel-Type) length=6
[08/28 23:38:03.982] SEC:       Value: 13
[08/28 23:38:03.982] SEC:    Attribute 7 (?Unknown?) length=6
[08/28 23:38:03.982] SEC:    Attribute 6 (?Unknown?) length=6
```

5. PEAP, TTLS TUNNEL TERMINATION -STARNET RADIUS SUPPORT

5.1 Overview

PEAP uses Transport Layer Security (TLS) to create an encrypted channel between an authenticating PEAP client, such as a wireless computer, and a PEAP authenticator, such as an Internet Authentication Service (IAS) or Remote Authentication Dial-In User Service (RADIUS) server. PEAP does not specify an authentication method, but provides additional security for other EAP authentication protocols, such as EAP-MS-CHAP v2, that can operate through the TLS encrypted channel provided by PEAP. PEAP is used as an authentication method for 802.1X wireless client computers.

PEAP authentication process

There are two stages in the PEAP authentication process between PEAP client and authenticator. The first stage sets up a secure channel between the PEAP client and the authenticating server. The second stage provides EAP authentication between the EAP client and authenticator.

PEAP stage one: TLS encrypted channel

The wireless client associates with a wireless access point. An IEEE 802.11-based association provides an Open System or Shared Key authentication before a secure association is created between the client and access point. After the IEEE 802.11-based association is successfully established between the client and access point, the TLS session is negotiated with the access point. After authentication is successfully completed between the wireless client and the server (for example, an IAS server), the TLS session is negotiated between them. The key that is derived during this negotiation is used to encrypt all subsequent communication.

PEAP stage two: EAP-authenticated communication

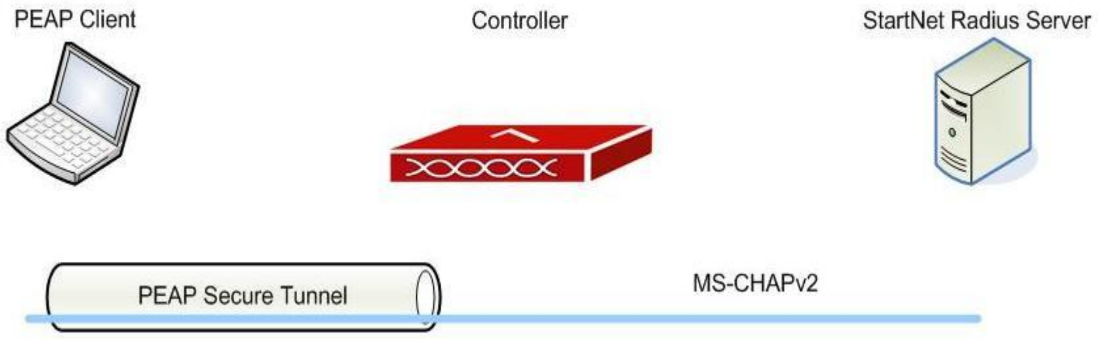
Complete EAP communication, including EAP negotiation, occurs inside the TLS channel created by PEAP during the first stage of the PEAP authentication process. The IAS server authenticates the user or the client computer with the method that is determined by the EAP type and selected for use within PEAP. For deployments of WPS technology, EAP-MS-CHAP v2 is the authentication type used within PEAP. The controller only forwards messages between wireless client and RADIUS server—the controller (or a person monitoring it) cannot decrypt these messages because it is not the TLS end point.

The structure of TTLS and PEAP are quite similar. Both are two-stage protocols that establish security in stage one and then exchange authentication in stage two. Stage one of both protocols establishes a TLS tunnel and authenticates the authentication server to the client with a certificate. Once that secure channel has been established, client authentication credentials are exchanged in the second stage.

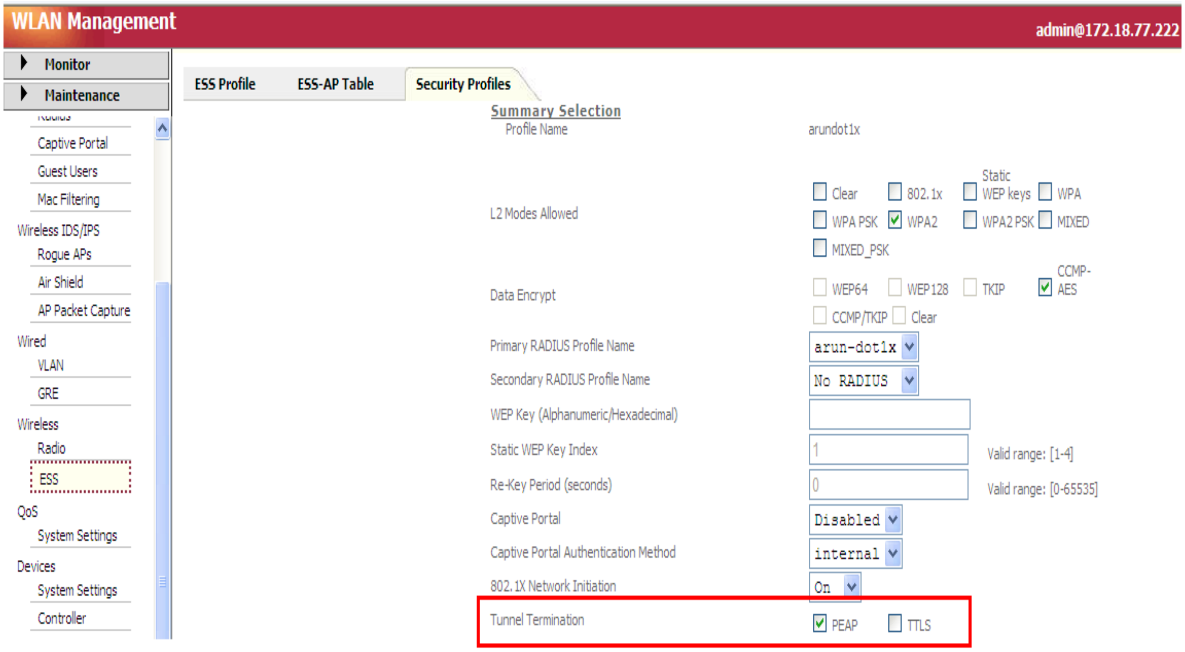
TTLS uses the TLS channel to exchange "attribute-value pairs" (AVPs). The general encoding of information allows a TTLS server to validate AVPs against any type of authentication mechanism. TTLS implementations today support all methods defined by EAP, as well as several older methods (CHAP, PAP, MS-CHAP and MS-CHAPv2).

PEAP Tunnel Termination

Starnet is a RADIUS server which does not understand PEAP messages and have limited support for EAP-MD5 and MS-CHAP-V2. As illustrated below, the PEAP tunnel is terminated in controller and only a supported authentication method (MS-CHAPv2 for example) is forwarded to the RADIUS server.



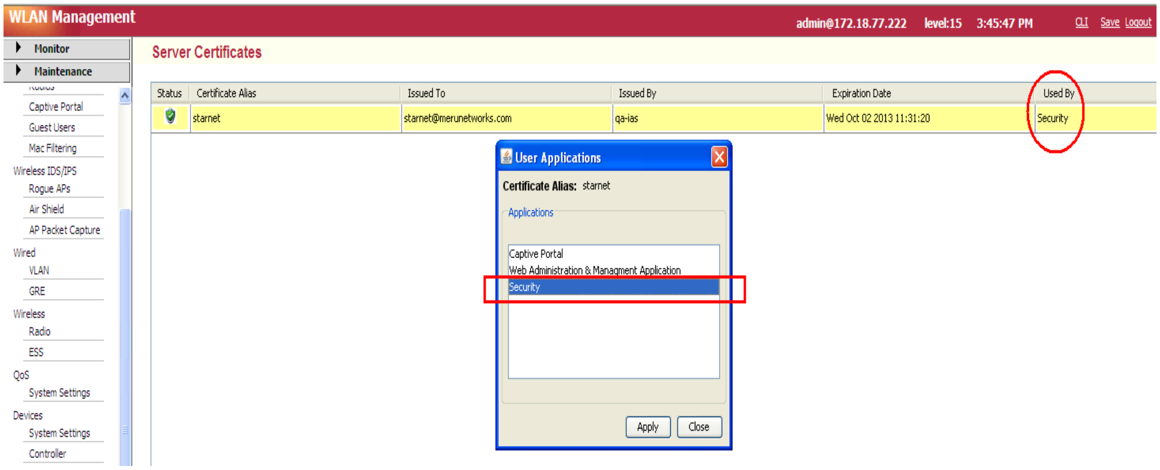
Configuration check box enabled in 802.1x security profile.



Summary Selection

Profile Name	arundot1x
L2 Modes Allowed	□ Clear □ 802.1x □ Static WEP keys □ WPA □ WPA PSK ☑ WPA2 □ WPA2 PSK □ MIXED □ MIXED_PSK
Data Encrypt	□ WEP64 □ WEP128 □ TKIP ☑ CCMP-AES □ CCMP/TKIP □ Clear
Primary RADIUS Profile Name	arun-dot1x
Secondary RADIUS Profile Name	No RADIUS
WEP Key (Alphanumeric/Hexadecimal)	
Static WEP Key Index	1 Valid range: [1-4]
Re-Key Period (seconds)	0 Valid range: [0-65535]
Captive Portal	Disabled
Captive Portal Authentication Method	internal
802.1X Network Initiation	On
Tunnel Termination	☑ PEAP □ TTLS

Custom certificates installed in the controller. Choose the option "Security".



Server Certificates

Status	Certificate Alias	Issued To	Issued By	Expiration Date	Used By
	starnet	starnet@merunetworks.com	qa-ias	Wed Oct 02 2013 11:31:20	Security

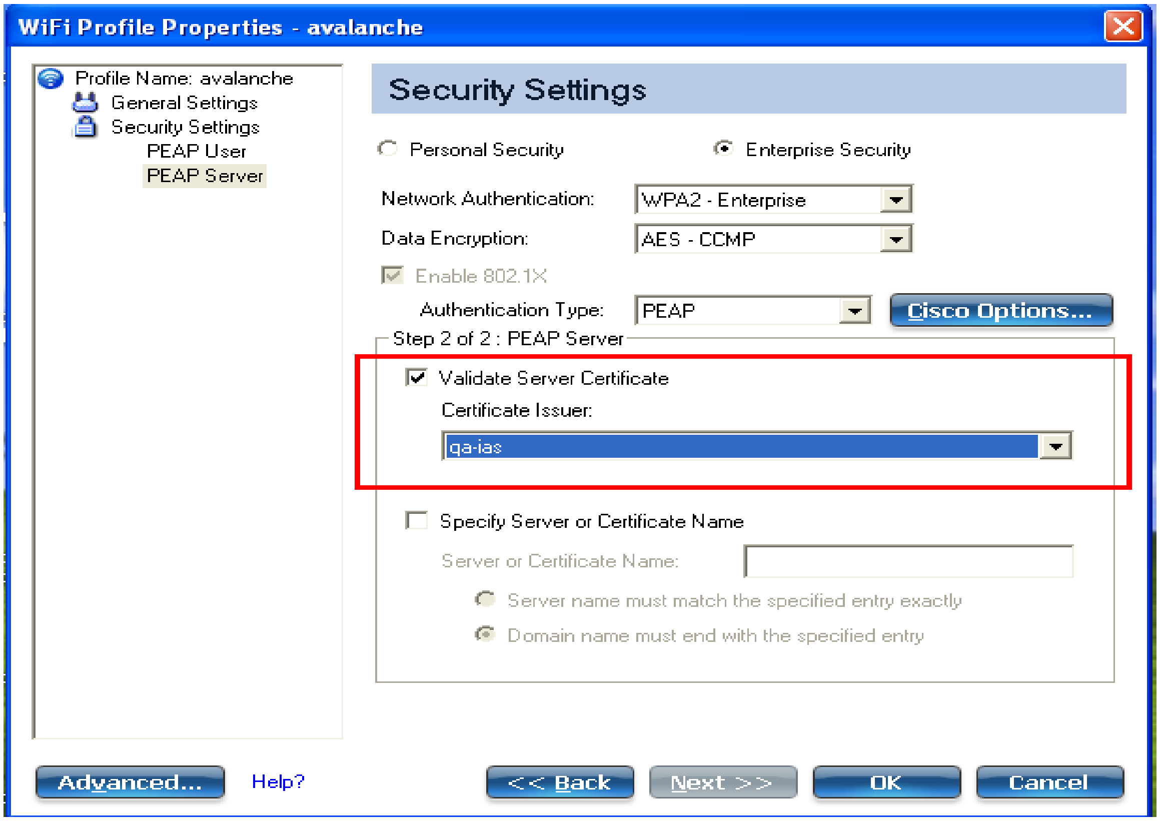
User Applications

Certificate Alias: starnet

Applications

- Captive Portal
- Web Administration & Managment Application
- Security

Server certificate installed in a client



Security Settings

○ Personal Security ● Enterprise Security

Network Authentication: WPA2 - Enterprise

Data Encryption: AES - CCMP

☑ Enable 802.1X

Authentication Type: PEAP

Step 2 of 2 : PEAP Server

☑ Validate Server Certificate

Certificate Issuer: qa-ias

☐ Specify Server or Certificate Name

Server or Certificate Name:

○ Server name must match the specified entry exactly

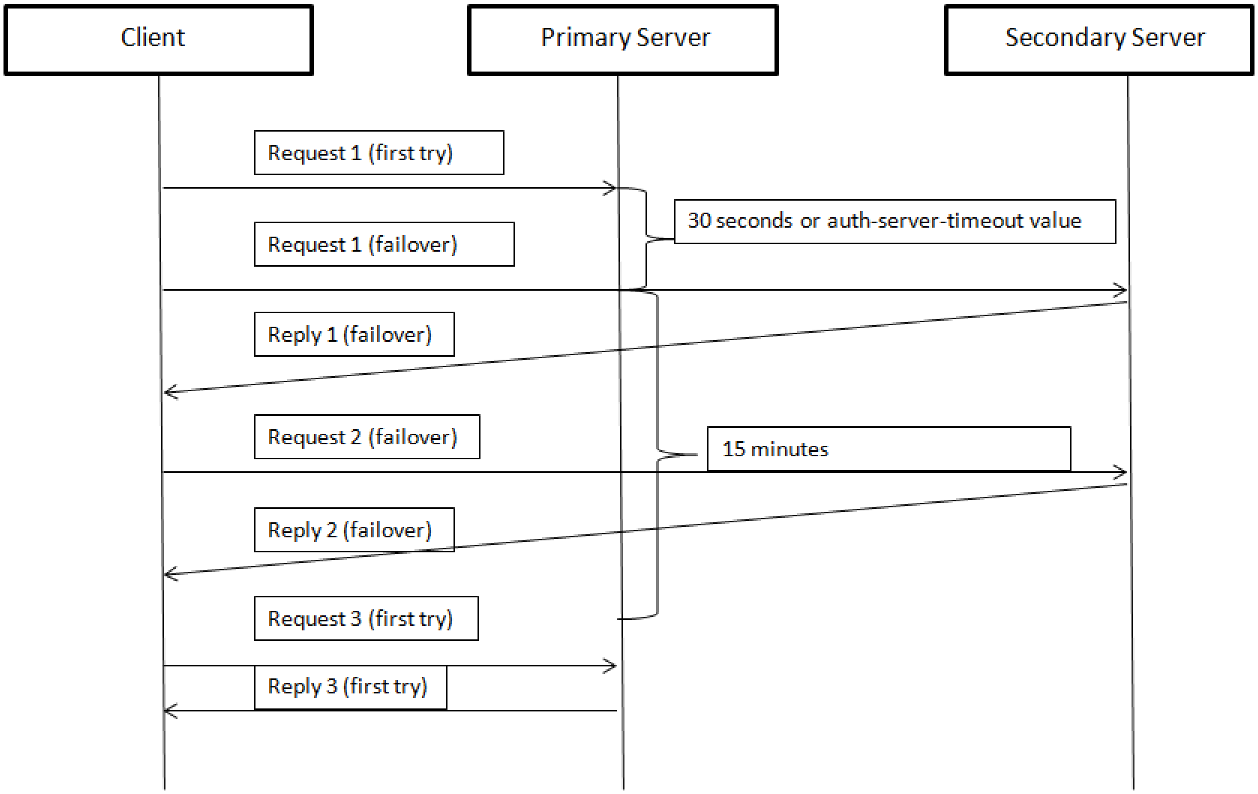
● Domain name must end with the specified entry

Note: Note sure of any use case scenarios from the real world that can be accomplished with this specific feature. Majority of today's enterprise RADIUS servers support almost all EAP types. For documentation purpose, it was tested in a limited Lab environment using NPS and by terminating PEAP in the controller.

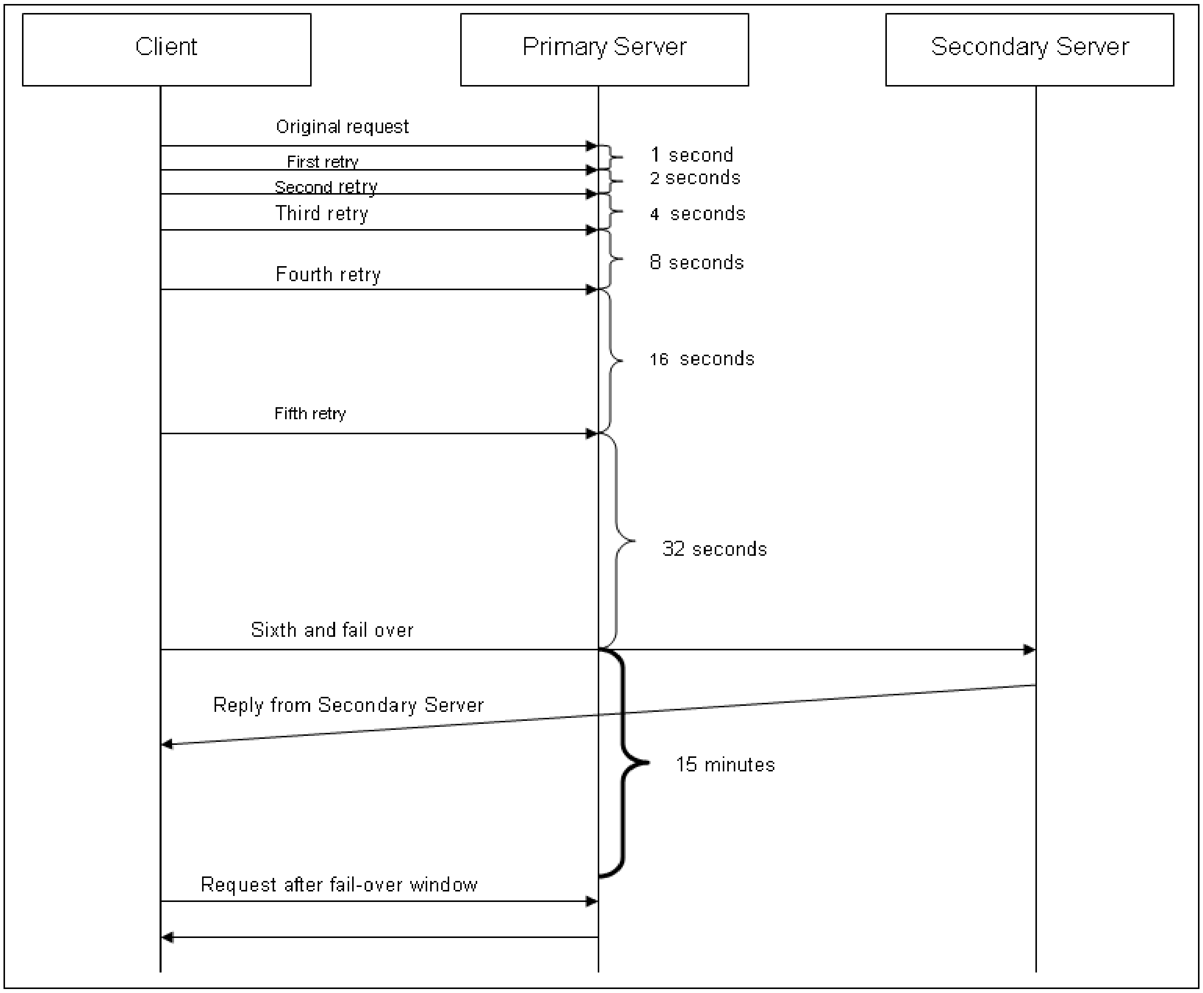
6. RADIUS FAILOVER AND HEALTH CHECK

There are 2 internal modules or services in a Meru controller which mandates the backend RADIUS authentication feature. Since its uses Meru proprietary engineering names or terms, we are calling the modules as category A and B. The failover method defined is different in each module as it depends on the type of user authentication. For example, standard 802.1x or enterprise WPA/WPA2 authentication /accounting is managed by category A and RADIUS-based MAC filtering, CP authentication/accounting, RADIUS-based access Management for WEBGUI falls in category B.

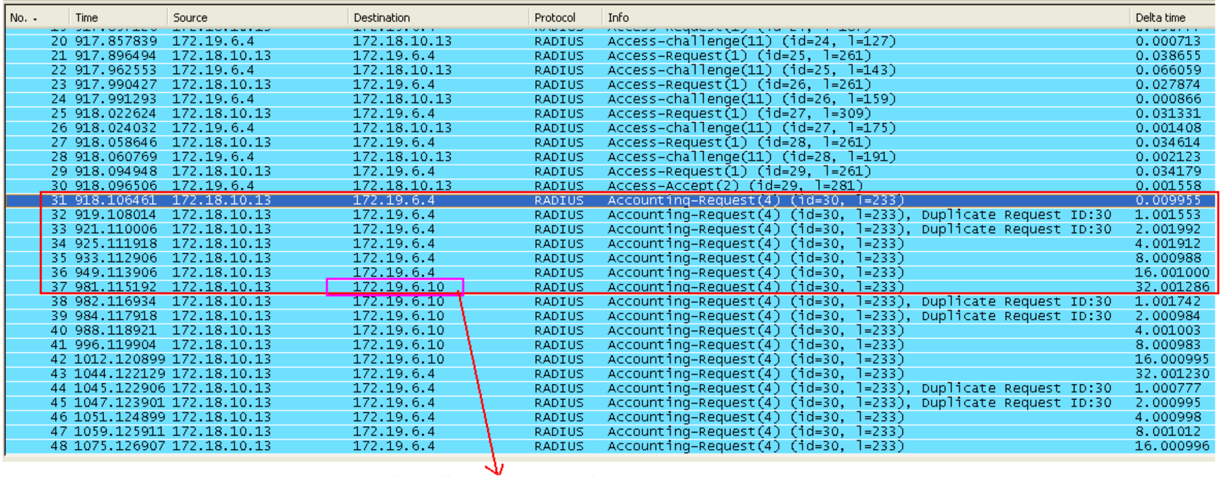
Category A: Authentication failover (802.1x)



Category A: Accounting failover (802.1x)



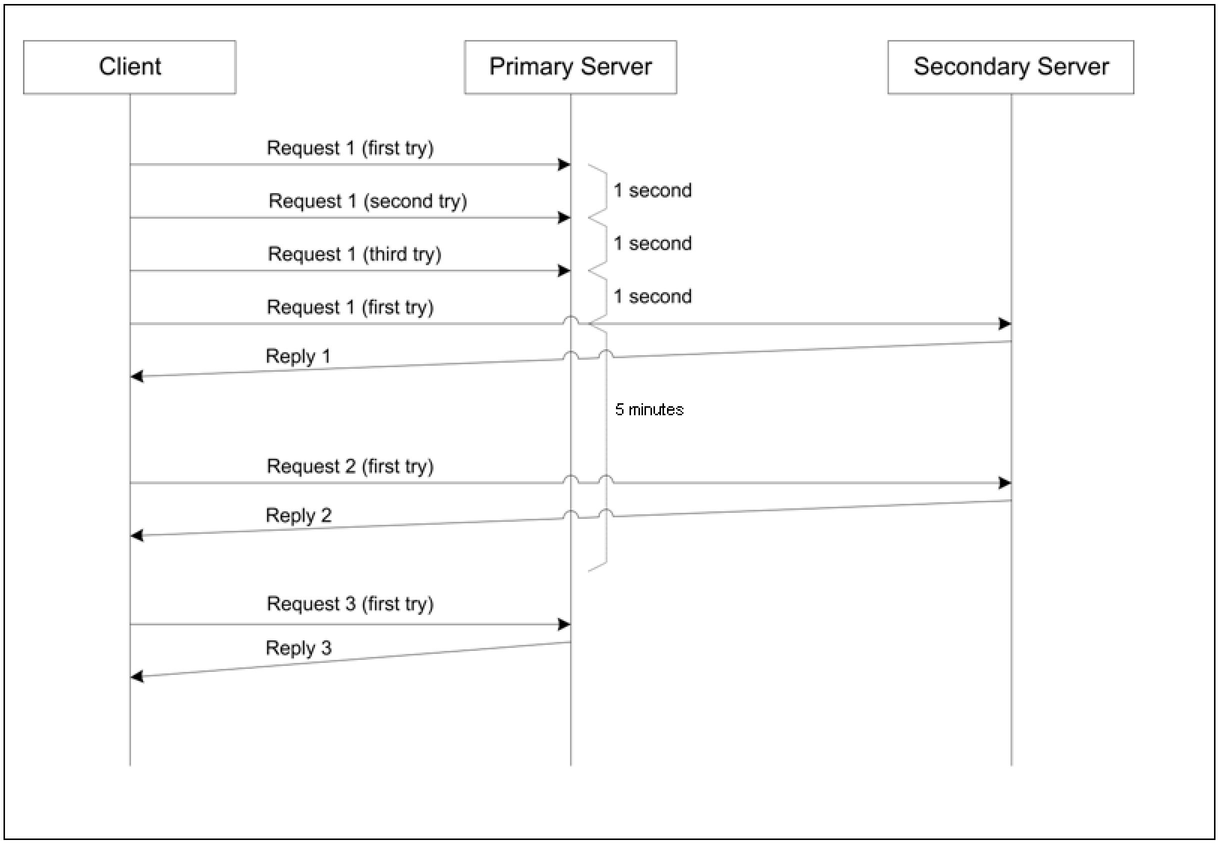
The sniffer capture



No.	Time	Source	Destination	Protocol	Info	Delta time
20	917.857839	172.19.6.4	172.18.10.13	RADIUS	Access-challenge(11) (id=24, l=127)	0.000713
21	917.896494	172.18.10.13	172.19.6.4	RADIUS	Access-Request(1) (id=25, l=261)	0.038655
22	917.962553	172.19.6.4	172.18.10.13	RADIUS	Access-challenge(11) (id=25, l=143)	0.066059
23	917.990427	172.18.10.13	172.19.6.4	RADIUS	Access-Request(1) (id=26, l=261)	0.027874
24	917.991293	172.19.6.4	172.18.10.13	RADIUS	Access-challenge(11) (id=26, l=159)	0.000866
25	918.022624	172.18.10.13	172.19.6.4	RADIUS	Access-Request(1) (id=27, l=309)	0.031331
26	918.024032	172.19.6.4	172.18.10.13	RADIUS	Access-challenge(11) (id=27, l=175)	0.001408
27	918.058646	172.18.10.13	172.19.6.4	RADIUS	Access-Request(1) (id=28, l=261)	0.034614
28	918.060769	172.19.6.4	172.18.10.13	RADIUS	Access-challenge(11) (id=28, l=191)	0.002123
29	918.094948	172.18.10.13	172.19.6.4	RADIUS	Access-Request(1) (id=29, l=261)	0.034179
30	918.096506	172.19.6.4	172.18.10.13	RADIUS	Access-Accept(2) (id=29, l=281)	0.001558
31	918.106461	172.18.10.13	172.19.6.4	RADIUS	Accounting-Request(4) (id=30, l=233)	0.009955
32	919.108014	172.18.10.13	172.19.6.4	RADIUS	Accounting-Request(4) (id=30, l=233), Duplicate Request ID:30	1.001553
33	921.110006	172.18.10.13	172.19.6.4	RADIUS	Accounting-Request(4) (id=30, l=233), Duplicate Request ID:30	2.001992
34	925.111918	172.18.10.13	172.19.6.4	RADIUS	Accounting-Request(4) (id=30, l=233)	4.001912
35	933.112906	172.18.10.13	172.19.6.4	RADIUS	Accounting-Request(4) (id=30, l=233)	8.000988
36	949.113906	172.18.10.13	172.19.6.4	RADIUS	Accounting-Request(4) (id=30, l=233)	16.001000
37	981.115192	172.18.10.13	172.19.6.10	RADIUS	Accounting-Request(4) (id=30, l=233)	32.001286
38	982.116934	172.18.10.13	172.19.6.10	RADIUS	Accounting-Request(4) (id=30, l=233), Duplicate Request ID:30	1.001742
39	984.117918	172.18.10.13	172.19.6.10	RADIUS	Accounting-Request(4) (id=30, l=233), Duplicate Request ID:30	2.000984
40	988.118921	172.18.10.13	172.19.6.10	RADIUS	Accounting-Request(4) (id=30, l=233)	4.001003
41	996.119904	172.18.10.13	172.19.6.10	RADIUS	Accounting-Request(4) (id=30, l=233)	8.000983
42	1012.120899	172.18.10.13	172.19.6.10	RADIUS	Accounting-Request(4) (id=30, l=233)	16.000995
43	1044.122129	172.18.10.13	172.19.6.4	RADIUS	Accounting-Request(4) (id=30, l=233)	32.001230
44	1045.122906	172.18.10.13	172.19.6.4	RADIUS	Accounting-Request(4) (id=30, l=233), Duplicate Request ID:30	1.000777
45	1047.123901	172.18.10.13	172.19.6.4	RADIUS	Accounting-Request(4) (id=30, l=233), Duplicate Request ID:30	2.000995
46	1051.124899	172.18.10.13	172.19.6.4	RADIUS	Accounting-Request(4) (id=30, l=233)	4.000998
47	1059.125911	172.18.10.13	172.19.6.4	RADIUS	Accounting-Request(4) (id=30, l=233)	8.001012
48	1075.126907	172.18.10.13	172.19.6.4	RADIUS	Accounting-Request(4) (id=30, l=233)	16.000996

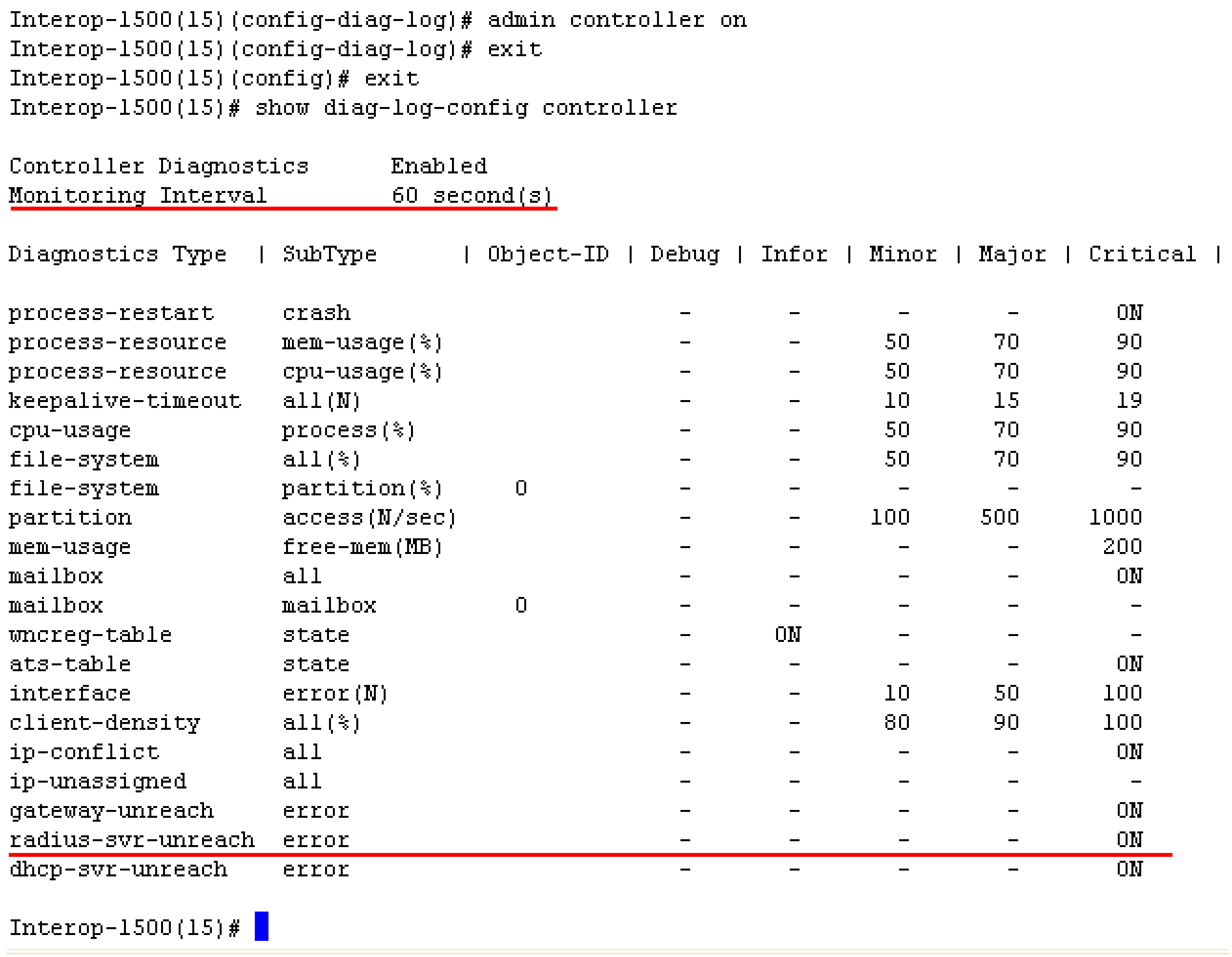
The Fail Over to Secondary

Category B: Authentication and accounting failover (Captive Portal, MAC-filtering etc)



5.1 Health Check:

There is no mechanism used by the controller to check the primary and secondary server availability or status besides sending standard RADIUS requests in predefined intervals described in above authentication and accounting scenarios. However if inference logs are enabled, controllers will send ICMP messages to configured RADIUS servers to report back the availability. The default interval for RADIUS health check is 60 seconds. The following command is used to enable logging in the CLI.



```
Interop-1500(15)(config-diag-log)# admin controller on
Interop-1500(15)(config-diag-log)# exit
Interop-1500(15)(config)# exit
Interop-1500(15)# show diag-log-config controller

Controller Diagnostics      Enabled
Monitoring Interval         60 second(s)

Diagnostics Type   | SubType       | Object-ID | Debug | Infor | Minor | Major | Critical |

process-restart    crash                         -       -       -       -       ON
process-resource   mem-usage(%)                  -       -       50      70      90
process-resource   cpu-usage(%)                  -       -       50      70      90
keepalive-timeout  all(N)                        -       -       10      15      19
cpu-usage          process(%)                    -       -       50      70      90
file-system        all(%)                        -       -       50      70      90
file-system        partition(%)     0            -       -       -       -       -
partition          access(N/sec)                 -       -       100     500     1000
mem-usage          free-mem(MB)                  -       -       -       -       200
mailbox            all                           -       -       -       -       ON
mailbox            mailbox          0            -       -       -       -       -
wncreg-table       state                         -       ON      -       -       -
ats-table          state                         -       -       -       -       ON
interface          error(N)                      -       -       10      50      100
client-density     all(%)                        -       -       80      90      100
ip-conflict        all                           -       -       -       -       ON
ip-unassigned      all                           -       -       -       -       -
gateway-unreach    error                         -       -       -       -       ON
radius-svr-unreach error                         -       -       -       -       ON
dhcp-svr-unreach   error                         -       -       -       -       ON

Interop-1500(15)#
```

7. MISCELLANEOUS:

- Presently the failover algorithm is defined on per-ESS basis. It means a failover scenario is not updated globally which makes users in other ESS profiles to send requests to an already failed primary server before switching to secondary.
- Run state RADIUS failover information is not carried forward during Nplus1 failover scenarios.
- The inference logs are classified as events. The system also generates syslog messages during RADIUS fail-over.
- Different failover algorithms are used for authentication and accounting in 802.1x, as per the system design.