```
!
! Configuration of RFS4000 version 5.5.1.0-017R
!
!
version 2.3
!
!
ip access-list BROADCAST-MULTICAST-CONTROL
permit tcp any any rule-precedence 10 rule-description "permit all TCP traffic"
permit udp any eq 67 any eq dhcpc rule-precedence 11 rule-description "permit DHCP replies"
deny udp any range 137 138 any range 137 138 rule-precedence 20 rule-description "deny windows
netbios"
deny ip any 224.0.0.0/4 rule-precedence 21 rule-description "deny IP multicast"
deny ip any host 255.255.255.255 rule-precedence 22 rule-description "deny IP local broadcast"
permit ip any any rule-precedence 100 rule-description "permit all IP traffic"
!
ip access-list nat-rule
permit ip 172.16.11.0/24 any rule-precedence 10
!
mac access-list PERMIT-ARP-AND-IPv4
permit any any type ip rule-precedence 10 rule-description "permit all IPv4 traffic"
permit any any type arp rule-precedence 20 rule-description "permit all ARP traffic"
!
firewall-policy default
no ip dos tcp-sequence-past-window
!
!
mint-policy global-default
!
meshpoint-qos-policy default
!
wlan-qos-policy default
qos trust dscp
qos trust wmm
!
radio-qos-policy default
!
aaa-policy default-external
authentication server 1 host 10.86.119.170 secret 0 cisco123
mac-address-format pair-colon case upper attributes all
attribute cisco-vsa audit-session-id
!
dns-whitelist ISE_whitelist
permit vsantau-ise2.cisco.com
```

permit vsantau-ise2
permit 10.86.119.170
!
captive-portal ISE
access-type no-auth
connection-mode https
server host on-boaring.com
server mode centralized-controller hosting-vlan-interface 16
webpage external login https://10.86.119.170/portal/gateway?portal=5dbe4590-c486-11e4-af78-005056bf4687&action=cwa
use aaa-policy default-external
use dns-whitelist ISE_whitelist
radius-vlan-assignment
!
captive-portal ISE-dynamic
access-type no-auth
server host on-boaring.com
server mode centralized-controller
webpage internal login title agreement
webpage internal agreement description You will be redirected to Cisco ISE portal
webpage internal agreement header ISE portal
use dns-whitelist ISE_whitelist
!
captive-portal ISEWebAuth
terms-agreement
use aaa-policy default-external
!
captive-portal default-external
server host guest-access.net
server mode centralized-controller
use aaa-policy default-external
!
wlan wlan-ISE1x
ssid motorolaISE1x
vlan 10
bridging-mode tunnel
encryption-type tkip
authentication-type eap
radius vlan-assignment
radius dynamic-authorization
use aaa-policy default-external
use captive-portal ISE-dynamic
captive-portal-enforcement fall-back
!

```
wlan wlan1
ssid motorolaISE
vlan 10
bridging-mode tunnel
encryption-type none
authentication-type none
radius vlan-assignment
radius dynamic-authorization
use aaa-policy default-external
use captive-portal ISEWebAuth
captive-portal-enforcement fall-back
!
ap300 default-ap300
interface radio1
interface radio2
!
radius-server-policy ISE-CoA
!
dhcp-server-policy DHCPPolicy
dhcp-pool vlan11
network 172.16.12.0/24
address range 172.16.12.22 172.16.12.99
domain-name cisco2.com
default-router 172.16.12.1
dhcp-pool main
network 172.16.11.0/24
address range 172.16.11.10 172.16.11.250
domain-name cisco.com
default-router 172.16.11.1
dns-server 172.16.11.1
!
!
management-policy default
no http server
https server
ssh
user admin password 1 115ed7702f6dfc585e5effcdd6d9975d1719ff406fb1ca81241762ffa6ad0632 role
superuser access all
snmp-server community 0 public ro
snmp-server user snmptrap v3 encrypted des auth md5 0 motorola
snmp-server user snmpmanager v3 encrypted des auth md5 0 motorola
!
l2tpv3 policy default
!
```

```
profile rfs4000 default-rfs4000
ip default-gateway 10.86.116.1
autoinstall configuration
autoinstall firmware
crypto ikev1 policy ikev1-default
isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ikev2 policy ikev2-default
isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
crypto ikev1 remote-vpn
crypto ikev2 remote-vpn
crypto auto-ipsec-secure
crypto remote-vpn-client
interface radio1
wlan wlan-ISE1x bss 2 primary
interface radio2
wlan wlan-ISE1x bss 2 primary
interface up1
switchport mode access
switchport access vlan 16
ip dhcp trust
qos trust dscp
qos trust 802.1p
interface ge1
ip dhcp trust
qos trust dscp
qos trust 802.1p
interface ge2
ip dhcp trust
qos trust dscp
qos trust 802.1p
interface ge3
ip dhcp trust
qos trust dscp
qos trust 802.1p
interface ge4
ip dhcp trust
qos trust dscp
qos trust 802.1p
interface ge5
ip dhcp trust
qos trust dscp
qos trust 802.1p
interface wwan1
```

```
interface pppoe1
use dhcp-server-policy DHCPPolicy
use firewall-policy default
use captive-portal server ISE
logging on
service pm sys-restart
router ospf
!
profile ap82xx default-ap82xx
autoinstall configuration
autoinstall firmware
crypto ikev1 policy ikev1-default
isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ikev2 policy ikev2-default
isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
crypto ikev1 remote-vpn
crypto ikev2 remote-vpn
crypto auto-ipsec-secure
crypto remote-vpn-client
interface radio1
wlan wlan1 bss 1 primary
interface radio2
wlan wlan1 bss 1 primary
interface radio3
interface ge1
ip dhcp trust
qos trust dscp
qos trust 802.1p
interface ge2
ip dhcp trust
qos trust dscp
qos trust 802.1p
interface vlan1
ip address dhcp
ip address zeroconf secondary
ip dhcp client request options all
interface wwan1
interface pppoe1
use firewall-policy default
service pm sys-restart
router ospf
!
profile ap81xx default-ap81xx
```

autoinstall configuration
autoinstall firmware
crypto ikev1 policy ikev1-default
isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ikev2 policy ikev2-default
isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
crypto ikev1 remote-vpn
crypto ikev2 remote-vpn
crypto auto-ipsec-secure
crypto remote-vpn-client
interface radio1
wlan wlan1 bss 1 primary
interface radio2
wlan wlan1 bss 1 primary
interface radio3
interface ge1
ip dhcp trust
qos trust dscp
qos trust 802.1p
interface ge2
ip dhcp trust
qos trust dscp
qos trust 802.1p
interface vlan1
ip address dhcp
ip address zeroconf secondary
ip dhcp client request options all
interface wwan1
interface pppoe1
use firewall-policy default
service pm sys-restart
router ospf
!
profile ap71xx default-ap71xx
autoinstall configuration
autoinstall firmware
crypto ikev1 policy ikev1-default
isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ikev2 policy ikev2-default
isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
crypto ikev1 remote-vpn
crypto ikev2 remote-vpn

```
crypto auto-ipsec-secure
crypto remote-vpn-client
interface radio1
wlan wlan1 bss 1 primary
interface radio2
wlan wlan1 bss 1 primary
interface radio3
interface ge1
ip dhcp trust
qos trust dscp
qos trust 802.1p
interface ge2
ip dhcp trust
qos trust dscp
qos trust 802.1p
interface vlan1
ip address dhcp
ip address zeroconf secondary
ip dhcp client request options all
interface wwan1
interface pppoe1
use firewall-policy default
service pm sys-restart
router ospf
!
profile ap6532 default-ap6532
autoinstall configuration
autoinstall firmware
crypto ikev1 policy ikev1-default
isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ikev2 policy ikev2-default
isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
crypto ikev1 remote-vpn
crypto ikev2 remote-vpn
crypto auto-ipsec-secure
crypto load-management
crypto remote-vpn-client
interface radio1
wlan wlan1 bss 1 primary
interface radio2
wlan wlan1 bss 1 primary
interface ge1
ip dhcp trust
```

```
qos trust dscp
qos trust 802.1p
interface vlan1
ip address dhcp
ip address zeroconf secondary
ip dhcp client request options all
interface pppoe1
use firewall-policy default
service pm sys-restart
router ospf
!
profile ap650 default-ap650
autoinstall configuration
autoinstall firmware
crypto ikev1 policy ikev1-default
isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ikev2 policy ikev2-default
isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
crypto ikev1 remote-vpn
crypto ikev2 remote-vpn
crypto auto-ipsec-secure
crypto load-management
crypto remote-vpn-client
interface radio1
wlan wlan1 bss 1 primary
interface radio2
wlan wlan1 bss 1 primary
interface ge1
ip dhcp trust
qos trust dscp
qos trust 802.1p
interface vlan1
ip address dhcp
ip address zeroconf secondary
ip dhcp client request options all
interface pppoe1
use firewall-policy default
service pm sys-restart
!
profile ap6521 default-ap6521
autoinstall configuration
autoinstall firmware
interface radio1
```

```
wlan wlan1 bss 1 primary
interface ge1
ip dhcp trust
qos trust dscp
qos trust 802.1p
interface vlan1
ip address dhcp
ip address zeroconf secondary
ip dhcp client request options all
interface pppoe1
use firewall-policy default
service pm sys-restart
!
profile ap621 default-ap621
autoinstall configuration
autoinstall firmware
interface radio1
wlan wlan1 bss 1 primary
interface ge1
ip dhcp trust
qos trust dscp
qos trust 802.1p
interface vlan1
ip address dhcp
ip address zeroconf secondary
ip dhcp client request options all
use firewall-policy default
service pm sys-restart
!
profile ap6511 default-ap6511
autoinstall configuration
autoinstall firmware
interface radio1
wlan wlan1 bss 1 primary
interface up1
ip dhcp trust
qos trust dscp
qos trust 802.1p
interface fe1
ip dhcp trust
qos trust dscp
qos trust 802.1p
interface fe2
ip dhcp trust
```

```
qos trust dscp
qos trust 802.1p
interface fe3
ip dhcp trust
qos trust dscp
qos trust 802.1p
interface fe4
ip dhcp trust
qos trust dscp
qos trust 802.1p
interface vlan1
ip address dhcp
ip address zeroconf secondary
ip dhcp client request options all
interface pppoe1
use firewall-policy default
service pm sys-restart
!
profile ap6562 default-ap6562
autoinstall configuration
autoinstall firmware
crypto ikev1 policy ikev1-default
isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ikev2 policy ikev2-default
isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
crypto ikev1 remote-vpn
crypto ikev2 remote-vpn
crypto auto-ipsec-secure
crypto load-management
crypto remote-vpn-client
interface radio1
placement outdoor
wlan wlan1 bss 1 primary
interface radio2
placement outdoor
wlan wlan1 bss 1 primary
interface ge1
ip dhcp trust
qos trust dscp
qos trust 802.1p
interface vlan1
ip address dhcp
ip address zeroconf secondary
```

ip dhcp client request options all
interface pppoe1
use firewall-policy default
service pm sys-restart
router ospf
!
profile ap6522 default-ap6522
autoinstall configuration
autoinstall firmware
crypto ikev1 policy ikev1-default
isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ikev2 policy ikev2-default
isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
crypto ikev1 remote-vpn
crypto ikev2 remote-vpn
crypto auto-ipsec-secure
crypto load-management
crypto remote-vpn-client
interface radio1
wlan wlan1 bss 1 primary
interface radio2
wlan wlan1 bss 1 primary
interface ge1
ip dhcp trust
qos trust dscp
qos trust 802.1p
interface vlan1
ip address dhcp
ip address zeroconf secondary
ip dhcp client request options all
interface pppoe1
use firewall-policy default
service pm sys-restart
router ospf
!
profile ap622 default-ap622
autoinstall configuration
autoinstall firmware
crypto ikev1 policy ikev1-default
isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ikev2 policy ikev2-default
isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac

```
crypto ikev1 remote-vpn
crypto ikev2 remote-vpn
crypto auto-ipsec-secure
crypto load-management
crypto remote-vpn-client
interface radio1
wlan wlan1 bss 1 primary
interface radio2
wlan wlan1 bss 1 primary
interface ge1
ip dhcp trust
qos trust dscp
qos trust 802.1p
interface vlan1
ip address dhcp
ip address zeroconf secondary
ip dhcp client request options all
use firewall-policy default
service pm sys-restart
router ospf
!
rf-domain default
timezone America/New_York
country-code us
!
rfs4000 B4-C7-99-DD-F5-5E
use profile default-rfs4000
use rf-domain default
hostname rfs4000-DDF55E
license AP DEFAULT-6AP-LICENSE
license ADSEC DEFAULT-ADV-SEC-LICENSE
service radius dynamic-authorization additional-port 3799
ip name-server 161.44.124.122
ip name-server 64.102.6.247
ip domain-name cisco.com
use radius-server-policy ISE-CoA
interface radio1
wlan wlan-ISE1x bss 1 primary
interface radio2
wlan wlan-ISE1x bss 2 primary
interface up1
switchport mode trunk
switchport trunk native vlan 16
no switchport trunk native tagged
```

```
switchport trunk allowed vlan 10-11,16
interface vlan1
ip address 192.168.0.1/24
ip dhcp client request options all
no ip nat
shutdown
interface vlan10
ip address 172.16.11.1/24
no ip dhcp client request options all
ip nat inside
no dhcp-relay-incoming
interface vlan11
ip address 172.16.12.1/24
ip nat inside
interface vlan16
description "Virtual Interface for WAN"
ip address 10.86.119.145/22
no ip dhcp client request options all
ip nat outside
no dhcp-relay-incoming
use dhcp-server-policy DHCPPolicy
use captive-portal server ISE-dynamic
ip dns-server-forward
logging on
logging console warnings
logging buffered warnings
ip nat inside source list nat-rule precedence 10 interface vlan16 overload
!
!
end
```