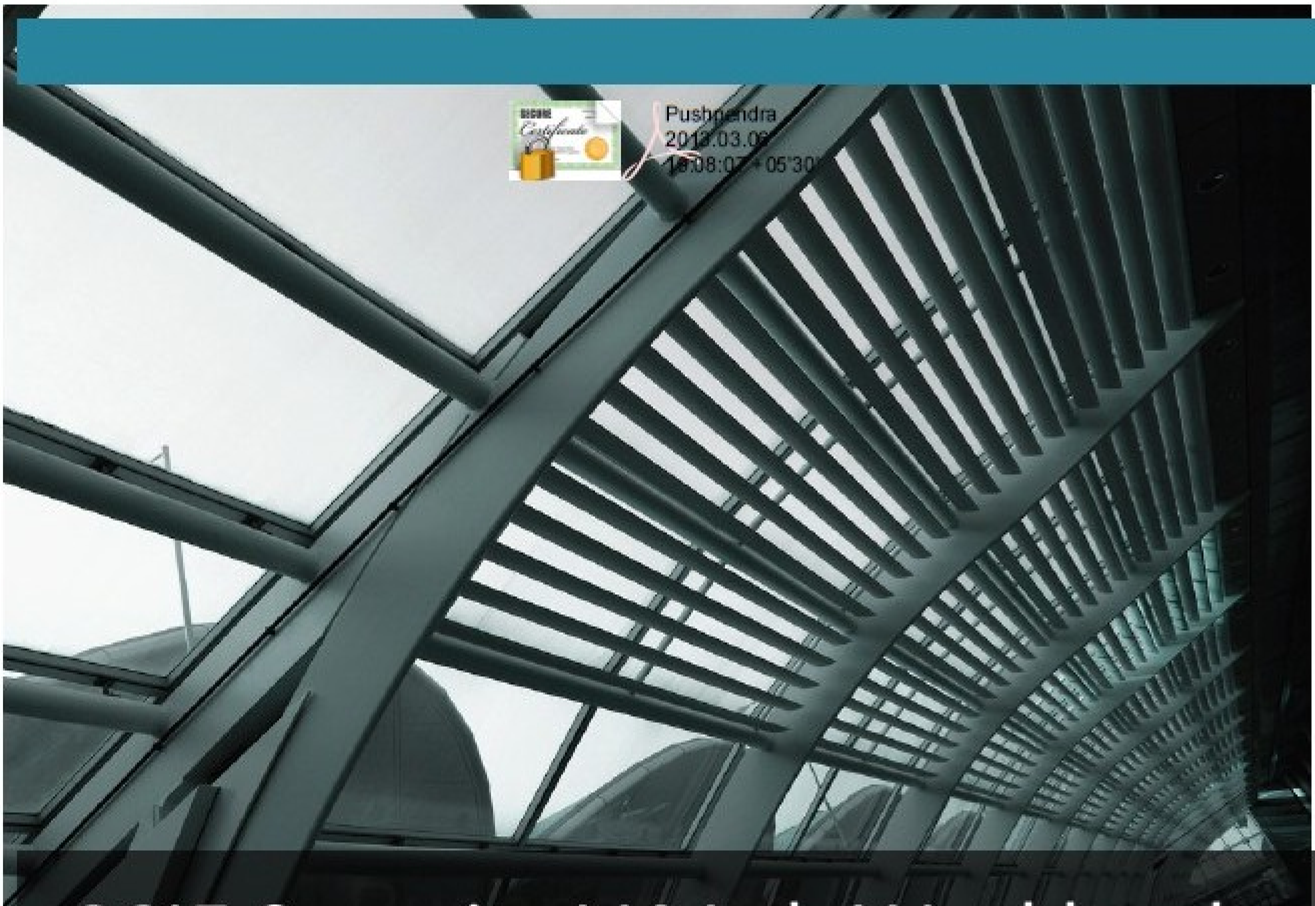


CCIE Security V4 Lab Workbook Vol. 3

Piotr Matusiak
CCIE #19860
R&S, Security
C|EH, CCSI #33705

Narbik Kocharians
CCIE #12410
R&S, Security, SP
CCSI #30832

Table of Contents

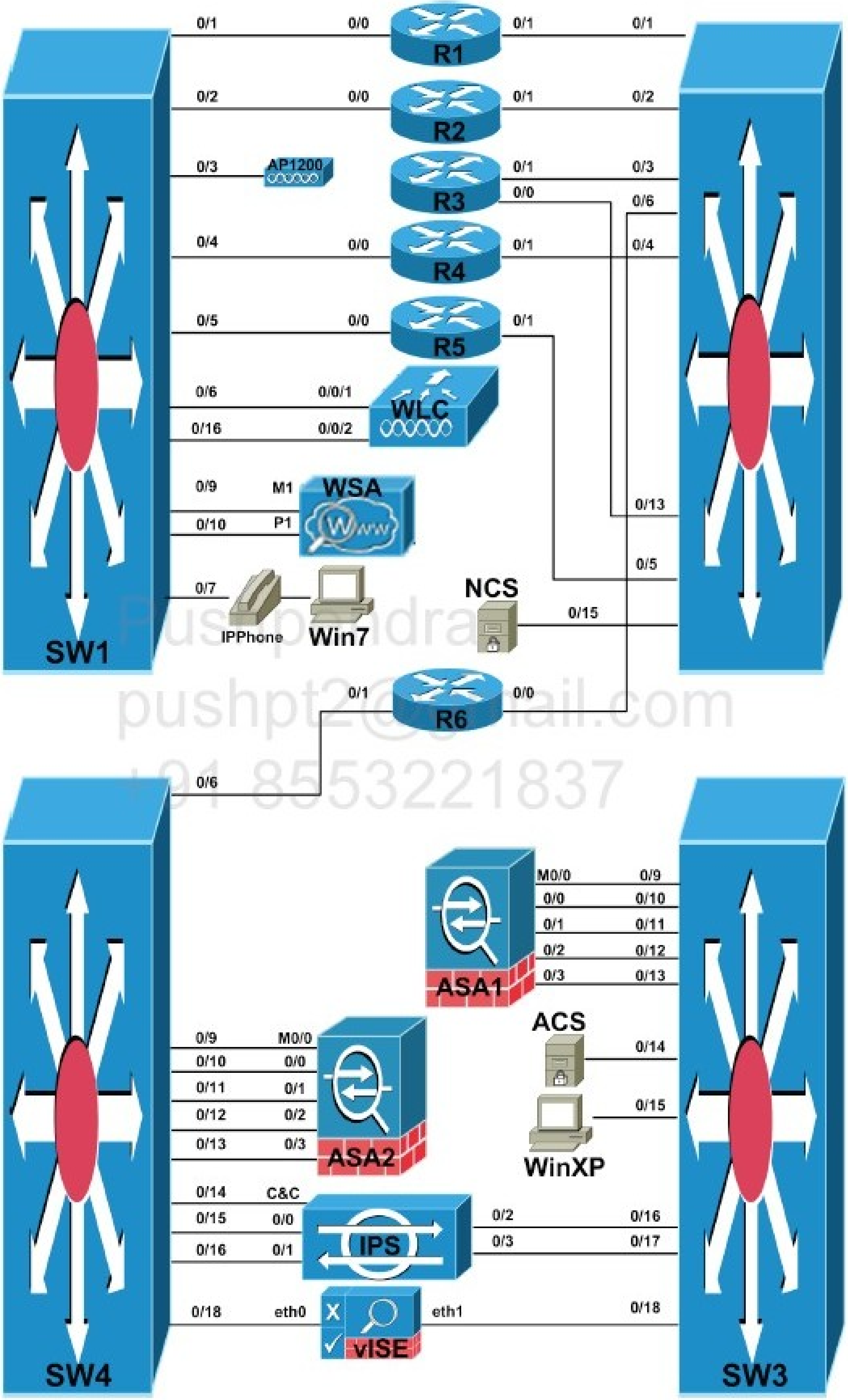
Identity Management - ISE

IOS Advanced Security

Control and Management Plane Security

Network Attacks

Physical Topology


SW1
SW3
SW4
R1
R2
R3
R4
R5
R6
AP1200
WLC
WSA
M1
P1
IPPhone
Win7
NCS
ASA1
ASA2
ACS
WinXP
IPS
C&C
vISE
eth0
eth1
0/1
0/0
0/1
0/1
0/2
0/0
0/1
0/2
0/3
0/1
0/3
0/0
0/6
0/4
0/0
0/1
0/4
0/5
0/0
0/1
0/6
0/0/1
0/16
0/0/2
0/9
0/10
0/13
0/5
0/7
0/15
0/1
0/0
0/6
M0/0
0/9
0/0
0/10
0/1
0/11
0/2
0/12
0/3
0/13
0/14
0/15
0/9
M0/0
0/10
0/0
0/11
0/1
0/12
0/2
0/13
0/3
0/14
0/15
0/0
0/16
0/1
0/2
0/16
0/3
0/17
0/18
0/18

This page is intentionally left blank.

Advanced
CCIE SECURITY v4
LAB WORKBOOK

Identity Management

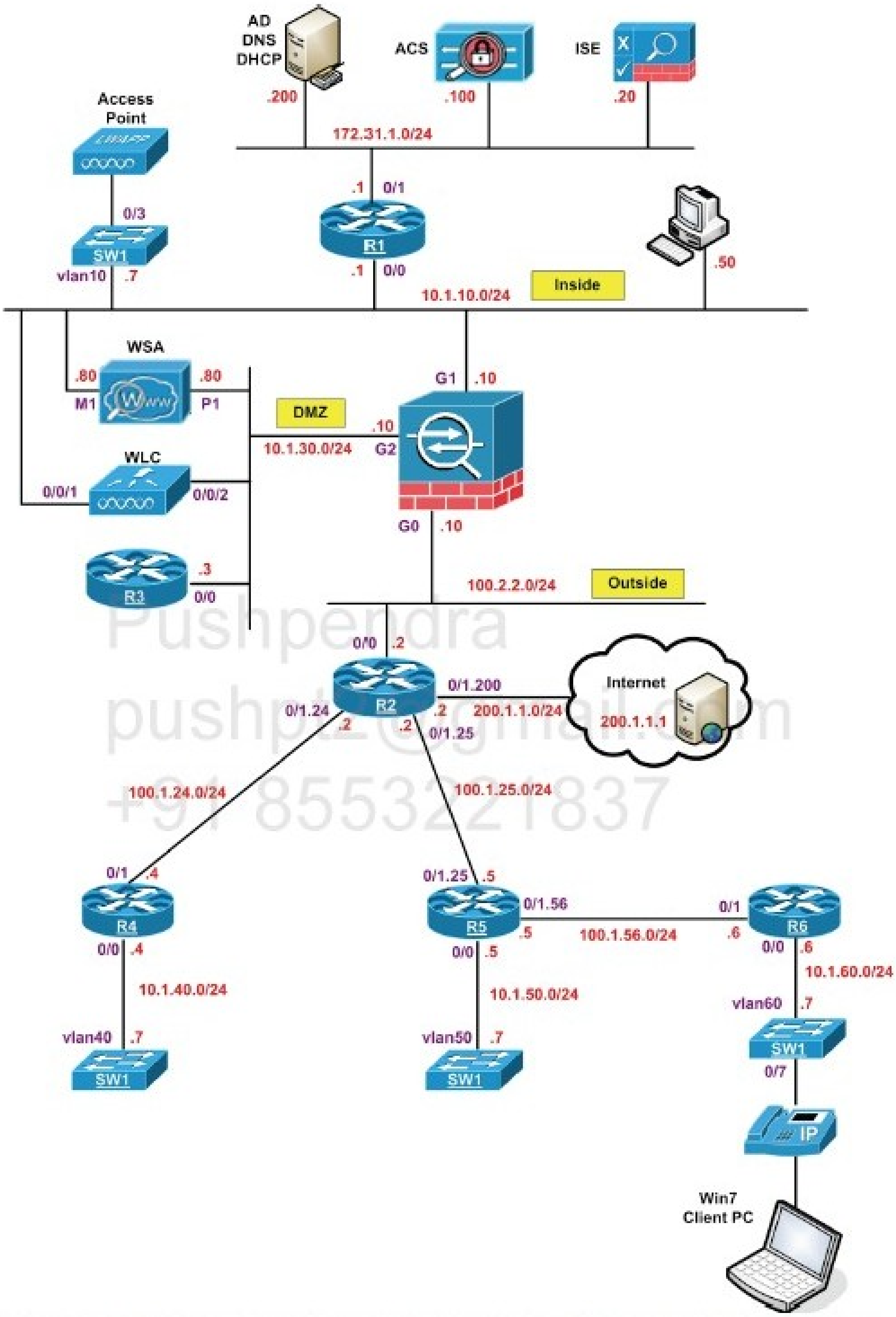
ISE

Narbik Kocharians
CCIE #12410 (R&S, Security, SP)
CCSI #30832

Piotr Matusiak
CCIE #19860 (R&S, Security)
C|EH, CCSI #33705

www.MicronicsTraining.com

Logical Topology for ISE labs



ISE v1.1 is connected to the network behind Router1 and has IP address of 172.31.1.20. Default gateway should be set to R1.

Management access to ISE should be allowed from WinXP PC (10.1.10.50).

LAB 3.1. ISE Installation (optional)

Objectives

This lab introduces Identity Service Engine v1.1 and verifies basic connectivity with other network elements.

IP Addressing and devices

Device	Interface	IP address
ISE	NIC	172.31.1.20
R1	Lo0 E0/0 E0/1	1.1.1.1/32 10.1.10.1/24 172.31.1.1/24
R2	Lo0 E0/0	2.2.2.2/32 100.2.2.2/24
WinXP	NIC	10.1.10.50/24

This is an optional task. If the ISE is already pre-installed, you can go directly to next task.

Task

Perform ISE installation and bootstrapping. Provide the following information during the installation process:

- Hostname: ISE
- IP Address and mask: 172.31.1.20/24
- Default gateway: 172.31.1.1
- Domain name and nameserver: micronics.local, 172.31.1.200
- NTP server and timezone: 172.31.1.200, UTC

Configuration

Complete these steps:

Step 1 Log into the ISE Virtual Appliance console (if you have access to it). You should see the following prompt:

```
**********************************************
Please type 'setup' to configure the appliance
**********************************************
localhost login:
```

Enter **setup** as a username to start configuration wizard.

Step 2 Go through the configuration wizard.

```
Press 'Ctrl-C' to abort setup
Enter hostname[]: ise
Enter IP address []: 172.31.1.20
Enter IP default netmask[]: 255.255.255.0
Enter IP default gateway[]: 172.31.1.1
Enter default DNS domain[]: micronics.local
Enter Primary nameserver[]: 172.31.1.200
Add secondary nameserver? Y/N [N]: <enter>
Enter Primary NTP server[time.nist.gov]: 172.31.1.1
Add another NTP server? Y/N [N]: <enter>
Enter system timezone[UTC]: <enter>
Enter username[admin]: <enter>
Enter password: Micronics1
Enter password again: Micronics1

Bringing up network interface...
Pinging the gateway...
Pinging the primary nameserver ...
Virtual machine detected, configuring VMware tools...
Do not use 'Ctrl-C' from this point on...
Appliance is configured Installing applications...
Installing ise ...
The mode has been set to licensed.
```

Step 3 ISE installation. Provide passwords for ISE databased during installation.

```
Application bundle (ise) installed successfully
=== Initial Setup for Application: ise ===
Welcome to the ISE initial setup. The purpose of this setup is
to provision the internal ISE database. This setup requires
you create a database administrator password and also create a
database user password.
Please follow the prompts below to create the database
administrator password.
Enter new database admin password: Micronics1234
Confirm new database admin password: Micronics1234
Successfully created database administrator password.
Please follow the prompts below to create the data base user
password:
Enter new database user password: Micronics1234
Confirm new Database user password: Micronics1234
Successfully created database user password.
Running database cloning script...
Running database network config assistant tool...
Extracting ISE database content...
Starting ISE database processes...
Creating ISE M&T session directory...
Performing ISE database priming...
Generating configuration...
Rebooting...
```

Verification

Connect to ISE using SSH and provide username/password of **admin/Micronics1**. Check and note the following:

- ISE application version
- ISE daemon status
- Interface configuration
- Routing table (with default gateway)
- Clock configuration
- Timezone configuration

Connect to the GUI from WinXP desktop and check license and ISE deployment options.

Run Putty and connect using SSH to IP address of 172.31.1.20

Verify that ISE is installed properly

Cisco ISE is an application installed on underlying operating system called Cisco ADE. Once you're connected to ADE you must check what applications are installed. Then you can use application name (in our case 'ise) in all other commands.

```
ISE/admin# show application
<name>          <Description>
ise             Cisco Identity Services Engine
ISE/admin#
```

Check ISE version

```
ISE/admin# show application version ise

Cisco Identity Services Engine
---------------------------------------------
Version      : 1.1.0.665
Build Date   : Wed Mar  7 22:51:03 2012
Install Date : Wed Jan  2 17:12:33 2013
```

The main version is 1.1 and the patch level is 665. The build depends on the development stage. By default ISE is in EVAL mode for 90 days. You can install production license or use evaluation license. You do not need to provide any license file for ISE to be working.

Check status of ISE processes

```
ISE/admin# show application status ise

ISE Database listener is running, PID: 4166
ISE Database is running, number of processes: 26
ISE Application Server is running, PID: 5694
ISE M&T Session Database is running, PID: 3826
ISE M&T Log Collector is running, PID: 5921
ISE M&T Log Processor is running, PID: 6005
ISE M&T Alert Process is running, PID: 5840
% WARNING: ISE DISK SIZE NOT LARGE ENOUGH FOR PRODUCTION USE
% RECOMMENDED DISK SIZE: 200 GB, CURRENT DISK SIZE: 64 GB
```

If there is other status than 'is running' it means theres something wrong with a particular ISE subsystem/process. To fix that you can try to restart ISE application using 'application stop ise' and then 'application start ise'. Be patient as it may take a while to start all ISE processes.

Check interface configuration and verify IP address and netmask

```
ISE/admin# show interface
GigabitEthernet 0
        Link encap:Ethernet  HWaddr 00:50:56:AE:A1:34
          inet addr:172.31.1.20  Bcast:172.31.1.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:feae:a134/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:70970 errors:0 dropped:0 overruns:0 frame:0
          TX packets:90676 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8304352 (7.9 MiB)  TX bytes:15921119 (15.1 MiB)
          Interrupt:59 Base address:0x2024

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:29034318 errors:0 dropped:0 overruns:0 frame:0
          TX packets:29034318 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:501930492 (478.6 MiB)  TX bytes:501930492 (478.6 MiB)

sit0      Link encap:IPv6-in-IPv4
          NOARP  MTU:1480  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
```

Make sure that you see RX and TX packets and no error counters increasing. This is the first indicator that something can be wrong with connectivity. If you do not see GigabitEhernet0 interface that usually means the interface is down.
You may see more interfaces depending on ISE installation. Some interfaces may be used for profiling services.

Check routing table and default gateway

```
ISE/admin# show ip route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
172.31.1.0      0.0.0.0         255.255.255.0   U     0      0        0 eth0
0.0.0.0         172.31.1.1      0.0.0.0         UG    0      0        0 eth0
```

Note that there is still interface 'eth0' in the command output. This interface is a pointer to GigabitEthernet0.

Check basic connectivity to the gateway and to other network elements

```
ISE/admin# ping 172.31.1.1
PING 172.31.1.1 (172.31.1.1) 56(84) bytes of data.
64 bytes from 172.31.1.1: icmp_seq=1 ttl=255 time=0.853 ms
64 bytes from 172.31.1.1: icmp_seq=2 ttl=255 time=0.810 ms
64 bytes from 172.31.1.1: icmp_seq=3 ttl=255 time=0.776 ms
64 bytes from 172.31.1.1: icmp_seq=4 ttl=255 time=0.886 ms

--- 172.31.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.776/0.831/0.886/0.046 ms

ISE/admin# ping 10.1.10.10
PING 10.1.10.10 (10.1.10.10) 56(84) bytes of data.
64 bytes from 10.1.10.10: icmp_seq=1 ttl=254 time=67.9 ms
64 bytes from 10.1.10.10: icmp_seq=2 ttl=254 time=1.17 ms
64 bytes from 10.1.10.10: icmp_seq=3 ttl=254 time=16.3 ms
64 bytes from 10.1.10.10: icmp_seq=4 ttl=254 time=57.0 ms

--- 10.1.10.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 1.172/35.622/67.910/27.663 ms
```

You may not reach ASa firewall at this stage. If not, check if ASA has static route to 172.31.1.0/24 network configured.

```
ISE/admin# ping 10.1.10.50
PING 10.1.10.50 (10.1.10.50) 56(84) bytes of data.
64 bytes from 10.1.10.50: icmp_seq=1 ttl=127 time=0.862 ms
64 bytes from 10.1.10.50: icmp_seq=2 ttl=127 time=0.909 ms
64 bytes from 10.1.10.50: icmp_seq=3 ttl=127 time=1.00 ms
64 bytes from 10.1.10.50: icmp_seq=4 ttl=127 time=0.896 ms

--- 10.1.10.50 ping statistics ---
```

```
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 0.862/0.917/1.004/0.064 ms
```

Check the name server and domain configuration. Verify if DNS works asking to resolve FQDN of **ise.micronics.local**

```
ISE/admin# show running-config | inc name
hostname ISE
ip domain-name micronics.local
ip name-server 172.31.1.200
username admin password hash $1$pAzQ9DDO$zWBNlRgM8m1mlZPZLRh0Y1 role admin
  no-username

ISE/admin# ping 172.31.1.200
PING 172.31.1.200 (172.31.1.200) 56(84) bytes of data.
64 bytes from 172.31.1.200: icmp_seq=1 ttl=128 time=0.345 ms
64 bytes from 172.31.1.200: icmp_seq=2 ttl=128 time=0.348 ms
64 bytes from 172.31.1.200: icmp_seq=3 ttl=128 time=0.382 ms
64 bytes from 172.31.1.200: icmp_seq=4 ttl=128 time=0.417 ms

--- 172.31.1.200 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.345/0.373/0.417/0.029 ms

ISE/admin# nslookup ise.micronics.local
Trying "ise.micronics.local"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47970
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;ise.micronics.local.           IN      ANY

;; ANSWER SECTION:
ise.micronics.local.    3600    IN      A       172.31.1.20

Received 53 bytes from 172.31.1.200#53 in 1 ms
```

Check clock and timezone configuration

```
ISE/admin# show clock
Fri Jan 18 14:02:13 UTC 2013

ISE/admin# show timezone
UTC
```

If there is a different timezone configured you can always change it to the correct value using 'clock timezone UTC' command in the global configurtion. To check what timezone names are available use 'show timezones' command.

```
ISE/admin# show ntp
Configured NTP Servers:
  172.31.1.1

Unable to talk to NTP daemon. Is it running?

% To restart NTP do 'no ntp server' followed by 'ntp server <servername>'
```

If you experience the above issue try to reapply the NTP server configuration.

```
ISE/admin# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ISE/admin(config)# ntp server 172.31.1.1
ISE/admin(config)# end
```

NTP synchronization is very important especially when ISE is a part of Active Directory domain. If you plan to join AD then clock between Domain Controller and ISE must be synchronized. The NTP related issues are causing most problems with AD integration.
You can also check application logs when syncing with NTP.
Note that ISE may not synchronize with a source that is not reliable (the source gets time from its local clock).

```
ISE/admin# show ntp
Configured NTP Servers:
  172.31.1.1

unsynchronised
  time server re-starting
   polling server every 64 s

     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 127.127.1.0     .LOCL.          10 l    3   64    1    0.000    0.000   0.001
 172.31.1.1      LOCAL(1)         8 u    2   64    1    0.930   -0.146   0.001

* Current time source, + Candidate

Warning: Output results may conflict during periods of changing synchronization.
```

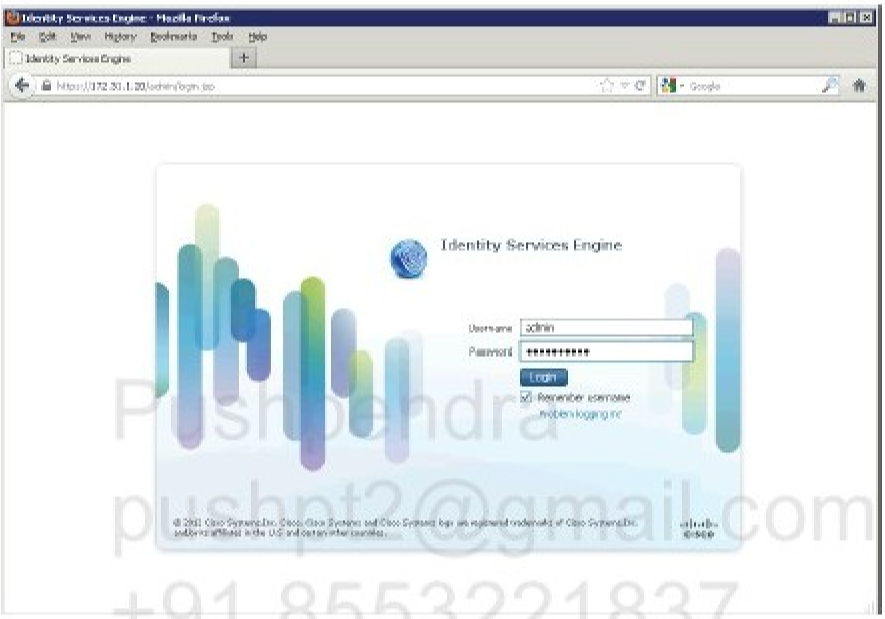
<after a while>

```
ISE/admin# show ntp
Configured NTP Servers:
  172.31.1.1

synchronised to NTP server (172.31.1.1) at stratum 9
   time correct to within 944 ms
   polling server every 64 s

     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 127.127.1.0     .LOCL.          10 l   29   64   77    0.000    0.000   0.001
```

```
*172.31.1.1      LOCAL(1)        8 u   26   64   77    0.778    0.357   0.529

* Current time source, + Candidate

Warning: Output results may conflict during periods of changing synchronization.
```

Connect through the GUI and check license. Open up web browser (IE or FF) and enter the following URL https://172.31.1.20

- Authenticate as **admin/Micronics1**.

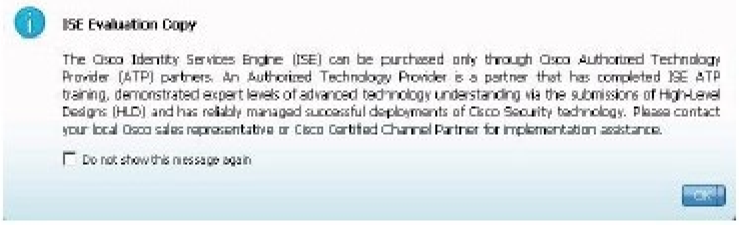


Identity Services Engine - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Identity Services Engine
https://172.31.1.20/admin/login.jsp
Identity Services Engine

Username admin
Password ••••••••••••

Login
☑ Remember username
Problem logging in?

- You may see the following message while connecting to the ISE for the first time.

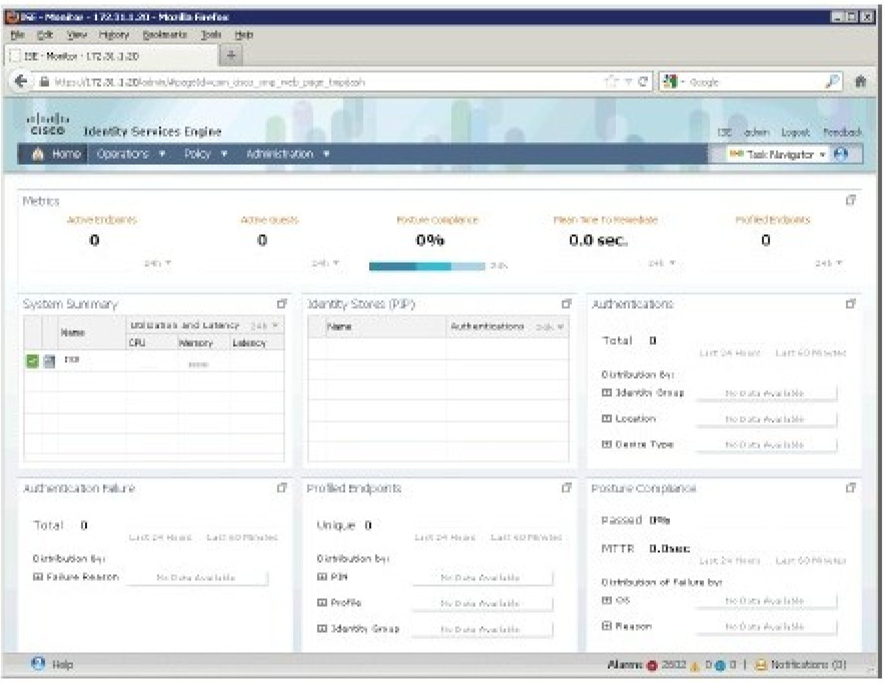


ISE Evaluation Copy

The Cisco Identity Services Engine (ISE) can be purchased only through Cisco Authorized Technology Provider (ATP) partners. An Authorized Technology Provider is a partner that has completed ISE ATP training, demonstrated expert levels of advanced technology understanding via the submissions of High-Level Designs (HLD) and has reliably managed successful deployments of Cisco Security technology. Please contact your local Cisco sales representative or Cisco Certified Channel Partner for implementation assistance.

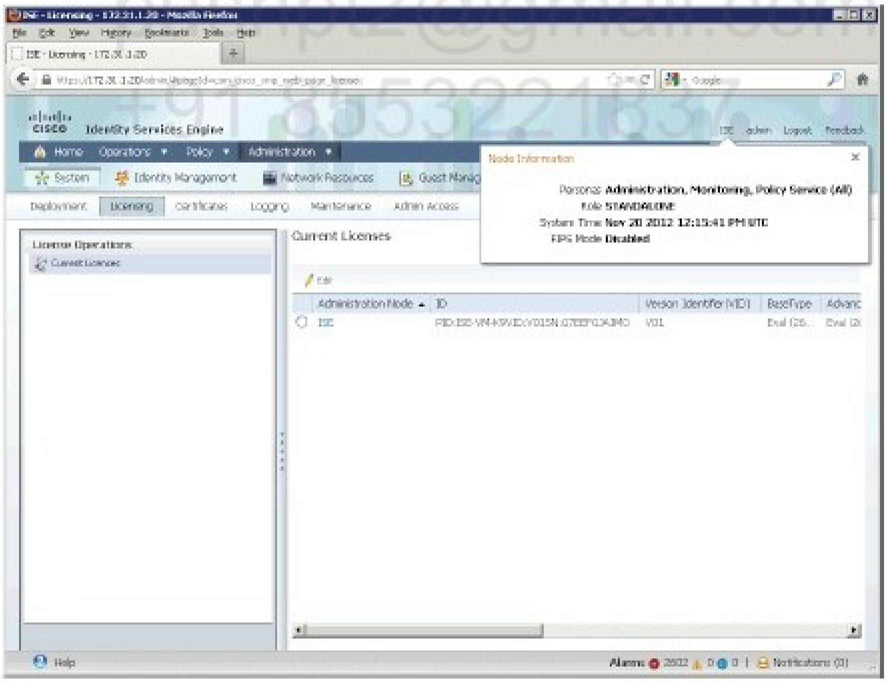
☐ Do not show this message again

- Pick **Do not show this message again** and then click **OK**.



Metrics: Active Endpoints 0, Active Guests 0, Posture Compliance 0%, Mean Time To Remediate 0.0 sec., Profiled Endpoints 0

- Check the deployment mode by selecting **ise** on the top right of the current window. To check license you must go to **Administration -> System -> Licensing**.



Node Information

Persona: Administration, Monitoring, Policy Service (All)
Role STANDALONE
System Time Nov 20 2012 12:15:41 PM UTC
FIPS Mode Disabled

Current Licenses

	Administration Node	ID	Version Identifer (VID)	BaseType	Advanc
○	ISE	PID:ISE-VM-K9VID:V01SN:07EEF0JA3MO	V01	Eval (26...	Eval (2

LAB 3.2. Generate and install a certificate

Objectives

This lab shows how to import a certificate to ISE.

IP Addressing and devices

Device	Interface	IP address
ISE	NIC	172.31.1.20
R1	Lo0 E0/0 E0/1	1.1.1.1/32 10.1.10.1/24 172.31.1.1/24
WinXP	NIC	10.1.10.50/24

Task

Create CSR (Certificate Signig Request) on ISE and send it to Microsoft CA to issue a certificate. The CSR should have the following information:

- RSA key length: 2048
- Hashing: SHA-1
- X.509 Distinguished Name (DN):
    - Common name: ise.micronics.local
    - Organizational Unit: lab
    - Company: Micronics
    - Country: US
    - State: CA

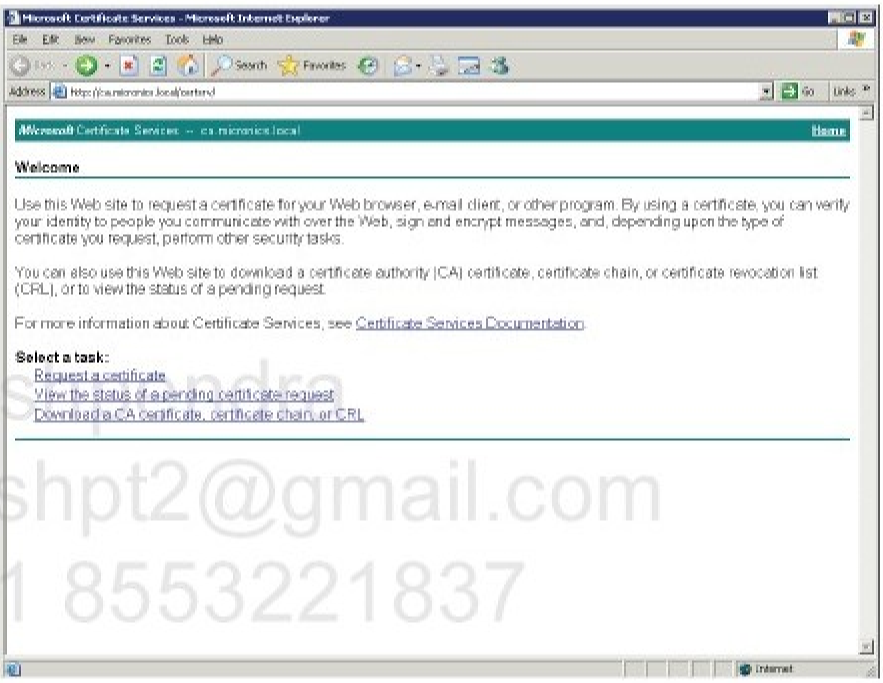
The certificate must be usable for management and EAP methods. Use Microsoft CA server at http://ca.micronics.local/certsrv to issue a certificate. To access the server use caadmin/Micronics1 user credentials.

Configuration

Complete these steps:

Step 1 Get CA Certificate and import it on ISE.

- Open up web browser (IE preferred) and go to http://ca.micronics.local/certsrv to **Download a CA certificate, certificate chain, or CRL**. To access the server use caadmin/Micronics1 user credentials.


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://ca.micronics.local/certsrv/
Go Links
Microsoft Certificate Services -- ca.micronics.local
Home
Internet

Welcome

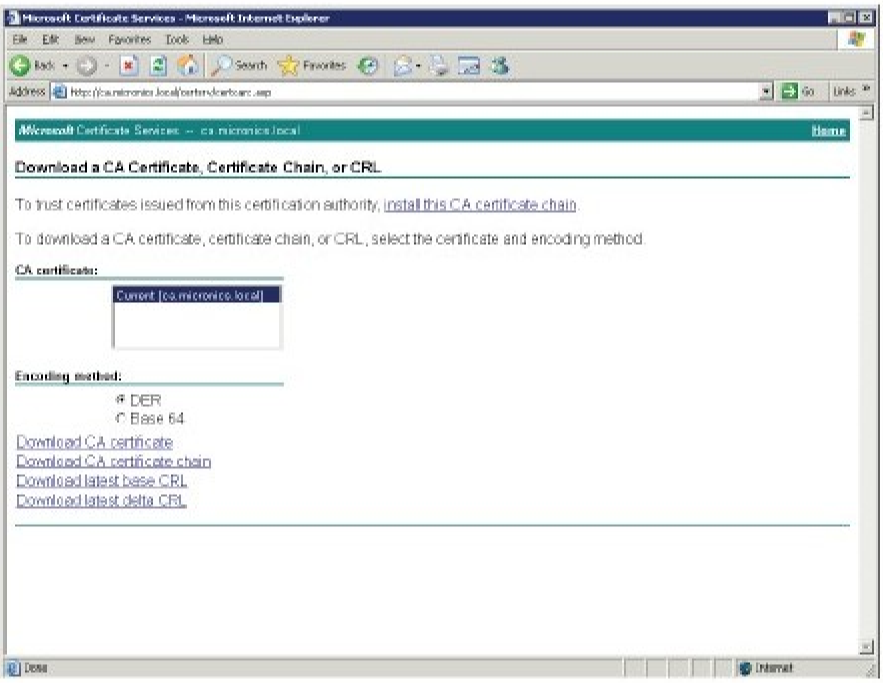
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see Certificate Services Documentation.

Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

- Click on **Download CA certificate** link and save the file as **ca-cert.cer**



Microsoft Certificate Services -- ca.micronics.local

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate chain.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current [ca.micronics.local]

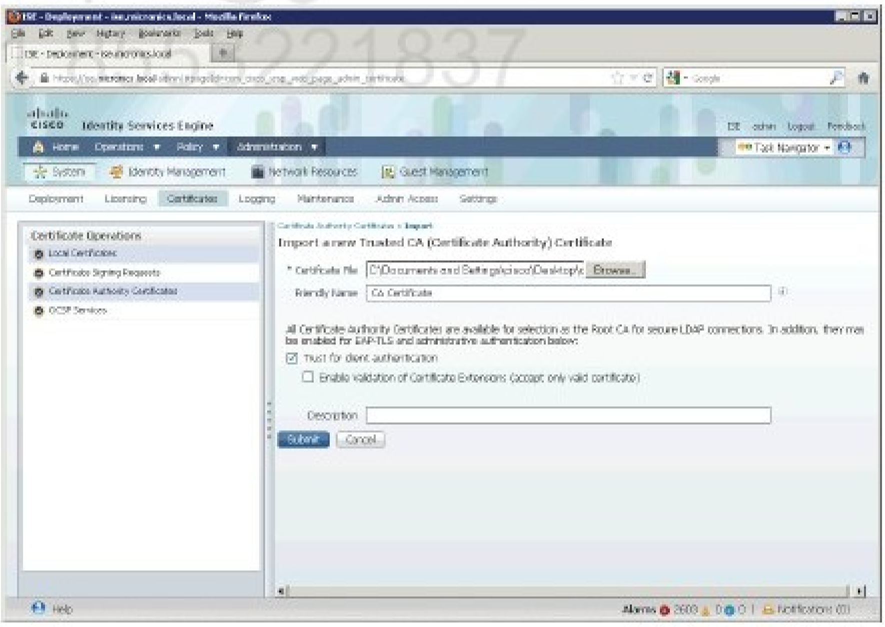
Encoding method:

● DER
○ Base 64

Download CA certificate
Download CA certificate chain
Download latest base CRL
Download latest delta CRL

Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://ca.micronics.local/certsrv/certcarc.asp
Go Links
Home
Done
Internet

- Go to ISE **Administration > System > Certificates > Certificate Authority Certificates** and click **Import**. Select **ca-cert.cer** file and pick **trust for client authentication** checkbox. Click **Submit**.



Certificate Authority Certificates > Import

Import a new Trusted CA (Certificate Authority) Certificate

* Certificate File: C:\Documents and Settings\cisco\Desktop\c

Friendly Name: CA Certificate

All Certificate Authority Certificates are available for selection as the Root CA for secure LDAP connections. In addition, they may be enabled for EAP-TLS and administrative authentication below:

☑ Trust for client authentication

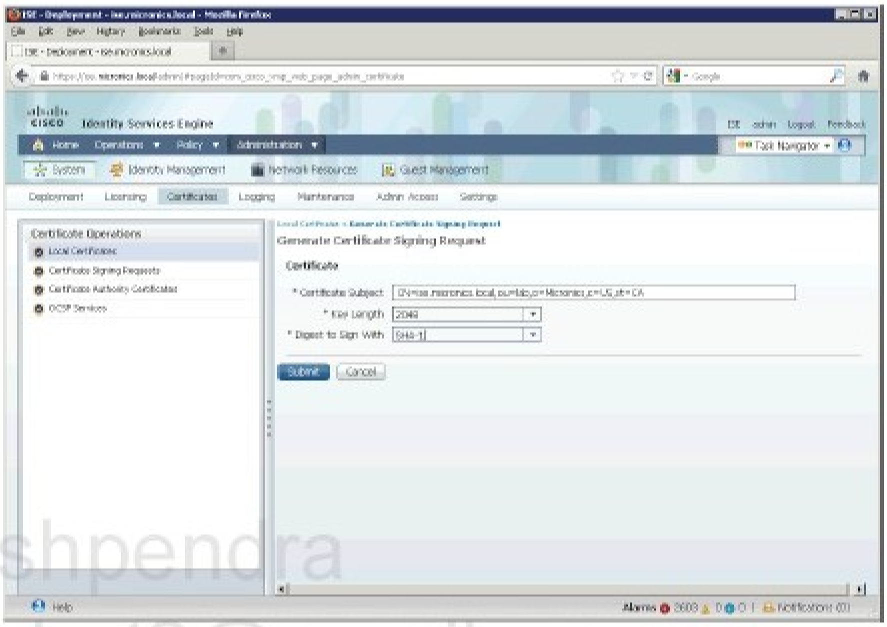
□ Enable Validation of Certificate Extensions (accept only valid certificate)

Description:

ISE - Deployment - ise.micronics.local - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Identity Services Engine
ISE admin Logout Feedback
Home Operations Policy Administration
Task Navigator
System Identity Management Network Resources Guest Management
Deployment Licensing Certificates Logging Maintenance Admin Access Settings
Certificate Operations
Local Certificates
Certificate Signing Requests
Certificate Authority Certificates
OCSP Services
Browse...
Submit
Cancel
Help
Alarms 2603 0 0
Notifications (0)

Step 2 Create CSR on ISE.

- Go to ISE **Administration > System > Certificates > Local Certificates**, click **Add > Generate Certificate Signing Request** and provide **Certificate Subject** in the correct DN format. Also, pick **SHA-1** for **Digest to Sign With**.



Generate Certificate Signing Request

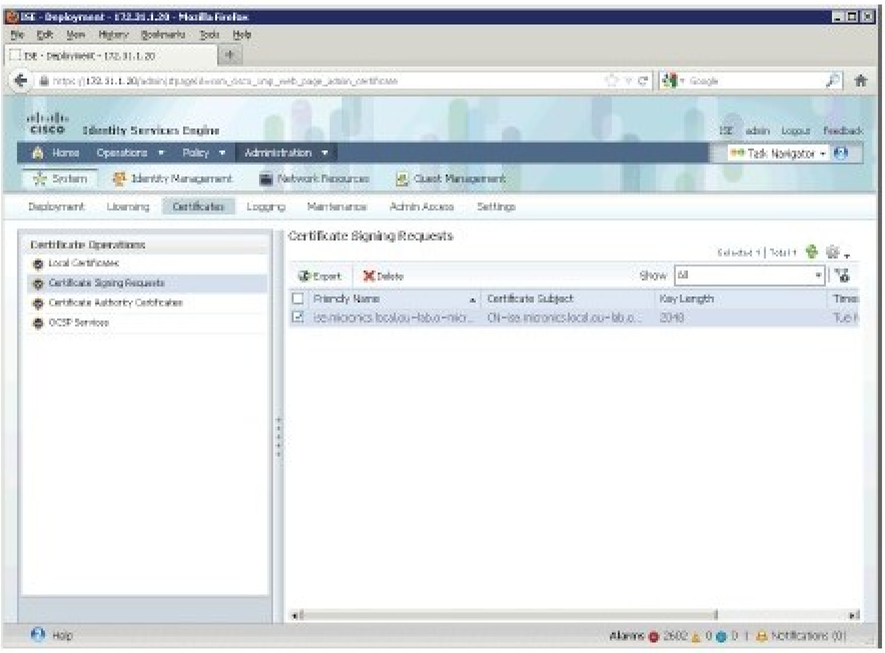
Certificate

* Certificate Subject: CN=ise.micronics.local,ou=lab,o=Micronics,c=US,st=CA

* Key Length: 2048

* Digest to Sign With: SHA-1

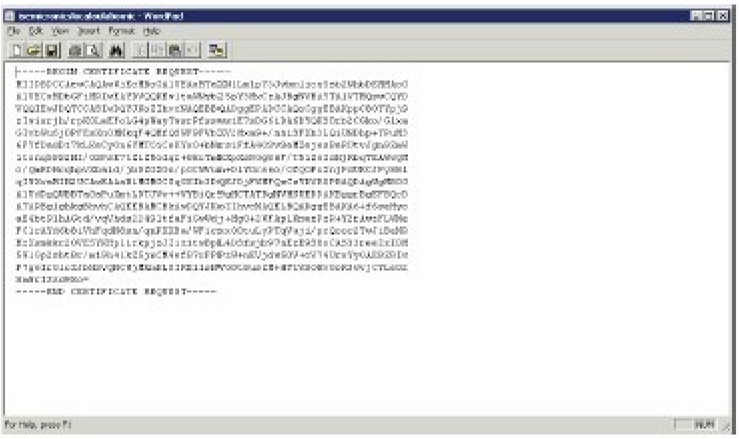
- Once CSR is generated, pick it from the list and click **Export**. Save it to the file or open directly in Wordpad.



Certificate Signing Requests

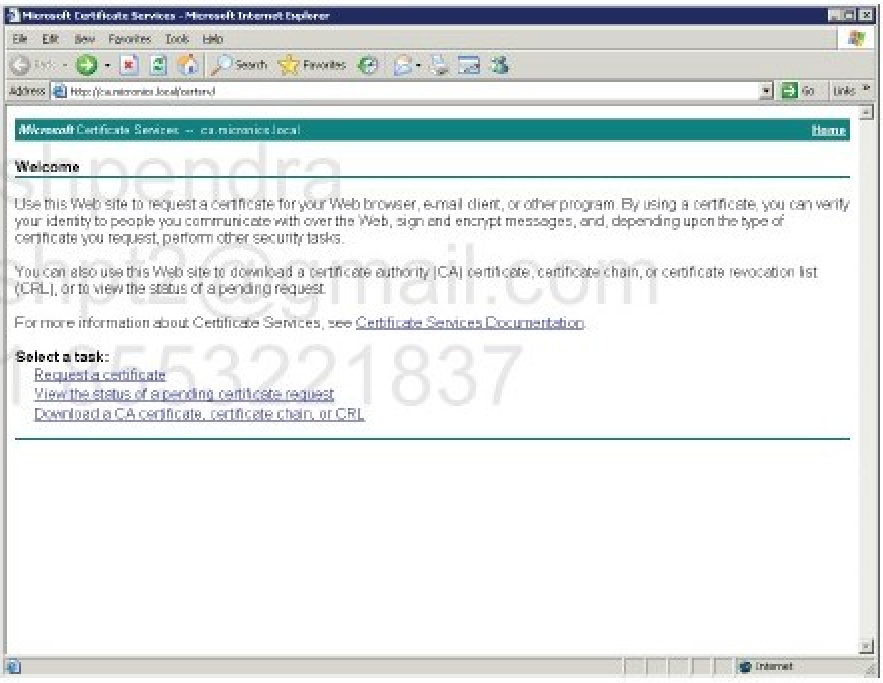
☐	Friendly Name	Certificate Subject	Key Length	Time
☑	ise.micronics.local,ou=lab,o=micr...	CN=ise.micronics.local,ou=lab,o...	2048	Tue

- Once opened, copy all text to the clipboard.



```
-----BEGIN CERTIFICATE REQUEST-----
[illegible]
-----END CERTIFICATE REQUEST-----
```

- Open up web browser (IE preferred) and go to http://ca.micronics.local/certsrv to **Request a certificate**.



Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://ca.micronics.local/certsrv/
Go Links
Internet

Microsoft Certificate Services -- ca.micronics.local **Home**

Welcome

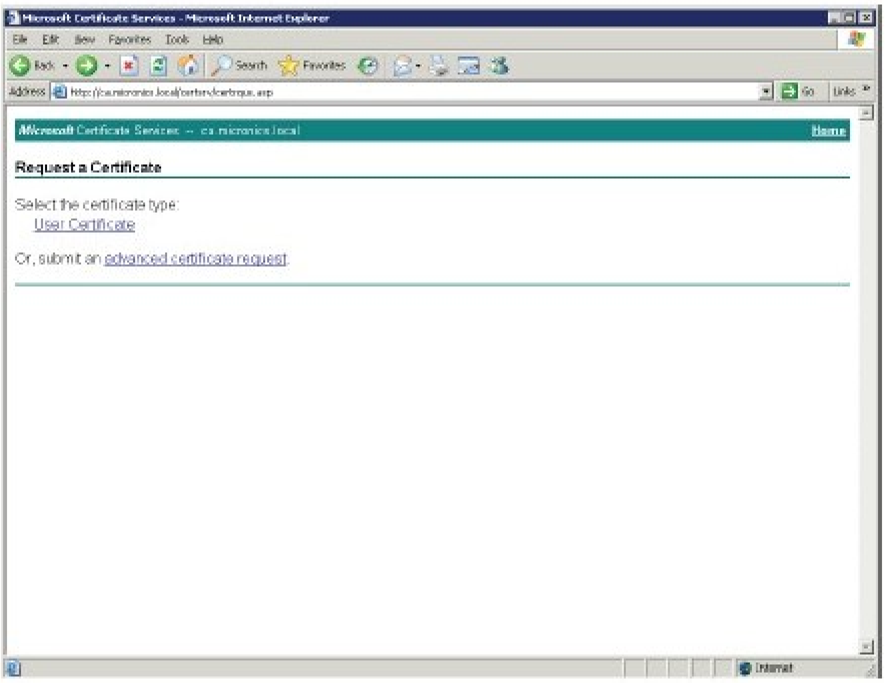
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see Certificate Services Documentation.

Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

- Click **advanced certificate request**.


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://ca.micronics.local/certsrv/certrqus.asp
Go Links
Home
Internet

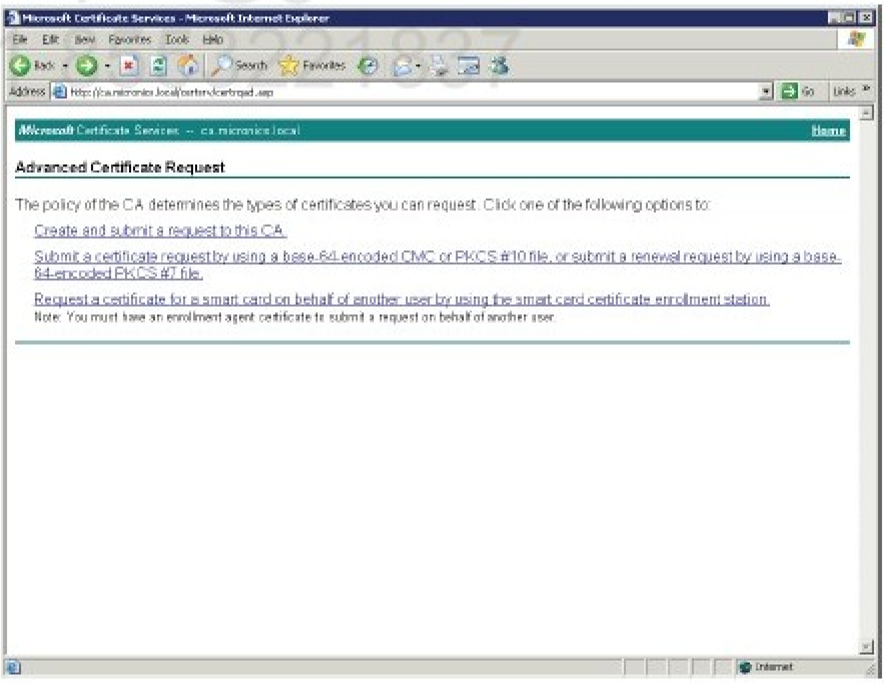
Microsoft Certificate Services -- ca.micronics.local

Request a Certificate

Select the certificate type:
User Certificate

Or, submit an advanced certificate request.

- Click **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file** link.


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://ca.micronics.local/certsrv/certrqad.asp
Go Links
Home
Internet

Microsoft Certificate Services -- ca.micronics.local

Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

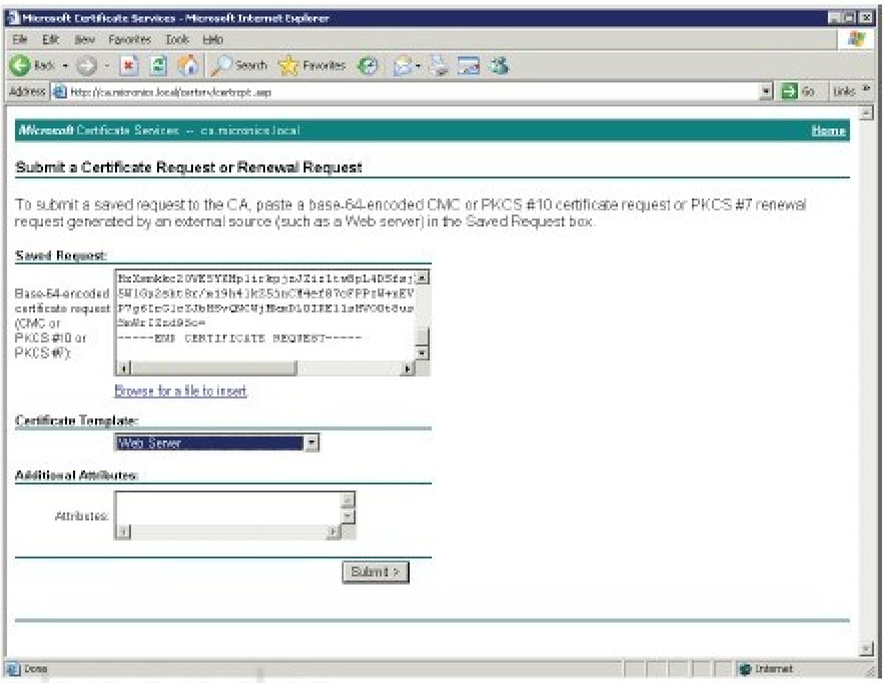
Create and submit a request to this CA.

Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station.
Note: You must have an enrollment agent certificate to submit a request on behalf of another user.

- Paste the CSR from the clipboard to **Base-64-encoded certificate request** field, chose **Web Server** as **Certificate Template** and click

Submit >.



Microsoft Certificate Services - Microsoft Internet Explorer

Address: http://ca.micronics.local/certsrv/certrqxt.asp

Microsoft Certificate Services -- ca.micronics.local

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
HzXmmkkc20VK5YXMplickpjzJZicltw8pL4D5faj
5W1Gs2skt8r/m19h4lK55nCM4ef87cFPPrW+xEV
P7g6IrGlcZJbH5vQMCWjMmmD101IE11aHVO0t6us
ZmWcI2zd95c=
-----END CERTIFICATE REQUEST-----
```

Browse for a file to insert.

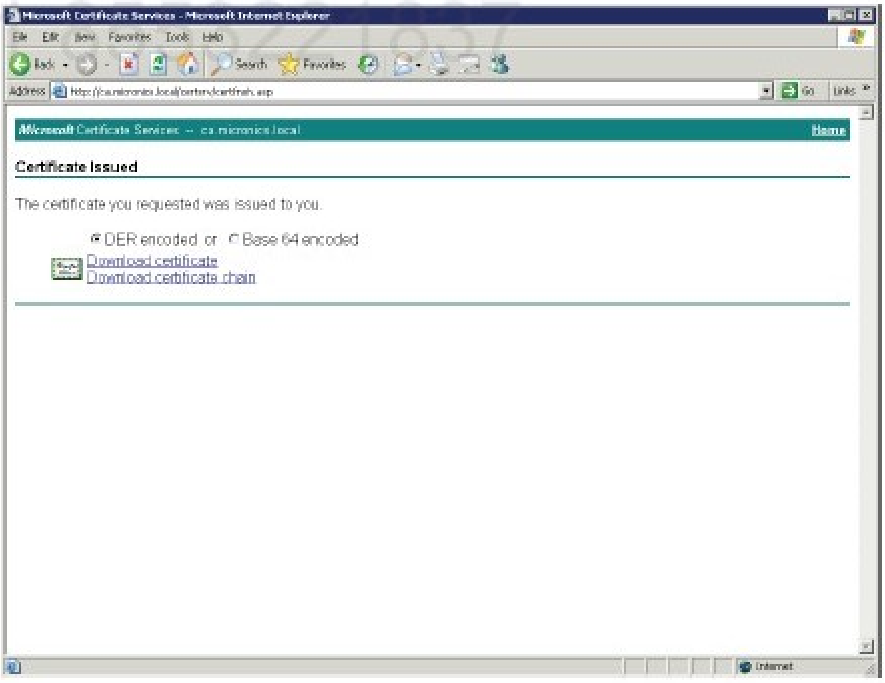
Certificate Template:

Web Server

Additional Attributes:

Attributes:

- Click on **Download certificate** with **DER encoded** option. Save it to **ise-cert.cer** file.



Microsoft Certificate Services - Microsoft Internet Explorer

Address: http://ca.micronics.local/certsrv/certfnsh.asp

Microsoft Certificate Services -- ca.micronics.local

Certificate Issued

The certificate you requested was issued to you.

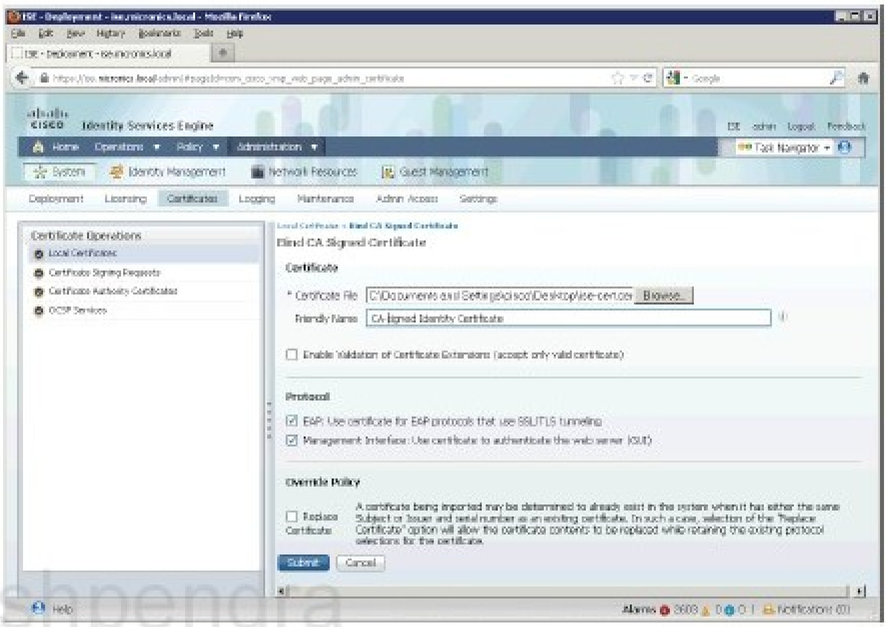
● DER encoded or ○ Base 64 encoded

Download certificate

Download certificate chain

- Go to ISE **Administration > System > Certificates > Local Certificates**, click **Add > Bind CA Signed Certificate** and provide

ise-cert.cer file. Enter a **Friendly Name** e.g. **CA-signed Identity Certificate**, pick options **EAP** and **Management Interface** and click **Submit**.



Local Certificates > Bind CA Signed Certificate

Bind CA Signed Certificate

Certificate

* Certificate File: C:\Documents and Settings\cisco\Desktop\ise-cert.cer

Friendly Name: CA-signed Identity Certificate

□ Enable Validation of Certificate Extensions (accept only valid certificate)

Protocol

☑ EAP: Use certificate for EAP protocols that use SSL/TLS tunneling

☑ Management Interface: Use certificate to authenticate the web server (GUI)

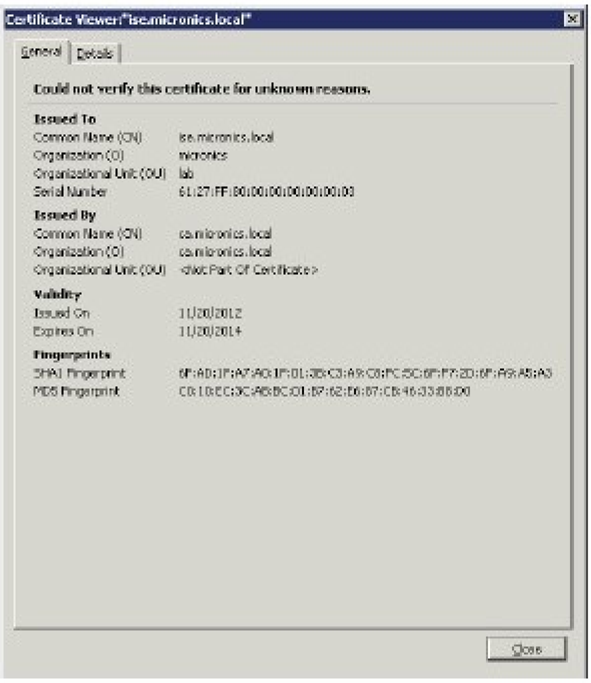
Override Policy

□ Replace Certificate — A certificate being imported may be determined to already exist in the system when it has either the same Subject or Issuer and serial number as an existing certificate. In such a case, selection of the "Replace Certificate" option will allow the certificate contents to be replaced while retaining the existing protocol selections for the certificate.

- Certificate should be imported successfuly and ISE should be restarted. You will be disconnected from the GUI. Try to reconnect after a while. Meanwhile you can check **show application status ise** command output to see the ISE restarting.

Verification

Restart the web browser and check if ISE provides new certificate to the client.



Certificate Viewer:"ise.micronics.local"

Could not verify this certificate for unknown reasons.

Issued To

Common Name (CN)	ise.micronics.local
Organization (O)	micronics
Organizational Unit (OU)	lab
Serial Number	61:27:FF:80:00:00:00:00:00:03

Issued By

Common Name (CN)	ca.micronics.local
Organization (O)	ca.micronics.local
Organizational Unit (OU)	<Not Part Of Certificate>

Validity

Issued On	11/20/2012
Expires On	11/20/2014

Fingerprints

SHA1 Fingerprint	6F:AD:1F:A7:AC:1F:01:3B:C3:A9:C8:FC:5C:6F:F7:2D:6F:A9:A5:A3
MD5 Fingerprint	C8:10:EC:3C:A6:BC:01:B7:62:E6:87:CB:46:33:88:D0

LAB 3.3. Administrative access to ISE

Objectives

This lab shows how to setup an administrative access to ISE.

IP Addressing and devices

Device	Interface	IP address
ISE	NIC	172.31.1.20
R1	Lo0	1.1.1.1/32
	E0/0	10.1.10.1/24
	E0/1	172.31.1.1/24
WinXP	NIC	10.1.10.50/24

Task

Configure the following settings for administrative access to the ISE:

- Access is allowed from the WinXP management station only
- Idle session timeout set to 30 minutes

Create **helpdesk** administrative user with a password of Help123 and access to **Operations** menu only. You can use pre-configured user settings.

Set the following password policy for all accounts created on the ISE:

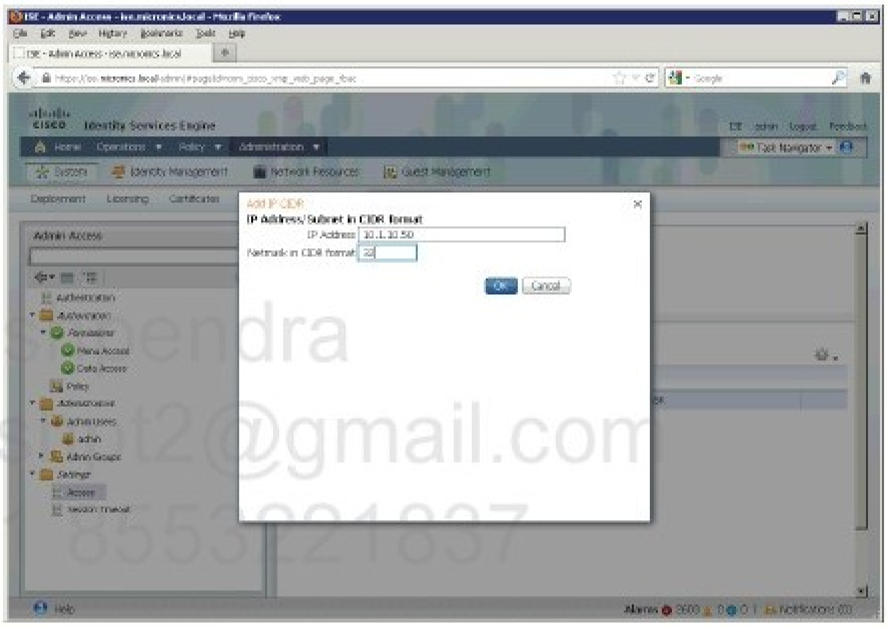
- Minimum password length is 6 characters
- Password must not contain the admin name nor words like 'cisco' and 'test'
- Password must contain at least one lowercase alphabetic character and one numeric character
- The admin account should not be disabled automatically

Configuration

Complete these steps:

Step 1 Limit the administrative access to ISE from management workstation only.

- Go to **Administration > System > Admin Access > Settings > Access** and click **Allow only listed IP addresses to connect**. Then click **Add** and provide the following settings. Then click **OK**.



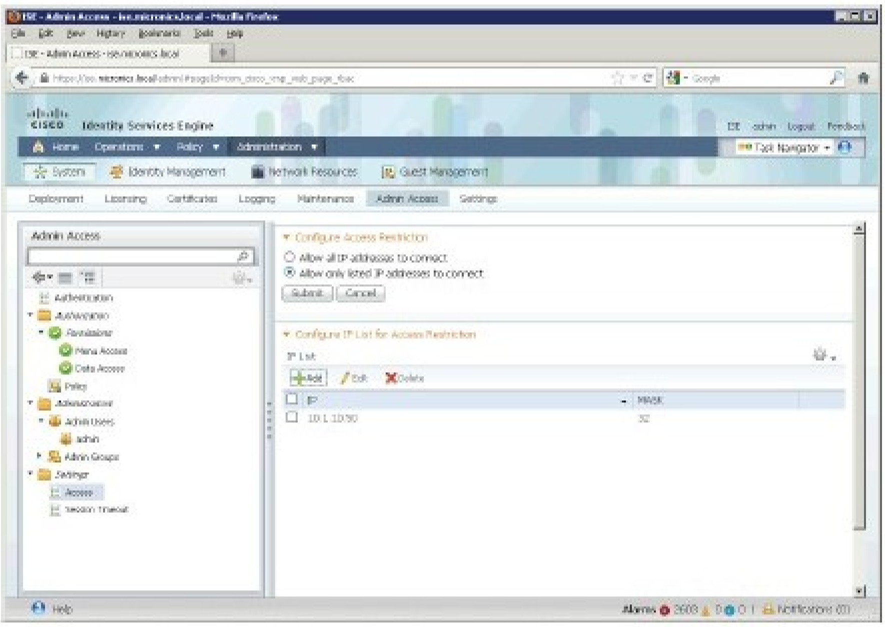
Add IP CIDR

IP Address/Subnet in CIDR format

IP Address: 10.1.10.50

Netmask in CIDR format: 32

- Click **Submit**.



Configure Access Restriction

○ Allow all IP addresses to connect
● Allow only listed IP addresses to connect

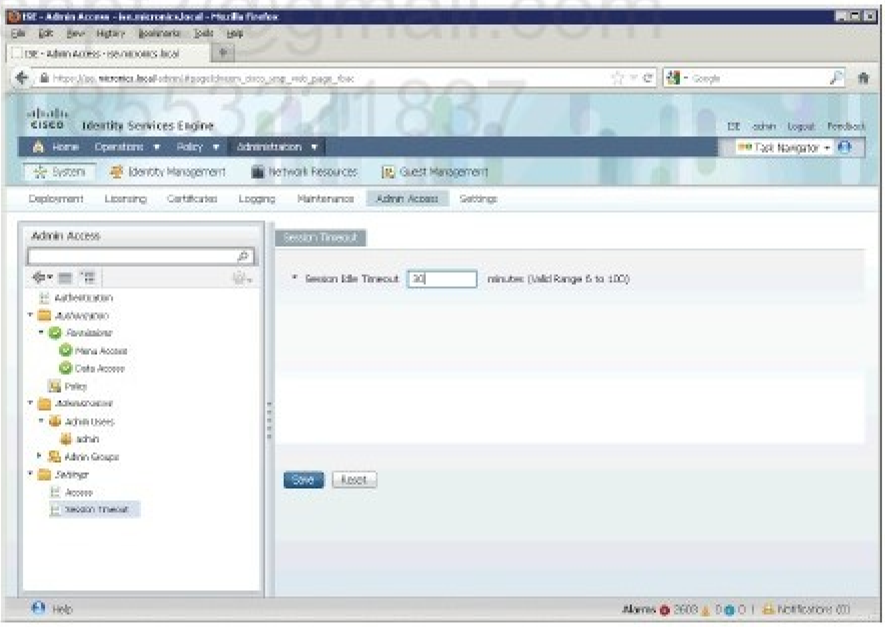
Submit Cancel

Configure IP List for Access Restriction

IP List

IP	MASK
10.1.10.50	32

- Go to **Administration > System > Admin Access > Settings > Session Timeout** and set it to 30 minutes. Click **Save**.



Session Timeout

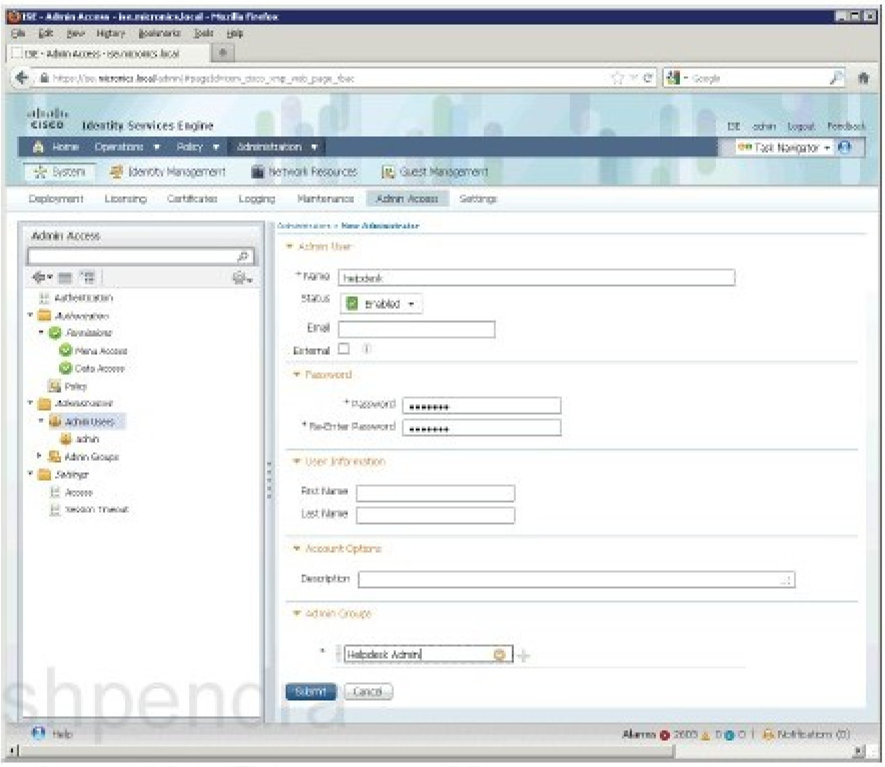
* Session Idle Timeout 30 minutes (Valid Range 6 to 100)

Save Reset

Step 2 Create **helpdesk** user.

- Go to **Administration > System > Admin Access > Administrators > Admin Users** and click **Add > Create an Admin User**. Provide **Name**, password and select **Helpdesk Admin** for **Admin Groups**.

Click **Submit**.



Administrators > New Administrator

Admin User

* Name: helpdesk

Status: Enabled

Email:

External: □

Password

* Password: •••••••

* Re-Enter Password: •••••••

User Information

First Name:

Last Name:

Account Options

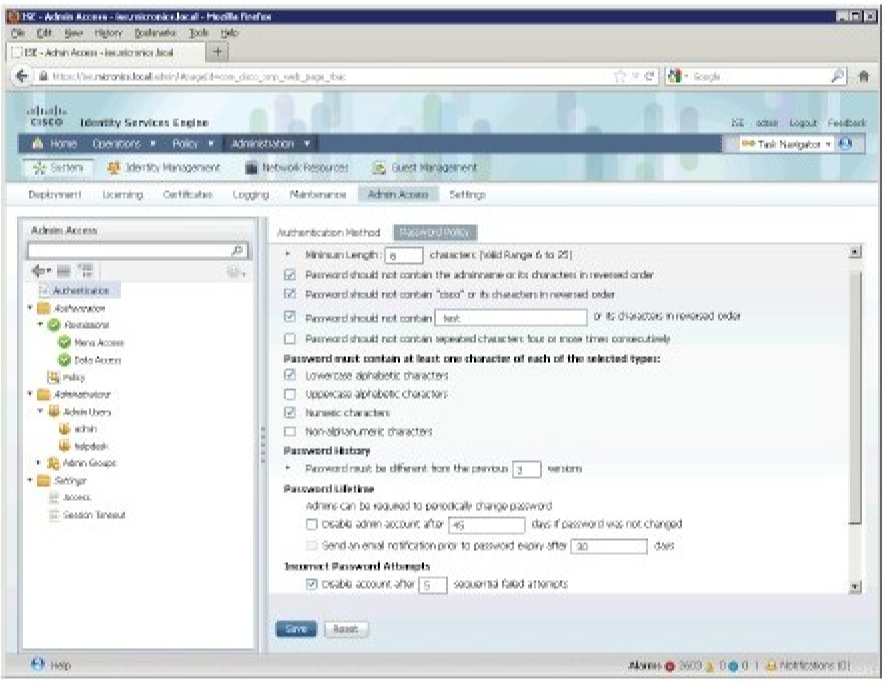
Description:

Admin Groups

* Helpdesk Admin

Step 3 Set up password policy.

- Go to **Administration > System > Admin Access > Authentication > Password Policy (tab)**. Change all required options as shown below. Click **Save**.


ISE - Admin Access - ise.micronics.local - Mozilla Firefox
Identity Services Engine
ISE admin Logout Feedback
Home Operations Policy Administration
Task Navigator
System Identity Management Network Resources Guest Management
Deployment Licensing Certificates Logging Maintenance Admin Access Settings
Admin Access
Authentication
Authorization
Permissions
Menu Access
Data Access
Policy
Administrators
Admin Users
admin
helpdesk
Admin Groups
Settings
Access
Session Timeout
Authentication Method
Password Policy
Save
Reset
Help
Alarms 2603 0 0 1 Notifications (0)

- Minimum Length: 6 characters (Valid Range 6 to 25)

☑ Password should not contain the adminname or its characters in reversed order

☑ Password should not contain "cisco" or its characters in reversed order

☑ Password should not contain test or its characters in reversed order

□ Password should not contain repeated characters four or more times consecutively

Password must contain at least one character of each of the selected types:

☑ Lowercase alphabetic characters

□ Uppercase alphabetic characters

☑ Numeric characters

□ Non-alphanumeric characters

Password History

- Password must be different from the previous 3 versions

Password Lifetime

Admins can be required to periodically change password

□ Disable admin account after 45 days if password was not changed

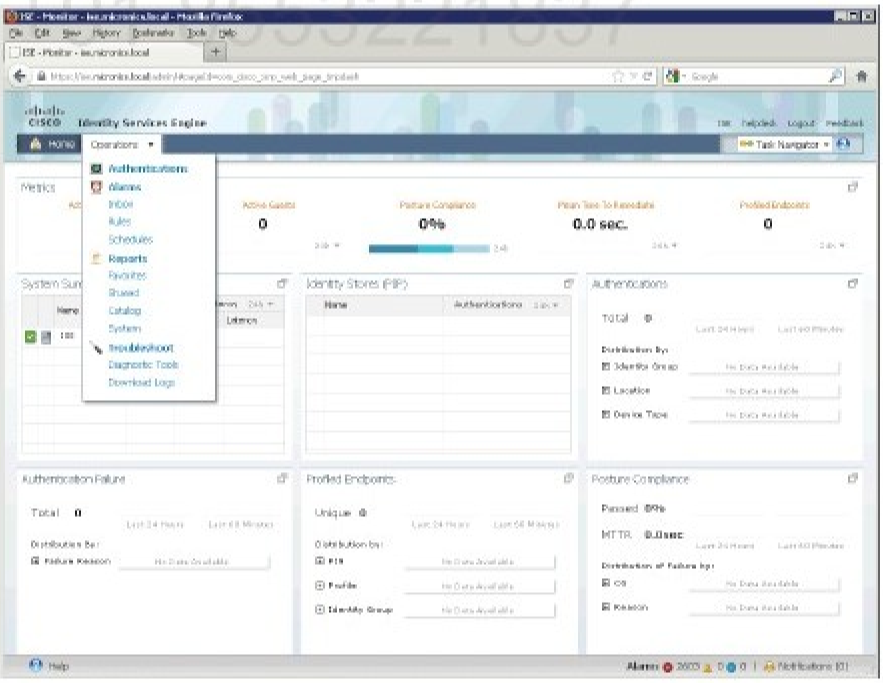
□ Send an email notification prior to password expiry after 30 days

Incorrect Password Attempts

☑ Disable account after 5 sequential failed attempts

Verification

Logout and re-login using helpdesk user. Check if you have access to the required options.



Note the helpdesk username in the top right corner. Only Operations menu is available.

LAB 3.4. Integration with Active Directroy

Objectives

This lab shows how to integrate ISE with Microsoft Active Directory.

IP Addressing and devices

Device	Interface	IP address
ISE	NIC	172.31.1.20
R1	Lo0	1.1.1.1/32
	E0/0	10.1.10.1/24
	E0/1	172.31.1.1/24
AD	NIC	172.31.1.200
WinXP	NIC	10.1.10.50/24

Task

Configure ISE to join Active Directory domain of **micronics.local**. Use AD user credentials of employee1/Micronics1 to join the domain. Import the following groups from AD to the ISE:

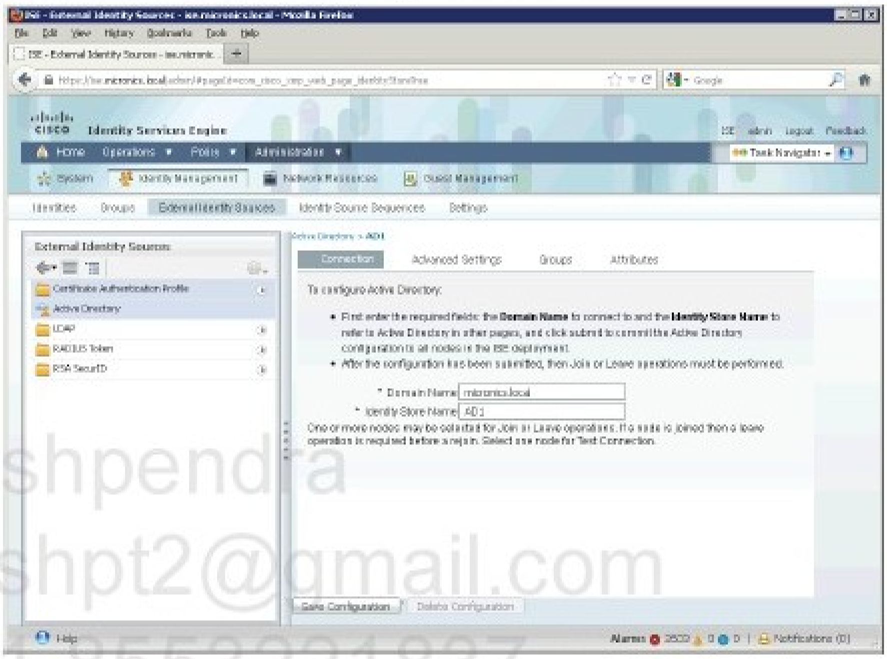
- micronics.local/Users/contractors
- micronics.local/Users/employees
- micronics.local/Users/students

Configuration

Complete these steps:

Step 1 Join the Active Directory domain.

- Go to **Administration > Identity Management > External Identity Sources > Active Directory** and provide **micronics.local** as Domain Name. Leave the default **Identity Store Name**.



To configure Active Directory:

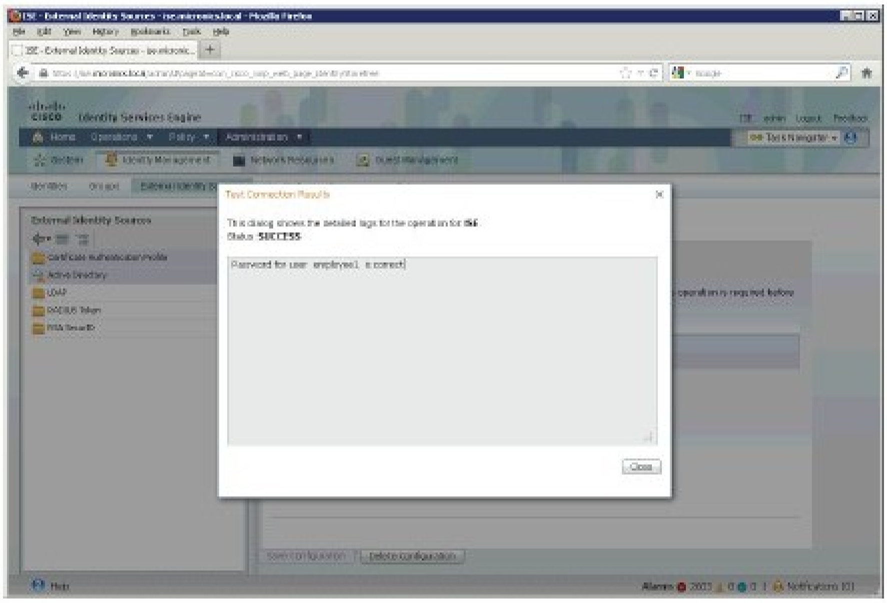
- First enter the required fields: the **Domain Name** to connect to and the **Identity Store Name** to refer to Active Directory in other pages, and click submit to commit the Active Directory configuration to all nodes in the ISE deployment.
- After the configuration has been submitted, then Join or Leave operations must be performed.

* Domain Name: micronics.local

* Identity Store Name: AD1

One or more nodes may be selected for Join or Leave operations. If a node is joined then a leave operation is required before a rejoin. Select one node for Test Connection.

- Click on **Save Changes** to save the changes. There will be a new entry on the domain list. Pick the checkbox and click **Test Connection > Basic Test**. Provide username and password and click **OK**.



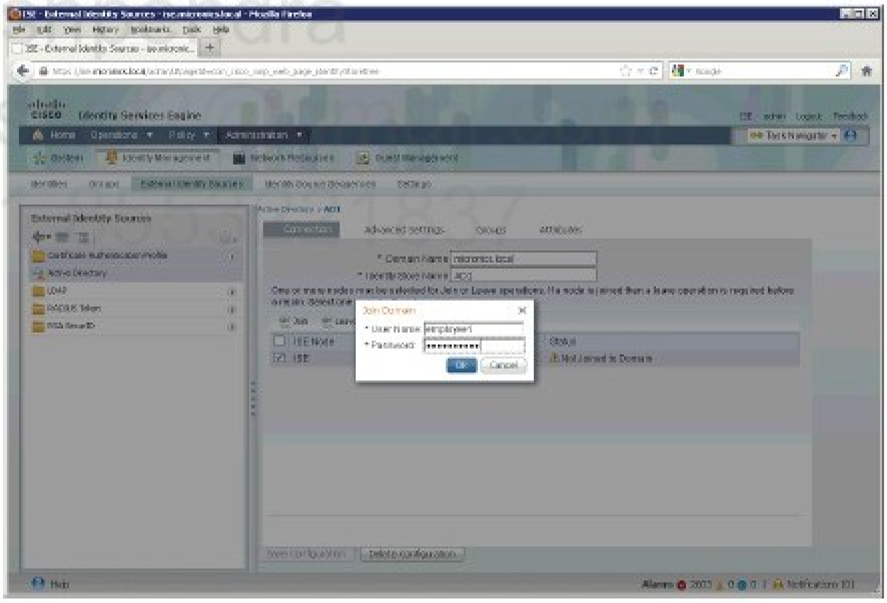
Test Connection Results

This dialog shows the detailed logs for the operation for ISE

Status: SUCCESS

Password for user employee1 is correct

- Click **Close** and get back to the domain list. Click **Join** and provide credentials for employee1 user. Click **OK**.



Active Directory > AD1

* Domain Name: micronics.local

* Identity Store Name: AD1

One or more nodes may be selected for Join or Leave operations. If a node is joined then a leave operation is required before a rejoin. Select one

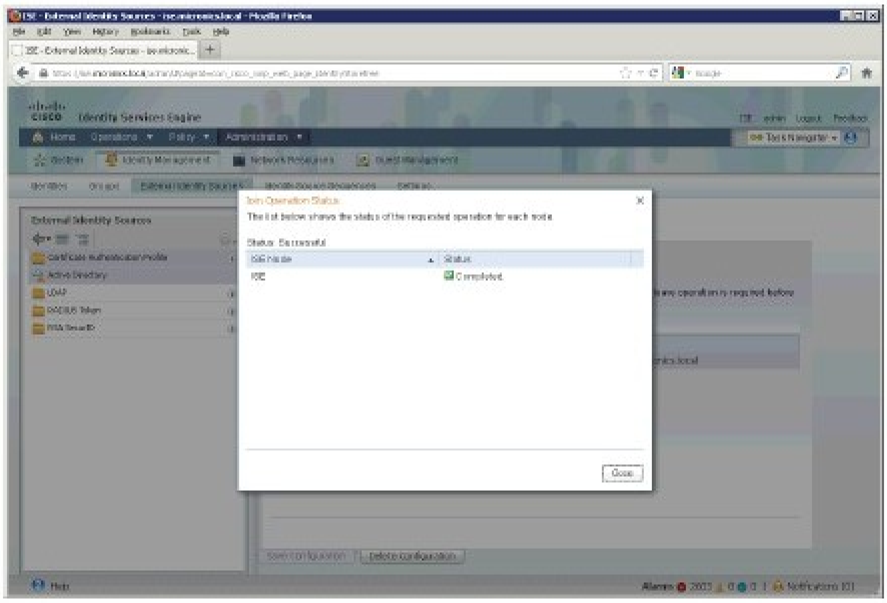
Join Domain

* User Name: employee1

* Password: ••••••••••••

	ISE Node	Status
☑	ISE	Not Joined to Domain

- You should get the following success message. Click **Close**.



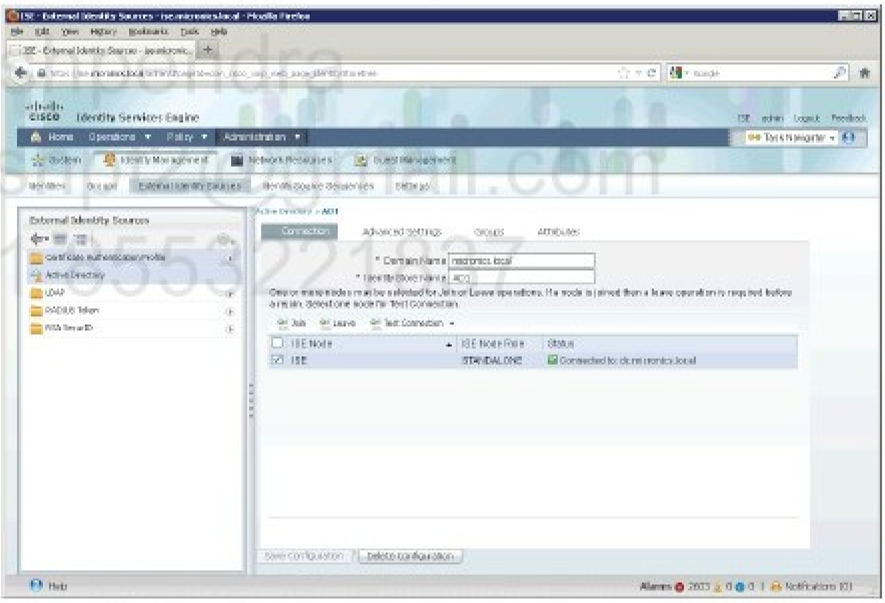
Join Operation Status

The list below shows the status of the requested operation for each node.

Status: Successful

ISE Node	Status
ISE	Completed

Now the **Status** indicates the ISE joined the AD domain.



Active Directory > AD1

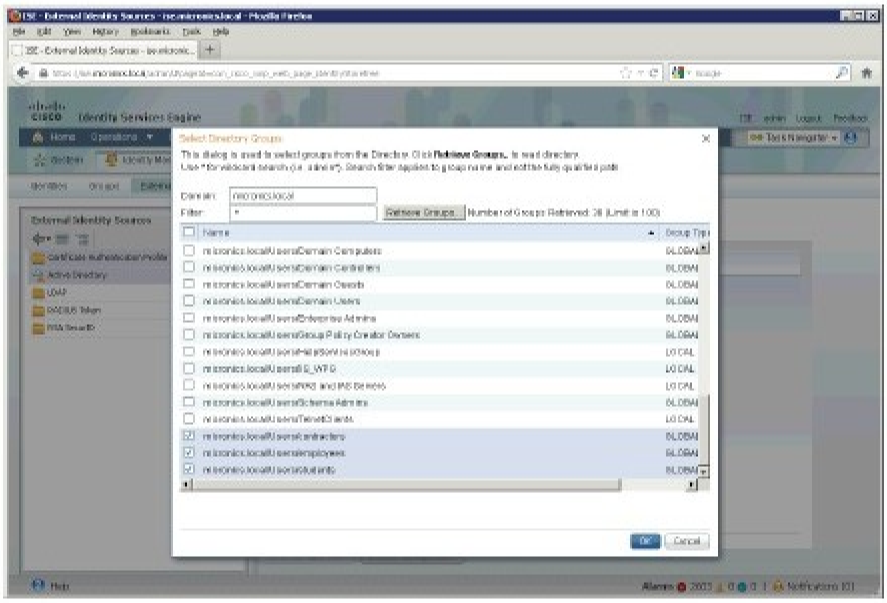
* Domain Name: micronics.local

* Identity Store Name: AD1

☐	ISE Node	ISE Node Role	Status
☑	ISE	STANDALONE	Connected to: dc.micronics.local

Step 2 Import AD groups into ISE.

- Go to **Groups** tab and click **Add > Select Groups From Directory**. Click **Retrive Groups** to list all groups from AD. Select those three to import them and click **OK**.



Select Directory Groups

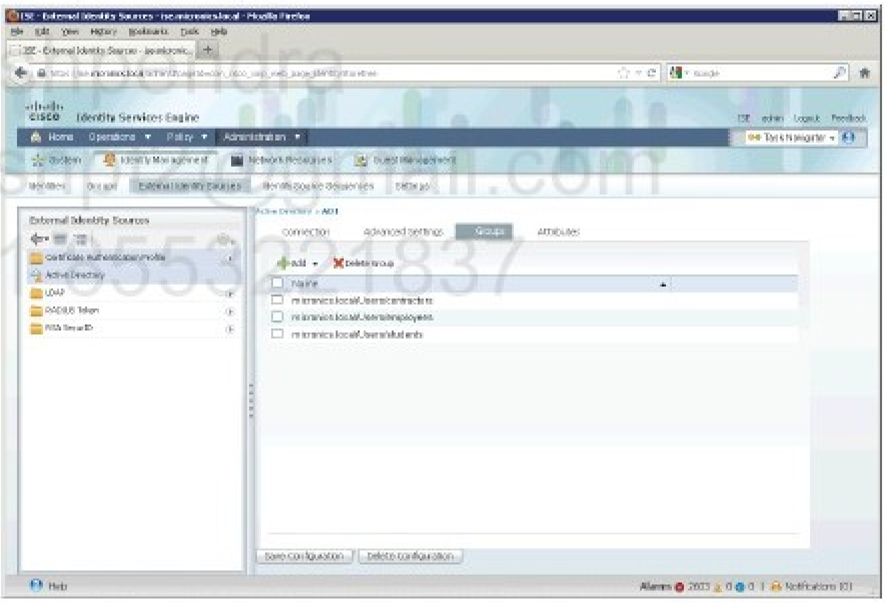
This dialog is used to select groups from the Directory. Click **Retrieve Groups..** to read directory.
Use * for wildcard search (i.e. admin*). Search filter applies to group name and not the fully qualified path.

Domain: micronics.local
Filter: *

Retrieve Groups... Number of Groups Retrieved: 28 (Limit is 100)

☐	Name	Group Type
☐	micronics.local/Users/Domain Computers	GLOBAL
☐	micronics.local/Users/Domain Controllers	GLOBAL
☐	micronics.local/Users/Domain Guests	GLOBAL
☐	micronics.local/Users/Domain Users	GLOBAL
☐	micronics.local/Users/Enterprise Admins	GLOBAL
☐	micronics.local/Users/Group Policy Creator Owners	GLOBAL
☐	micronics.local/Users/HelpServicesGroup	LOCAL
☐	micronics.local/Users/IIS_WPG	LOCAL
☐	micronics.local/Users/RAS and IAS Servers	LOCAL
☐	micronics.local/Users/Schema Admins	GLOBAL
☐	micronics.local/Users/TelnetClients	LOCAL
☑	micronics.local/Users/contractors	GLOBAL
☑	micronics.local/Users/employees	GLOBAL
☑	micronics.local/Users/students	GLOBAL

- Click **Save Configuration**.



Active Directory > AD1

Connection | Advanced Settings | Groups | Attributes

☐	Name
☐	micronics.local/Users/contractors
☐	micronics.local/Users/employees
☐	micronics.local/Users/students

Save Configuration | Delete Configuration

Verification

There is no verification for that task.

LAB 3.5. Configure ISE for MAB

Objectives

This lab shows how to configure MAC Authentication Bypass on switch and use ISE as Autorization Server.

IP Addressing and devices

Device	Interface	IP address
ISE	NIC	172.31.1.20
R1	Lo0 E0/0 E0/1	1.1.1.1/32 10.1.10.1/24 172.31.1.1/24
AD	NIC	172.31.1.200
WinXP	NIC	10.1.10.50/24

Task

There is a Windows 7 host connected to SW1 port 0/7 through the IP Phone. Configure the switch to authenticate IP Phone basing on its MAC address. The Voice domain should be authorized to Voice VLAN (VVLAN). You may use static policy assignment to preconfigured policy on the ISE.

Enable RADIUS authentication, authorization and accounting to the ISE ports UDP/1812, UDP/1813 with a secret key of cisco123 sourcing the RADIUS packets from vlan10 interface. Also, enable RADIUS Change of Authorization (CoA) using the same credentials as for AAA. Configure two Network Devices Groups based on Device Type: Wireless and Wired. Add SW1 to the Wired NDG. You can enable EPM logging for verification.

Configuration

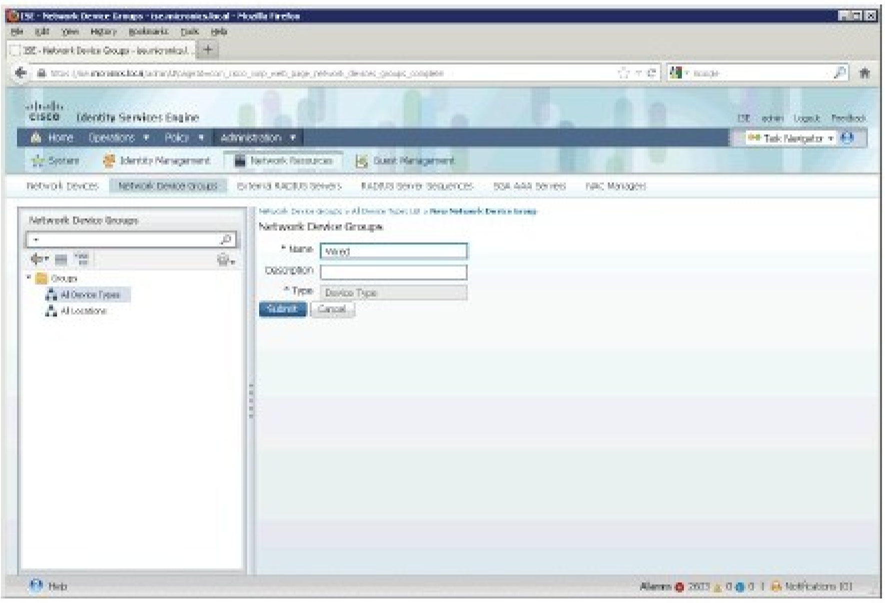
Complete these steps:

Step 1 Configure SW1 for 802.1x

```
!
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
aaa server radius dynamic-author
 client 172.31.1.20 server-key 0 cisco123
!
radius-server host 172.31.1.20 auth-port 1812 acct-port 1813
radius-server key cisco123
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
ip radius source-interface vlan 10
!
dot1x system-auth-control
!
interface FastEthernet0/7
 description IPP + Win7
 switchport access vlan 10
 switchport mode access
 switchport voice vlan 500
 authentication host-mode multi-domain
 authentication order mab dot1x
 authentication priority dot1x mab
 authentication port-control auto
 mab
 dot1x pae authenticator
 spanning-tree portfast
!
epm logging
!
```

Step 2 Configure NDGs on ISE.

- Go to **Administration > Network Resources > Network Device Groups > Groups > All Device Types** and click **Add**. Enter **Wired** as name and click **Submit**.


Network Device Groups > All Device Types List > New Network Device Group

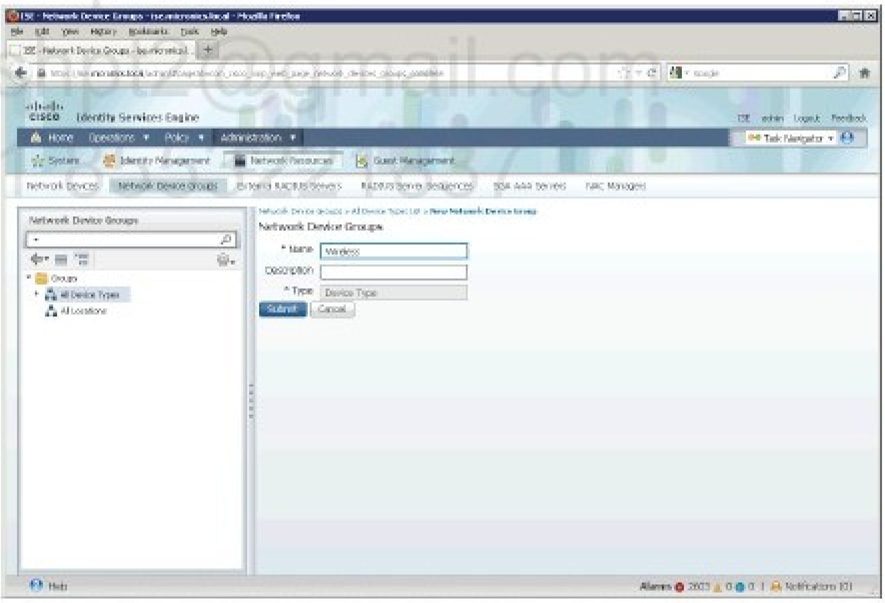
Network Device Groups

* Name: Wired

Description:

* Type: Device Type

- Go to **Administration > Network Resources > Network Device Groups > Groups > All Device Types** and click **Add**. Enter **Wireless** as name and click **Submit**.


Network Device Groups > All Device Types List > New Network Device Group

Network Device Groups

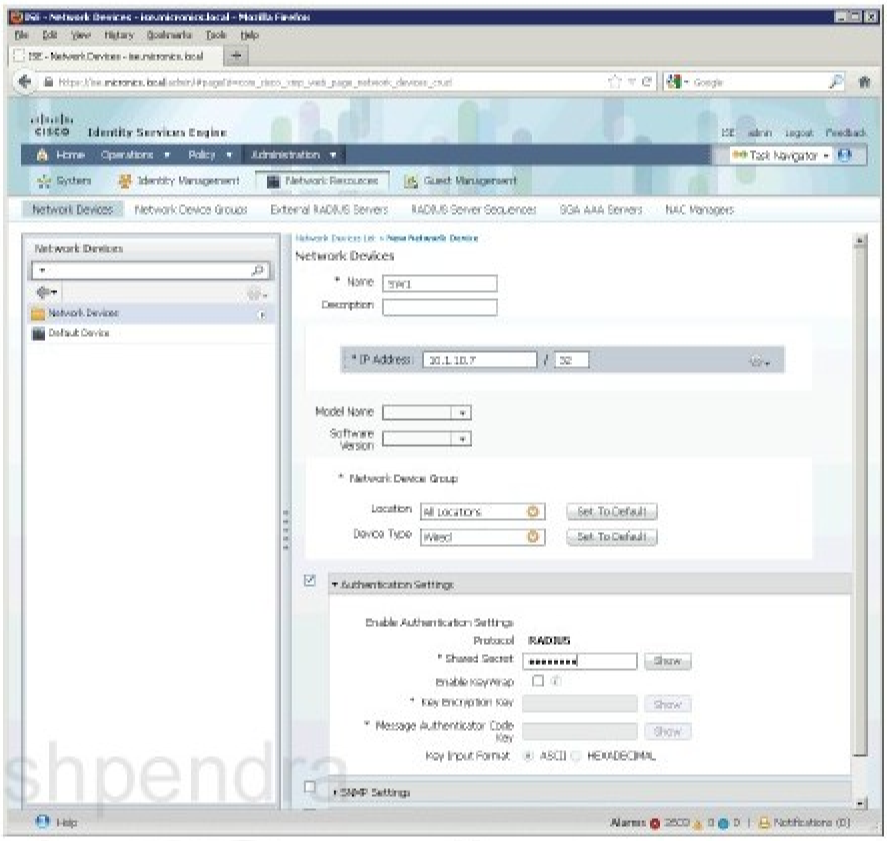
* Name: Wireless

Description:

* Type: Device Type

Step 3 Add SW1 as AAA client.

- Go to **Administration > Network Resources > Network Devices** and click **Add**. Enter **SW1** as name, provide IP address of SW1's vlan10 interface, assign it to **Wired** Device Type, set **Shared Secret** and click **Submit**.


ISE - Network Devices - ise.micronics.local - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Identity Services Engine
ISE admin Logout Feedback
Home Operations Policy Administration
Task Navigator
System Identity Management Network Resources Guest Management
Network Devices Network Device Groups External RADIUS Servers RADIUS Server Sequences SGA AAA Servers NAC Managers
Network Devices
Default Device
Network Devices List > New Network Device
Set To Default
Show
Help
Alarms 2800 0 0 Notifications (0)

Network Devices

* Name SW1

Description

* IP Address: 10.1.10.7 / 32

Model Name

Software Version

* Network Device Group

Location All Locations

Device Type Wired

☑ Authentication Settings

Enable Authentication Settings

Protocol RADIUS

* Shared Secret ●●●●●●●●

Enable KeyWrap □

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ● ASCII ○ HEXADECIMAL

□ SNMP Settings

Step 4 Add IP Phone MAC address to ISE Endpoins Identity store.

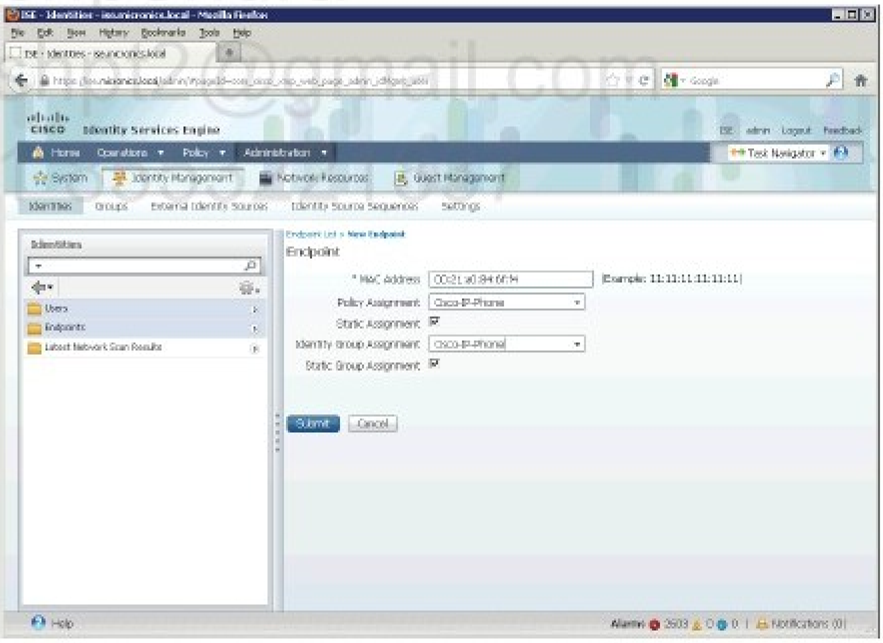
- Bounce switch port to restart authentication.

```
SW1(config)#int f0/7
SW1(config-if)#shut
*Mar  1 16:37:39.779: %LINK-5-CHANGED: Interface FastEthernet0/7,
changed state to administratively down
SW1(config-if)#no shut
SW1(config-if)#



%LINK-3-UPDOWN: Interface FastEthernet0/7, changed state to up
%AUTHMGR-5-START: Starting 'mab' for client (0021.a084.6ff4) on
Interface Fa0/7 AuditSessionID 0A010A070000000903920AB7
%MAB-5-FAIL: Authentication failed for client (0021.a084.6ff4) on
Interface Fa0/7 AuditSessionID 0A010A070000000903920AB7
%AUTHMGR-7-RESULT: Authentication result 'no-response' from 'mab' for
client (0021.a084.6ff4) on Interface Fa0/7 AuditSessionID
0A010A070000000903920AB7
%AUTHMGR-7-FAILOVER: Failing over from 'mab' for client
(0021.a084.6ff4) on Interface Fa0/7 AuditSessionID
0A010A070000000903920AB7
%AUTHMGR-5-START: Starting 'dot1x' for client (0021.a084.6ff4) on
Interface Fa0/7 AuditSessionID 0A010A070000000903920AB7
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7,
changed state to up
```

- Note MAC address of IP Phone connected to the port.

```
SW1#sh mac address-table interface f0/7
Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  10    0015.17a7.2497    STATIC      Drop
 500    0021.a084.6ff4    STATIC      Drop
Total Mac Addresses for this criterion: 2
```

- Go to **Administration > Identity Management > Identities > Endpoints** and click **Add**. Enter **MAC Address** of IP Phone, select **Policy Assignment** as preconfigured **Cisco-IP-Phone**, select **Identity Group Assignment** as preconfigured **Cisco-IP-Phone** and click **Submit**.



ISE - Identities - isesnicronics.local - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Identity Services Engine
ISE admin Logout Feedback
Home Operations Policy Administration
Task Navigator
System Identity Management Network Resources Guest Management
Identities Groups External Identity Sources Identity Source Sequences Settings
Identities
Users
Endpoints
Latest Network Scan Results
Endpoint List > New Endpoint
Endpoint
Submit Cancel
Help
Alarms 2603 0 0 Notifications (0)

* MAC Address: 00:21:a0:84:6f:f4 [Example: 11:11:11:11:11:11]
Policy Assignment: Cisco-IP-Phone
Static Assignment: ☑
Identity Group Assignment: Cisco-IP-Phone
Static Group Assignment: ☑

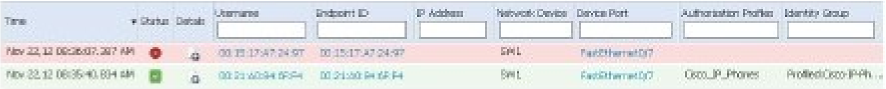
Verification

Bounce the switch port to restart authentication. You should see what's happeing when 'epm logging' is enabled.

```
SW1#show authentication sessions interface f0/7
No Auth Manager contexts currently exist

       // this indicates that dot1x process is not working. You must bounce the port
       to restart authentication.

SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#int f0/7
SW1(config-if)#shut
SW1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down
SW1(config-if)#no shut
SW1(config-if)#end
SW1#

%LINK-3-UPDOWN: Interface FastEthernet0/7, changed state to up
%AUTHMGR-5-START: Starting 'mab' for client (0021.a084.6ff4) on Interface Fa0/7
AuditSessionID 0A010A070000000E0397EC24
%MAB-5-SUCCESS: Authentication successful for client (0021.a084.6ff4) on Interface
Fa0/7 AuditSessionID 0A010A070000000E0397EC24
%AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client
(0021.a084.6ff4) on Interface Fa0/7 AuditSessionID 0A010A070000000E0397EC24
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
%AUTHMGR-5-SUCCESS: Authorization succeeded for client (0021.a084.6ff4) on Interface
Fa0/7 AuditSessionID 0A010A070000000E0397EC24
SW1#
SW1#show authentication sessions interface f0/7
            Interface:  FastEthernet0/7
          MAC Address:  0021.a084.6ff4
           IP Address:  Unknown
            User-Name:  00-21-A0-84-6F-F4
               Status:  Authz Success
               Domain:  VOICE
       Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A010A070000000E0397EC24
      Acct Session ID:  0x00000011
               Handle:  0x2300000E

Runnable methods list:
       Method   State
       mab      Authc Success
```

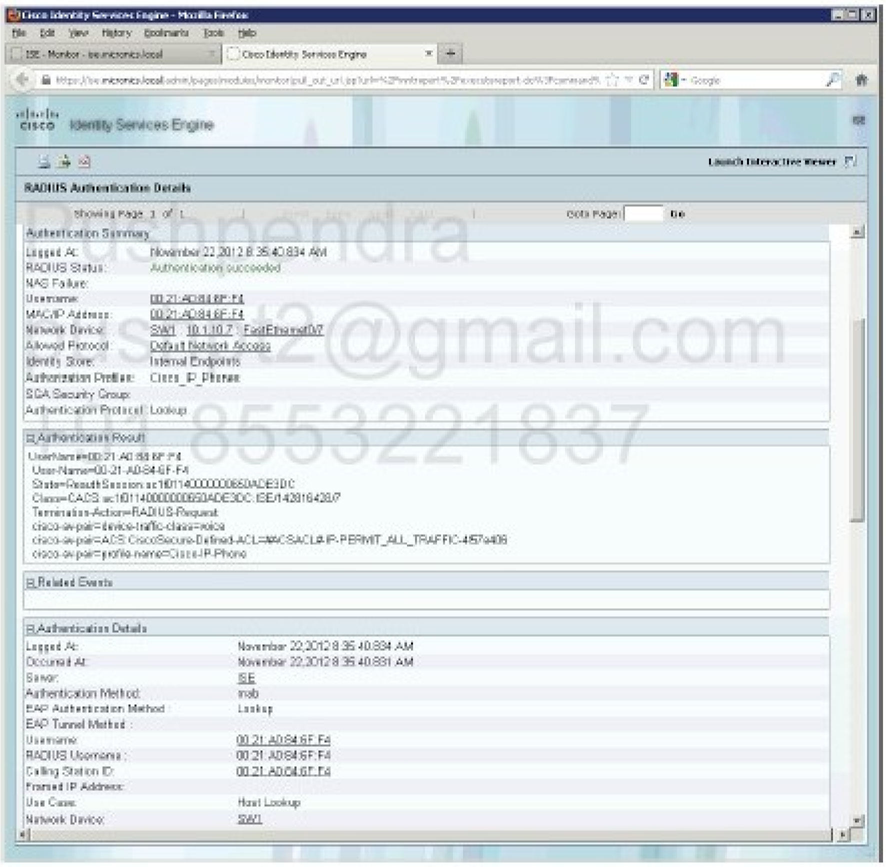
```
dot1x    Not run

// note that MAC address is used as a username for MAB. You can check that in
RADIUS logs if 'debug radius' is enabled. Also note that the authetication has
passed for VOICE domain. You may see Authc Failed for UNKNOWN or DATA domain if
multi-domain authentication is enabled.
```

Check ISE logs.



Time	Status	Details	Username	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Identity Group
Nov 22,12 08:36:07.387 AM	●		00:15:17:47:24:97	00:15:17:47:24:97		SW1	FastEthernet0/7		
Nov 22,12 08:35:40.834 AM	✓		00:21:A0:84:6F:F4	00:21:A0:84:6F:F4		SW1	FastEthernet0/7	Cisco_IP_Phones	Profiled:Cisco-IP-Ph...

```
// as you see in the logs, the IP Phone authentication is successful but PC
authentication is not.
```


Cisco Identity Services Engine - Mozilla Firefox
File Edit View History Bookmarks Tools Help
ISE - Monitor - ise.micronics.local
Cisco Identity Services Engine
cisco Identity Services Engine
Launch Interactive Viewer
Showing Page 1 of 1
Goto Page: Go

RADIUS Authentication Details

Authentication Summary

```
Logged At:               November 22,2012 8:35:40.834 AM
RADIUS Status:           Authentication succeeded
NAS Failure:
Username:                00:21:A0:84:6F:F4
MAC/IP Address:          00:21:A0:84:6F:F4
Network Device:          SW1 : 10.1.10.7 : FastEthernet0/7
Allowed Protocol:        Default Network Access
Identity Store:          Internal Endpoints
Authorization Profiles:  Cisco_IP_Phones
SGA Security Group:
Authentication Protocol: Lookup
```

Authentication Result

```
UserName=00:21:A0:84:6F:F4
 User-Name=00-21-A0-84-6F-F4
 State=ReauthSession:ac1f011400000000650ADE3DC
 Class=CACS:ac1f011400000000650ADE3DC:ISE/142816428/7
 Termination-Action=RADIUS-Request
 cisco-av-pair=device-traffic-class=voice
 cisco-av-pair=ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-PERMIT_ALL_TRAFFIC-4f57e408
 cisco-av-pair=profile-name=Cisco-IP-Phone
```

Related Events

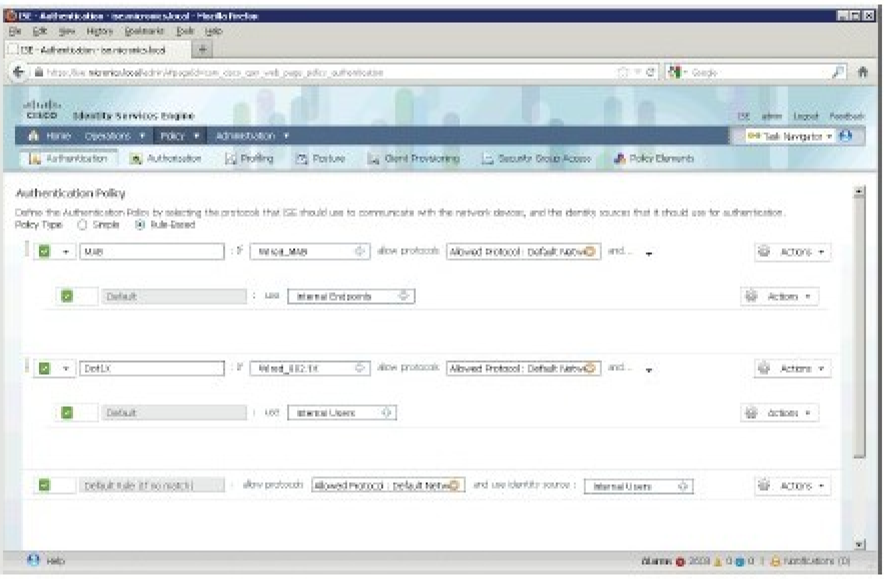
Authentication Details

```
Logged At:                  November 22,2012 8:35:40.834 AM
Occured At:                 November 22,2012 8:35:40.831 AM
Server:                     ISE
Authentication Method:      mab
EAP Authentication Method : Lookup
EAP Tunnel Method :
Username:                   00:21:A0:84:6F:F4
RADIUS Username :           00:21:A0:84:6F:F4
Calling Station ID:         00:21:A0:84:6F:F4
Framed IP Address:
Use Case:                   Host Lookup
Network Device:             SW1
```

Check ISE configuration to see how the above authentication works.

1. **Authentication.**

   The Authentication policy has two rules by default. There is a rule for MAB clients and Wired 802.1x clients.



Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

Policy Type ○ Simple ● Rule-Based

☑ MAB : If Wired_MAB allow protocols Allowed Protocol : Default Network and ...

☑ Default : use Internal Endpoints

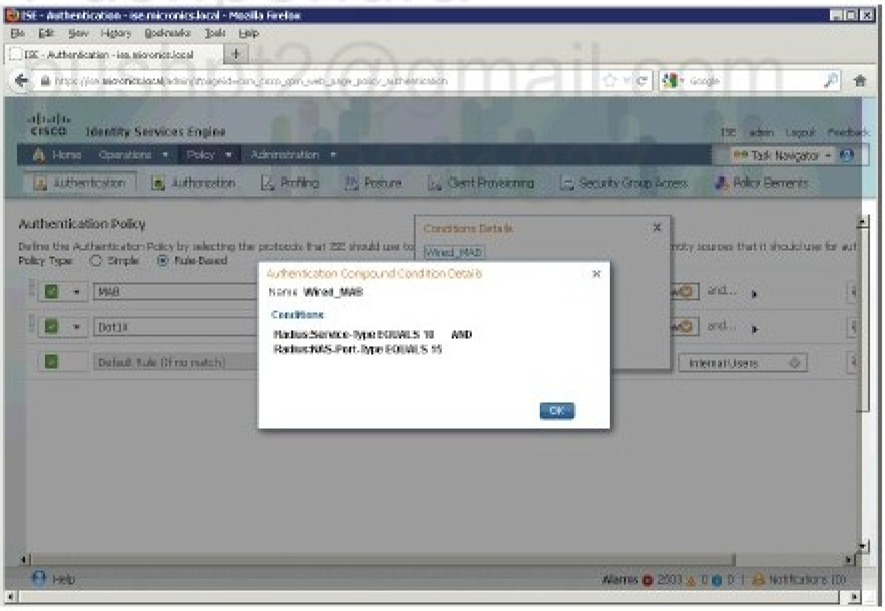
☑ Dot1X : If Wired_802.1X allow protocols Allowed Protocol : Default Network and ...

☑ Default : use Internal Users

☑ Default Rule (If no match) : allow protocols Allowed Protocol : Default Network and use identity source : Internal Users

How does ISE know the type of authentication?

Move the mouse pointer onto **Wired_MAB** condition and click a special pointer sign when appears. The rule details will show up.



Conditions Details

Wired_MAB

Authentication Compound Condition Details

Name: Wired_MAB

Conditions

Radius:Service-Type EQUALS 10 AND
Radius:NAS-Port-Type EQUALS 15

As you see ISE recognizes to connection type based on two RADIUS attributes. In this particular case **Service-Type = 10** (Call Check) and **NAS-Port = 15** (Ethernet).

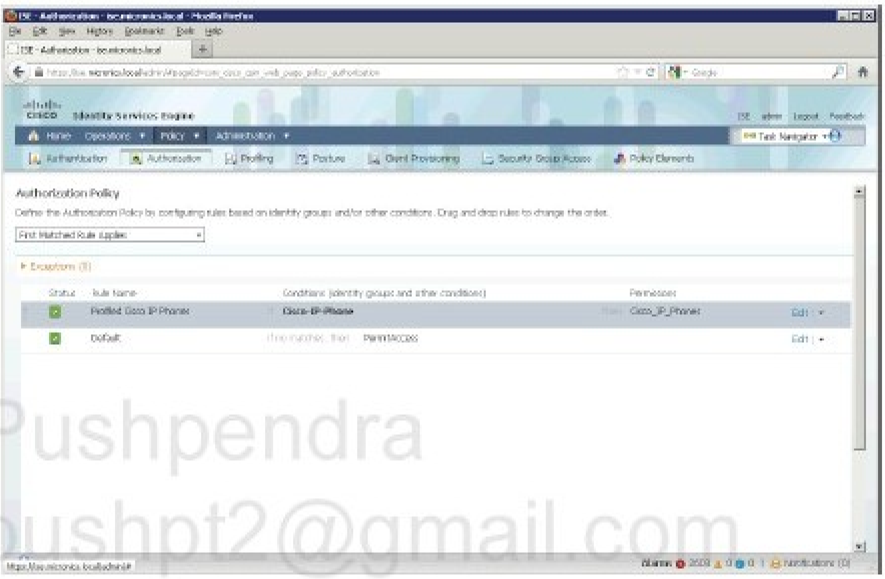
If the connection match that rule, theIdentity Store used for authentication is **Internal Endpoints**.

2. **Authorization.**

   ISE check Authorization rules. There are two default rules:

   - Profiled Cisco IP Phone
   - Default

   The first rule matches IP Phone connection and provides RADIUS attributes specified in **Cisco_IP_Phones** authorization profile to the switch.



Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

▸ Exceptions (0)

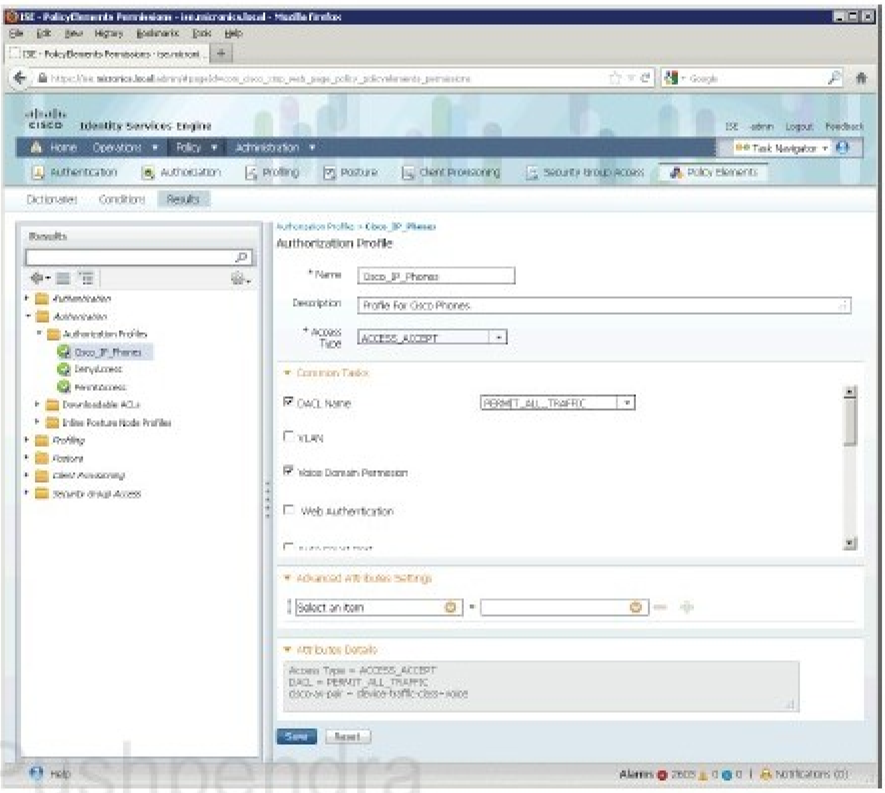
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions	
✓	Profiled Cisco IP Phones	if Cisco-IP-Phone then	Cisco_IP_Phones	Edit ▾
✓	Default	if no matches, then PermitAccess		Edit ▾

What is authorization profile?

When you go to **Policy > Policy Elements > Results > Authorization > Authorization Profiles > Cisco_IP_Phones** you'll see what RADIUS attributes are set. In this particular case there are two attributes configured:

- DACL Name = PERMIT_ALL_TRAFFIC
- Voice Domain Permission

The DACL is there to authorize the device to access specific resources. There must be RADIUS network authorization enabled to download DACL by the switch.



Authorization Profile > Cisco_IP_Phones

Authorization Profile

* Name: Cisco_IP_Phones

Description: Profile For Cisco Phones

* Access Type: ACCESS_ACCEPT

Common Tasks

☑ DACL Name: PERMIT_ALL_TRAFFIC

☐ VLAN

☑ Voice Domain Permission

☐ Web Authentication

Advanced Attributes Settings

Select an item =

Attributes Details

```
Access Type = ACCESS_ACCEPT
DACL = PERMIT_ALL_TRAFFIC
cisco-av-pair = device-traffic-class=voice
```

Save Reset

LAB 3.6. Configure MAC Whitelist

Objectives

This lab shows how to configure MAC Whitelist on ISE to quickly authenticate endpoints based on their MAC address.

IP Addressing and devices

Device	Interface	IP address
ISE	NIC	172.31.1.20
R1	Lo0	1.1.1.1/32
	E0/0	10.1.10.1/24
	E0/1	172.31.1.1/24
AD	NIC	172.31.1.200
WinXP	NIC	10.1.10.50/24

Task

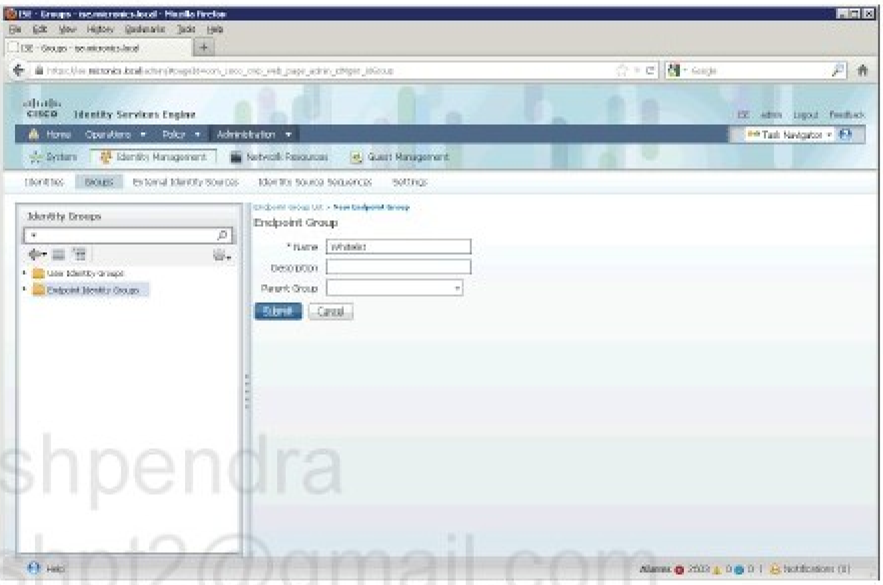
Configure a rule on ISE to enforce authorization for all MAC addresses added to the Whietlist group. This must work no matter what device is connecting to the switch. Add IP Phone MAC address to the Whitelist group for verification. Change the default authorization rule so that all devices will be denied if not matched by any rule.

Configuration

Complete these steps:

Step 1 Create whitelist group on ISE.

- Go to **Administration > Identity Management > Groups > Endpoint Identity Groups** and click **Add**. Enter **Whitelist** as name and click **Submit**.

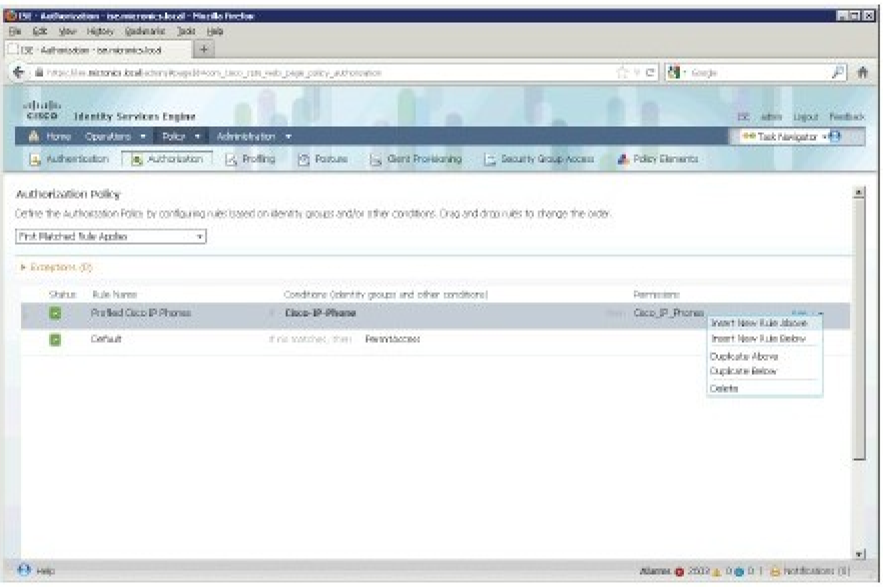


Endpoint Group

* Name: Whitelist
Description:
Parent Group:

Step 2 Create Authorization rule on ISE.

- Go to **Policy > Authorization** and click arrow next to **Edit** button of the first line. Chose **Insert New Rule Above** option.



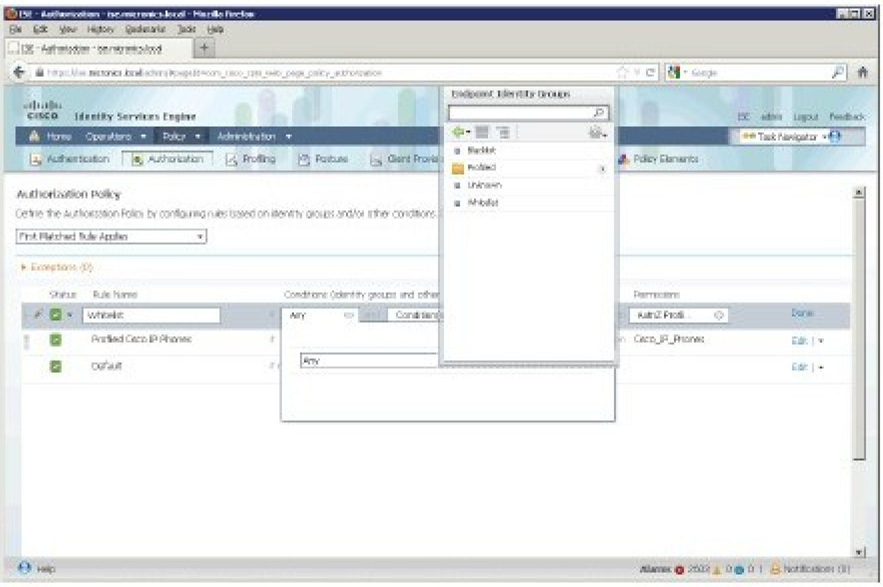
Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

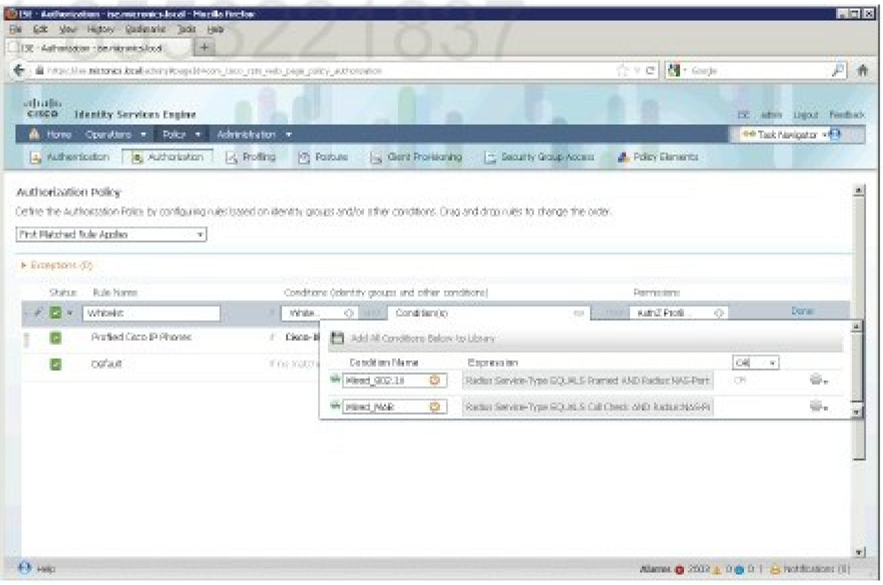
First Matched Rule Applies

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Profiled Cisco IP Phones	Cisco-IP-Phone	Cisco_IP_Phones
✓	Default	if no matches, then PermitAccess	

- Enter name for the new rule e.g. **Whitelist**, click plus to add identity condition and select **Endpoint Identity Groups > Whitelist**.

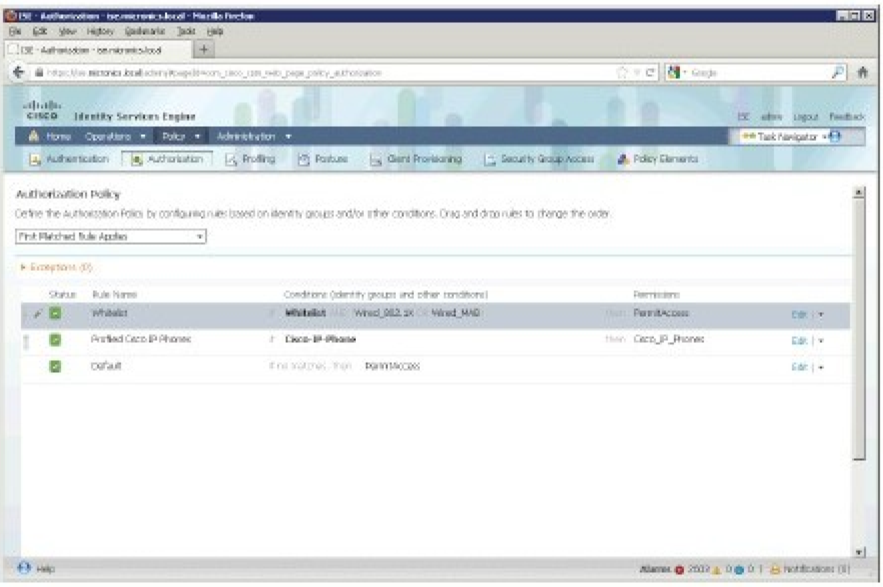


- Click plus button to add additional compound conditions to the rule. Select two conditions from the library **Wired_802_1X** OR **Wired_MAB**.



Condition Name	Expression
Wired_802.1X	Radius:Service-Type EQUALS Framed AND Radius:NAS-Port
Wired_MAB	Radius:Service-Type EQUALS Call Check AND Radius:NAS-P

- For **Permissions** select **PermitAccess**.



Authorization Policy

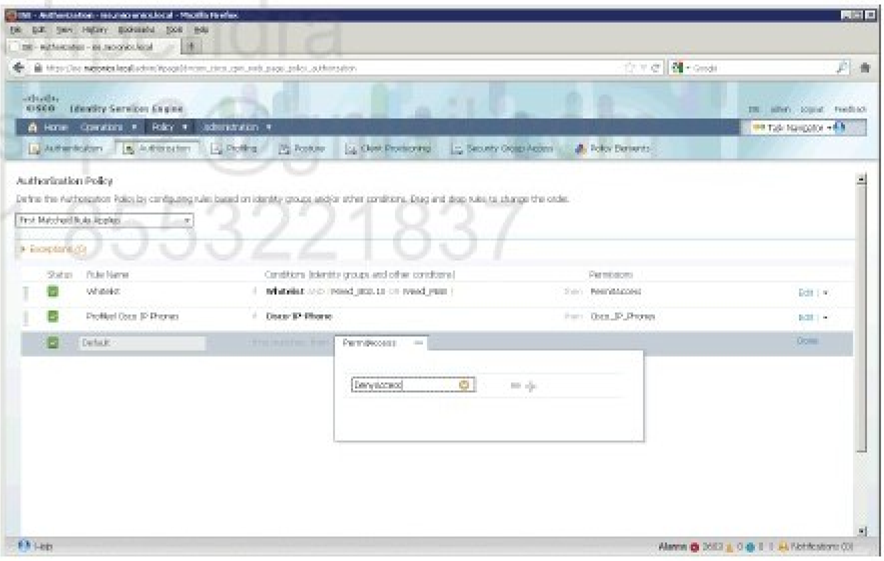
Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

▸ Exceptions (0)

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions	
☑	Whitelist	if Whitelist AND Wired_802.1X OR Wired_MAB	then PermitAccess	Edit | ▾
☑	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones	Edit | ▾
☑	Default	if no matches, then PermitAccess		Edit | ▾

- Click **Edit** button in the last (Default) rule. Change permissions to **DenyAccess**.



Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

▸ Exceptions (0)

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions	
☑	Whitelist	if Whitelist AND Wired_802.1X OR Wired_MAB	then PermitAccess	Edit | ▾
☑	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones	Edit | ▾
☑	Default	if no matches, then PermitAccess		Done

DenyAccess

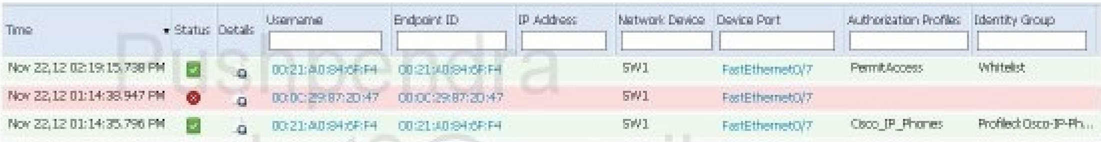
- Click **Done** and **Save** to finish.

Verification

Bounce the switch port to restart authentication.

```
SW1(config)#int f0/7
SW1(config-if)#shut
SW1(config-if)#no shut

%LINK-3-UPDOWN: Interface FastEthernet0/7, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up
%AUTHMGR-5-START: Starting 'mab' for client (0021.a084.6ff4) on Interface Fa0/7
AuditSessionID 0A010A070000001804D2745B
%MAB-5-SUCCESS: Authentication successful for client (0021.a084.6ff4) on Interface
Fa0/7 AuditSessionID 0A010A070000001804D2745B
%AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client
(0021.a084.6ff4) on Interface Fa0/7 AuditSessionID 0A010A070000001804D2745B
%AUTHMGR-5-SUCCESS: Authorization succeeded for client (0021.a084.6ff4) on Interface
Fa0/7 AuditSessionID 0A010A070000001804D2745B
```

Check what rule the connection was authorized by.



Time	Status	Details	Username	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Identity Group
Nov 22,12 02:19:15.738 PM	✓		00:21:A0:84:6F:F4	00:21:A0:84:6F:F4		SW1	FastEthernet0/7	PermitAccess	Whitelist
Nov 22,12 01:14:38.947 PM	✗		00:0C:29:87:2D:47	00:0C:29:87:2D:47		SW1	FastEthernet0/7		
Nov 22,12 01:14:35.796 PM	✓		00:21:A0:84:6F:F4	00:21:A0:84:6F:F4		SW1	FastEthernet0/7	Cisco_IP_Phones	Profiled:Cisco-IP-Ph...

```
// The previous authorization (last line) was matched by Cisco_IP_Phones rule.
The latest authorization (first line) has been matched by Whitelist rule.
```

LAB 3.7. MAB with VLAN authorization

Objectives

This lab shows how to configure VLAN authorization.

IP Addressing and devices

Device	Interface	IP address
ISE	NIC	172.31.1.20
R1	Lo0 E0/0 E0/1	1.1.1.1/32 10.1.10.1/24 172.31.1.1/24
AD	NIC	172.31.1.200
WinXP	NIC	10.1.10.50/24

Task

There is a Wireless Access Point connected to port 0/3 on SW1. Enable MAB on the switch port and authorize the AP to be part of VLAN 10. You should use AP endpoint group to accomplish this task.

Configuration

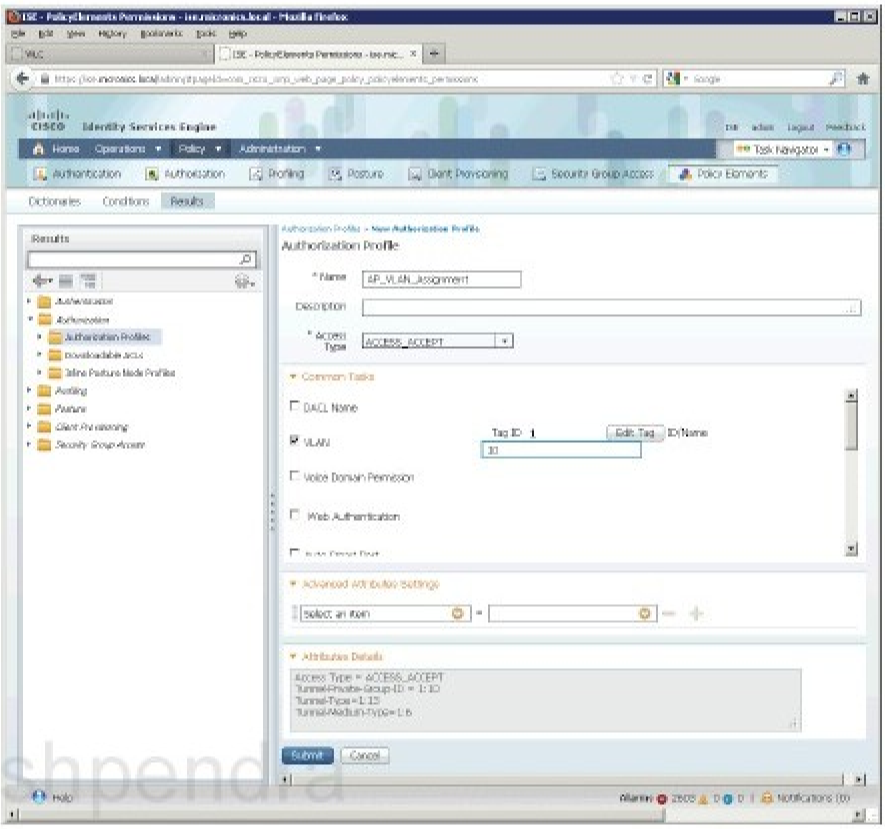
Complete these steps:

Step 1 SW1 configuration.

```
!
interface FastEthernet0/3
 authentication port-control auto
 mab
!

Note that just after configuring the port (or unshut the port) you'll
get the following MAB failing messages. This is because there is no MAC
address in the ISE Endpoint Identity store yet.

%AUTHMGR-5-START: Starting 'mab' for client (c47d.4f39.8423) on
Interface Fa0/3 AuditSessionID 0A010A070000001A04FF13BE
%MAB-5-FAIL: Authentication failed for client (c47d.4f39.8423) on
Interface Fa0/3 AuditSessionID 0A010A070000001A04FF13BE
%AUTHMGR-7-RESULT: Authentication result 'no-response' from 'mab' for
client (c47d.4f39.8423) on Interface Fa0/3 AuditSessionID
0A010A070000001A04FF13BE
%AUTHMGR-7-FAILOVER: Failing over from 'mab' for client
(c47d.4f39.8423) on Interface Fa0/3 AuditSessionID
0A010A070000001A04FF13BE
%AUTHMGR-7-NOMOREMETHODS: Exhausted all authentication methods for
client (c47d.4f39.8423) on Interface Fa0/3 AuditSessionID
0A010A070000001A04FF13BE
%AUTHMGR-5-FAIL: Authorization failed for client (c47d.4f39.8423) on
Interface Fa0/3 AuditSessionID 0A010A070000001A04FF13BE
```

Step 2 Create new authorization profile for AP.

- Go to **Policy > Policy Elements > Results > Authorization > Authorization Profiles** and click **Add**. Enter **AP_VLAN_Assignment** as name, check **VLAN** option and set it to **10**, and click **Submit**.



Authorization Profile

* Name: AP_VLAN_Assignment

Description:

* Access Type: ACCESS_ACCEPT

Common Tasks

☐ DACL Name

☑ VLAN   Tag ID 1   ID/Name 10

☐ Voice Domain Permission

☐ Web Authentication

Advanced Attributes Settings

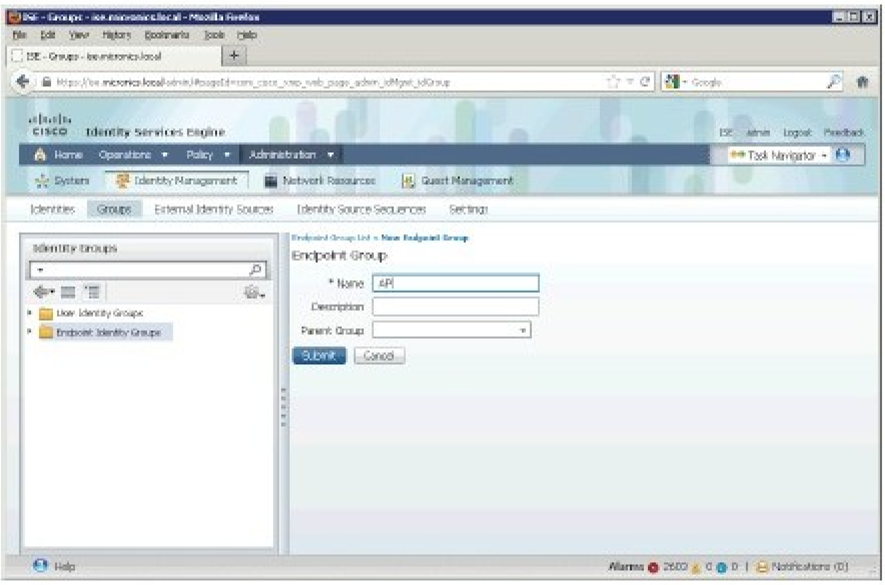
Select an item =

Attributes Details

```
Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:10
Tunnel-Type=1:13
Tunnel-Medium-Type=1:6
```

Step 3 Create new endpoint group and assign AP to that group.

- Go to **Administration > Identity Management > Groups > Endpoint Identity Groups** and click **Add**. Enter **AP** as a name and click **Submit**.



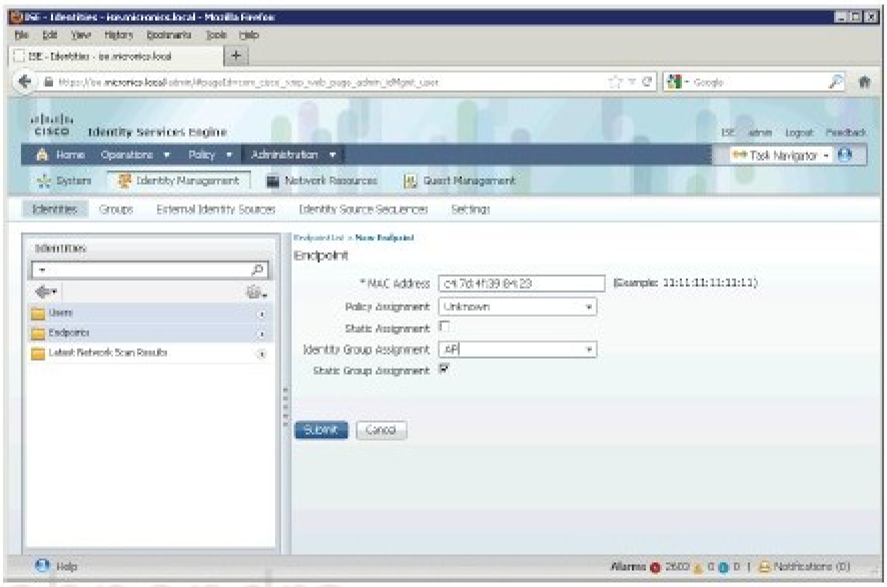
Endpoint Group

* Name: AP

Description:

Parent Group:

- Go to **Administration > Identity Management > Identities > Endpoints** and click **Add**. Enter AP MAC address taken from the switch assign it to the **AP** group. Click **Submit**.



Endpoint List > New Endpoint

Endpoint

* MAC Address: c4:7d:4f:39:84:23 (Example: 11:11:11:11:11:11)

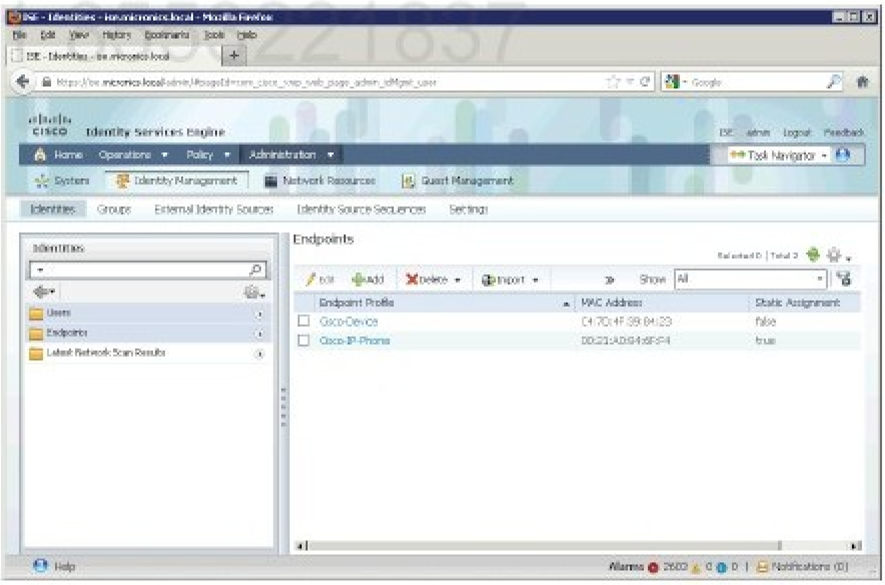
Policy Assignment: Unknown

Static Assignment: □

Identity Group Assignment: AP

Static Group Assignment: ☑

- Notice that the **Endpoint Profile** is **Cisco-Device**. This is because the MAC address OUI was recognized as beloning to Cisco Systems.

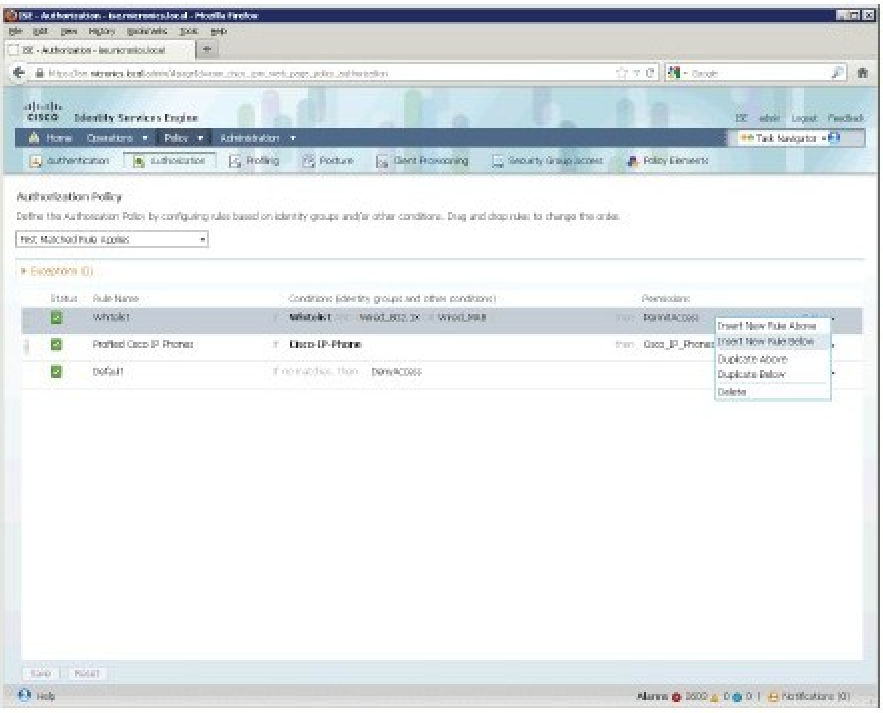


Endpoints

	Endpoint Profile	MAC Address	Static Assignment
□	Cisco-Device	C4:7D:4F:39:84:23	false
□	Cisco-IP-Phone	00:21:A0:94:6F:F4	true

Step 4 Create new authorization rule for AP.

- Go to **Policy > Authorization** and click arrow next to **Edit** button in the first rule and chose **Insert New Rule Below**.



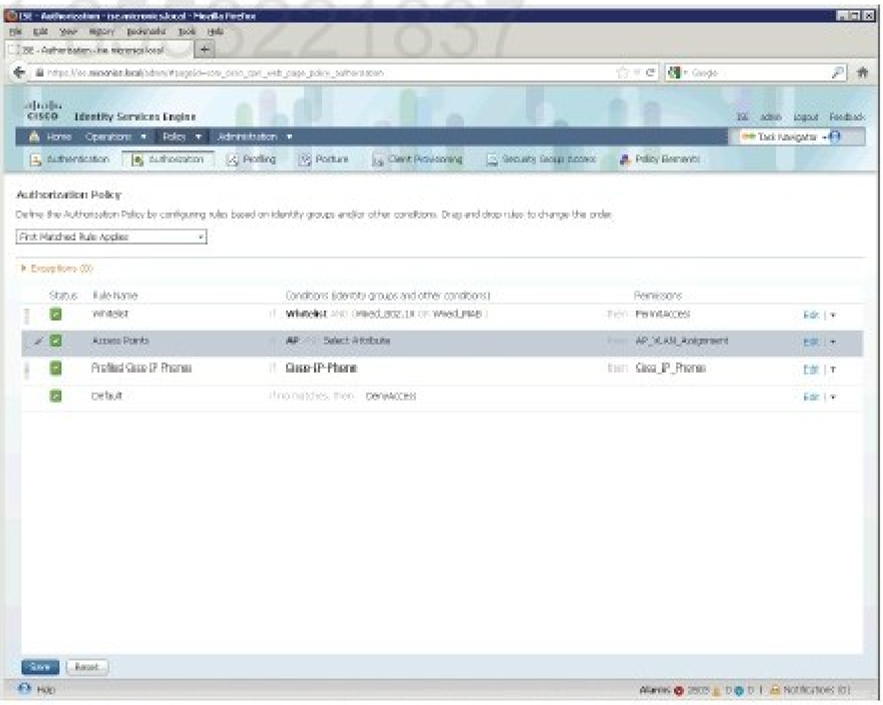
Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Whitelist	if Whitelist AND Wired_802.1X OR Wired_MAB	then PermitAccess
✓	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones
✓	Default	if no matches, then DenyAccess	

- Enter name for new rule e.g. **Access Points**, select **AP** endopoint group for conditions and assign **AP_VLAN_Assignment** authorization profile for permissions. Click **Done** and **Submit**.



Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

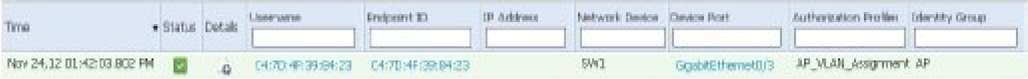
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Whitelist	if Whitelist AND (Wired_802.1X OR Wired_MAB)	then PermitAccess
✓	Access Points	if AP AND Select Attribute	then AP_VLAN_Assignment
✓	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones
✓	Default	if no matches, then DenyAccess	

Verification

Check switch commands and logs.

```
SW1#sh authentication sess int f0/3
            Interface:  FastEthernet0/3
          MAC Address:  c47d.4f39.8423
           IP Address:  Unknown
            User-Name:  C4-7D-4F-39-84-23
               Status:  Authz Success
               Domain:  DATA
       Oper host mode:  single-host
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  10
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A010A070000001A04FF13BE
      Acct Session ID:  0x00000027
               Handle:  0xBB00001A

Runnable methods list:
       Method   State
       mab      Authc Success

SW1#sh vlan id 10

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
10   ASA-Inside                       active    Gi0/3, Gi0/6, Gi0/7, Gi0/24

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
10   enet  100010     1500  -      -      -        -    -        0      0
```

Check ISE logs to see Authorization Profile and Identity Group.



Time	Status	Details	Username	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Identity Group
Nov 24,12 01:42:03.802 PM	✓		C4:7D:4F:39:84:23	C4:7D:4F:39:84:23		SW1	GigabitEthernet0/3	AP_VLAN_Assignment	AP

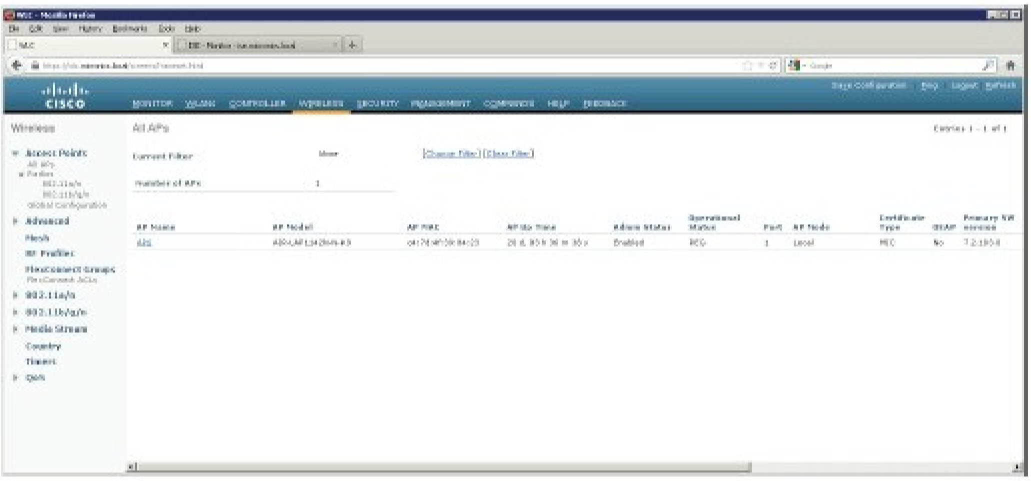
The AP should get an IP address from local DHCP server on SW1.

```
SW1#sh ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
10.1.10.101         01c4.7d4f.3984.23       Mar 03 1993 03:40 AM    Automatic
```

You should see the following AP initialization messages (if you have access to AP's console).

```
%CAPWAP-3-ERRORLOG: Not sending discovery request AP does not have an Ip !!
%CAPWAP-3-ERRORLOG: Not sending discovery request AP does not have an Ip !!
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0, changed state to up
Not in Bound state.
%CAPWAP-3-ERRORLOG: Not sending discovery request AP does not have an Ip !!
%CAPWAP-3-DHCP_RENEW: Could not discover WLC using DHCP IP. Renewing DHCP IP.
%CAPWAP-3-ERRORLOG: Invalid event 38 & state 2 combination.
%DHCP-6-ADDRESS_ASSIGN: Interface BVI1 assigned DHCP address 10.1.10.101, mask
255.255.255.0, hostname AP6

Translating "CISCO-CAPWAP-CONTROLLER.miconics.local"...domain server (172.31.1.200)
%CAPWAP-5-DHCP_OPTION_43: Controller address 10.1.10.5 obtained through DHCP
%CAPWAP-3-ERRORLOG: Did not get log server settings from DHCP.

%CAPWAP-3-ERRORLOG: Could Not resolve CISCO-CAPWAP-CONTROLLER.miconics.local
%CAPWAP-3-ERRORLOG: Go join a capwap controller wmmAC status is FALSE
%CAPWAP-5-DTLSREQSEND: DTLS connection request sent peer_ip: 10.1.10.5 peer_port: 5246
%CAPWAP-5-DTLSREQSUCC: DTLS connection created sucessfully peer_ip: 10.1.10.5
peer_port: 5246
%CAPWAP-5-SENDJOIN: sending Join Request to 10.1.10.5
%CAPWAP-3-ERRORLOG: CAPWAP parameters update to forwarding plane failed
%CAPWAP-3-ERRORLOG: CAPWAP parameters plumbing to forwarding plane failed
%CAPWAP-5-JOINEDCONTROLLER: AP has joined controller WLC
%LINK-5-CHANGED: Interface Dot11Radio1, changed state to administratively down
%LWAPP-3-CLIENTEVENTLOG: SSID MICRONICS added to the slot[0]
%LWAPP-3-CLIENTEVENTLOG: SSID MICRONICS added to the slot[1]
%WIDS-6-ENABLED: IDS Signature is loaded and enabled
%LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0, changed state to down
%LINK-3-UPDOWN: Interface Dot11Radio0, changed state to down
%LINK-5-CHANGED: Interface Dot11Radio0, changed state to reset
%LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0, changed state to up
```

Check WLC GUI if there is Access Point.



All APs

Entries 1 - 1 of 1

Current Filter None [Change Filter] [Clear Filter]

Number of APs 1

AP Name	AP Model	AP MAC	AP Up Time	Admin Status	Operational Status	Port	AP Mode	Certificate Type	OEAP	Primary SW Version
AP1	AIR-LAP1142N-A-K9	c4:7d:4f:39:84:23	28 d, 03 h 36 m 35 s	Enabled	REG	1	Local	MIC	No	7.2.103.0

LAB 3.8. Windows 7 AD Integration (optional)

Objectives

This lab shows how to add Windows 7 PC client to Active Directory. This step is useful to perform Machine authentication in the later task.

IP Addressing and devices

Device	Interface	IP address
ISE	NIC	172.31.1.20
R1	Lo0 E0/0 E0/1	1.1.1.1/32 10.1.10.1/24 172.31.1.1/24
AD	NIC	172.31.1.200
WinXP	NIC	10.1.10.50/24
WLC	G0/0/1 (mgmt.) G0/0/2	10.1.10.5/24 10.1.30.5/24
ASA1	G0/0 (outside) G0/1 (inside) G0/2 (dmz)	100.2.2.10/24 10.1.10.10/24 10.1.30.10/24
Win7 PC	LAN NIC (LAB-Network) WLAN NIC	DHCP-Assigned 10.1.30.x (DHCP)

Task

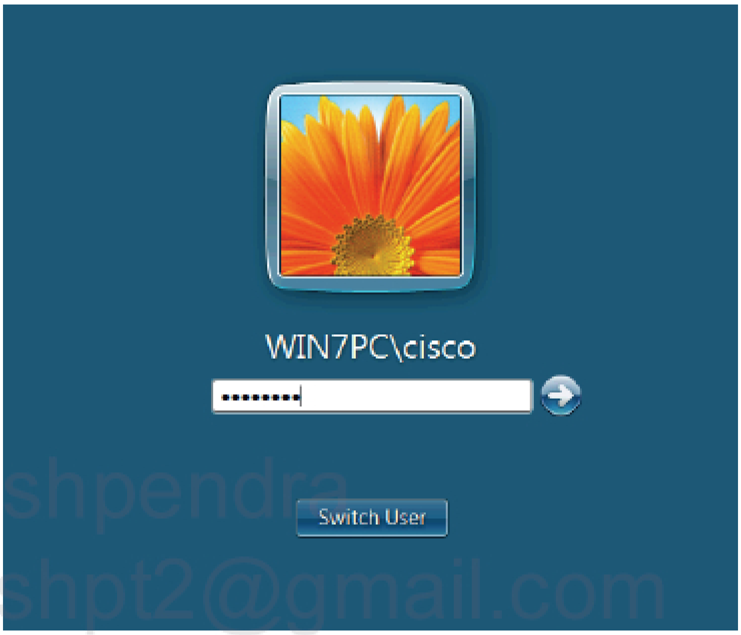
There is a Windows 7 host connected to SW1 port 0/7 through the IP Phone. By default the PC is placed in VLAN 10 and should get IP address from 10.1.10.0/24 network. The PC should be a member of Active Directory.
If not, re-join Active Directory domain **micronics.local** using **employee1/Micronics1** user credentials.

Configuration

Complete these steps:

Step 1 Win7 PC configuration.

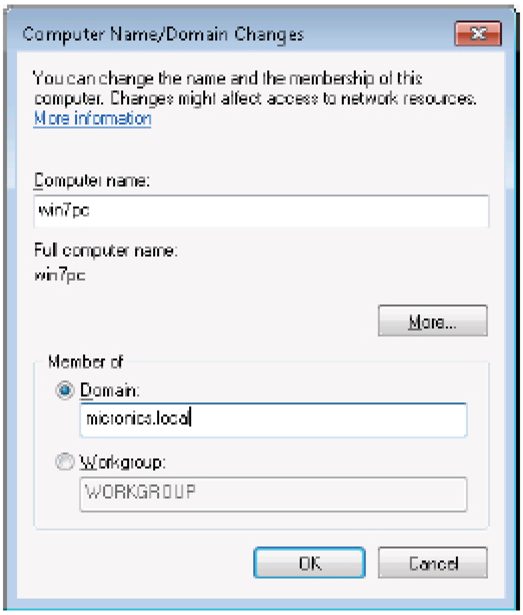
- Using VNC client connect to Win7 PC and authenticate using local account cisco/Student0.



WIN7PC\cisco

••••••••

- Right click on Computer and select Properties. On the following screen click Change Settings option next to the computer name. Check Domain option and provide the following settings. Click OK.



Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources. More information

Computer name:
win7pc

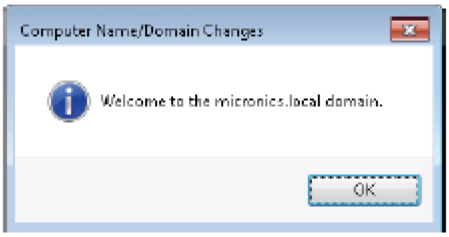
Full computer name:
win7pc

Member of

● Domain:
micronics.local

○ Workgroup:
WORKGROUP

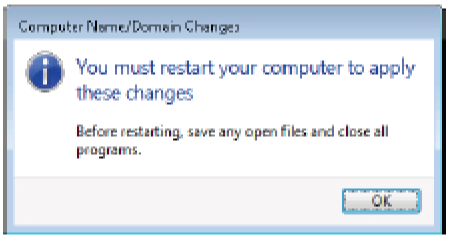
- Provide user's credentials of employee1/Micronics1 and click OK. After a while you should get the following successful message.



Computer Name/Domain Changes

Welcome to the micronics.local domain.

- You must restart the Win7 PC to apply the changes.



Computer Name/Domain Changes

You must restart your computer to apply these changes

Before restarting, save any open files and close all programs.

Step 2 Log in to Win7 PC using local user account of cisco/Student0.

LAB 3.9. Configure Wired 802.1x

Objectives

This lab shows how to configure 802.1x for wired environment.

IP Addressing and devices

Device	Interface	IP address
ISE	NIC	172.31.1.20
R1	Lo0	1.1.1.1/32
	E0/0	10.1.10.1/24
	E0/1	172.31.1.1/24
AD	NIC	172.31.1.200
WinXP	NIC	10.1.10.50/24
SW1	VLAN10	10.1.10.7/24

Task

There is a Windows 7 host connected to SW1 port 0/7 through the IP Phone. The IP Phone is authenticated using MAB configured in previous tasks. Configure Win7 PC to use its native supplicant with PEAP/MS-CHAPv2 only. Use Active Directory user employee1 and computer's account (member of Domain Computers AD group) for authentication. Upon successful authentication the user and machine should get full access to the network. Enable 802.1x low impact mode on the port and allow only DHCP, DNS, TFTP and ICMP traffic. Ensure the following authentication order:

- 802.1x
- MAB

The switch should time out 802.1x authentication method after 15 seconds and allow only one MAC address to be seen behind the IP Phone. If there are more MAC addresses the switch should NOT authenticate them and silently drop the packets.

You can disable Whitelist authorization rule and put the IP Phone back to the default Cisco-IP-Phone group.

Configuration

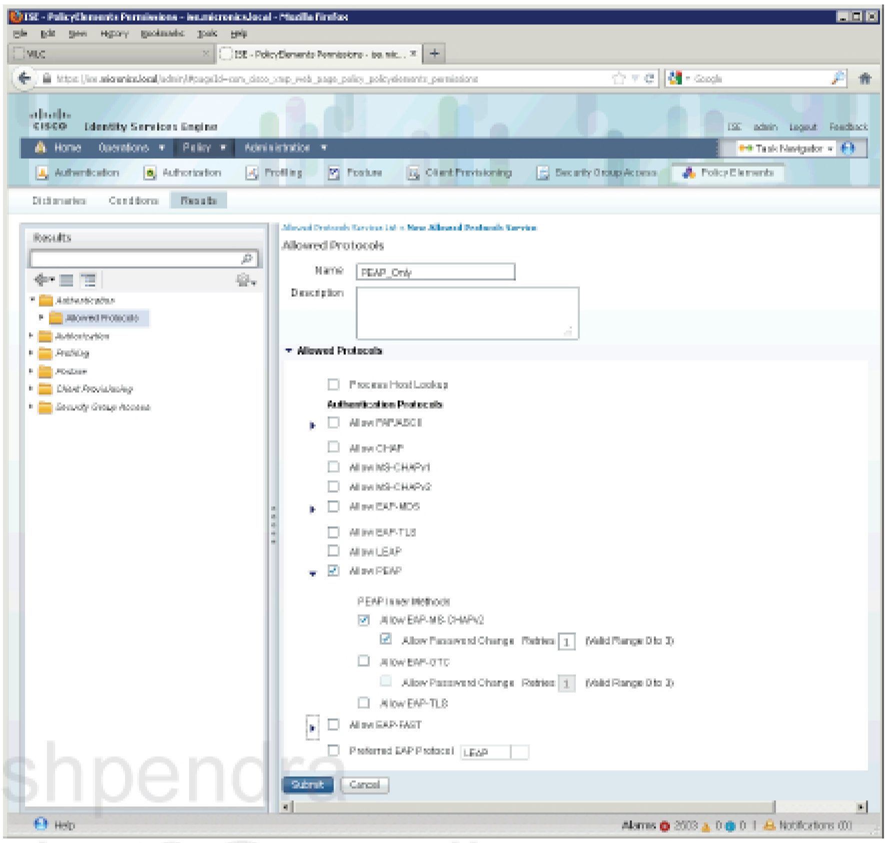
Complete these steps:

Step 1 Switch configuration.

```
!
ip access-list extended DEFAULT
remark DHCP
permit udp any eq bootpc any eq bootps
remark DNS
permit udp any any eq domain
remark TFTP
permit udp any any eq tftp
remark Ping
permit icmp any any
!
interface GigabitEthernet0/7
 ip access-group DEFAULT in
 authentication open
 authentication order dot1x mab
 dot1x timeout tx-period 5
!
ip device tracking
radius vsa send
!
```

Step 2 Create allowed protocols object.

- Go to **Policy > Policy Elements > Results > Authentication > Allowed Protocols** and click **Add**. Enter **PEAP_Only** as name, pick **Allow PEAP** with **Allow EAP-MS-CHAPv2**, uncheck all other methods and click **Submit**.



Allowed Protocols Services List > New Allowed Protocols Service

Allowed Protocols

Name PEAP_Only

Description

Allowed Protocols

□ Process Host Lookup

Authentication Protocols

□ Allow PAP/ASCII

□ Allow CHAP

□ Allow MS-CHAPv1

□ Allow MS-CHAPv2

□ Allow EAP-MD5

□ Allow EAP-TLS

□ Allow LEAP

☑ Allow PEAP

PEAP Inner Methods

☑ Allow EAP-MS-CHAPv2

☑ Allow Password Change Retries 1 (Valid Range 0 to 3)

□ Allow EAP-GTC

□ Allow Password Change Retries 1 (Valid Range 0 to 3)

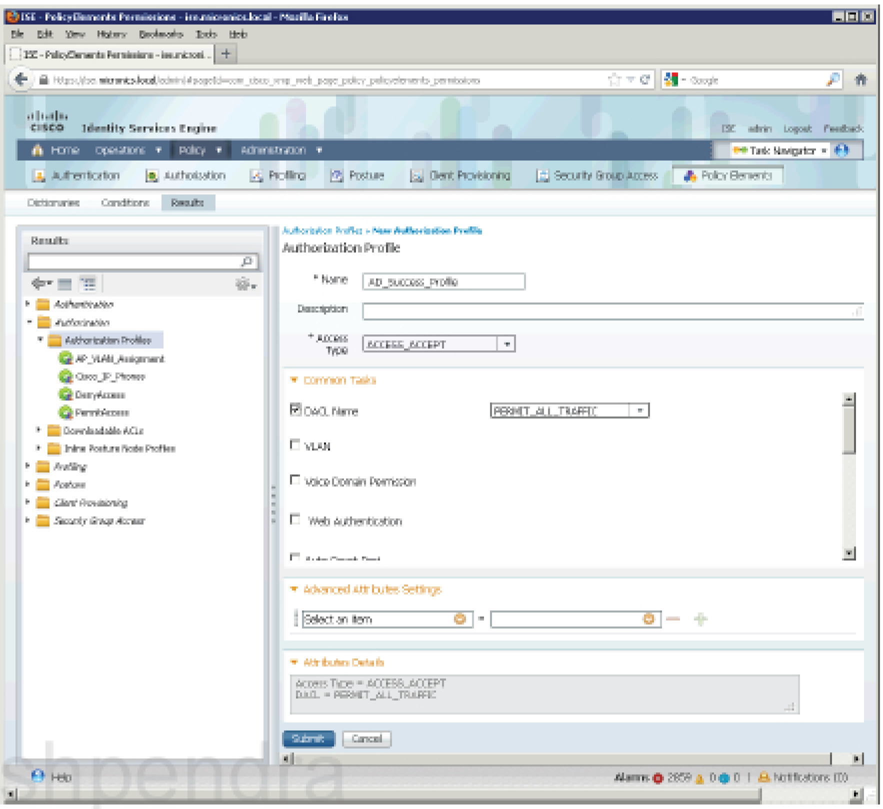
□ Allow EAP-TLS

□ Allow EAP-FAST

□ Preferred EAP Protocol LEAP

Step 3 Create authorization profile for AD clients to get full network access upon successful authorization.

- Go to **Policy > Policy Elements > Results > Authorization > Authorization Profiles** and click **Add**. Enter **AD_Success_Profile** as name, pick **DACL Name** checkbox and chose default **PERMIT_ALL_TRAFFIC** from the drop-down list. Click **Submit**.



Authorization Profiles > New Authorization Profile

Authorization Profile

* Name: AD_Success_Profile

Description:

* Access Type: ACCESS_ACCEPT

Common Tasks

☑ DACL Name: PERMIT_ALL_TRAFFIC

☐ VLAN

☐ Voice Domain Permission

☐ Web Authentication

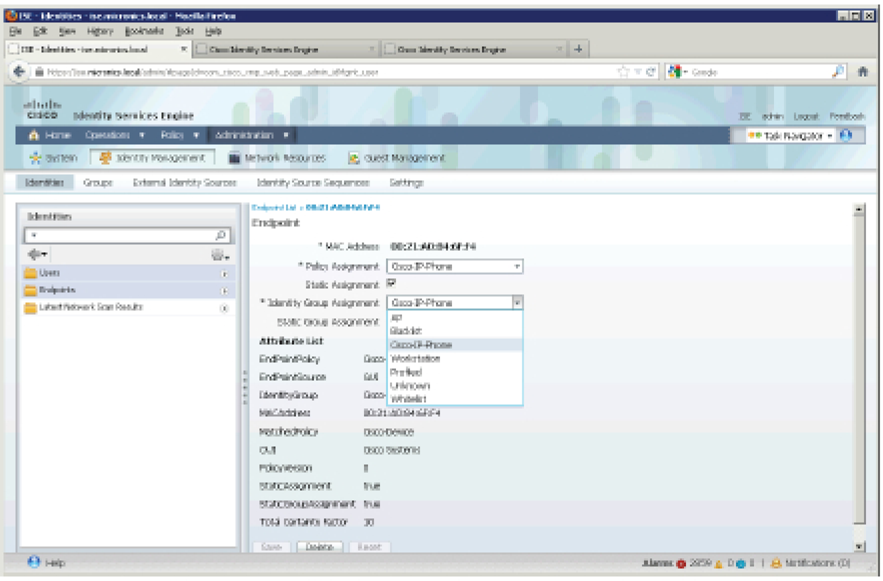
Advanced Attributes Settings

Attributes Details

Access Type = ACCESS_ACCEPT
DACL = PERMIT_ALL_TRAFFIC

Step 4 Move IP Phone MAC address to the default Identity Group and disable Whitelist authorization rule.

- Go to **Administration > Identity Management > Identities > Endpoints** and click **Cisco-IP-Phone** (an entry with IP Phone MAC address). Change the **Identity Group Assignment** to **Cisco-IP-Phone**. Click **Save**.



Endpoint List > 00:21:A0:84:6F:F4

Endpoint

* MAC Address: 00:21:A0:84:6F:F4

* Policy Assignment: Cisco-IP-Phone

Static Assignment: ☑

* Identity Group Assignment: Cisco-IP-Phone

Static Group Assignment:

Attribute List

EndPointPolicy: Cisco-

EndPointSource: GUI

IdentityGroup: Cisco-

MACAddress: 00:21:A0:84:6F:F4

MatchedPolicy: Cisco-Device

OUI: Cisco Systems

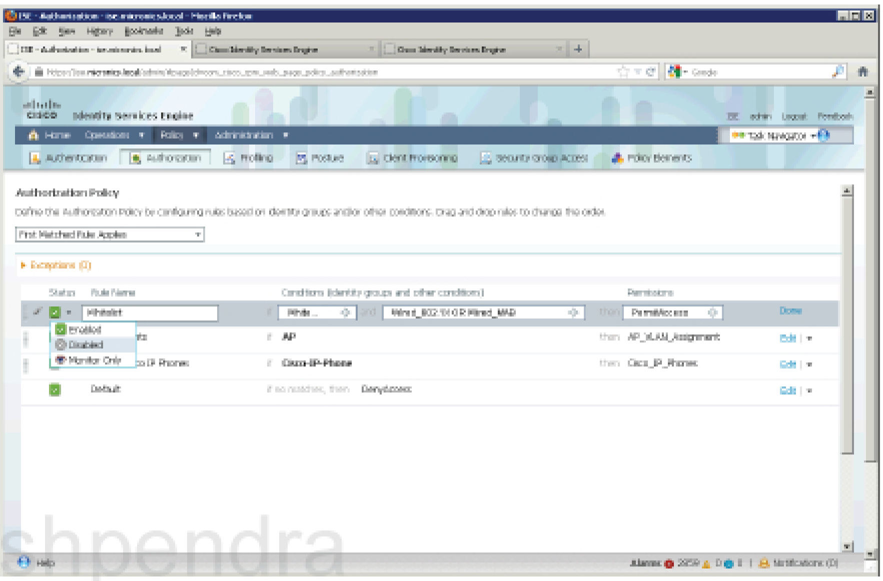
PolicyVersion: 8

StaticAssignment: true

StaticGroupAssignment: true

Total Certainty Factor: 30

- Go to **Policy > Authorization** and click **Edit** link next to the **Whitelist** rule. Click on the green icon and chose **Disabled**. Click **Done** and **Save**.



Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

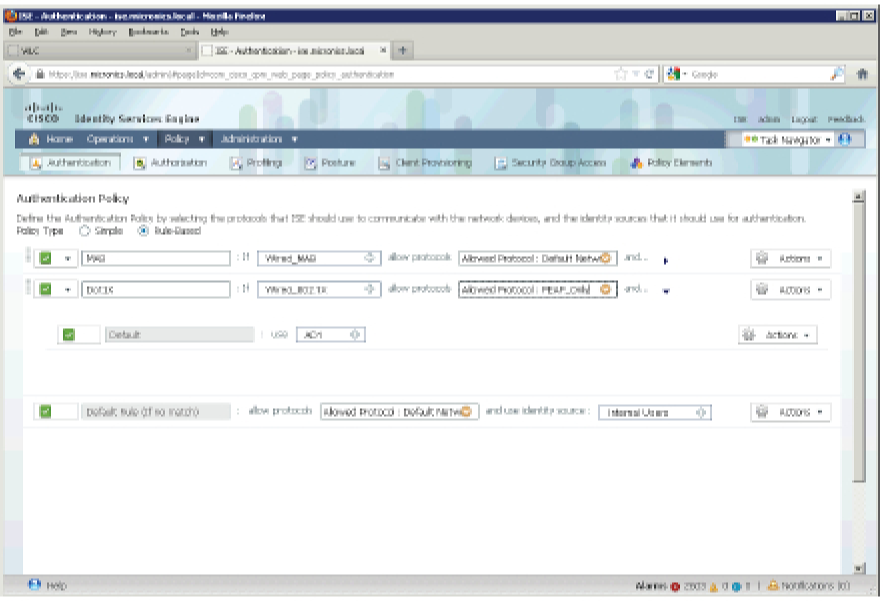
First Matched Rule Applies

Exceptions (0)

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions	
✓	Whitelist	if White... and Wired_802.1X OR Wired_MAB	then PermitAccess	Done
Enabled Disabled Monitor Only	...ts	if AP	then AP_VLAN_Assignment	Edit
	...to IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones	Edit
✓	Default	if no matches, then DenyAccess		Edit

Step 5 Add new authentication rule or edit default one.

- Go to **Policy > Authentication** and click orange arrow next to **Allowed Protocols** in **Dot1X** rule. Pick **PEAP_Only** from configured objects. Then click black arrow to show more options of the rule and change default identity source to **AD1**. Click **Save**.



Authentication Policy

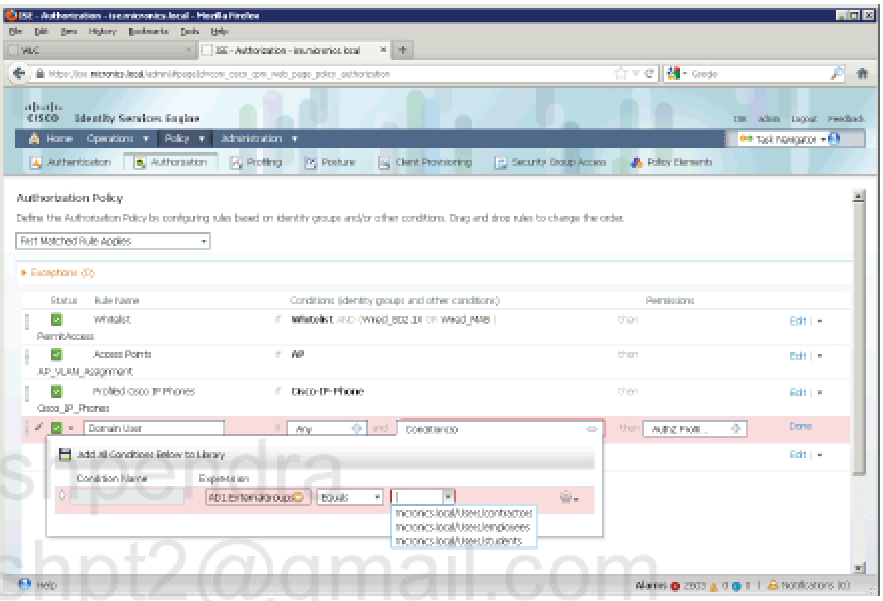
Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

Policy Type ○ Simple ● Rule-Based

✓	MAB	: If Wired_MAB	allow protocols Allowed Protocol : Default Netw...	and...
✓	Dot1X	: If Wired_802.1X	allow protocols Allowed Protocol : PEAP_Only	and...
✓	Default	: use AD1		
✓	Default Rule (If no match)	: allow protocols Allowed Protocol : Default Netw...	and use identity source : Internal Users	

Step 6 Create new authorization rule for domain users.

- Go to **Policy > Authorization** and insert new rule as a second to last (before the default one). Enter a name e.g. **Domain User** and create new Compound Condition where **AD1:ExternalGroup = micronics.local\Users/employees**.



Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

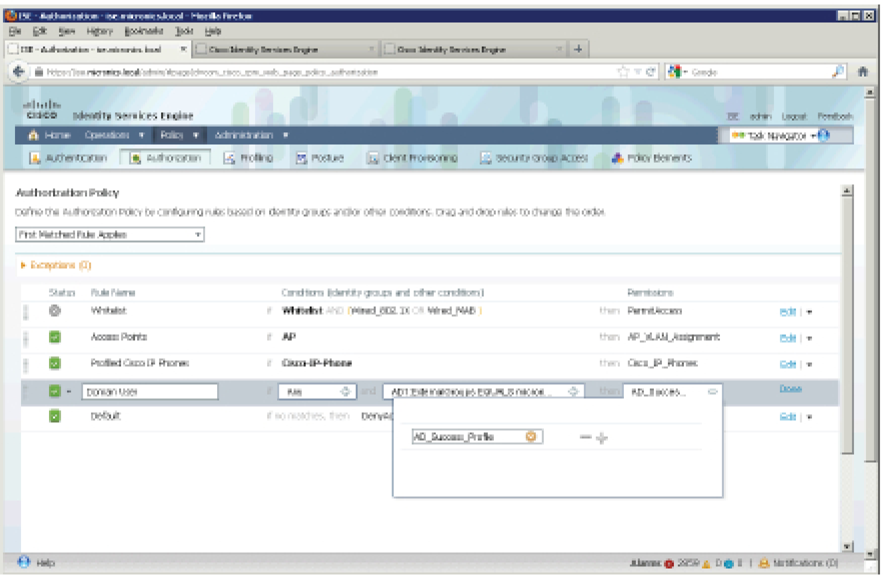
First Matched Rule Applies

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
✓	Whitelist	if	Whitelist AND (Wired_802.1X OR Wired_MAB)	then	PermitAccess
✓	Access Points	if	AP	then	AP_VLAN_Assignment
✓	Profiled Cisco IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phones
✓	Domain User	if	Any and Condition(s)	then	AuthZ Profil...

Condition Name: | Expression: AD1:ExternalGroups Equals

micronics.local/Users/contractors
micronics.local/Users/employees
micronics.local/Users/students

- As Permissions chose **AD_Success_Profile** already created in the previous steps. Click **Done**.



Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

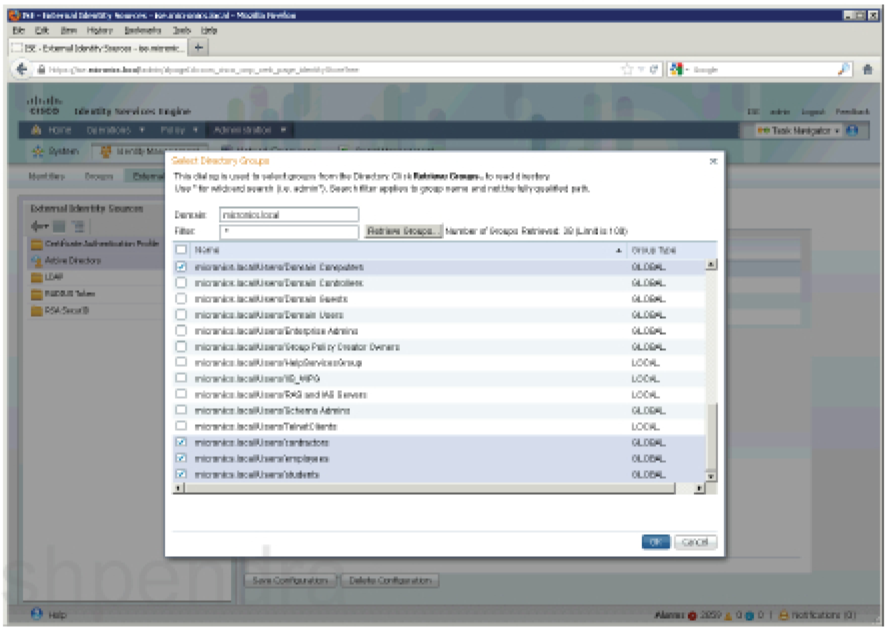
First Matched Rule Applies

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
○	Whitelist	if	Whitelist AND (Wired_802.1X OR Wired_MAB)	then	PermitAccess
✓	Access Points	if	AP	then	AP_VLAN_Assignment
✓	Profiled Cisco IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phones
✓	Domain User	if	Any and AD1:ExternalGroups EQUALS micron...	then	AD_Succes...
✓	Default		if no matches, then		DenyAccess

AD_Success_Profile

Step 7 Create authorization rule for domain computers.

- Go to **Administration > Identity Management > External Identity Sources > Active Directory** and click **Add > Select Groups From Directory** on **Groups** tab. Click **Retrieve Groups** and pick **micronics.local/Users/Domain Computers** group. Click **OK**.



Select Directory Groups

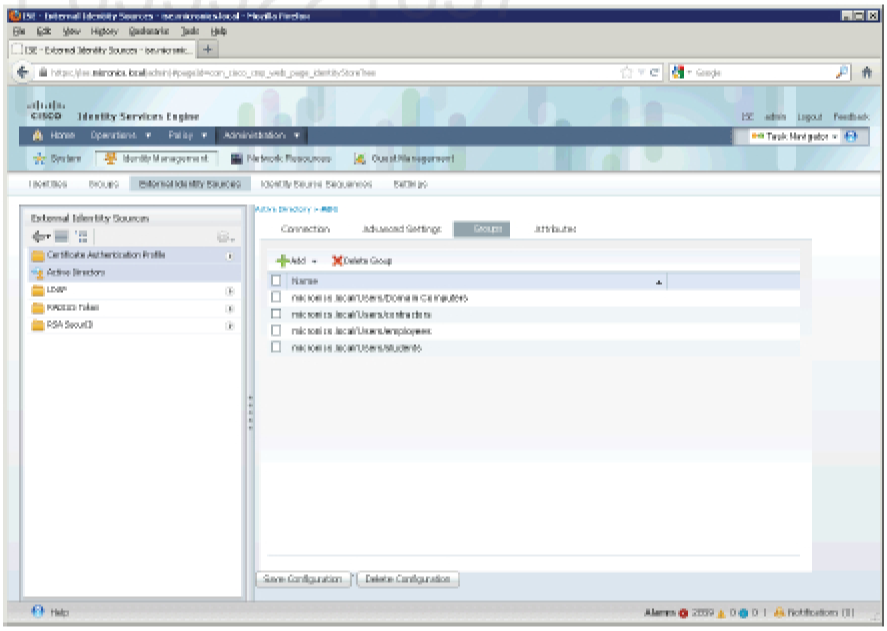
This dialog is used to select groups from the Directory. Click **Retrieve Groups..** to read directory.
Use * for wildcard search (i.e. admin*). Search filter applies to group name and not the fully qualified path.

Domain: micronics.local
Filter: *

Retrieve Groups.. Number of Groups Retrieved: 30 (Limit is 100)

□	Name	Group Type
☑	micronics.local/Users/Domain Computers	GLOBAL
□	micronics.local/Users/Domain Controllers	GLOBAL
□	micronics.local/Users/Domain Guests	GLOBAL
□	micronics.local/Users/Domain Users	GLOBAL
□	micronics.local/Users/Enterprise Admins	GLOBAL
□	micronics.local/Users/Group Policy Creator Owners	GLOBAL
□	micronics.local/Users/HelpServicesGroup	LOCAL
□	micronics.local/Users/IIS_WPG	LOCAL
□	micronics.local/Users/RAS and IAS Servers	LOCAL
□	micronics.local/Users/Schema Admins	GLOBAL
□	micronics.local/Users/TelnetClients	LOCAL
☑	micronics.local/Users/contractors	GLOBAL
☑	micronics.local/Users/employees	GLOBAL
☑	micronics.local/Users/students	GLOBAL

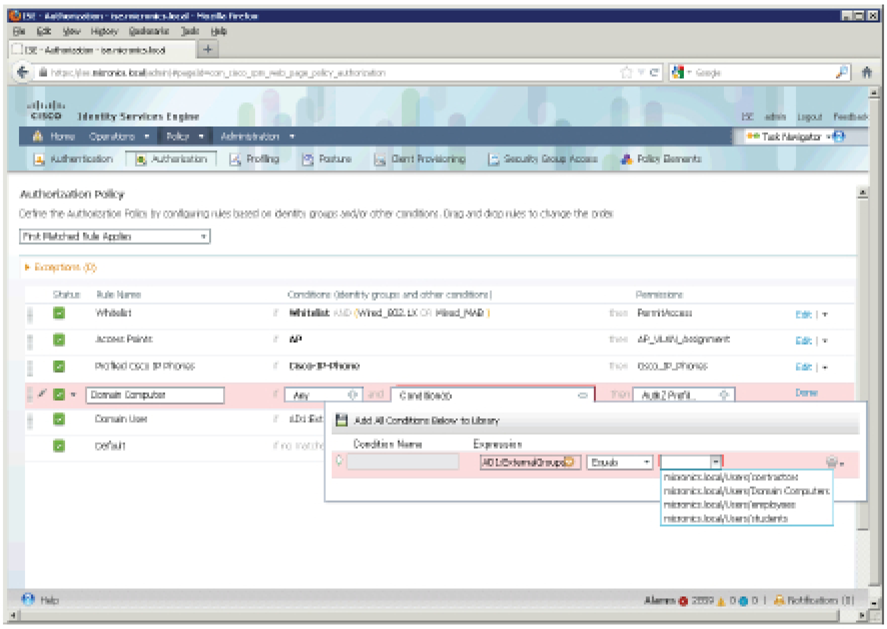
- Click **Save Configuration**.



Active Directory > ABC

□	Name
□	micronics.local/Users/Domain Computers
□	micronics.local/Users/contractors
□	micronics.local/Users/employees
□	micronics.local/Users/students

- Go to **Policy > Authorization** and insert new rule before **Domain User** rule. Enter a name e.g. **Domain Computer** and create new



Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

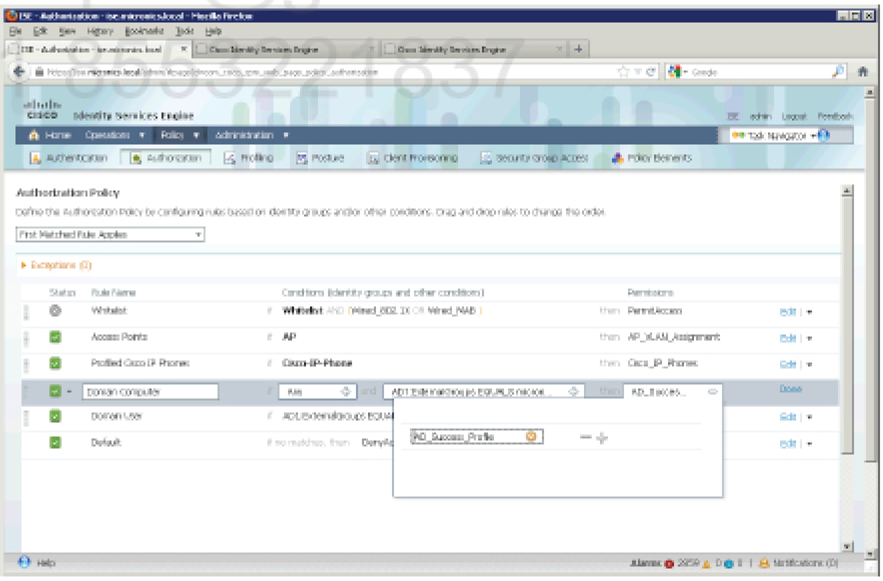
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Whitelist	if Whitelist AND (Wired_802.1X OR Wired_MAB)	then PermitAccess
✓	Access Points	if AP	then AP_VLAN_Assignment
✓	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones
✓	Domain Computer	if Any and Condition(s)	then AuthZ Profil...
✓	Domain User	if AD1:Ext...	
✓	Default	if no matche...	

Add All Conditions Below to Library

Condition Name	Expression		
	AD1:ExternalGroups	Equals	

micronics.local/Users/contractors
micronics.local/Users/Domain Computers
micronics.local/Users/employees
micronics.local/Users/students

- As Permissions chose **AD_Success_Profile** already created in the previous steps. Click **Done**.



Authorization Policy

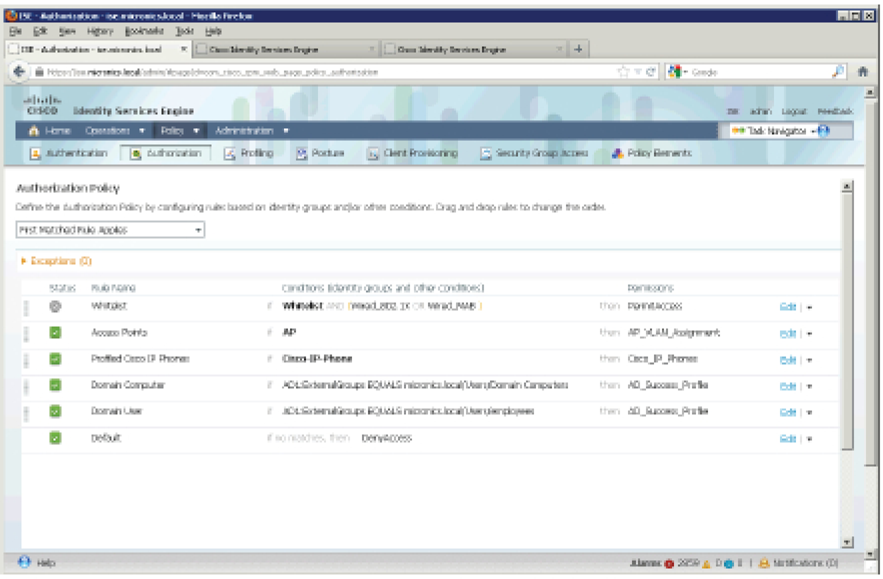
Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
○	Whitelist	if Whitelist AND (Wired_802.1X OR Wired_MAB)	then PermitAccess
✓	Access Points	if AP	then AP_VLAN_Assignment
✓	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones
✓	Domain Computer	if Any and AD1:ExternalGroups EQUALS microni...	then AD_Succes...
✓	Domain User	if AD1:ExternalGroups EQUA...	
✓	Default	if no matches, then DenyA...	

AD_Success_Profile

- Click **Save**.



Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

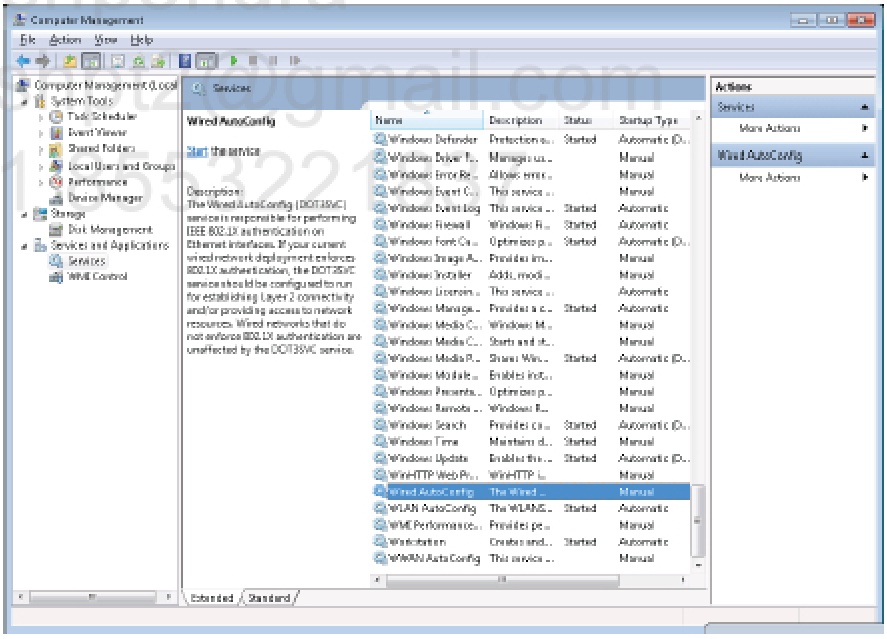
First Matched Rule Applies

Exceptions (0)

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
	Whitelist	if	**Whitelist** AND (Wired_802.1X OR Wired_MAB)	then	PermitAccess	Edit
✓	Access Points	if	**AP**	then	AP_VLAN_Assignment	Edit
✓	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones	Edit
✓	Domain Computer	if	AD1:ExternalGroups EQUALS micronics.local/Users/Domain Computers	then	AD_Success_Profile	Edit
✓	Domain User	if	AD1:ExternalGroups EQUALS micronics.local/Users/employees	then	AD_Success_Profile	Edit
✓	Default	if no matches, then	DenyAccess			Edit

Step 8 Win7 PC native supplicant configuration.

- Go to **Services** (services.msc) and Enable/Start **WiredAutoConfig** service.



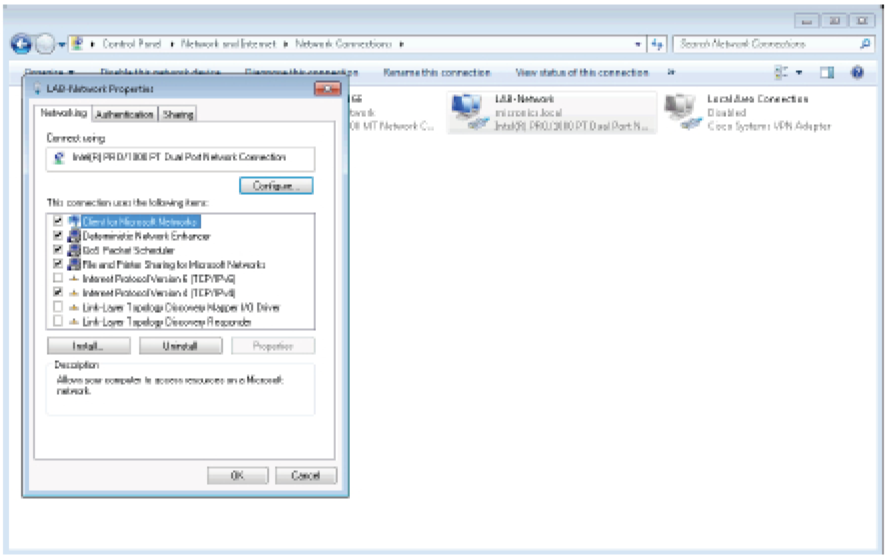
Wired AutoConfig

Start the service

Description:
The Wired AutoConfig (DOT3SVC) service is responsible for performing IEEE 802.1X authentication on Ethernet interfaces. If your current wired network deployment enforces 802.1X authentication, the DOT3SVC service should be configured to run for establishing Layer 2 connectivity and/or providing access to network resources. Wired networks that do not enforce 802.1X authentication are unaffected by the DOT3SVC service.

Name	Description	Status	Startup Type
Windows Defender	Protection a...	Started	Automatic (D...
Windows Driver F...	Manages us...		Manual
Windows Error Re...	Allows errs...		Manual
Windows Event C...	This service ...		Manual
Windows Event Log	This service ...	Started	Automatic
Windows Firewall	Windows Fi...	Started	Automatic
Windows Font Ca...	Optimizes p...	Started	Automatic (D...
Windows Image A...	Provides im...		Manual
Windows Installer	Adds, modi...		Manual
Windows Licensin...	This service ...		Automatic
Windows Manage...	Provides a c...	Started	Automatic
Windows Media C...	Windows M...		Manual
Windows Media C...	Starts and st...		Manual
Windows Media P...	Shares Win...	Started	Automatic (D...
Windows Module...	Enables inst...		Manual
Windows Presenta...	Optimizes p...		Manual
Windows Remote ...	Windows R...		Manual
Windows Search	Provides co...	Started	Automatic (D...
Windows Time	Maintains d...	Started	Manual
Windows Update	Enables the...	Started	Automatic (D...
WinHTTP Web Pr...	WinHTTP i...		Manual
Wired AutoConfig	The Wired ...		Manual
WLAN AutoConfig	The WLANS...	Started	Automatic
WMI Performance...	Provides pe...		Manual
Workstation	Creates and...	Started	Automatic
WWAN AutoConfig	This service ...		Manual

- Go to **Network Connections** right click on **LAB-Network** and select **Properties**. You should see **Authentication** tab.



Control Panel ▸ Network and Internet ▸ Network Connections ▸

LAB-Network Properties

Networking | Authentication | Sharing

Connect using:

Intel(R) PRO/1000 PT Dual Port Network Connection

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ Deterministic Network Enhancer
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☐ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☐ Link-Layer Topology Discovery Mapper I/O Driver
- ☐ Link-Layer Topology Discovery Responder

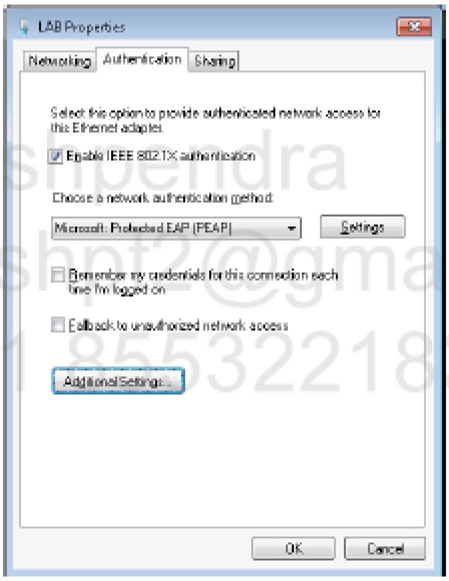
Description

Allows your computer to access resources on a Microsoft network.

LAB-Network
micronics.local
Intel(R) PRO/1000 PT Dual Port N...

Local Area Connection
Disabled
Cisco Systems VPN Adapter

- On the **Authentication** tab select options as follows:



LAB Properties

Networking | Authentication | Sharing

Select this option to provide authenticated network access for this Ethernet adapter.

☑ Enable IEEE 802.1X authentication

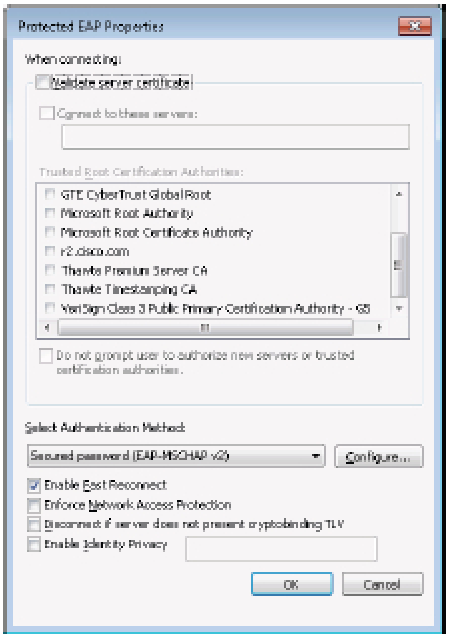
Choose a network authentication method:

Microsoft: Protected EAP (PEAP)

☐ Remember my credentials for this connection each time I'm logged on

☐ Fallback to unauthorized network access

Click on **Settings** button and uncheck **Validate server certificate** option.



Protected EAP Properties

When connecting:

□ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

□ GTE CyberTrust Global Root
□ Microsoft Root Authority
□ Microsoft Root Certificate Authority
□ r2.cisco.com
□ Thawte Premium Server CA
□ Thawte Timestamping CA
□ VeriSign Class 3 Public Primary Certification Authority - G5

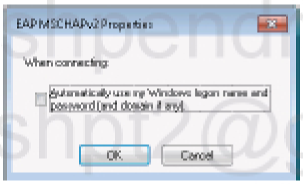
□ Do not prompt user to authorize new servers or trusted certification authorities.

Select Authentication Method:

Secured password (EAP-MSCHAP v2)

☑ Enable Fast Reconnect
□ Enforce Network Access Protection
□ Disconnect if server does not present cryptobinding TLV
□ Enable Identity Privacy

- Click on **Configure** button and uncheck the option:

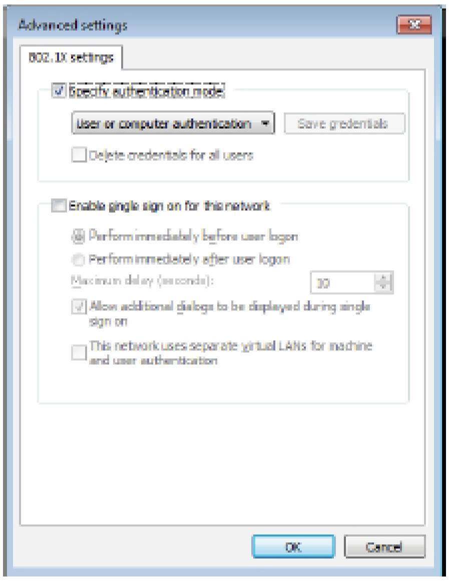


EAP MSCHAPv2 Properties

When connecting:

□ Automatically use my Windows logon name and password (and domain if any).

- Click **OK** and go back to the **Authentication** tab. Click **Additional Settings** button and check **Specify authentication mode** and select **User or computer authentication**. Click **OK** and close network adapter properties window.



Advanced settings

802.1X settings

☑ Specify authentication mode

User or computer authentication

□ Delete credentials for all users

□ Enable single sign on for this network

● Perform immediately before user logon
○ Perform immediately after user logon

Maximum delay (seconds): 10

☑ Allow additional dialogs to be displayed during single sign on

□ This network uses separate virtual LANs for machine and user authentication

Verification

Enable debugging on the switch:

```
debug radius
debug dot1x event
```

Bounce the switchport and check debug output.

```
SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#int g0/7
SW1(config-if)#shut
SW1(config-if)#no shu
SW1(config-if)#^Z

       // see the AuthManager state before authentication. The domain is UNKNOWN at
       the moment but there is MAC address on the port. Note that dot1x is running but
       it will fail over to mab after timeout.

SW1#sh auth sess int g0/7
            Interface:  GigabitEthernet0/7
          MAC Address:  0021.a084.6ff4
           IP Address:  Unknown
               Status:  Running
               Domain:  UNKNOWN
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-domain
     Oper control dir:  both
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A010A070000002F00ED9839
      Acct Session ID:  0x00000034
               Handle:  0x3500002F

Runnable methods list:
       Method   State
       dot1x    Running
       mab      Not run

       // First the IP Phone is being authenticated.

dot1x-ev(Gi0/7): New client notification from AuthMgr for 0x04000059 - 0021.a084.6ff4
%AUTHMGR-5-START: Starting 'dot1x' for client (0021.a084.6ff4) on Interface Gi0/7
AuditSessionID 0A010A070000002F00ED9839
%LINK-3-UPDOWN: Interface GigabitEthernet0/7, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/7, changed state to up

       // two dot1x retransmissions are configured by default
```

```
dot1x-ev(Gi0/7): Sending EAPOL packet to 0021.a084.6ff4
dot1x-ev(Gi0/7): Role determination not required
dot1x-ev(Gi0/7): Sending out EAPOL packet

dot1x-ev(Gi0/7): Sending EAPOL packet to 0021.a084.6ff4
dot1x-ev(Gi0/7): Role determination not required
dot1x-ev(Gi0/7): Sending out EAPOL packet

dot1x-ev(Gi0/7): Received an EAP Timeout
%DOT1X-5-FAIL: Authentication failed for client (0021.a084.6ff4) on Interface Gi0/7
AuditSessionID
dot1x-ev(Gi0/7): Sending event (2) to Auth Mgr for 0021.a084.6ff4
%AUTHMGR-7-RESULT: Authentication result 'no-response' from 'dot1x' for client
(0021.a084.6ff4) on Interface Gi0/7 AuditSessionID 0A010A070000002F00ED9839
dot1x-ev(Gi0/7): Received Authz fail for the client  0x04000059 (0021.a084.6ff4)
dot1x-ev(Gi0/7): Deleting client 0x04000059 (0021.a084.6ff4)
%AUTHMGR-7-FAILOVER: Failing over from 'dot1x' for client (0021.a084.6ff4) on Interface
Gi0/7 AuditSessionID 0A010A070000002F00ED9839

        // dot1x has failed for IP Phone because the phone has no dot1x supplicant, now
        the MAB is running

%AUTHMGR-5-START: Starting 'mab' for client (0021.a084.6ff4) on Interface Gi0/7
AuditSessionID 0A010A070000002F00ED9839
dot1x-ev:Delete auth client (0x04000059) message
dot1x-ev:Auth client ctx destroyed
dot1x-ev:Aborted posting message to authenticator state machine: Invalid client
RADIUS/ENCODE(00000034):Orig. component type = DOT1X
RADIUS(00000034): Config NAS IP: 10.1.10.7
RADIUS/ENCODE(00000034): acct_session_id: 52
RADIUS(00000034): sending

        // RADIUS authentication message is sent to ISE. Note that username is MAC
        address of the IP Phone and we have Service-Type=10 and NAS-Port-Type=15 in the
        message. The ISE will match that connection to the correct authentication rule
        based on those attributes.

RADIUS(00000034): Send Access-Request to 172.31.1.20:1812 id 1645/160, len 209
RADIUS:  authenticator B9 13 0A 78 2E E0 32 C7 - 75 A0 6C 56 0D D3 27 93
RADIUS:  User-Name           [1]   14  "0021a0846ff4"
RADIUS:  User-Password       [2]   18  *
RADIUS:  Service-Type        [6]   6   Call Check                [10]
RADIUS:  Framed-MTU          [12]  6   1500
RADIUS:  Called-Station-Id   [30]  19  "C4-64-13-6C-E8-07"
RADIUS:  Calling-Station-Id  [31]  19  "00-21-A0-84-6F-F4"
RADIUS:  Message-Authenticato[80]  18
RADIUS:   48 AF 08 93 30 FB 6C FA FD FB 10 37 56 E1 42 F5            [ H017VB]
RADIUS:  EAP-Key-Name        [102] 2   *
RADIUS:  Vendor, Cisco       [26]  49
RADIUS:   Cisco AVpair       [1]   43  "audit-session-id=0A010A070000002F00ED9839"
RADIUS:  NAS-Port-Type       [61]  6   Ethernet                  [15]
```

```
RADIUS:  NAS-Port            [5]    6   50007
RADIUS:  NAS-Port-Id         [87]   20  "GigabitEthernet0/7"
RADIUS:  NAS-IP-Address      [4]    6   10.1.10.7
RADIUS(00000034): Started 5 sec timeout
```

// RADIUS reply is received. This is an Access-Accept RADIUS message type so it contains some additional attributes. The most important attributes here are 'device-traffic-class=voice' and dACL name. The first attribute is very important in case of Multi-Auth. The switch knows what 'authentication domain' to use. Without this attribute the IP Phone could be authenticated in DATA domain as the MAC address of the phone is 'visible' in two VLANs (data vlan and voice vlan).

Also note that there is just dACL name in the RADIUS message. There are no dACL entries yet. The switch must ask for that dACL again to download ACEs (Access List Entries).

```
RADIUS: Received from id 1645/160 172.31.1.20:1812, Access-Accept, len 297
RADIUS:  authenticator 89 F8 81 A9 CD 82 74 B9 - C0 87 50 16 98 AF B0 7A
RADIUS:  User-Name           [1]    19  "00-21-A0-84-6F-F4"
RADIUS:  State               [24]   40
RADIUS:   52 65 61 75 74 68 53 65 73 73 69 6F 6E 3A 30 41  [ReauthSession:0A]
RADIUS:   30 31 30 41 30 37 30 30 30 30 30 30 32 46 30 30  [010A070000002F00]
RADIUS:   45 44 39 38 33 39                [ ED9839]
RADIUS:  Class               [25]   50
RADIUS:   43 41 43 53 3A 30 41 30 31 30 41 30 37 30 30 30  [CACS:0A010A07000]
RADIUS:   30 30 30 32 46 30 30 45 44 39 38 33 39 3A 49 53  [0002F00ED9839:IS]
RADIUS:   45 2F 31 34 33 35 35 38 35 35 33 2F 33 30 32 39  [ E/143558553/3029]
RADIUS:  Termination-Action  [29]   6   1
RADIUS:  Message-Authenticato[80]   18
RADIUS:   53 41 4D 42 74 C4 90 4F AB 57 80 A8 86 99 66 5D         [ SAMBtOWf]]
RADIUS:  Vendor, Cisco       [26]   34
RADIUS:   Cisco AVpair       [1]    28  "device-traffic-class=voice"
RADIUS:  Vendor, Cisco       [26]   75
RADIUS:   Cisco AVpair       [1]    69  "ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-
PERMIT_ALL_TRAFFIC-4f57e406"
RADIUS:  Vendor, Cisco       [26]   35
RADIUS:   Cisco AVpair       [1]    29  "profile-name=Cisco-IP-Phone"
RADIUS(00000034): Received from id 1645/160
RADIUS/DECODE: parse unknown cisco vsa "profile-name" - IGNORE
%MAB-5-SUCCESS: Authentication successful for client (0021.a084.6ff4) on Interface
Gi0/7 AuditSessionID 0A010A070000002F00ED9839
%AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client
(0021.a084.6ff4) on Interface Gi0/7 AuditSessionID 0A010A070000002F00ED9839
%EPM-6-POLICY_REQ: IP 0.0.0.0| MAC 0021.a084.6ff4| AuditSessionID
0A010A070000002F00ED9839| AUTHTYPE DOT1X| EVENT APPLY
%EPM-6-AAA: POLICY xACSACLx-IP-PERMIT_ALL_TRAFFIC-4f57e406| EVENT DOWNLOAD-REQUEST
RADIUS/ENCODE(00000000):Orig. component type = INVALID
RADIUS(00000000): Config NAS IP: 10.1.10.7
RADIUS(00000000): sending
```

```
    // The switch must download ACL from ISE. This is done by another RADIUS request
    where username is a dACL name. There must be three things configured on the switch
    to make this happen:
    -   aaa authorization network
    -   ip device tracking
    -   radius vsa send

RADIUS(00000000): Send Access-Request to 172.31.1.20:1812 id 1645/161, len 147
RADIUS:  authenticator D4 CD 40 0E F3 F8 F9 70 - 58 99 86 E7 AB 82 94 42
RADIUS:  NAS-IP-Address      [4]   6   10.1.10.7
RADIUS:  User-Name           [1]   41  "#ACSACL#-IP-PERMIT_ALL_TRAFFIC-4f57e406"
RADIUS:  Vendor, Cisco       [26]  32
RADIUS:   Cisco AVpair       [1]   26  "aaa:service=ip_admission"
RADIUS:  Vendor, Cisco       [26]  30
RADIUS:   Cisco AVpair       [1]   24  "aaa:event=acl-download"
RADIUS:  Message-Authenticato[80]  18
RADIUS:   D6 19 B1 96 C2 84 8C 39 B6 F8 59 11 B4 D5 CE 32               [ 9Y2]
RADIUS(00000000): Started 5 sec timeout

       // with the RADIUS Access-Accept message the switch gets ACl entries.

RADIUS: Received from id 1645/161 172.31.1.20:1812, Access-Accept, len 211
RADIUS:  authenticator FA 1C F2 32 B9 39 44 C8 - 62 9D 53 67 81 1D 8C EF
RADIUS:  User-Name           [1]   41  "#ACSACL#-IP-PERMIT_ALL_TRAFFIC-4f57e406"
RADIUS:  State               [24]  40
RADIUS:   52 65 61 75 74 68 53 65 73 73 69 6F 6E 3A 61 63  [ReauthSession:ac]
RADIUS:   31 66 30 31 31 34 30 30 30 30 30 42 37 32 35 31  [1f011400000B7251]
RADIUS:   30 36 42 36 44 44                 [ 06B6DD]
RADIUS:  Class               [25]  50
RADIUS:   43 41 43 53 3A 61 63 31 66 30 31 31 34 30 30 30  [CACS:ac1f0114000]
RADIUS:   30 30 42 37 32 35 31 30 36 42 36 44 44 3A 49 53  [00B725106B6DD:IS]
RADIUS:   45 2F 31 34 33 35 35 38 35 35 33 2F 33 30 33 30  [ E/143558553/3030]
RADIUS:  Termination-Action  [29]  6   1
RADIUS:  Message-Authenticato[80]  18
RADIUS:   8D 04 C6 C4 03 39 C9 E4 71 09 BB 6B D7 76 9F 5D             [ 9qkv]]
RADIUS:  Vendor, Cisco       [26]  36
RADIUS:   Cisco AVpair       [1]   30  "ip:inacl#1=permit ip any any"
RADIUS(00000000): Received from id 1645/161
%EPM-6-AAA: POLICY xACSACLx-IP-PERMIT_ALL_TRAFFIC-4f57e406| EVENT DOWNLOAD-SUCCESS
%EPM-6-IPEVENT: IP 0.0.0.0| MAC 0021.a084.6ff4| AuditSessionID
0A010A070000002F00ED9839| AUTHTYPE DOT1X| EVENT IP-WAIT
%AUTHMGR-5-SUCCESS: Authorization succeeded for client (0021.a084.6ff4) on Interface
Gi0/7 AuditSessionID 0A010A070000002F00ED9839
RADIUS/ENCODE(00000034):Orig. component type = DOT1X
RADIUS(00000034): Config NAS IP: 10.1.10.7
RADIUS(00000034): sending

       // if RADIUS accounting is enabled, another message is sent

RADIUS(00000034): Send Accounting-Request to 172.31.1.20:1813 id 1646/26, len 290
RADIUS:  authenticator 53 F1 C6 46 5A C5 72 97 - DC 43 AF C1 61 2B 4F 96
RADIUS:  Acct-Session-Id     [44]  10  "00000034"
```

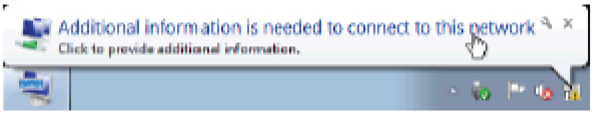
```
RADIUS:  Vendor, Cisco       [26]  49
RADIUS:   Cisco AVpair       [1]   43  "audit-session-id=0A010A070000002F00ED9839"
RADIUS:  User-Name           [1]   19  "00-21-A0-84-6F-F4"
RADIUS:  Vendor, Cisco       [26]  32
RADIUS:   Cisco AVpair       [1]   26  "connect-progress=Call Up"
RADIUS:  Acct-Authentic      [45]  6   RADIUS                    [1]
RADIUS:  Acct-Status-Type    [40]  6   Start                     [1]
RADIUS:  NAS-Port-Type       [61]  6   Ethernet                  [15]
RADIUS:  NAS-Port            [5]   6   50007
RADIUS:  NAS-Port-Id         [87]  20  "GigabitEthernet0/7"
RADIUS:  Called-Station-Id   [30]  19  "C4-64-13-6C-E8-07"
RADIUS:  Calling-Station-Id  [31]  19  "00-21-A0-84-6F-F4"
RADIUS:  Class               [25]  50
RADIUS:   43 41 43 53 3A 30 41 30 31 30 41 30 37 30 30 30  [CACS:0A010A07000]
RADIUS:   30 30 30 32 46 30 30 45 44 39 38 33 39 3A 49 53  [0002F00ED9839:IS]
RADIUS:   45 2F 31 34 33 35 35 38 35 35 33 2F 33 30 32 39  [ E/143558553/3029]
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  NAS-IP-Address      [4]   6   10.1.10.7
RADIUS:  Unsupported         [151] 10
RADIUS:   44 45 37 41 45 41 43 37          [ DE7AEAC7]
RADIUS:  Acct-Delay-Time     [41]  6   0
RADIUS(00000034): Started 5 sec timeout
RADIUS: Received from id 1646/26 172.31.1.20:1813, Accounting-response, len 20
RADIUS:  authenticator 61 24 0C 05 95 95 5F 37 - 32 D5 DA 19 89 98 FD 40
```

// check the authentication session again. You should see correct domain (VOICE) based on the attribute received from the ISE, and ACL name. You will not see ACL entries here.

```
SW1#sh auth sess int g0/7
            Interface:  GigabitEthernet0/7
          MAC Address:  0021.a084.6ff4
           IP Address:  Unknown
            User-Name:  00-21-A0-84-6F-F4
               Status:  Authz Success
               Domain:  VOICE
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
              ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-4f57e406
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A010A070000002F00ED9839
      Acct Session ID:  0x00000034
               Handle:  0x3500002F

Runnable methods list:
       Method   State
```

```
dot1x    Failed over
mab      Authc Success
```

Bounce the Win7 NIC (LAB-Network) to trigger dot1x and check debug output. Click on the balloon message that appears and provide user/pass of employee1/Micronics1 to authenticate.



Additional information is needed to connect to this network

Click to provide additional information.

```
dot1x-ev(Gi0/7): Dot1x authentication started for 0xC300005B (0026.55d0.0d56)
%AUTHMGR-5-START: Starting 'dot1x' for client (0026.55d0.0d56) on Interface Gi0/7
AuditSessionID 0A010A070000003100EE1DEA

        // you may see more dot1x reties here. It depends on configured tx-period and
        how quickly you provide username and password to the supplicant.

dot1x-ev(Gi0/7): Sending EAPOL packet to 0026.55d0.0d56
dot1x-ev(Gi0/7): Role determination not required
dot1x-ev(Gi0/7): Sending out EAPOL packet

dot1x-ev(Gi0/7): Sending EAPOL packet to 0026.55d0.0d56
dot1x-ev(Gi0/7): Role determination not required
dot1x-ev(Gi0/7): Sending out EAPOL packet

dot1x-ev(Gi0/7): Role determination not required
dot1x-ev:Enqueued the eapol packet to the global authenticator queue
EAPOL pak dump rx
EAPOL Version: 0x1  type: 0x0  length: 0x000E
dot1x-ev: dot1x_auth_queue_event: Int Gi0/7 CODE= 2,TYPE= 1,LEN= 14

dot1x-ev(Gi0/7): Received pkt saddr =0026.55d0.0d56 , daddr = 0180.c200.0003,
                    pae-ether-type = 888e.0100.000e
dot1x-ev(Gi0/7): dot1x_sendRespToServer: Response sent to the server from 0xC300005B
(0026.55d0.0d56)
RADIUS/ENCODE(00000036):Orig. component type = DOT1X
RADIUS(00000036): Config NAS IP: 10.1.10.7
RADIUS/ENCODE(00000036): acct_session_id: 54
RADIUS(00000036): sending

        // RADIUS authentication message is sent. It includes provided username and
        Service-Type=2 and NAS-Port-Type=15 which should be matched by ISE to the
        correct authentication rule. Note that the ISE is configured with Allowed
        Protocols where only PEAP/MS-CHAPv2 is selected. This will trigger another set
        of RADIUS messages to negotiate and build TLS tunnel and authenticate securely
        over that tunnel.

RADIUS(00000036): Send Access-Request to 172.31.1.20:1812 id 1645/162, len 204
```

```
RADIUS:  authenticator 07 CE 7D 37 DF DA B8 D6 - 00 16 97 E8 97 BC 0F 4F
RADIUS:  User-Name           [1]   11  "employee1"
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  Framed-MTU          [12]  6   1500
RADIUS:  Called-Station-Id   [30]  19  "C4-64-13-6C-E8-07"
RADIUS:  Calling-Station-Id  [31]  19  "00-26-55-D0-0D-56"
RADIUS:  EAP-Message         [79]  16
RADIUS:   02 01 00 0E 01 65 6D 70 6C 6F 79 65 65 31         [ employee1]
RADIUS:  Message-Authenticato[80]  18
RADIUS:   9C 1F 81 CF 9F 9E 64 34 E5 DA AC 68 D2 57 C1 41             [ d4hWA]
RADIUS:  EAP-Key-Name        [102] 2   *
RADIUS:  Vendor, Cisco       [26]  49
RADIUS:   Cisco AVpair       [1]   43  "audit-session-id=0A010A070000003100EE1DEA"
RADIUS:  NAS-Port-Type       [61]  6   Ethernet                  [15]
RADIUS:  NAS-Port            [5]   6   50007
RADIUS:  NAS-Port-Id         [87]  20  "GigabitEthernet0/7"
RADIUS:  NAS-IP-Address      [4]   6   10.1.10.7
RADIUS(00000036): Started 5 sec timeout

       // RADIUS challenge message is to negotiate PEAP and build TLS tunnel.

RADIUS: Received from id 1645/162 172.31.1.20:1812, Access-Challenge, len 119
RADIUS:  authenticator 5B FB D9 3A 4B B5 74 93 - 4C 54 58 C8 BC A1 08 56
RADIUS:  State               [24]  73
RADIUS:   33 37 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 30  [37CPMSessionID=0]
RADIUS:   41 30 31 30 41 30 37 30 30 30 30 30 30 33 31 30  [A010A070000000310]
RADIUS:   30 45 45 31 44 45 41 3B 32 38 53 65 73 73 69 6F  [0EE1DEA;28Sessio]
RADIUS:   6E 49 44 3D 49 53 45 2F 31 34 33 35 35 38 35 35  [nID=ISE/14355855]
RADIUS:   33 2F 33 30 33 32 3B           [ 3/3032;]
RADIUS:  EAP-Message         [79]  8
RADIUS:   01 47 00 06 19 21                [ G!]
RADIUS:  Message-Authenticato[80]  18
RADIUS:   48 01 CE 89 9D 3B 52 D4 77 5C 83 63 A8 16 D2 31           [ H;Rw\cl]
RADIUS(00000036): Received from id 1645/162
RADIUS/DECODE: EAP-Message fragments, 6, total 6 bytes
dot1x-ev(Gi0/7): Sending EAPOL packet to 0026.55d0.0d56
dot1x-ev(Gi0/7): Role determination not required
dot1x-ev(Gi0/7): Sending out EAPOL packet
dot1x-ev(Gi0/7): Role determination not required
dot1x-ev:Enqueued the eapol packet to the global authenticator queue
EAPOL pak dump rx
EAPOL Version: 0x1  type: 0x0  length: 0x007B
dot1x-ev: dot1x_auth_queue_event: Int Gi0/7 CODE= 2,TYPE= 25,LEN= 123

dot1x-ev(Gi0/7): Received pkt saddr =0026.55d0.0d56 , daddr = 0180.c200.0003,
                    pae-ether-type = 888e.0100.007b
dot1x-ev(Gi0/7): dot1x_sendRespToServer: Response sent to the server from 0xC300005B
(0026.55d0.0d56)
RADIUS/ENCODE(00000036):Orig. component type = DOT1X
RADIUS(00000036): Config NAS IP: 10.1.10.7
RADIUS/ENCODE(00000036): acct_session_id: 54
```

```
RADIUS(00000036): sending

        // another RADIUS request is sent. Note that RADIUS message does NOT contain
        any password. There is just username. The username/password will be carried
        securely by EAP which is sent using RADIUS AVP/79.

RADIUS(00000036): Send Access-Request to 172.31.1.20:1812 id 1645/163, len 386
RADIUS:  authenticator F0 57 7F CA 9E 1E DE B0 - 69 9F 41 77 5C 32 EC CE
RADIUS:  User-Name           [1]   11  "employee1"
RADIUS:  Service-Type        [6]   6   Framed                  [2]
RADIUS:  Framed-MTU          [12]  6   1500
RADIUS:  Called-Station-Id   [30]  19  "C4-64-13-6C-E8-07"
RADIUS:  Calling-Station-Id  [31]  19  "00-26-55-D0-0D-56"
RADIUS:  EAP-Message         [79]  125
RADIUS:   02 47 00 7B 19 80 00 00 00 71 16 03 01 00 6C 01 00 00 68 03 01 51 06 B6 F7 BA
BC F9 9E 91 CF 87 8E 3C FF 03 AF E3 E6 F2 65 29 F8 20 0F D5 12 97 87 AF DA 54 E1 00 00
18 00 2F 00 35 00 05 00 0A C0 13 C0 14 C0 09 C0 0A 00 32 00 38 00 13 00 04 01 00 00 27
[G{qlhQ<e) T/528']
RADIUS:   FF 01 00 01 00 00 00 00 0E 00 0C 00 00 09 65 6D 70 6C 6F 79 65 65 31 00 0A 00
06 00 04 00 17 00 18 00 0B 00 02 01 00         [ employee1]
RADIUS:  Message-Authenticato[80]  18
RADIUS:   24 89 84 4A A5 44 1A 9A CC AA 7F 82 07 25 5E 03             [ $JD?^]
RADIUS:  EAP-Key-Name        [102] 2   *
RADIUS:  Vendor, Cisco       [26]  49
RADIUS:   Cisco AVpair       [1]   43  "audit-session-id=0A010A070000003100EE1DEA"
RADIUS:  NAS-Port-Type       [61]  6   Ethernet                [15]
RADIUS:  NAS-Port            [5]   6   50007
RADIUS:  NAS-Port-Id         [87]  20  "GigabitEthernet0/7"
RADIUS:  State               [24]  73
RADIUS:   33 37 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 30  [37CPMSessionID=0]
RADIUS:   41 30 31 30 41 30 37 30 30 30 30 30 30 33 31 30  [A010A07000000310]
RADIUS:   30 45 45 31 44 45 41 3B 32 38 53 65 73 73 69 6F  [0EE1DEA;28Sessio]
RADIUS:   6E 49 44 3D 49 53 45 2F 31 34 33 35 35 38 35 35  [nID=ISE/14355855]
RADIUS:   33 2F 33 30 33 32 3B             [ 3/3032;]
RADIUS:  NAS-IP-Address      [4]   6   10.1.10.7
RADIUS(00000036): Started 5 sec timeout

        // This RADIUS challenge message is for ISE authentication. PEAP uses server
        side authentication using digital certificate. This is why that message is so
        long - it contains ISE certificate.

RADIUS: Received from id 1645/163 172.31.1.20:1812, Access-Challenge, len 1131
RADIUS:  authenticator F0 C8 1D 6C 96 CE 6F 38 - 6D DD 18 94 6A 57 24 5C
RADIUS:  State               [24]  73
RADIUS:   33 37 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 30  [37CPMSessionID=0]
RADIUS:   41 30 31 30 41 30 37 30 30 30 30 30 30 33 31 30  [A010A07000000310]
RADIUS:   30 45 45 31 44 45 41 3B 32 38 53 65 73 73 69 6F  [0EE1DEA;28Sessio]
RADIUS:   6E 49 44 3D 49 53 45 2F 31 34 33 35 35 38 35 35  [nID=ISE/14355855]
RADIUS:   33 2F 33 30 33 32 3B             [ 3/3032;]
RADIUS:  EAP-Message         [79]  255
RADIUS:   01 48 03 F4 19 C0 00 00 0B 0A 16 03 01 00 51 02 00 00 4D 03 01 51 06 B6 F7 B2 45 7B 2C BF 39 30 04 98 52 3A 89 85 30 4A 89 92 1E 26 D3 58 28  [BQMQE[,90R:0J&X(]
RADIUS:   47 51 80 49 E1 00 20 FC B0 69 4B BC A5 C8 70 0C F6 3B E4 B6 3A 69 A8 2C FF 50 33 13 0A FA AA FC 60 5E 60 FA 57  [GQI iKp:,P3'^'W]
RADIUS:   77 6A 00 35 00 00 05 FF 01 00 01 00 16 03 01 0A A6 0B 00 0A A2 00 0A 9F 00 06 06 30 82 06 02 30 82 04 EA A0 03 02 01 02 02 0A 61 27 FF 80 00 00 00 00 00 03 30 0D 06
09 2A 86 48 86 F7 0D 01 01 05 05 00 30 4F 31 15 30 13 06 0A 09 92 26 89 93 F2 2C  [wj5 00a'0*H001 0&,]
```

```
RADIUS:   64 01 19 16 05 6C 6F 63 61 6C 31 19 30 17 06 0A 09 92 26 89 93 F2 2C 64 01 19 16 09 6D 69 63 72 6F  [dlocal10i,dmicro]
RADIUS:   6E 69 63 73 31 1B 30 19 06 03 55 04 03 13 12 63 61 2E 6D 69 63 72 6F 6E  [nics10Uca.micron]
RADIUS:   69 63 73 2E 6C 6F 63 61 6C 30 1E 17 0D 31 32 31 31 32 30  [ics.local0121120]
RADIUS:   31 39 34 39 31 36 5A 17 0D 31 34          [ 194916Z14]
RADIUS:  EAP-Message         [79]  255
RADIUS:   31 31 32 30 31 39 34 39 31 36 5A 30 5A 31 0B 30 09 06 03 55  [1120194916Z0Z10U]
RADIUS:   04 06 13 02 75 73 31 0B 30 09 06 03 55 04 08 13 02 63 61 31 12 30 10 06 03 55 04 0A 13 09 6D 69 63 72 6F 6E  [us10Uca10Umicron]
RADIUS:   69 63 73 31 0C 30 0A 06 03 55 04 0B 13 03 6C 61 62 31 1C 30 1A 06 03 55 04 03 13 13 69 73 65 2E  [ics10Ulab10Uise.]
RADIUS:   6D 69 63 72 6F 6E 69 63 73 2E 6C 6F 63 61 6C 30  [micronics.local0]
RADIUS:   82 01 22 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01 05 00 03 82 01 0F 00 30 82 01 0A 02 82 01 01 00 B1 23 13 7A 04 C5 03 F4 95 32 21 93 02 0B 3C CF BF 6C A2 F0 0B FC 12
0F B7 C9 05 05 F5 35 B6 71 1A 6E 0C 38 A3 07 98 11 1E 4F  ["0*H0#z2!<l5qn80]
RADIUS:   BA 25 51 70 FB F5 7B C0 2C 82 C8 44 92 3A C1 47 85 6D 23 BF 2B C6 B0 4A 15 C0 FA FC 70 3E D6 94 4D DB 4E  [%Qp{,D:G'#.Jp>MN]
RADIUS:   F0 0D F0 89 4C 60 C8 59 61 AE 0E 61 75 70 55 51 15 18 84 5C E0 36 DA 01 C9 78 37 12 1E FA 25 6F E0 9F 0C 66 33 B8 98 D5   [ L'YaupUQ\6)7?f3]
RADIUS:  EAP-Message         [79]  255
RADIUS:   14 91 6B AF 74 93 29 5A 11 9B E0 31 C8 E0 84 B6 B3 48 64 A1 35 AF A0 90 1B BA 02 DA 36 2A 0B 81 6A BA 1B 1A 22 6A 78 F1 17 C9 01 CE 6B 48 53  [kt)Z1Hd5*j"xmHS]
RADIUS:   B8 44 1C 13 62 7E EE EB 6C EE 40 1D F3 FA 3B F0 84 3A C5 8A 76 86 C6 67 8D 3D 9A 0B CF 19 43 A6 07 B3 DC 0E 3F DE 24 30 C9 0D 5E 0E 69  [Db~l@:vg=C?$0^i]
RADIUS:   6F 8D 3E 95 BC 5B B3 F5 DC 0B 0D DC C6 D2 5B C0 54 9F CC F5 1A 01 4E BE 51 5B AC 16 45 F7 27 76 A2 73 FA 3C 3F 2E 06 19 C9 20  [o>[TNQ[E'vs<?. ]
RADIUS:   87 C2 A4 14 6D 02 03 01 00 01 A3 82 02 83 30 82 02 CF 30 0B 06 03 55 1D 0F 04 04 03 02 05 A0 30 1D 06 03 55 1D 0E 04 16 04 14 0A 39 A3 EE 5E 6B 4B 00 32 55 BF EF 95
6D 1B 9D AF B8 07 09 30 13 06 03 55 1D 25  [m000U0U9^kK2U'0U%]
RADIUS:   04 0C 30 0A 06 08 2B 06 01 05 05 07 03 01 30 1F 06 03 55 1D 23 04 18 30 16 80 14 4E 48 F2 B6 65 69 20 34 9F F9 7B 81 62 B0 58 34  [0+0U#0NHei (4)bX4]
RADIUS:   B3 86 31 44 30 82 01              [ 1D0]
RADIUS:  EAP-Message         [79]  255
RADIUS:   0E 06 03 55 1D 1F 04 82 01 05 30 82 01 01 30 81 FE A0 81 FB A0 81 F8 86 81 B8 6C 64 61 70 3A 2F 2F 2F 43 4E 3D 63 61  [U001ldap:///CN=ca]
RADIUS:   2E 6D 69 63 72 6F 6E 69 63 73 2E 6C 6F 63 61 6C  [.micronics.local]
RADIUS:   2C 43 4E 3D 64 63 2C 43 4E 3D 43 44 50 2C 43 4E  [,CN=dc,CN=CDP,CN]
RADIUS:   3D 50 75 62 6C 69 63 25 32 30 4B 65 79 25 32 30  [=Public%20Key%20]
RADIUS:   53 65 72 76 69 63 65 73 2C 43 4E 3D 53 65 72 76  [Services,CN=Serv]
RADIUS:   69 63 65 73 2C 43 4E 3D 43 6F 6E 66 69 67 75 72  [ices,CN=Configur]
RADIUS:   61 74 69 6F 6E 2C 44 43 3D 6D 69 63 72 6F 6E 69  [ation,DC=microni]
RADIUS:   63 73 2C 44 43 3D 6C 6F 63 61 6C 3F 63 65 72 74  [cs,DC=local?cert]
RADIUS:   69 66 69 63 61 74 65 52 65 76 6F 63 61 74 69 6F  [ificateRevocatio]
RADIUS:   6E 4C 69 73 74 3F 62 61 73 65 3F 6F 62 6A 65 63  [nList?base?objec]
RADIUS:   74 43 6C 61 73 73 3D 63 52 4C 44 69 73 74 72 69  [tClass=cRLDistri]
RADIUS:   62 75 74 69 6F 6E 50 6F 69 6E 74 86 3B 68 74 74 70  [butionPoint;http]
RADIUS:   3A 2F 2F 64 63 2E 6D 69 63 72 6F 6E 69 63 73 2E  [://dc.micronics.]
RADIUS:   6C 6F 63 61 6C 2F 43 65 72 74 45 6E 72 6F 6C 6C  [local/CertEnroll]
RADIUS:   2F 63 61 2E 63            [ /ca.c]
RADIUS:  Message-Authenticato[80]  18
RADIUS:   A1 DC DF 16 43 95 CA 9C B4 3C 55 31 71 31 41 01           [ C<U1q1A]
RADIUS(00000036): Received from id 1645/163
RADIUS/DECODE: EAP-Message fragments, 253+253+253+253, total 1012 bytes

<snip>

dot1x-ev(Gi0/7): Received pkt saddr =0026.55d0.0d56 , daddr = 0180.c200.0003,
                    pae-ether-type = 888e.0100.002b
dot1x-ev(Gi0/7): dot1x_sendRespToServer: Response sent to the server from 0xC300005B
(0026.55d0.0d56)
RADIUS/ENCODE(00000036):Orig. component type = DOT1X
RADIUS(00000036): Config NAS IP: 10.1.10.7
RADIUS/ENCODE(00000036): acct_session_id: 54
RADIUS(00000036): sending
RADIUS(00000036): Send Access-Request to 172.31.1.20:1812 id 1645/171, len 306
RADIUS:  authenticator 3F 59 C2 9B F2 19 B0 62 - 48 B9 7F 62 62 24 C0 46
RADIUS:  User-Name           [1]   11  "employee1"
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  Framed-MTU          [12]  6   1500
RADIUS:  Called-Station-Id   [30]  19  "C4-64-13-6C-E8-07"
RADIUS:  Calling-Station-Id  [31]  19  "00-26-55-D0-0D-56"
RADIUS:  EAP-Message         [79]  45
RADIUS:   02 4F 00 2B 19 00 17 03 01 00 20 37 07 D7 71 29 9D 4D 7D 5B C6 3D 7C 85 4A 3F
4F 83 2A 08 77  [O+ 7q)M}[=|J?O*w]
RADIUS:   39 7C 4A E6 44 13 12 04 AE C3 16 13              [ 9|JD]
RADIUS:  Message-Authenticato[80]  18
RADIUS:   87 6A 31 76 49 99 00 6F 6E 59 EB 04 26 99 F0 F5           [ j1vIonY&]
RADIUS:  EAP-Key-Name        [102] 2   *
RADIUS:  Vendor, Cisco       [26]  49
RADIUS:   Cisco AVpair       [1]   43  "audit-session-id=0A010A070000003100EE1DEA"
RADIUS:  NAS-Port-Type       [61]  6   Ethernet                  [15]
RADIUS:  NAS-Port            [5]   6   50007
```

```
RADIUS:  NAS-Port-Id          [87]  20  "GigabitEthernet0/7"
RADIUS:  State                [24]  73
RADIUS:   33 37 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 30  [37CPMSessionID=0]
RADIUS:   41 30 31 30 41 30 37 30 30 30 30 30 30 33 31 30  [A010A07000000310]
RADIUS:   30 45 45 31 44 45 41 3B 32 38 53 65 73 73 69 6F  [0EE1DEA;28Sessio]
RADIUS:   6E 49 44 3D 49 53 45 2F 31 34 33 35 35 38 35 35  [nID=ISE/14355855]
RADIUS:   33 2F 33 30 33 32 3B              [ 3/3032;]
RADIUS:  NAS-IP-Address       [4]   6   10.1.10.7
RADIUS(00000036): Started 5 sec timeout

       // RADIUS Access-Accept message after successful authentication. It contains
       additional authorization attributes like dACL name.

RADIUS: Received from id 1645/171 172.31.1.20:1812, Access-Accept, len 409
RADIUS:  authenticator 04 9F 01 D2 2B 18 12 C3 - 69 57 CC 9E EB C4 BE 7F
RADIUS:  User-Name            [1]   11  "employee1"
RADIUS:  State                [24]  40
RADIUS:   52 65 61 75 74 68 53 65 73 73 69 6F 6E 3A 30 41  [ReauthSession:0A]
RADIUS:   30 31 30 41 30 37 30 30 30 30 30 30 33 31 30 30  [010A070000003100]
RADIUS:   45 45 31 44 45 41               [ EE1DEA]
RADIUS:  Class                [25]  50
RADIUS:   43 41 43 53 3A 30 41 30 31 30 41 30 37 30 30 30  [CACS:0A010A07000]
RADIUS:   30 30 30 33 31 30 30 45 45 31 44 45 41 3A 49 53  [0003100EE1DEA:IS]
RADIUS:   45 2F 31 34 33 35 35 38 35 35 33 2F 33 30 33 32  [ E/143558553/3032]
RADIUS:  Termination-Action   [29]  6   1
RADIUS:  EAP-Message          [79]  6
RADIUS:   03 4F 00 04                    [ O]
RADIUS:  Message-Authenticato[80]  18
RADIUS:   E5 83 8E 2B 05 75 3F B9 2F 1B 48 A3 17 A7 A4 FA            [ +u?/H]
RADIUS:  EAP-Key-Name         [102] 67  *
RADIUS:  Vendor, Cisco        [26]  75
RADIUS:   Cisco AVpair        [1]   69  "ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-
PERMIT_ALL_TRAFFIC-4f57e406"
RADIUS:  Vendor, Microsoft    [26]  58
RADIUS:   MS-MPPE-Send-Key    [16]  52  *
RADIUS:  Vendor, Microsoft    [26]  58
RADIUS:   MS-MPPE-Recv-Key    [17]  52  *
RADIUS(00000036): Received from id 1645/171
RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes
%DOT1X-5-SUCCESS: Authentication successful for client (0026.55d0.0d56) on Interface
Gi0/7 AuditSessionID
dot1x-ev(Gi0/7): Sending event (2) to Auth Mgr for 0026.55d0.0d56
%AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client
(0026.55d0.0d56) on Interface Gi0/7 AuditSessionID 0A010A070000003100EE1DEA

%EPM-6-POLICY_REQ: IP 0.0.0.0| MAC 0026.55d0.0d56| AuditSessionID
0A010A070000003100EE1DEA| AUTHTYPE DOT1X| EVENT APPLY
%EPM-6-IPEVENT: IP 0.0.0.0| MAC 0026.55d0.0d56| AuditSessionID
0A010A070000003100EE1DEA| AUTHTYPE DOT1X| EVENT IP-WAIT
%AUTHMGR-5-SUCCESS: Authorization succeeded for client (0026.55d0.0d56) on Interface
Gi0/7 AuditSessionID 0A010A070000003100EE1DEA
```

```
        // Note that there is no ACL download in this case. This is because the ACL of
        the same name has been already downloaded in the previous steps (IP Phone
        authorization).

dot1x-ev(Gi0/7): Received Authz Success for the client 0xC300005B (0026.55d0.0d56)
dot1x-ev(Gi0/7): Sending EAPOL packet to 0026.55d0.0d56
dot1x-ev(Gi0/7): Role determination not required
dot1x-ev(Gi0/7): Sending out EAPOL packet
RADIUS/ENCODE(00000036):Orig. component type = DOT1X
RADIUS(00000036): Config NAS IP: 10.1.10.7
RADIUS(00000036): sending

        // RADIUS accounting message is sent

RADIUS(00000036): Send Accounting-Request to 172.31.1.20:1813 id 1646/27, len 282
RADIUS:  authenticator 7F 96 5F 1E FA 14 C5 4A - 7F 46 CA 57 CD 62 E1 46
RADIUS:  Acct-Session-Id     [44]  10  "00000036"
RADIUS:  Vendor, Cisco       [26]  49
RADIUS:   Cisco AVpair       [1]   43  "audit-session-id=0A010A070000003100EE1DEA"
RADIUS:  User-Name           [1]   11  "employee1"
RADIUS:  Vendor, Cisco       [26]  32
RADIUS:   Cisco AVpair       [1]   26  "connect-progress=Call Up"
RADIUS:  Acct-Authentic      [45]  6   RADIUS                    [1]
RADIUS:  Acct-Status-Type    [40]  6   Start                     [1]
RADIUS:  NAS-Port-Type       [61]  6   Ethernet                  [15]
RADIUS:  NAS-Port            [5]   6   50007
RADIUS:  NAS-Port-Id         [87]  20  "GigabitEthernet0/7"
RADIUS:  Called-Station-Id   [30]  19  "C4-64-13-6C-E8-07"
RADIUS:  Calling-Station-Id  [31]  19  "00-26-55-D0-0D-56"
RADIUS:  Class               [25]  50
RADIUS:   43 41 43 53 3A 30 41 30 31 30 41 30 37 30 30 30  [CACS:0A010A07000]
RADIUS:   30 30 30 33 31 30 30 45 45 31 44 45 41 3A 49 53  [0003100EE1DEA:IS]
RADIUS:   45 2F 31 34 33 35 35 38 35 35 33 2F 33 30 33 32  [ E/143558553/3032]
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  NAS-IP-Address      [4]   6   10.1.10.7
RADIUS:  Unsupported         [151] 10
RADIUS:   39 41 43 35 39 42 43 31          [ 9AC59BC1]
RADIUS:  Acct-Delay-Time     [41]  6   0
RADIUS(00000036): Started 5 sec timeout
RADIUS: Received from id 1646/27 172.31.1.20:1813, Accounting-response, len 20
RADIUS:  authenticator 10 CE B8 8F 9C 12 10 FA - A5 76 EF 72 17 01 E7 94
RADIUS/ENCODE(00000036):Orig. component type = DOT1X
RADIUS(00000036): Config NAS IP: 10.1.10.7
RADIUS(00000036): sending
%EPM-6-IPEVENT: IP 10.1.10.104| MAC 0026.55d0.0d56| AuditSessionID
0A010A070000003100EE1DEA| AUTHTYPE DOT1X| EVENT IP-ASSIGNMENT
%EPM-6-POLICY_APP_SUCCESS: IP 10.1.10.104| MAC 0026.55d0.0d56| AuditSessionID
0A010A070000003100EE1DEA| AUTHTYPE DOT1X| POLICY_TYPE Named ACL| POLICY_NAME xACSACLx-
IP-PERMIT_ALL_TRAFFIC-4f57e406| RESULT SUCCESS
```

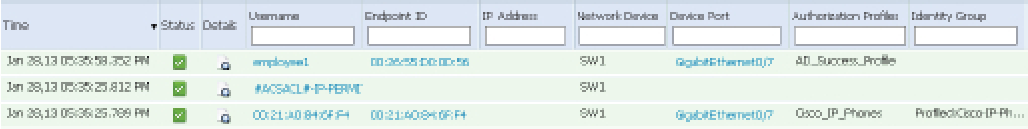
```
%EPM-6-IPEVENT: IP 10.1.10.104| MAC 0026.55d0.0d56| AuditSessionID
0A010A070000003100EE1DEA| AUTHTYPE DOT1X| EVENT IP-RELEASE
%EPM-6-IPEVENT: IP 10.1.10.104| MAC 0026.55d0.0d56| AuditSessionID
0A010A070000003100EE1DEA| AUTHTYPE DOT1X| EVENT IP-WAIT
%EPM-6-IPEVENT: IP 10.1.10.104| MAC 0026.55d0.0d56| AuditSessionID
0A010A070000003100EE1DEA| AUTHTYPE DOT1X| EVENT IP-ASSIGNMENT
%EPM-6-POLICY_APP_SUCCESS: IP 10.1.10.104| MAC 0026.55d0.0d56| AuditSessionID
0A010A070000003100EE1DEA| AUTHTYPE DOT1X| POLICY_TYPE Named ACL| POLICY_NAME xACSACLx-
IP-PERMIT_ALL_TRAFFIC-4f57e406| RESULT SUCCESS
```

// check out authentication sessions on the port. You should see two separate domains (VOICE and DATA) each authenticated separately.

```
SW1#sh auth sess int g0/7
            Interface:  GigabitEthernet0/7
          MAC Address:  0026.55d0.0d56
           IP Address:  10.1.10.104
            User-Name:  employee1
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
           Vlan Group:  N/A
              ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-4f57e406
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A010A070000003100EE1DEA
      Acct Session ID:  0x00000036
               Handle:  0xAE000031

Runnable methods list:
       Method   State
       dot1x    Authc Success
       mab      Not run

----------------------------------------
            Interface:  GigabitEthernet0/7
          MAC Address:  0021.a084.6ff4
           IP Address:  Unknown
            User-Name:  00-21-A0-84-6F-F4
               Status:  Authz Success
               Domain:  VOICE
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
```

```
                    ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-4f57e406
            Session timeout:  N/A
               Idle timeout:  N/A
          Common Session ID:  0A010A070000002F00ED9839
            Acct Session ID:  0x00000034
                     Handle:  0x3500002F

      Runnable methods list:
             Method    State
             dot1x     Failed over
             mab       Authc Success
```

Check ISE logs.



Time	Status	Details	Username	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Identity Group
Jan 28,13 05:35:58.352 PM	☑		employee1	00:26:55:D0:DD:56		SW1	GigabitEthernet0/7	AD_Success_Profile	
Jan 28,13 05:35:25.812 PM	☑		#ACSACL#-IP-PERMI			SW1			
Jan 28,13 05:35:25.789 PM	☑		00:21:A0:84:6F:F4	00:21:A0:84:6F:F4		SW1	GigabitEthernet0/7	Cisco_IP_Phones	Profiled:Cisco-IP-Ph...

Check is the NIC is up and running.

LAB-Network
micronics.local
Intel(R) PRO/1000 PT Dual Port N...

LAB 3.10. Wired 802.1x VLAN assignment

Objectives

This lab shows how to configure 802.1x for wired environment with VLAN assignment.

IP Addressing and devices

Device	Interface	IP address
ISE	NIC	172.31.1.20
R1	Lo0 E0/0 E0/1	1.1.1.1/32 10.1.10.1/24 172.31.1.1/24
AD	NIC	172.31.1.200
WinXP	NIC	10.1.10.50/24
SW1	VLAN10	10.1.10.7/24

Task

Configure ISE so that it authorizes user from AD Contractors group to VLAN 60. The users should get access to Web Server at 200.1.1.1 and be reauthenticated every 6 minutes.

Configuration

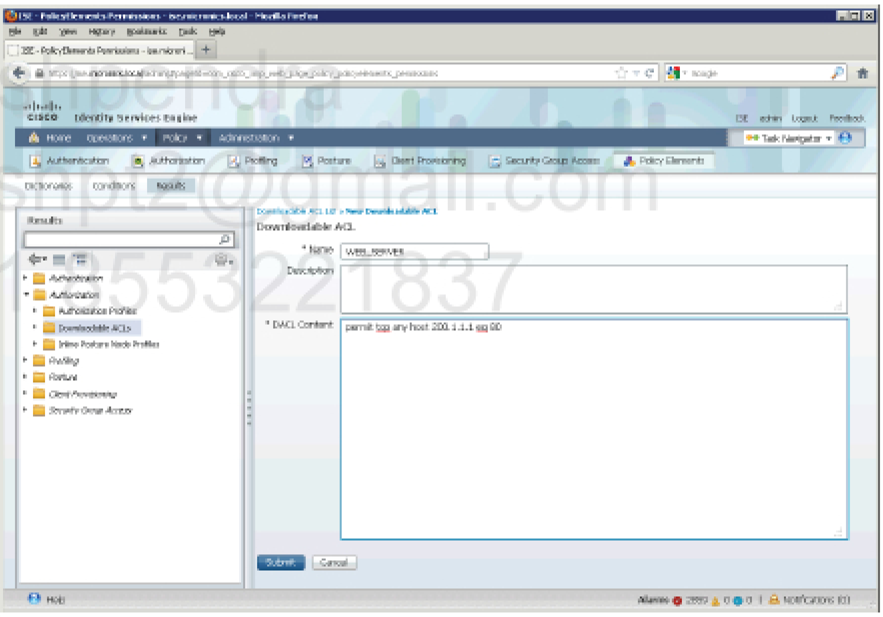
Complete these steps:

Step 1 Switch configuration.

```
!
interface GigabitEthernet0/7
 authentication periodic
 authentication timer reauthenticate server
!
```

Step 2 Create Downloadable ACL.

- Go to **Policy > Policy Elements > Results > Authorization > Downloadable ACLs** and click **Add**. Enter **WEB_SERVER** as name, enter ‘permit tcp any host 200.1.1.1 eq 80’ into **DACL Content** field and click **Submit**.



Downloadable ACL

* Name: WEB_SERVER

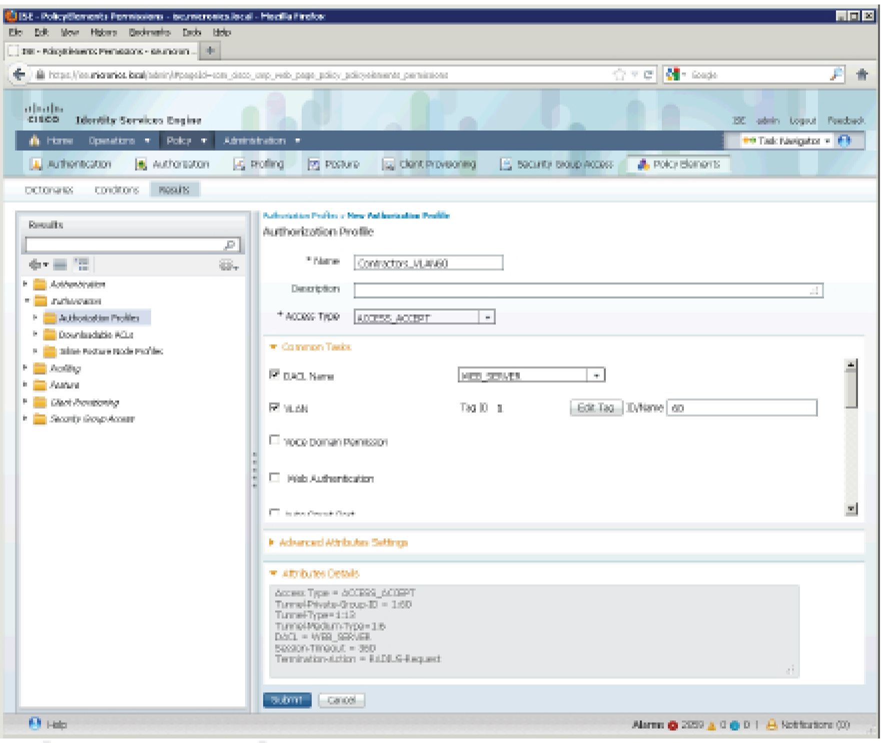
Description:

* DACL Content: permit tcp any host 200.1.1.1 eq 80

ISE - Policy Elements Permissions - Mozilla Firefox
File Edit View History Bookmarks Tools Help
cisco Identity Services Engine
ISE admin Logout Feedback
Home Operations Policy Administration
Task Navigator
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements
Dictionaries Conditions Results
Downloadable ACL List > New Downloadable ACL
Results
Authentication
Authorization
Authorization Profiles
Downloadable ACLs
Inline Posture Node Profiles
Profiling
Posture
Client Provisioning
Security Group Access
Submit
Cancel
Help
Alarms
Notifications

Step 3 Create Authorization Profile.

- Go to **Policy > Policy Elements > Results > Authorization > Authorization Profiles** and click **Add**. Enter **Contractors_VLAN60** as name and select the following options:
  - **DACL Name = WEB_SERVER**
  - **VLAN = 60**
  - **Reauthentication = 360**



Authorization Profiles > New Authorization Profile

Authorization Profile

* Name: Contractors_VLAN60

Description:

* Access Type: ACCESS_ACCEPT

Common Tasks

☑ DACL Name: WEB_SERVER

☑ VLAN: Tag ID 1, ID/Name 60

□ Voice Domain Permission

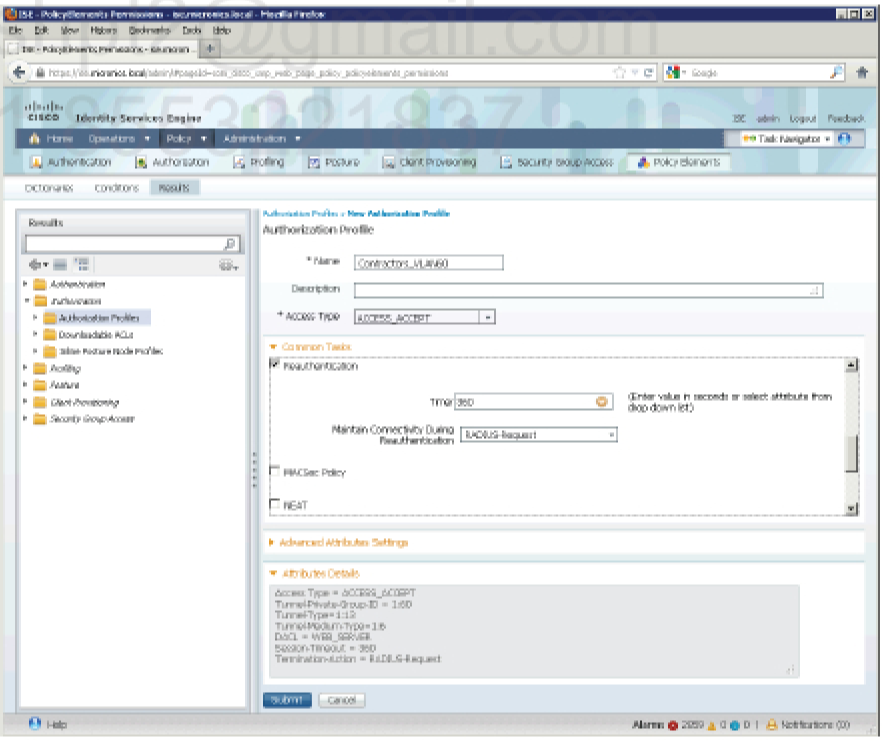
□ Web Authentication

Advanced Attributes Settings

Attributes Details

```
Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:60
Tunnel-Type=1:13
Tunnel-Medium-Type=1:6
DACL = WEB_SERVER
Session-Timeout = 360
Termination-Action = RADIUS-Request
```

- Click **Submit**.



Authorization Profiles > New Authorization Profile

Authorization Profile

* Name: Contractors_VLAN60

Description:

* Access Type: ACCESS_ACCEPT

Common Tasks

☑ Reauthentication

Timer: 360 (Enter value in seconds or select attribute from drop down list)

Maintain Connectivity During Reauthentication: RADIUS-Request

□ MACSec Policy

□ NEAT

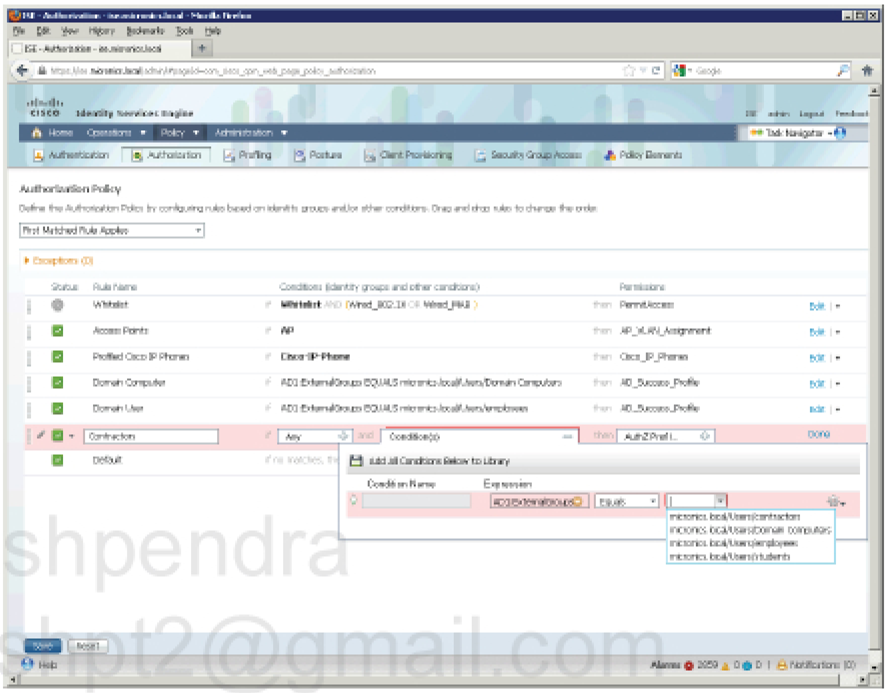
Advanced Attributes Settings

Attributes Details

```
Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:60
Tunnel-Type=1:13
Tunnel-Medium-Type=1:6
DACL = WEB_SERVER
Session-Timeout = 360
Termination-Action = RADIUS-Request
```

Step 4 Create new authorization rule.

- Go to **Policy > Authorization** and add new rule at the end of the ruleset (before default rule). Enter a name and select cpompund condition of **AD1:ExternalGroups Equals micronics.local/Users/contractors**.



Identity Services Engine
Home | Operations | Policy | Administration
Authentication | Authorization | Profiling | Posture | Client Provisioning | Security Group Access | Policy Elements

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

Exceptions (0)

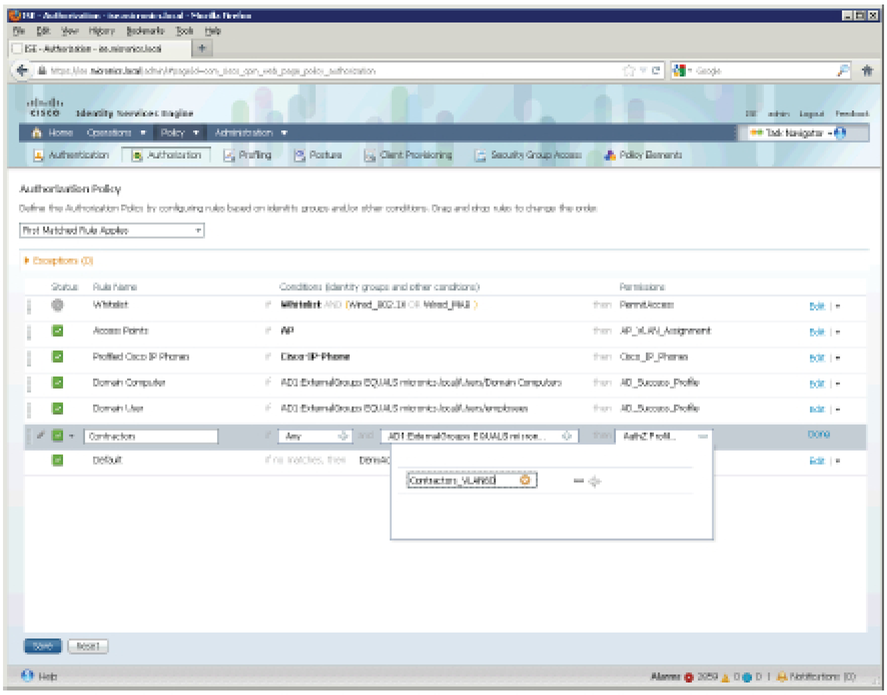
Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
○	Whitelist	if	**Whitelist** AND (Wired_802.1X OR Wired_MAB)	then	PermitAccess	Edit | ▾
✓	Access Points	if	**AP**	then	AP_VLAN_Assignment	Edit | ▾
✓	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones	Edit | ▾
✓	Domain Computer	if	AD1:ExternalGroups EQUALS micronics.local/Users/Domain Computers	then	AD_Success_Profile	Edit | ▾
✓	Domain User	if	AD1:ExternalGroups EQUALS micronics.local/Users/employees	then	AD_Success_Profile	Edit | ▾
✓	Contractors	if	Any and Condition(s)	then	AuthZ Profil...	Done
✓	Default		if no matches, then			

Add All Conditions Below to Library

Condition Name	Expression		
	AD1:ExternalGroups	Equals	

micronics.local/Users/contractors
micronics.local/Users/Domain Computers
micronics.local/Users/employees
micronics.local/Users/students

- Select **Contractors_VLAN60** for Permissions and click **Done**.



Identity Services Engine
Home | Operations | Policy | Administration
Authentication | Authorization | Profiling | Posture | Client Provisioning | Security Group Access | Policy Elements

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

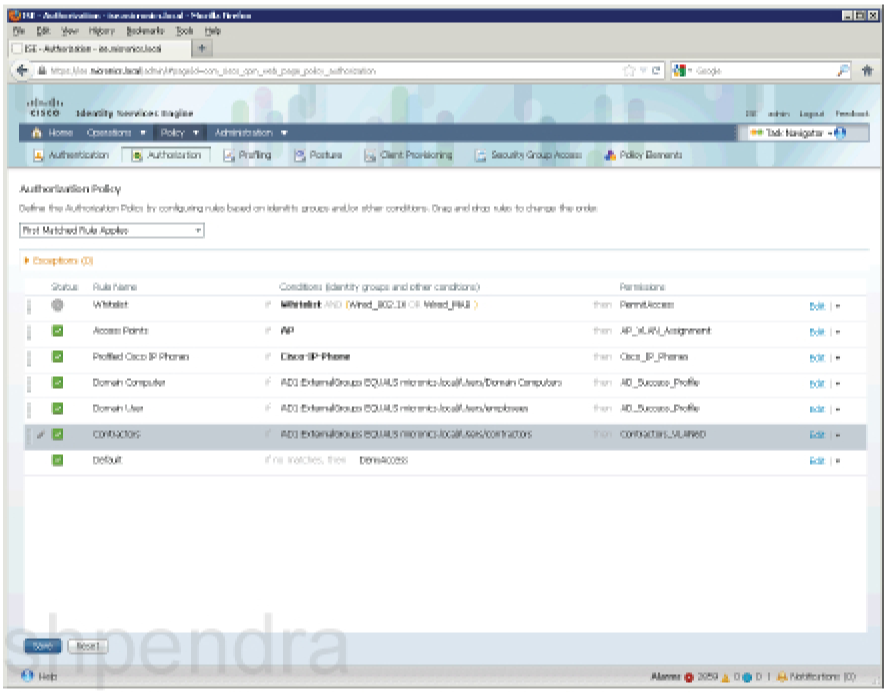
First Matched Rule Applies

Exceptions (0)

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
○	Whitelist	if	**Whitelist** AND (Wired_802.1X OR Wired_MAB)	then	PermitAccess	Edit | ▾
✓	Access Points	if	**AP**	then	AP_VLAN_Assignment	Edit | ▾
✓	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones	Edit | ▾
✓	Domain Computer	if	AD1:ExternalGroups EQUALS micronics.local/Users/Domain Computers	then	AD_Success_Profile	Edit | ▾
✓	Domain User	if	AD1:ExternalGroups EQUALS micronics.local/Users/employees	then	AD_Success_Profile	Edit | ▾
✓	Contractors	if	Any and AD1:ExternalGroups EQUALS micronic...	then	AuthZ Profil...	Done
✓	Default		if no matches, then		DenyAc	Edit | ▾

Contractors_VLAN60

- Click **Save** to apply the changes.



Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

Exceptions (0)

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
○	Whitelist	if	**Whitelist** AND (Wired_802.1X OR Wired_MAB)	then	PermitAccess	Edit | ▾
☑	Access Points	if	**AP**	then	AP_VLAN_Assignment	Edit | ▾
☑	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones	Edit | ▾
☑	Domain Computer	if	AD1:ExternalGroups EQUALS micronics.local/Users/Domain Computers	then	AD_Success_Profile	Edit | ▾
☑	Domain User	if	AD1:ExternalGroups EQUALS micronics.local/Users/employees	then	AD_Success_Profile	Edit | ▾
☑	contractors	if	AD1:ExternalGroups EQUALS micronics.local/Users/contractors	then	contractors_VLAN60	Edit | ▾
☑	Default	if no matches, then	DenyAccess			Edit | ▾

Verification

Enable debugging on the switch:

```
debug radius
debug dot1x event
```

Bounce Win7 NIC (LAB-Network) and check debug output.

```
dot1x-ev(Gi0/7): Received pkt saddr =0026.55d0.0d56 , daddr = 0180.c200.0003,
                    pae-ether-type = 888e.0100.002b
dot1x-ev(Gi0/7): dot1x_sendRespToServer: Response sent to the server from 0x4100007B
(0026.55d0.0d56)
RADIUS/ENCODE(0000003E):Orig. component type = DOT1X
RADIUS(0000003E): Config NAS IP: 10.1.10.7
RADIUS/ENCODE(0000003E): acct_session_id: 62
RADIUS(0000003E): sending

        // RADIUS authentication request for contractor1 user is sent.

RADIUS(0000003E): Send Access-Request to 172.31.1.20:1812 id 1645/241, len 314
RADIUS:  authenticator C1 05 31 1E D7 5D EF 6F - A1 66 F0 6A 07 00 2A 6C
RADIUS:  User-Name           [1]   13  "contractor1"
RADIUS:  Service-Type        [6]   6   Framed                  [2]
```

```
RADIUS:  Framed-IP-Address    [8]    6   10.1.10.104
RADIUS:  Framed-MTU           [12]   6   1500
RADIUS:  Called-Station-Id    [30]   19  "C4-64-13-6C-E8-07"
RADIUS:  Calling-Station-Id   [31]   19  "00-26-55-D0-0D-56"
RADIUS:  EAP-Message          [79]   45
RADIUS:   02 4F 00 2B 19 00 17 03 01 00 20 FE DF 1F 34 0B F5 AA A8 24 C2 EC 0E 53 D8 FF
99 87 55 CE 2D 78 7C 0F AD 58 FB 0F D3 FA 97 E1 29      [ O+ 4$SU-x|X)]
RADIUS:  Message-Authenticato[80]   18
RADIUS:   38 6A 82 99 26 F2 50 E6 2A B9 D5 50 88 F6 B3 D1            [ 8j&P*P]
RADIUS:  EAP-Key-Name         [102] 2    *
RADIUS:  Vendor, Cisco        [26]   49
RADIUS:   Cisco AVpair        [1]    43  "audit-session-id=0A010A070000003704BE32CA"
RADIUS:  NAS-Port-Type        [61]   6   Ethernet                   [15]
RADIUS:  NAS-Port             [5]    6   50007
RADIUS:  NAS-Port-Id          [87]   20  "GigabitEthernet0/7"
RADIUS:  State                [24]   73
RADIUS:   33 37 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 30  [37CPMSessionID=0]
RADIUS:   41 30 31 30 41 30 37 30 30 30 30 30 30 33 37 30  [A010A07000000370]
RADIUS:   34 42 45 33 32 43 41 3B 32 38 53 65 73 73 69 6F  [4BE32CA;28Sessio]
RADIUS:   6E 49 44 3D 49 53 45 2F 31 34 33 35 35 38 35 35  [nID=ISE/14355855]
RADIUS:   33 2F 33 30 36 34 3B             [ 3/3064;]
RADIUS:  NAS-IP-Address       [4]    6   10.1.10.7
RADIUS(0000003E): Started 5 sec timeout

        // RADIUS Access-Accept message with authorization attributes is received.
        Notice all configured attributes.

RADIUS: Received from id 1645/241 172.31.1.20:1812, Access-Accept, len 426
RADIUS:  authenticator 38 73 89 7D FC F8 48 65 - 7C 8E 22 67 04 DD 47 E0
RADIUS:  User-Name            [1]    13  "contractor1"
RADIUS:  State                [24]   40
RADIUS:   52 65 61 75 74 68 53 65 73 73 69 6F 6E 3A 30 41  [ReauthSession:0A]
RADIUS:   30 31 30 41 30 37 30 30 30 30 30 30 33 37 30 34  [010A070000003704]
RADIUS:   42 45 33 32 43 41              [ BE32CA]
RADIUS:  Class                [25]   50
RADIUS:   43 41 43 53 3A 30 41 30 31 30 41 30 37 30 30 30  [CACS:0A010A07000]
RADIUS:   30 30 30 33 37 30 34 42 45 33 32 43 41 3A 49 53  [0003704BE32CA:IS]
RADIUS:   45 2F 31 34 33 35 35 38 35 35 33 2F 33 30 36 34  [ E/143558553/3064]
RADIUS:  Session-Timeout      [27]   6   360
RADIUS:  Termination-Action   [29]   6   1
RADIUS:  Tunnel-Type          [64]   6   01:VLAN                    [13]
RADIUS:  Tunnel-Medium-Type   [65]   6   01:ALL_802                 [6]
RADIUS:  EAP-Message          [79]   6
RADIUS:   03 4F 00 04                   [ O]
RADIUS:  Message-Authenticato[80]   18
RADIUS:   38 FA E1 C9 40 A1 44 C1 D1 50 D9 89 7A 2C A8 E9            [ 8@DPz,]
RADIUS:  Tunnel-Private-Group[81]   5   01:"60"
RADIUS:  EAP-Key-Name         [102] 67   *
RADIUS:  Vendor, Cisco        [26]   67
RADIUS:   Cisco AVpair        [1]    61  "ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-
WEB_SERVER-5107a5db"
```

```
RADIUS:  Vendor, Microsoft   [26]  58
RADIUS:   MS-MPPE-Send-Key   [16]  52  *
RADIUS:  Vendor, Microsoft   [26]  58
RADIUS:   MS-MPPE-Recv-Key   [17]  52  *
RADIUS(0000003E): Received from id 1645/241
RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes
%DOT1X-5-SUCCESS: Authentication successful for client (0026.55d0.0d56) on Interface
Gi0/7 AuditSessionID
dot1x-ev(Gi0/7): Sending event (2) to Auth Mgr for 0026.55d0.0d56
%AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client
(0026.55d0.0d56) on Interface Gi0/7 AuditSessionID 0A010A070000003704BE32CA

        // Based on received attributes VLAN 60 is applied to the port.

%AUTHMGR-5-VLANASSIGN: VLAN 60 assigned to Interface Gi0/7 AuditSessionID
0A010A070000003704BE32CA
%EPM-6-POLICY_REQ: IP 0.0.0.0| MAC 0026.55d0.0d56| AuditSessionID
0A010A070000003704BE32CA| AUTHTYPE DOT1X| EVENT APPLY
%EPM-6-AAA: POLICY xACSACLx-IP-WEB_SERVER-5107a5db| EVENT DOWNLOAD-REQUEST
RADIUS/ENCODE(00000000):Orig. component type = INVALID
RADIUS(00000000): Config NAS IP: 10.1.10.7
RADIUS(00000000): sending

        // Another RADIUS request is needed to download ACL entries.

RADIUS(00000000): Send Access-Request to 172.31.1.20:1812 id 1645/242, len 139
RADIUS:  authenticator 9D 0B 06 22 FE EF 84 43 - CC B3 69 1C 6B 00 1A 16
RADIUS:  NAS-IP-Address      [4]   6   10.1.10.7
RADIUS:  User-Name           [1]   33  "#ACSACL#-IP-WEB_SERVER-5107a5db"
RADIUS:  Vendor, Cisco       [26]  32

RADIUS:   Cisco AVpair       [1]   26  "aaa:service=ip_admission"
RADIUS:  Vendor, Cisco       [26]  30
RADIUS:   Cisco AVpair       [1]   24  "aaa:event=acl-download"
RADIUS:  Message-Authenticato[80]  18
RADIUS:   07 A5 43 68 A8 51 C3 36 76 79 4A D4 F3 18 4D 04          [ ChQ6vyJM]
RADIUS(00000000): Started 5 sec timeout
RADIUS: Received from id 1645/242 172.31.1.20:1812, Access-Accept, len 221
RADIUS:  authenticator 40 C6 E1 37 75 D6 CD E5 - F1 40 1C 5D 6E FF 4A AD
RADIUS:  User-Name           [1]   33  "#ACSACL#-IP-WEB_SERVER-5107a5db"
RADIUS:  State               [24]  40
RADIUS:   52 65 61 75 74 68 53 65 73 73 69 6F 6E 3A 61 63  [ReauthSession:ac]
RADIUS:   31 66 30 31 31 34 30 30 30 30 30 42 37 33 35 31  [1f011400000B7351]
RADIUS:   30 37 42 30 45 34             [ 07B0E4]
RADIUS:  Class               [25]  50
RADIUS:   43 41 43 53 3A 61 63 31 66 30 31 31 34 30 30 30  [CACS:ac1f0114000]
RADIUS:   30 30 42 37 33 35 31 30 37 42 30 45 34 3A 49 53  [00B735107B0E4:IS]
RADIUS:   45 2F 31 34 33 35 35 38 35 35 33 2F 33 30 36 35  [ E/143558553/3065]
RADIUS:  Termination-Action  [29]  6   1
RADIUS:  Message-Authenticato[80]  18
RADIUS:   75 30 06 23 0A 46 62 60 17 D7 94 AA 29 4D 4D D3         [ u0#Fb`)MM]
```

```
RADIUS:  Vendor, Cisco       [26]   54
RADIUS:   Cisco AVpair       [1]    48  "ip:inacl#1=permit tcp any host 200.1.1.1 eq 80"
%AUTHMGR-5-SUCCESS: Authorization succeeded for client (0026.55d0.0d56) on Interface
Gi0/7 AuditSessionID 0A010A070000003704BE32CA
dot1x-ev(Gi0/7): Received Authz Success for the client 0x4100007B (0026.55d0.0d56)

%EPM-6-AAA: POLICY xACSACLx-IP-WEB_SERVER-5107a5db| EVENT DOWNLOAD-SUCCESS
%EPM-6-IPEVENT: IP 0.0.0.0| MAC 0026.55d0.0d56| AuditSessionID
0A010A070000003704BE32CA| AUTHTYPE DOT1X| EVENT IP-WAIT

       // Authorization is successful but the switch must include client's IP address
       in the downloaded ACL. The switch waits for the client to get an IP address
       from DHCP. When IP address is assigned, the switch reapplies the access list.

%EPM-6-IPEVENT: IP 10.1.60.100| MAC 0026.55d0.0d56| AuditSessionID
0A010A070000003704BE32CA| AUTHTYPE DOT1X| EVENT IP-ASSIGNMENT
%EPM-6-POLICY_APP_SUCCESS: IP 10.1.60.100| MAC 0026.55d0.0d56| AuditSessionID
0A010A070000003704BE32CA| AUTHTYPE DOT1X| POLICY_TYPE Named ACL| POLICY_NAME xACSACLx-
IP-WEB_SERVER-5107a5db| RESULT SUCCESS
```

Check commands output on the switch.

```
       // The following commands is most useful to see authentication on port. There
       is all information in one place including username, IP address, authentication
       domain and attributes downloaded from authorization server (ISE).

SW1#sh auth sess int g0/7
            Interface:  GigabitEthernet0/7
          MAC Address:  0026.55d0.0d56
           IP Address:  10.1.60.100
            User-Name:  contractor1
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  60
              ACS ACL:  xACSACLx-IP-WEB_SERVER-5107a5db
      Session timeout:  360s (server), Remaining: 268s
       Timeout action:  Reauthenticate
         Idle timeout:  N/A
    Common Session ID:  0A010A070000003D04ECD23D
      Acct Session ID:  0x00000044
               Handle:  0xA100003D

Runnable methods list:
       Method   State
       dot1x    Authc Success
       mab      Not run

----------------------------------------
            Interface:  GigabitEthernet0/7
          MAC Address:  0021.a084.6ff4
           IP Address:  Unknown
            User-Name:  00-21-A0-84-6F-F4
               Status:  Authz Success
               Domain:  VOICE
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
              ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-4f57e406
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A010A070000002F00ED9839
      Acct Session ID:  0x00000034
               Handle:  0x3500002F

Runnable methods list:
       Method   State
       dot1x    Failed over
       mab      Authc Success
```

// Use 'show ip device tracking' command to see IP addresses on ports where authentication is enabled.

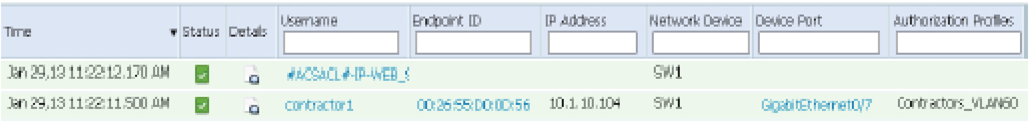
```
SW1#sh ip dev tra all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
IP Device Tracking Probe Delay Interval = 0
-----------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface                STATE
-----------------------------------------------------------------------
10.1.60.100     0026.55d0.0d56  60   GigabitEthernet0/7       ACTIVE
10.1.10.101     c47d.4f39.8423  10   GigabitEthernet0/3       ACTIVE

Total number interfaces enabled: 2
Enabled interfaces:
  Gi0/3, Gi0/7
```

// To see an access-list applied to the port use the following command. Note that there is a default access-list still applied to that port.

```
SW1#sh ip access-lists interface g0/7
     permit tcp host 10.1.60.100 host 200.1.1.1 eq www
```

```
        // Even though the port is statically configured in VLAN 10, the AuthManager
        overrides that.

SW1#sh vlan id 60

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
60   Win7                             active    Gi0/7, Gi0/24
```

Check ISE logs.



Time	Status	Details	Username	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles
Jan 29,13 11:22:12.170 AM	✓	🔍	#ACSACL#-IP-WEB_(			SW1		
Jan 29,13 11:22:11.500 AM	✓	🔍	contractor1	00:26:55:DD:0D:56	10.1.10.104	SW1	GigabitEthernet0/7	Contractors_VLAN60

LAB 3.11. Configure Wireless 802.1x

Objectives

This lab shows how to configure 802.1x for wireless environment.

IP Addressing and devices

Device	Interface	IP address
ISE	NIC	172.31.1.20
R1	Lo0 E0/0 E0/1	1.1.1.1/32 10.1.10.1/24 172.31.1.1/24
AD	NIC	172.31.1.200
WinXP	NIC	10.1.10.50/24
WLC	G0/0/1 G0/0/2	10.1.10.5/24 10.1.30.5/24

Task

There is a Wireless Controller (WLC) installed at https://wlc.micronics.local and Access Point having an IP address in VLAN 10 assigned automatically. The WLC is pre-configured with SSID MICRONICS. Configure WPA2 with 802.1x authentication on this SSID so that users from micronics.local/Users/employees AD group have access to all Internet resources on port 80. Wireless clients should get IP address from 10.1.30.0/24 subnet from DHCP Server at 172.31.1.200. You must configure ASA firewall to pass that traffic as well as ICMP and TCP/80.

Create new NDG on ISE for Wireless devices, setup WLC as AAA client with ‘cisco123’ shared secret and enable CoA on the wireless controller.

Configuration

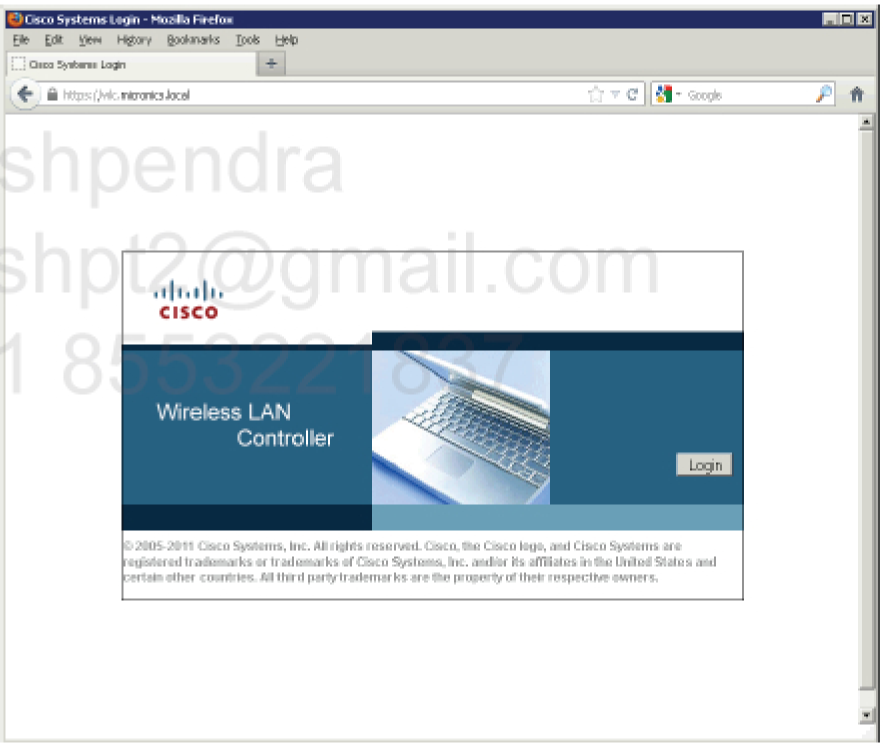
Complete these steps:

Step 1 ASA configuration.

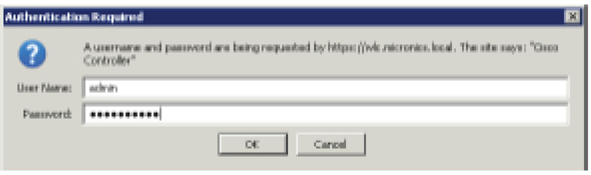
```
!
access-list DMZ_IN permit icmp any any
access-list DMZ_IN permit udp any host 172.31.1.200 eq bootps
access-list DMZ_IN permit tcp any any eq www
!
access-group DMZ_IN in interface dmz
!
```

Step 2 Enable WPA2/802.1x on WLC for MICRONICS SSID.

- Go to web browser and connet to http://wlc.micronics.local. Log in using admin/Micronics1 credentials.


Cisco Systems Login - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Cisco Systems Login
https://wlc.micronics.local
Google
CISCO
Wireless LAN
Controller
Login

© 2005-2011 Cisco Systems, Inc. All rights reserved. Cisco, the Cisco logo, and Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. All third party trademarks are the property of their respective owners.

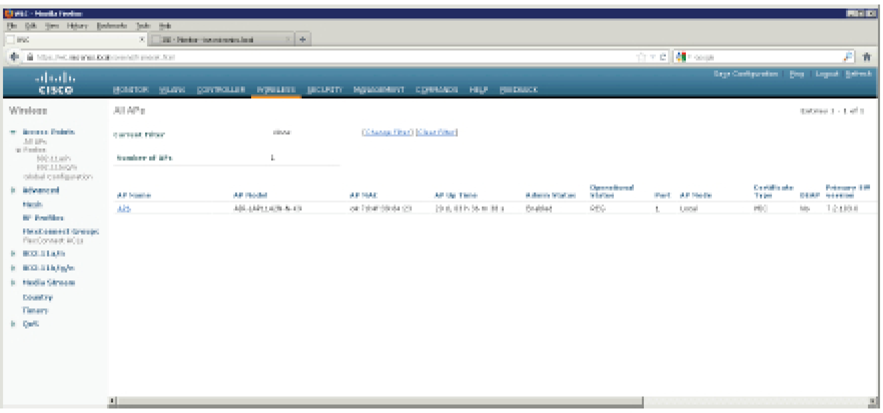


A username and password are being requested by https://wlc.micronics.local. The site says: "Cisco Controller"

User Name: admin

Password: •••••••••••

- Go to **WIRELESS > Access Points > All APs** and check if the WLC sees Access Point. The name of AP can be different depending on previous AP configuration.



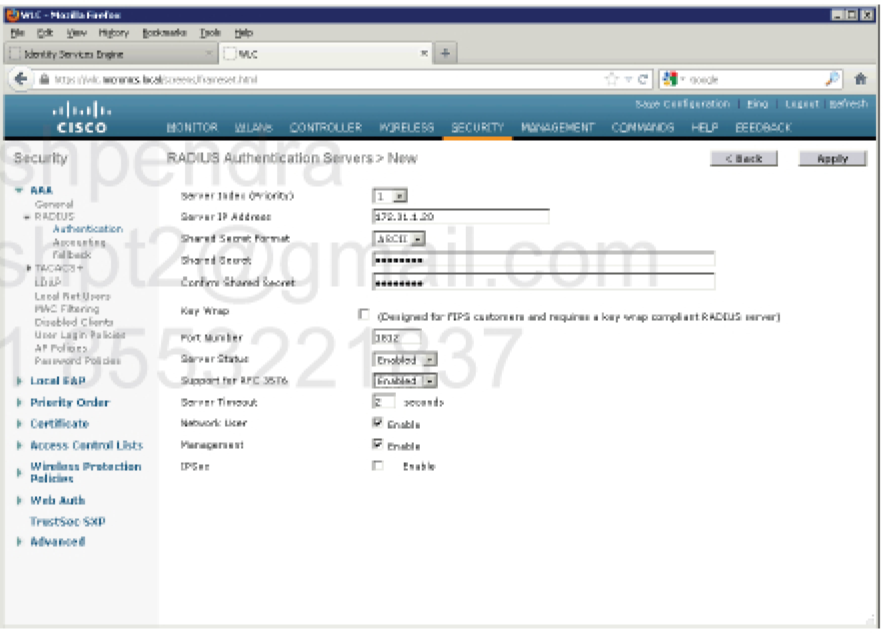
Wireless — All APs

Current Filter: None

Number of APs: 1

AP Name	AP Model	AP MAC	AP Up Time	Admin Status	Operational Status	Port	AP Mode	Certificate Type	OEAP	Primary S/W Version
[illegible]	[illegible]	[illegible]	[illegible]	Enabled	REG	1	Local	[illegible]	No	[illegible]

- Go to **SECURITY > AAA > RADIUS > Authentication** and click **New** to as RADIUS Server. Provide all required information. Make sure to enable support for RFC3576 (RADIUS CoA). Click **Apply**.



Security — RADIUS Authentication Servers > New

Server Index (Priority): 1

Server IP Address: 172.31.1.20

Shared Secret Format: ASCII

Shared Secret: ●●●●●●●●●

Confirm Shared Secret: ●●●●●●●●●

Key Wrap: □ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Port Number: 1812

Server Status: Enabled

Support for RFC 3576: Enabled

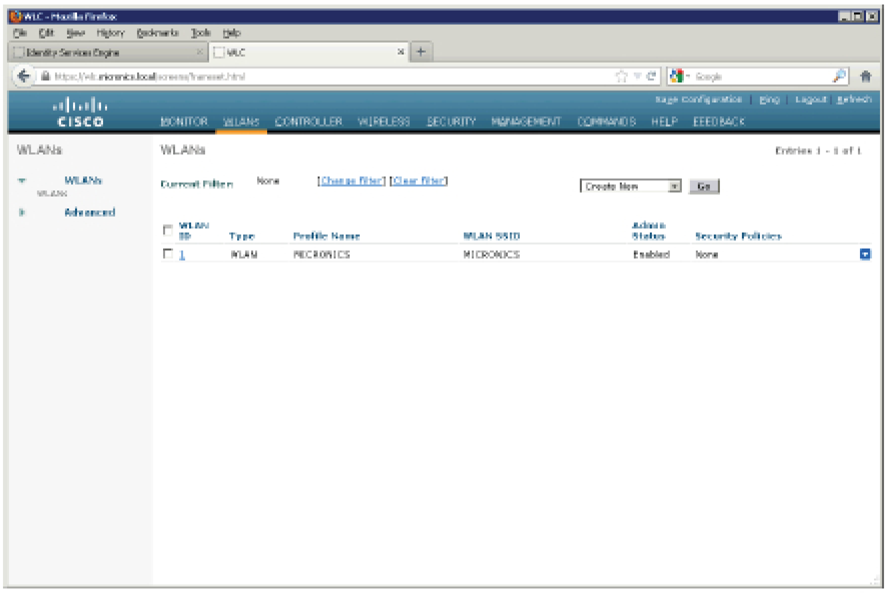
Server Timeout: 2 seconds

Network User: ☑ Enable

Management: ☑ Enable

IPSec: □ Enable

- Go to **WLANs** and check if there is **MICRONICS** SSID on the list. If so, click **1** to make changes to that WLAN.



WLANs

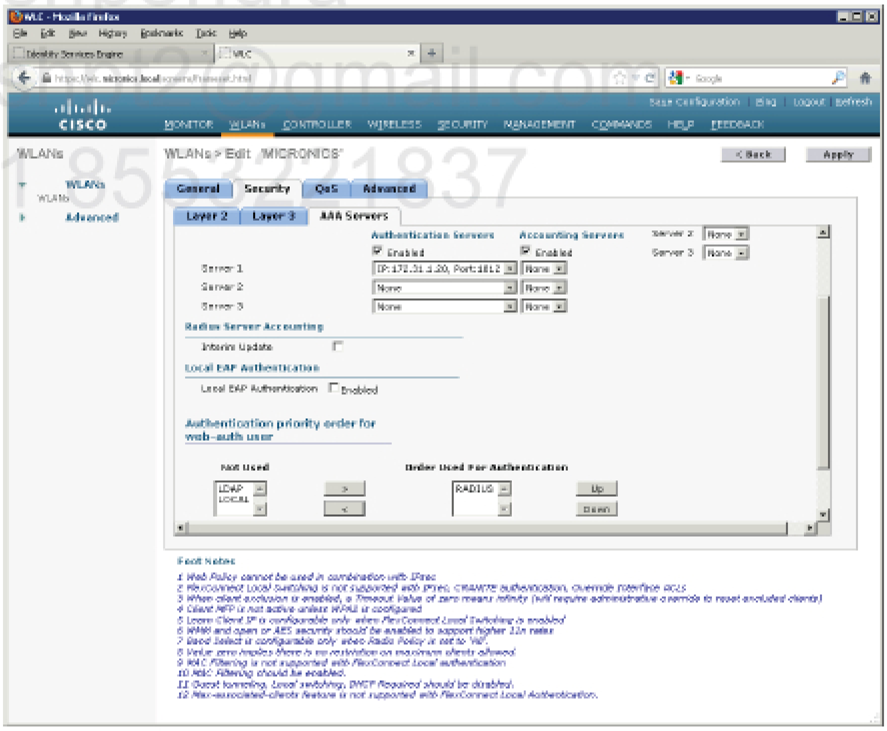
Current Filter: None [Change filter] [Clear filter]

Create New ▾ Go

Entries 1 - 1 of 1

□ WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
□ 1	WLAN	MICRONICS	MICRONICS	Enabled	None

- Go to **Security > AAA Servers** tab and pick RADIUS Server 1 from the list. Alter **Order Used for Authentication** list so that there is only RADIUS left.



WLANs > Edit 'MICRONICS'

General | Security | QoS | Advanced

Layer 2 | Layer 3 | AAA Servers

	Authentication Servers	Accounting Servers
	☑ Enabled	☑ Enabled
Server 1	IP:172.31.1.20, Port:1812	None
Server 2	None	None
Server 3	None	None

Radius Server Accounting

Interim Update □

Local EAP Authentication

Local EAP Authentication □ Enabled

Authentication priority order for web-auth user

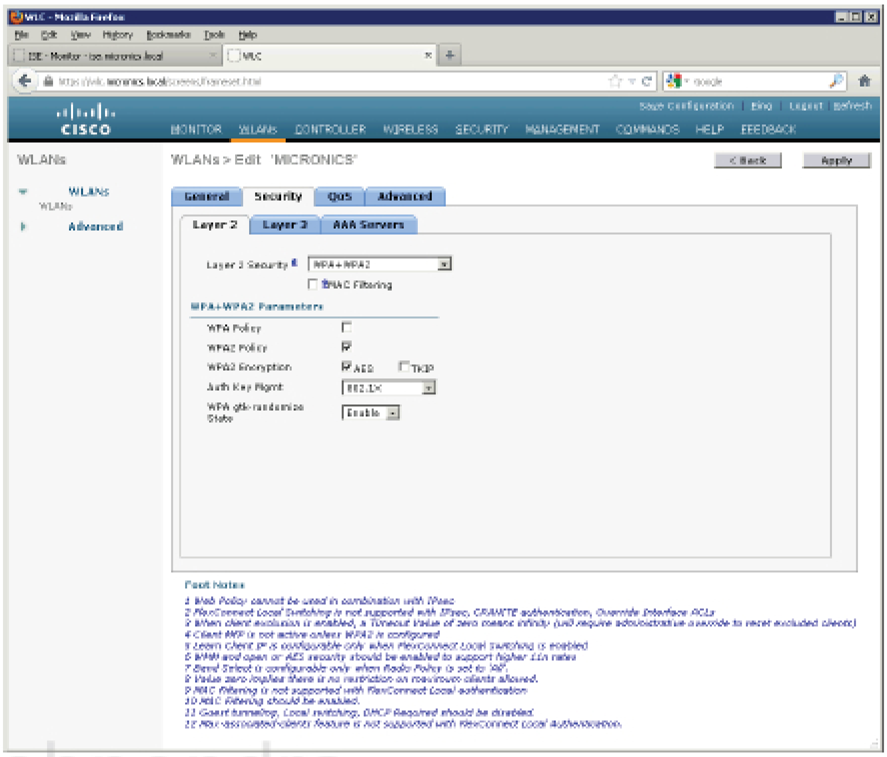
Not Used: LDAP, LOCAL

Order Used For Authentication: RADIUS

Foot Notes

1 Web Policy cannot be used in combination with IPsec
2 FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs
3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
4 Client MFP is not active unless WPA2 is configured
5 Learn Client IP is configurable only when FlexConnect Local Switching is enabled
6 WMM and open or AES security should be enabled to support higher 11n rates
7 Band Select is configurable only when Radio Policy is set to 'All'.
8 Value zero implies there is no restriction on maximum clients allowed.
9 MAC Filtering is not supported with FlexConnect Local authentication
10 MAC Filtering should be enabled.
11 Guest tunneling, Local switching, DHCP Required should be disabled.
12 Max-associated-clients feature is not supported with FlexConnect Local Authentication.

- Go to **Security > Layer 2** tab and select **WPA+WPA2** Layer 2 Security and pick **WPA2** with **AES**. Select **802.1x** for **Auth Key Mgmt**.


WLC - Mozilla Firefox
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Save Configuration | Ping | Logout | Refresh
WLANs
WLANs
Advanced
< Back
Apply
General Security QoS Advanced
Layer 2 Layer 3 AAA Servers

WLANs > Edit 'MICRONICS'

Layer 2 Security: WPA+WPA2
□ MAC Filtering

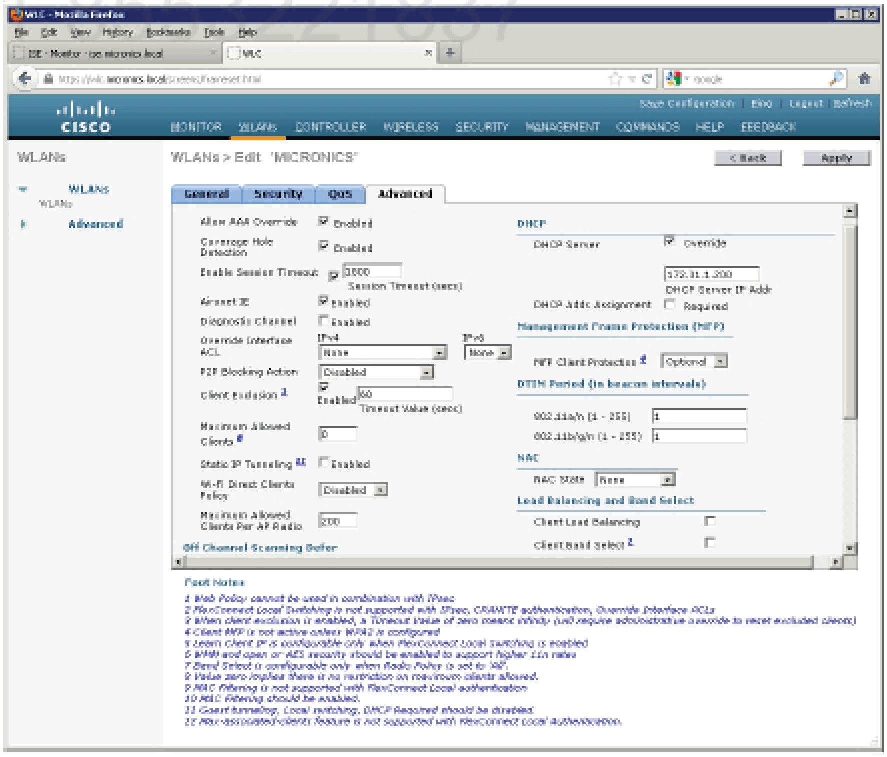
WPA+WPA2 Parameters

WPA Policy □
WPA2 Policy ☑
WPA2 Encryption ☑ AES □ TKIP
Auth Key Mgmt: 802.1X
WPA gtk-randomize State: Enable

Foot Notes

1 Web Policy cannot be used in combination with IPsec
2 FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs
3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
4 Client MFP is not active unless WPA2 is configured
5 Learn Client IP is configurable only when FlexConnect Local Switching is enabled
6 WMM and open or AES security should be enabled to support higher 11n rates
7 Band Select is configurable only when Radio Policy is set to 'All'.
8 Value zero implies there is no restriction on maximum clients allowed.
9 MAC Filtering is not supported with FlexConnect Local authentication
10 MAC Filtering should be enabled.
11 Guest tunneling, Local switching, DHCP Required should be disabled.
12 Max-associated-clients feature is not supported with FlexConnect Local Authentication.

- Go to **Advanced** tab and pick **Allow AAA Override** option. This option is required to allow the WLC apply downloaded ACL name. The ACL must be configured locally.


WLC - Mozilla Firefox
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Save Configuration | Ping | Logout | Refresh
WLANs
WLANs
Advanced
< Back
Apply
General Security QoS Advanced

WLANs > Edit 'MICRONICS'

Allow AAA Override ☑ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout ☑ 1800 Session Timeout (secs)
Aironet IE ☑ Enabled
Diagnostic Channel □ Enabled
Override Interface ACL IPv4 None IPv6 None
P2P Blocking Action Disabled
Client Exclusion 3 ☑ Enabled 60 Timeout Value (secs)
Maximum Allowed Clients 8 0
Static IP Tunneling 11 □ Enabled
Wi-Fi Direct Clients Policy Disabled
Maximum Allowed Clients Per AP Radio 200
Off Channel Scanning Defer

DHCP
DHCP Server ☑ Override
172.31.1.200 DHCP Server IP Addr
DHCP Addr. Assignment □ Required

Management Frame Protection (MFP)
MFP Client Protection 4 Optional

DTIM Period (in beacon intervals)
802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1

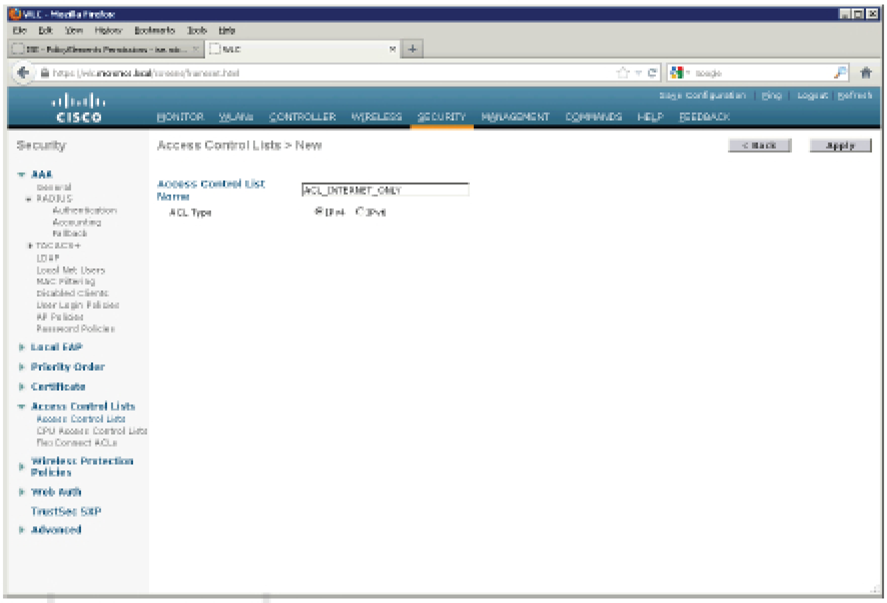
NAC
NAC State None

Load Balancing and Band Select
Client Load Balancing □
Client Band Select 7 □

Foot Notes

1 Web Policy cannot be used in combination with IPsec
2 FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs
3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
4 Client MFP is not active unless WPA2 is configured
5 Learn Client IP is configurable only when FlexConnect Local Switching is enabled
6 WMM and open or AES security should be enabled to support higher 11n rates
7 Band Select is configurable only when Radio Policy is set to 'All'.
8 Value zero implies there is no restriction on maximum clients allowed.
9 MAC Filtering is not supported with FlexConnect Local authentication
10 MAC Filtering should be enabled.
11 Guest tunneling, Local switching, DHCP Required should be disabled.
12 Max-associated-clients feature is not supported with FlexConnect Local Authentication.

- Go to **SECURITY > Access Control Lists > Access Control Lists** and click **New**. Enter a name for the ACL e.g. **ACL_INTERNET_ONLY** and click **Apply**.

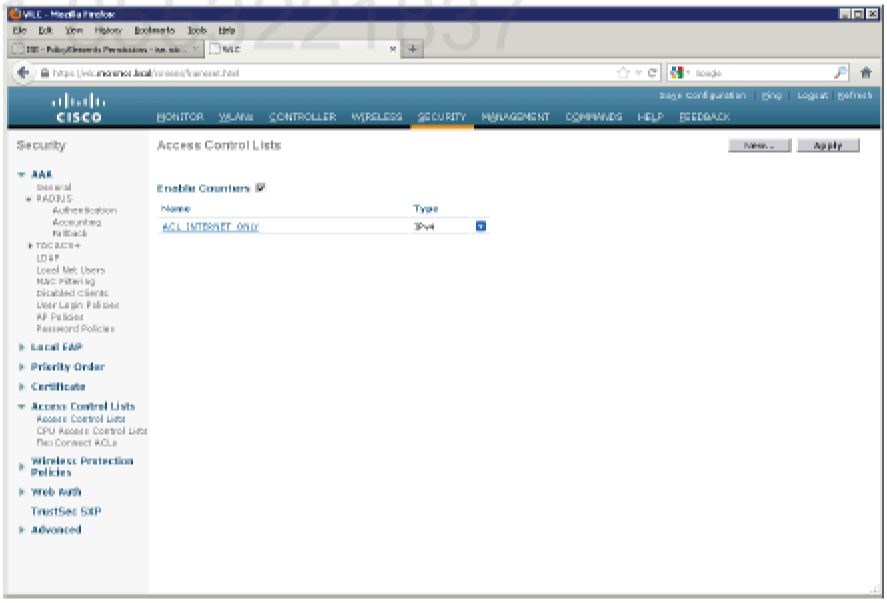


Access Control Lists > New

Access Control List Name: ACL_INTERNET_ONLY

ACL Type: ● IPv4 ○ IPv6

- Once the new ACL is created you should be able to edit it. On the following screen pick **Enable Counters** checkbox (optional but useful to see if ACL is working) and click on ACL name to create ACEs.

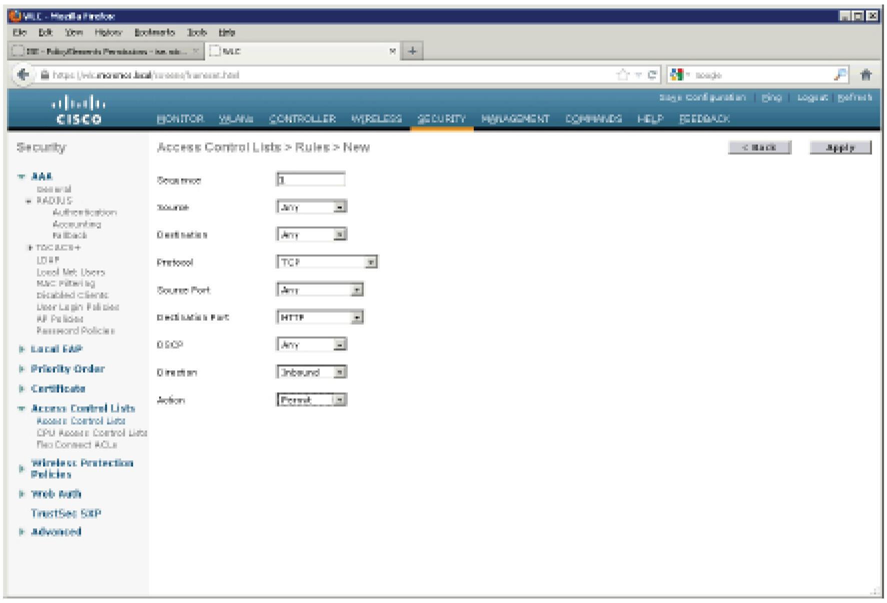


Access Control Lists

Enable Counters ☑

Name	Type
ACL_INTERNET_ONLY	IPv4

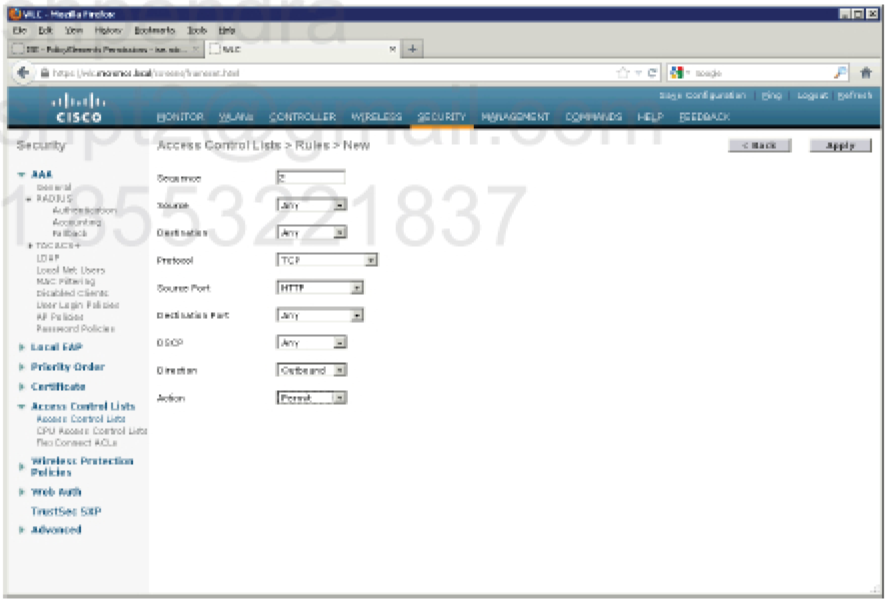
- Add new entry in the ACL as presented on the following screen and click **Apply**.



Access Control Lists > Rules > New

Sequence	1
Source	Any
Destination	Any
Protocol	TCP
Source Port	Any
Destination Port	HTTP
DSCP	Any
Direction	Inbound
Action	Permit

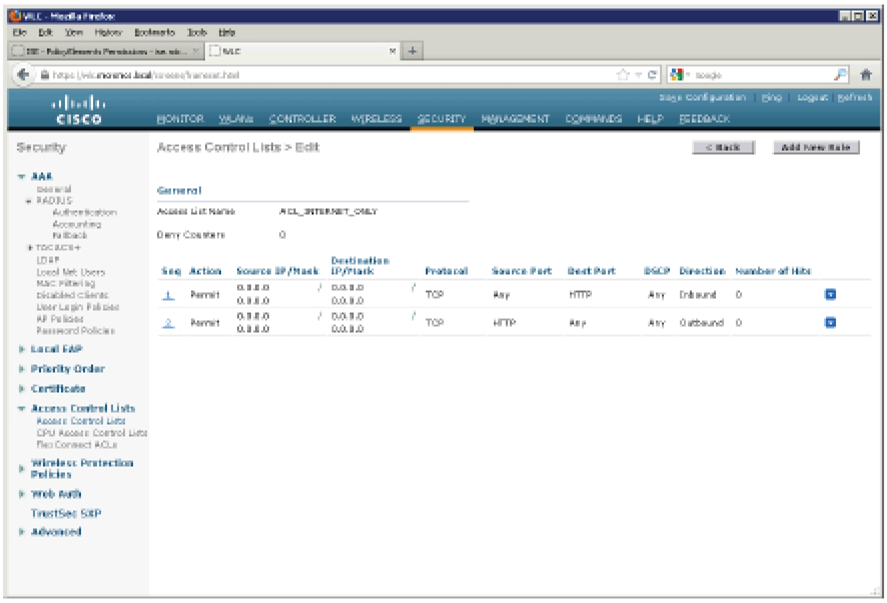
- Once again click **Add new rule** and add another entry as presented on the following screen and click **Apply**.



Access Control Lists > Rules > New

Sequence	2
Source	Any
Destination	Any
Protocol	TCP
Source Port	HTTP
Destination Port	Any
DSCP	Any
Direction	Outbound
Action	Permit

- The whole ACL should look like on the following screen.



Access Control Lists > Edit

General

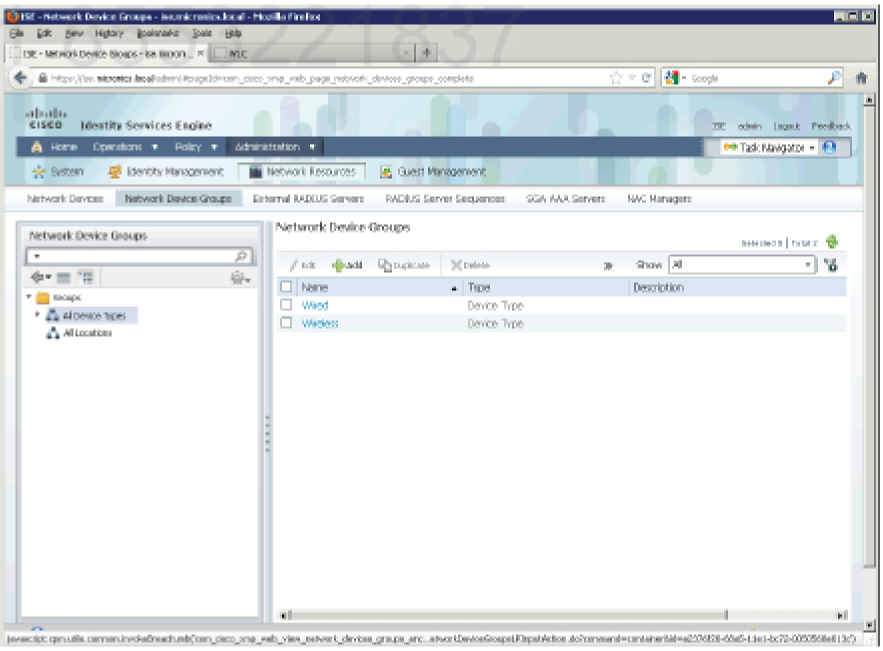
Access List Name ACL_INTERNET_ONLY

Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	TCP	Any	HTTP	Any	Inbound	0
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	TCP	HTTP	Any	Any	Outbound	0

Step 3 Configure ISE. Check if there is NDG for Wireless devices and add WLC as AAA Client.

- Go to **Administration > Network Resources > Network Device Groups > Groups > All Device Types** and check if there is **Wireless** group. The group should be there from previous tasks. If there is no such group – create it.

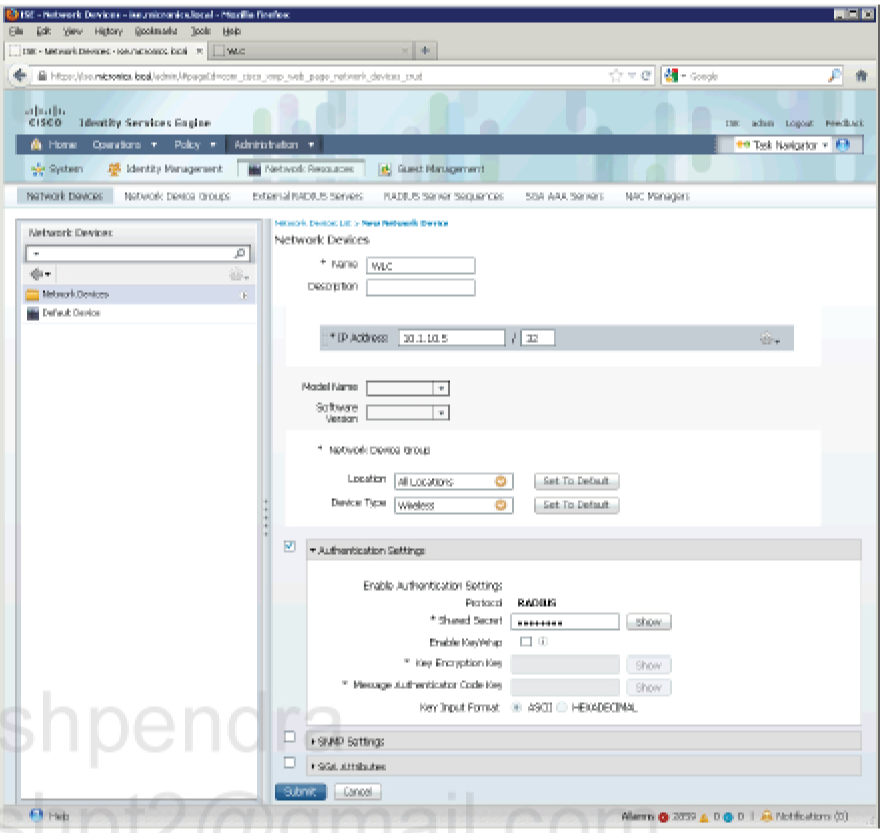


Network Device Groups

Name	Type	Description
Wired	Device Type	
Wireless	Device Type	

Identity Services Engine
Home Operations Policy Administration
System Identity Management Network Resources Guest Management
Network Devices Network Device Groups External RADIUS Servers RADIUS Server Sequences SGA AAA Servers NAC Managers
Groups
All Device Types
All Locations
Edit Add Duplicate Delete
Show All
Task Navigator

- Go to **Administration > Network Resources > Network Devices** and click **Add**. Enter a name for device and provide its IP address. Make it a member of **Wireless** NDG and configure RADIUS shared secret. Click **Submit**.



Network Devices

* Name: WLC

Description:

* IP Address: 10.1.10.5 / 32

Model Name:

Software Version:

* Network Device Group

Location: All Locations

Device Type: Wireless

☑ Authentication Settings

Enable Authentication Settings

Protocol: RADIUS

* Shared Secret: ••••••••

Enable KeyWrap: □

* Key Encryption Key:

* Message Authenticator Code Key:

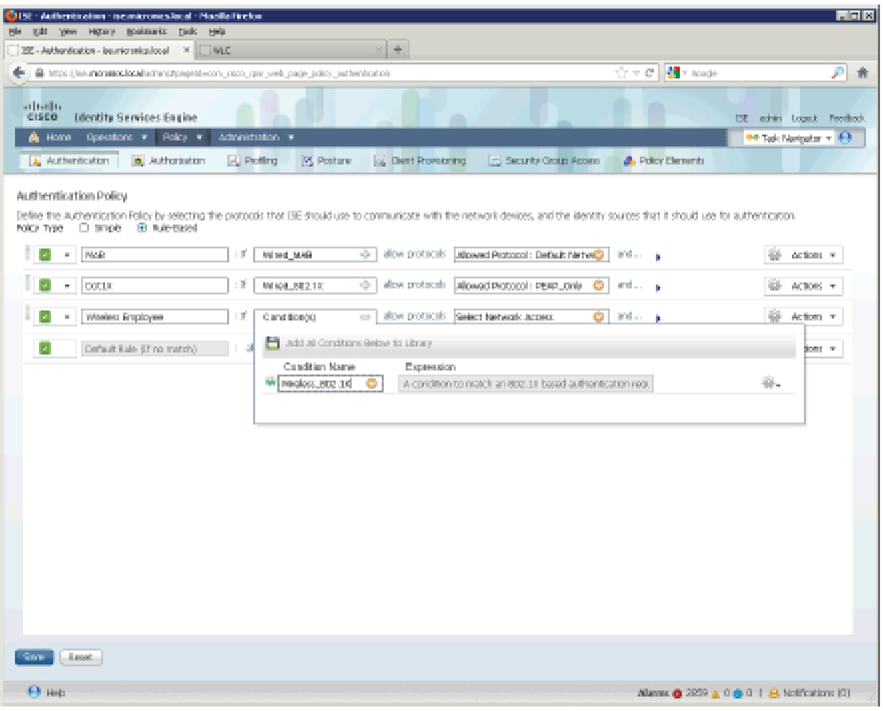
Key Input Format: ● ASCII ○ HEXADECIMAL

□ SNMP Settings

□ SGA Attributes

Step 4 Create new authentication policy.

- Go to **Policy > Authentication** and add a new rule before the last default rule. Enter a name for the rule e.g. **Wireless Employee** and select **Wireless_802.1X** as a condition (select it from library).



Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

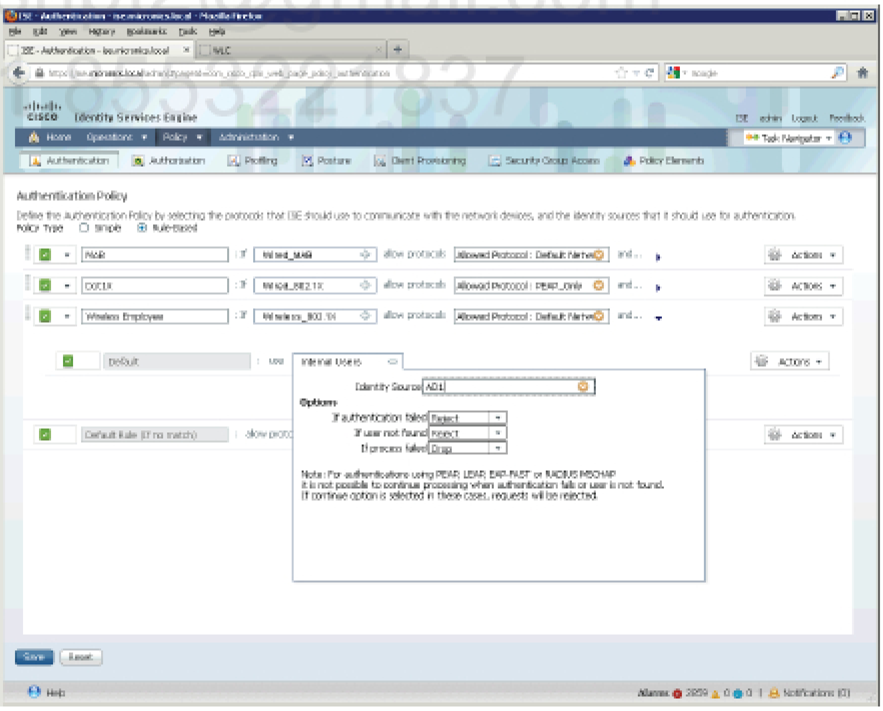
Policy Type ○ Simple ● Rule-Based

MAB	: If	Wired_MAB	allow protocols	Allowed Protocol : Default Netwo	and ...
Dot1X	: If	Wired_802.1X	allow protocols	Allowed Protocol : PEAP_Only	and ...
Wireless Employee	: If	Condition(s)	allow protocols	Select Network Access	and ...
Default Rule (If no match)					

Add All Conditions Below to Library

Condition Name	Expression
Wireless_802.1X	A condition to match an 802.1X based authentication requ

- Click black arrow on the left of the new rule to show more options. For Identity Source select **AD1**. Click **Save**.



Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

Policy Type ○ Simple ● Rule-Based

MAB	: If	Wired_MAB	allow protocols	Allowed Protocol : Default Netwo	and ...
Dot1X	: If	Wired_802.1X	allow protocols	Allowed Protocol : PEAP_Only	and ...
Wireless Employee	: If	Wireless_802.1X	allow protocols	Allowed Protocol : Default Netwo	and ...
Default	: use	Internal Users			
Default Rule (If no match)	: allow proto				

Identity Source AD1

Options

If authentication failed Reject

If user not found Reject

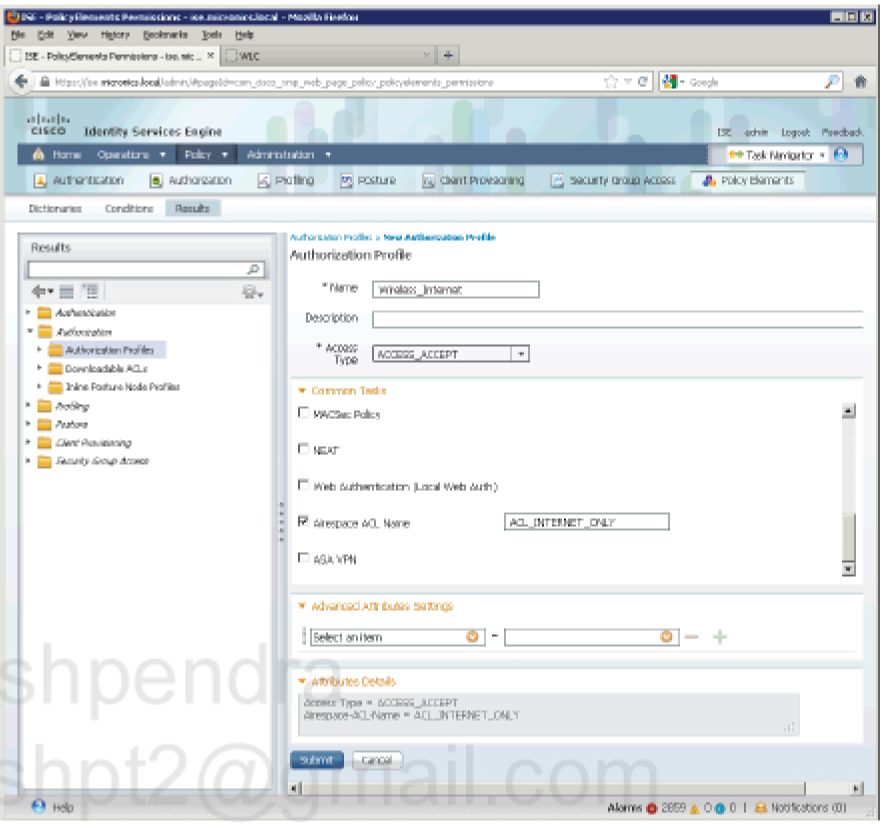
If process failed Drop

Note: For authentications using PEAP, LEAP, EAP-FAST or RADIUS MSCHAP
It is not possible to continue processing when authentication fails or user is not found.
If continue option is selected in these cases, requests will be rejected.

Step 5 Create new authorization rule.

- Go to **Policy > Policy Elelments > Authorization > Authorization Profiles** and click **Add**. Enter a name for the profile e.g. **Wireless_Internet** and pick **Airespace ACL Name** option. Provide

ACL name exactly as it is created on the WLC. In this case **ACL_INTERNET_ONLY** is the ACL name. Click **Submit**.



Authorization Profile > New Authorization Profile

Authorization Profile

* Name: Wireless_Internet

Description:

* Access Type: ACCESS_ACCEPT

Common Tasks

- □ MACSec Policy
- □ NEAT
- □ Web Authentication (Local Web Auth)
- ☑ Airespace ACL Name: ACL_INTERNET_ONLY
- □ ASA VPN

Advanced Attributes Settings

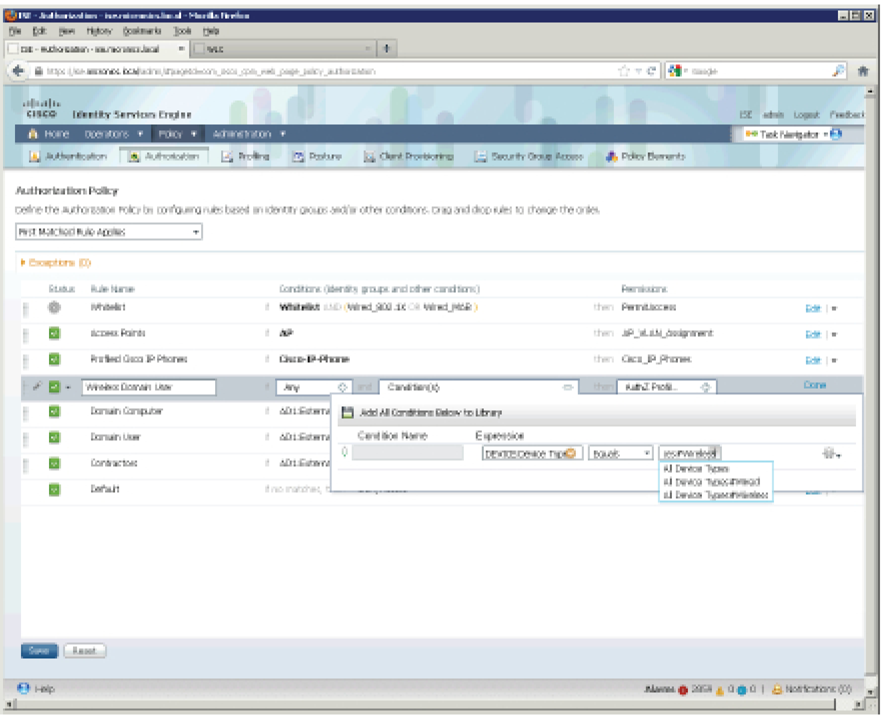
Select an item

Attributes Details

Access Type = ACCESS_ACCEPT
Airespace-ACL-Name = ACL_INTERNET_ONLY

- Go to **Policy > Authorization** and add a new rule before **Domain Computer** rule. Enter a name for the rule e.g. **Wireless Domain User** and select the following compound conditions:
  - The device through the user is connected to the network is in **Wireless** NDG

    AND
  - The user belongs to AD group **micronics.local/Users/employees**



Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

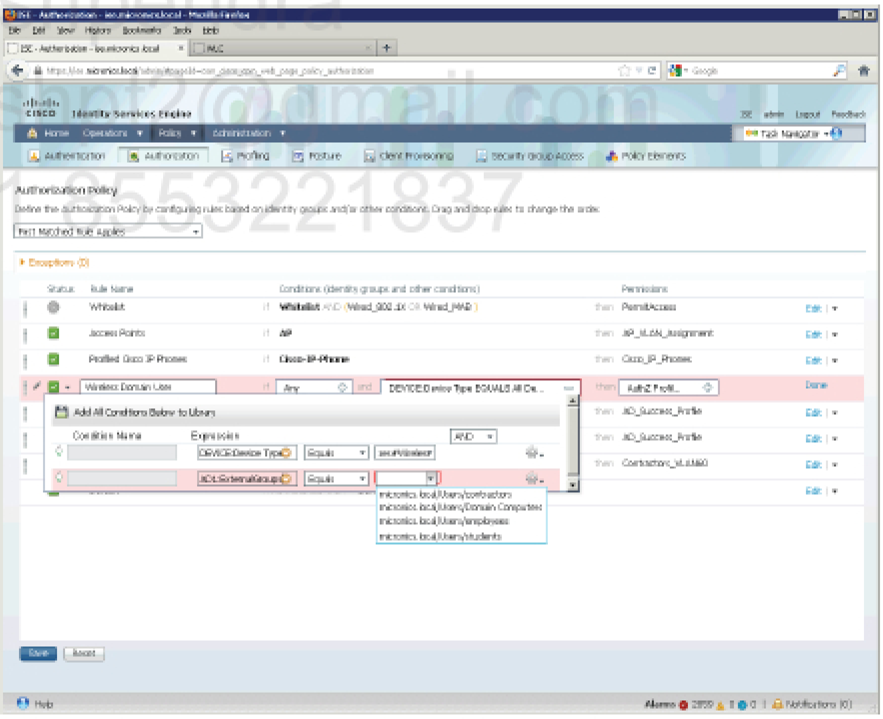
Exceptions (0)

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
	Whitelist	if	Whitelist AND (Wired_802.1X OR Wired_MAB)	then	PermitAccess
	Access Points	if	AP	then	AP_VLAN_Assignment
	Profiled Cisco IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phones
	Wireless Domain User	if	Any and Condition(s)	then	AuthZ Profil...
	Domain Computer	if	AD1:Externa...		
	Domain User	if	AD1:Externa...		
	Contractors	if	AD1:Externa...		
	Default	if no matches, t...			

Add All Conditions Below to Library

Condition Name	Expression		
	DEVICE:Device Type	Equals	All Device Types#Wireless

All Device Types
All Device Types#Wired
All Device Types#Wireless



Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

Exceptions (0)

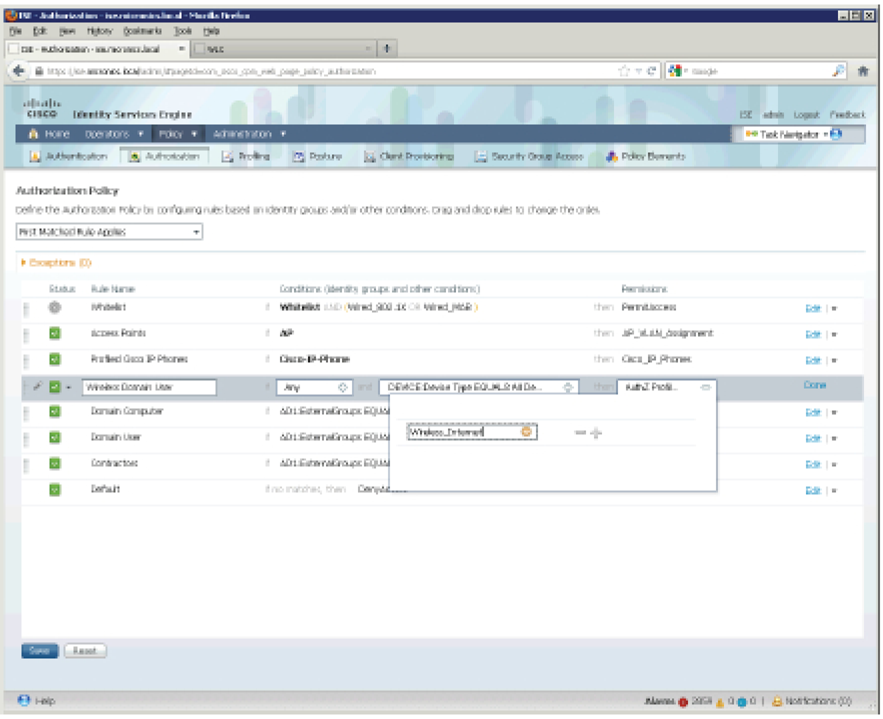
Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
	Whitelist	if	Whitelist AND (Wired_802.1X OR Wired_MAB)	then	PermitAccess
	Access Points	if	AP	then	AP_VLAN_Assignment
	Profiled Cisco IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phones
	Wireless Domain User	if	Any and DEVICE:Device Type EQUALS All De...	then	AuthZ Profil...
				then	AD_Success_Profile
				then	AD_Success_Profile
				then	Contractors_VLAN80

Add All Conditions Below to Library

Condition Name	Expression		
			AND
	DEVICE:Device Type	Equals	...es#Wireless
	AD1:ExternalGroups	Equals	

micronics.local/Users/contractors
micronics.local/Users/Domain Computers
micronics.local/Users/employees
micronics.local/Users/students

- For **Permissions** column select **Wireless_Internet** authorization profile.



Authorization Policy

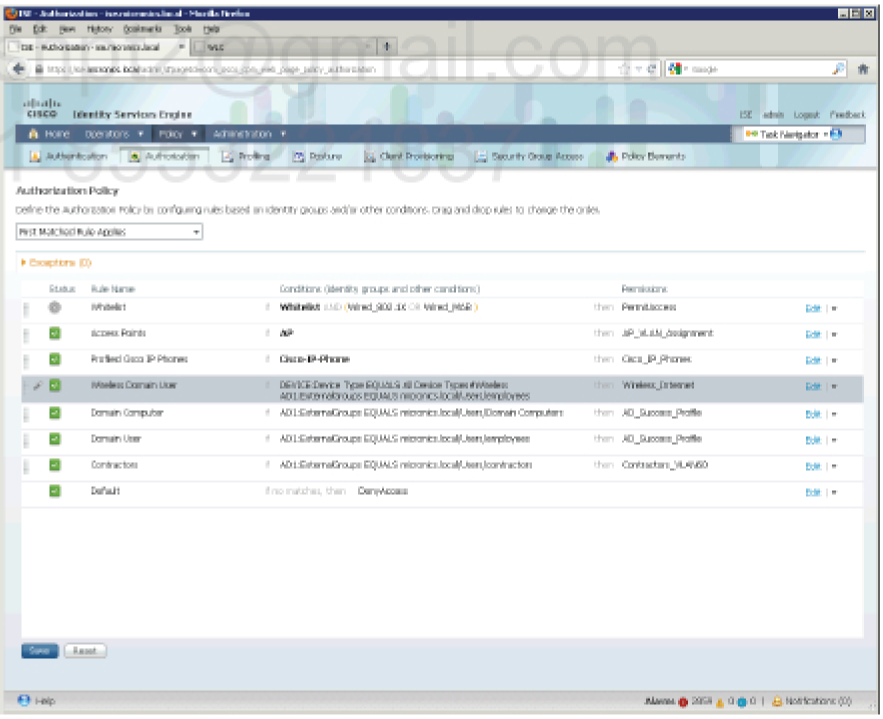
Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

▸ Exceptions (0)

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
●	Whitelist	if	Whitelist AND (Wired_802.1X OR Wired_MAB)	then	PermitAccess	Edit | ▾
☑	Access Points	if	AP	then	AP_VLAN_Assignment	Edit | ▾
☑	Profiled Cisco IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phones	Edit | ▾
☑	Wireless Domain User	if	Any and DEVICE:Device Type EQUALS All De...	then	AuthZ Profil... Wireless_Internet	Done
☑	Domain Computer	if	AD1:ExternalGroups EQUA...			Edit | ▾
☑	Domain User	if	AD1:ExternalGroups EQUA...			Edit | ▾
☑	Contractors	if	AD1:ExternalGroups EQUA...			Edit | ▾
☑	Default		if no matches, then DenyAccess			Edit | ▾

- Click **Save** to apply the changes.



Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

▸ Exceptions (0)

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
●	Whitelist	if	Whitelist AND (Wired_802.1X OR Wired_MAB)	then	PermitAccess	Edit | ▾
☑	Access Points	if	AP	then	AP_VLAN_Assignment	Edit | ▾
☑	Profiled Cisco IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phones	Edit | ▾
☑	Wireless Domain User	if	DEVICE:Device Type EQUALS All Device Types#Wireless AD1:ExternalGroups EQUALS netronics.local/Users/employees	then	Wireless_Internet	Edit | ▾
☑	Domain Computer	if	AD1:ExternalGroups EQUALS netronics.local/Users/Domain Computers	then	AD_Success_Profile	Edit | ▾
☑	Domain User	if	AD1:ExternalGroups EQUALS netronics.local/Users/employees	then	AD_Success_Profile	Edit | ▾
☑	Contractors	if	AD1:ExternalGroups EQUALS netronics.local/Users/contractors	then	Contractors_VLAN60	Edit | ▾
☑	Default		if no matches, then DenyAccess			Edit | ▾

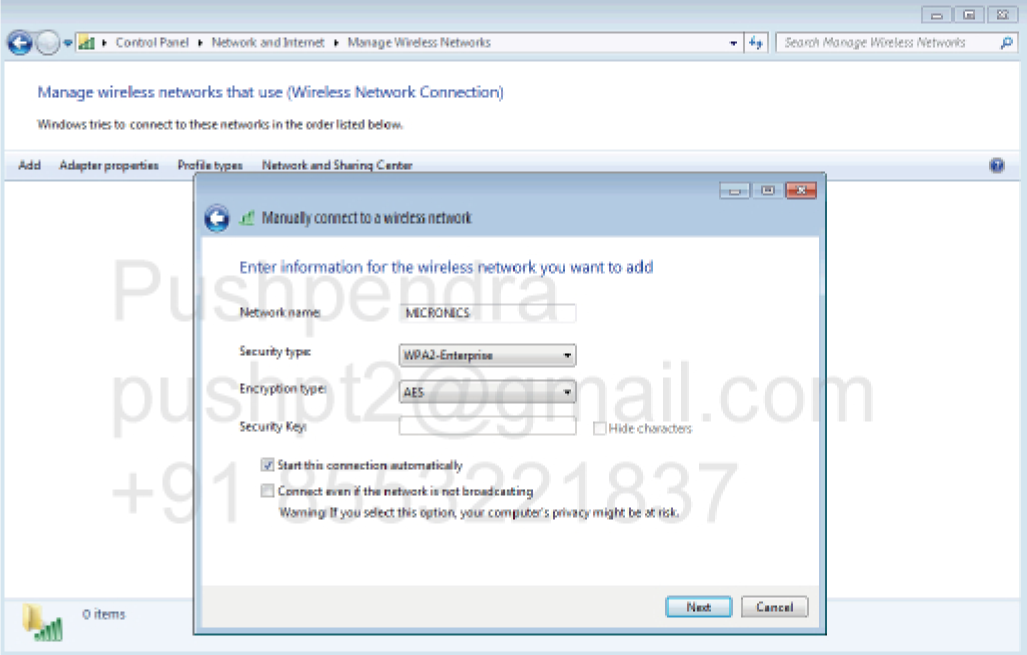
Verification

Enable debugging on the WLC:

```
debug client <client-MAC-address>
```

Create new connection on the Win7 PC.

- Go to **Control Panel > Network and Internet > Manage Wireless Networks** and click **Add**. Select **Manually create a network profile** option and provide the following settings:



Control Panel ▸ Network and Internet ▸ Manage Wireless Networks
Search Manage Wireless Networks
Add
Adapter properties
Profile types
Network and Sharing Center
0 items
Next
Cancel

Manage wireless networks that use (Wireless Network Connection)

Windows tries to connect to these networks in the order listed below.

Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name: MICRONICS

Security type: WPA2-Enterprise

Encryption type: AES

Security Key:

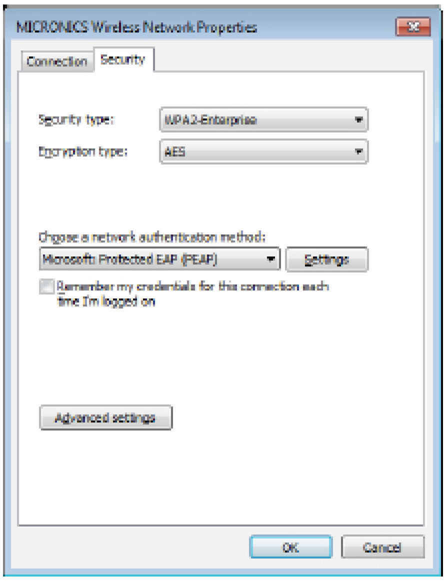
□ Hide characters

☑ Start this connection automatically

□ Connect even if the network is not broadcasting

Warning: If you select this option, your computer's privacy might be at risk.

- Click **Next** and then **Change connection settings.** On the **Security** tab select options as follows:



MICRONICS Wireless Network Properties

Security type: WPA2-Enterprise

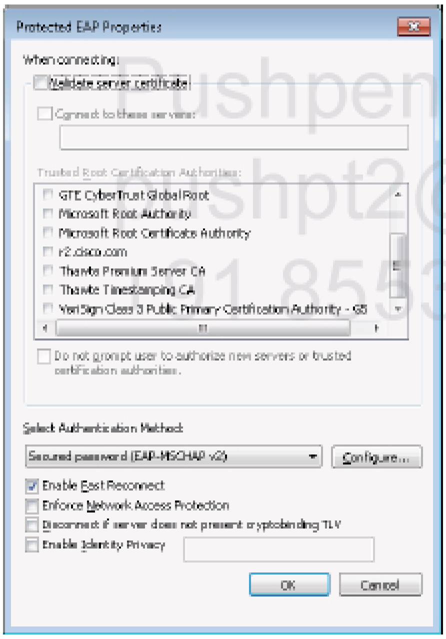
Encryption type: AES

Choose a network authentication method:

Microsoft: Protected EAP (PEAP)

□ Remember my credentials for this connection each time I'm logged on

- Click on **Settings** button and uncheck **Validate server certificate** option.



Protected EAP Properties

When connecting:

□ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

□ GTE CyberTrust Global Root
□ Microsoft Root Authority
□ Microsoft Root Certificate Authority
□ r2.cisco.com
□ Thawte Premium Server CA
□ Thawte Timestamping CA
□ VeriSign Class 3 Public Primary Certification Authority - G5

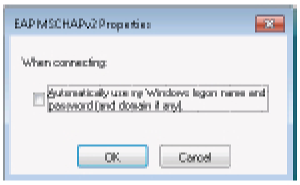
□ Do not prompt user to authorize new servers or trusted certification authorities.

Select Authentication Method:

Secured password (EAP-MSCHAP v2)

☑ Enable Fast Reconnect
□ Enforce Network Access Protection
□ Disconnect if server does not present cryptobinding TLV
□ Enable Identity Privacy

- Click on **Configure** button and uncheck the option:

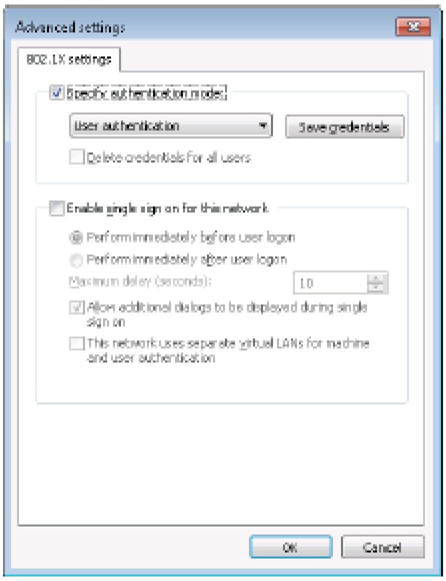


EAP MSCHAPv2 Properties

When connecting:

□ Automatically use my Windows logon name and password (and domain if any).

- Click **OK** and go back to the **Security** tab. Click **Advanced Settings** button and check **Specify authentication mode** and select **User authentication**. Click **OK** and close properties window.



Advanced settings

802.1X settings

☑ Specify authentication mode:

User authentication

□ Delete credentials for all users

□ Enable single sign on for this network

● Perform immediately before user logon

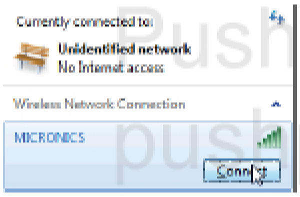
○ Perform immediately after user logon

Maximum delay (seconds): 10

☑ Allow additional dialogs to be displayed during single sign on

□ This network uses separate virtual LANs for machine and user authentication

- Click on network connection icon on the Windows tray and select **MICRONICS** network. Click **Connect**.



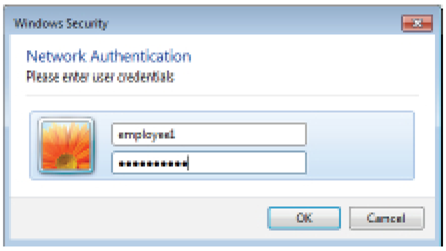
Currently connected to:

Unidentified network
No Internet access

Wireless Network Connection

MICRONICS

- Provide user credentials to connect to the network.

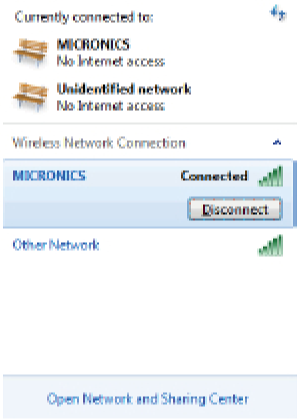


Windows Security

Network Authentication
Please enter user credentials

employee1
••••••••••

- You should see **Connected** status.



Currently connected to:

MICRONICS
No Internet access

Unidentified network
No Internet access

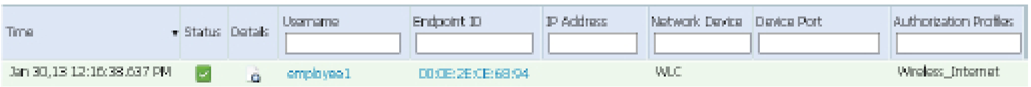
Wireless Network Connection

MICRONICS Connected

Other Network

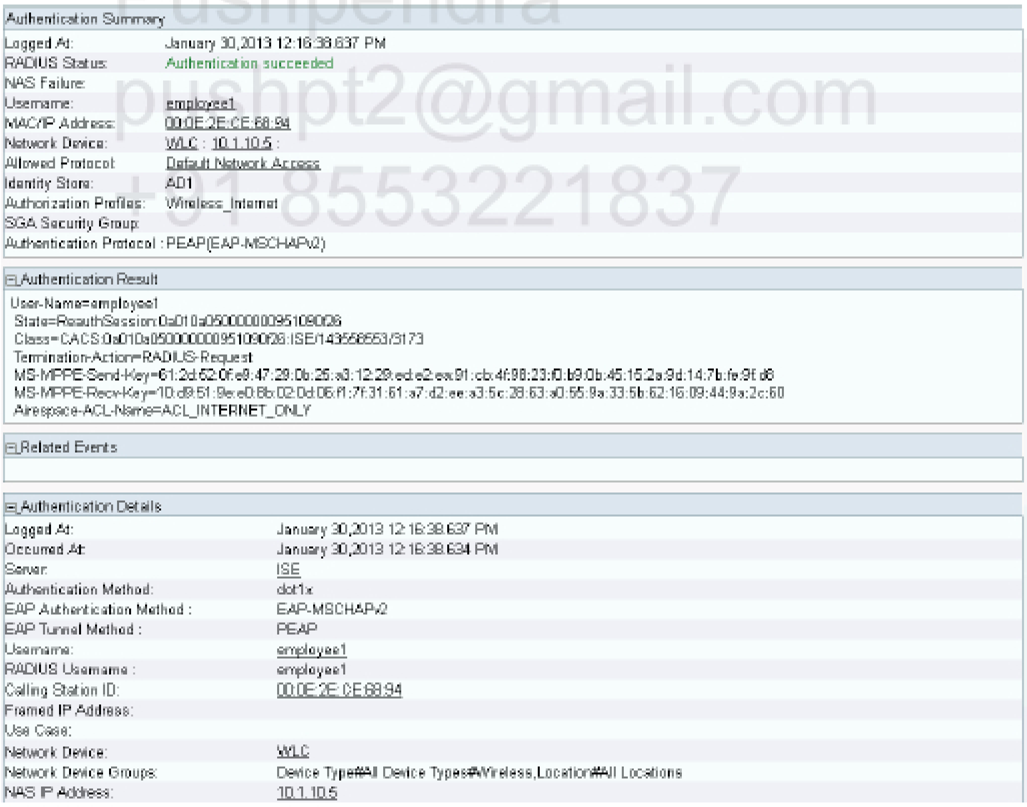
Open Network and Sharing Center

Go to ISE and check authentication logs.



Time	Status	Details	Username	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles
Jan 30,13 12:16:38.637 PM	✓		employee1	00:0E:2E:CE:68:94		WLC		Wireless_Internet

Click on details icon to see more information.



Authentication Summary

Logged At:	January 30,2013 12:16:38.637 PM
RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	employee1
MAC/IP Address:	00:0E:2E:CE:68:94
Network Device:	WLC : 10.1.10.5 :
Allowed Protocol:	Default Network Access
Identity Store:	AD1
Authorization Profiles:	Wireless_Internet
SGA Security Group:	
Authentication Protocol :	PEAP(EAP-MSCHAPv2)

⊟ Authentication Result

```
User-Name=employee1
 State=ReauthSession:0a010a0500000000951090f26
 Class=CACS:0a010a0500000000951090f26:ISE/143558553/3173
 Termination-Action=RADIUS-Request
 MS-MPPE-Send-Key=61:2d:62:0f:e9:47:29:0b:25:a3:12:29:ed:e2:ea:91:cb:4f:98:23:f0:b9:0b:45:15:2a:9d:14:7b:fe:9f:d8
 MS-MPPE-Recv-Key=10:d9:51:9e:e0:8b:02:0d:06:f1:7f:31:61:a7:d2:ee:a3:5c:28:63:a0:55:9a:33:5b:62:16:09:44:9a:2c:60
 Airespace-ACL-Name=ACL_INTERNET_ONLY
```

⊟ Related Events

⊟ Authentication Details

Logged At:	January 30,2013 12:16:38.637 PM
Occured At:	January 30,2013 12:16:38.634 PM
Server:	ISE
Authentication Method:	dot1x
EAP Authentication Method :	EAP-MSCHAPv2
EAP Tunnel Method :	PEAP
Username:	employee1
RADIUS Username :	employee1
Calling Station ID:	00:0E:2E:CE:68:94
Framed IP Address:	
Use Case:	
Network Device:	WLC
Network Device Groups:	Device Type#All Device Types#Wireless,Location#All Locations
NAS IP Address:	10.1.10.5

WLC debug while connecting the client.

```
(Cisco Controller) >debug client 00:0e:2e:ce:68:94
```

```
        // client debug is enabled. There is a new client discovered on AP with the
        following MAC address.

(Cisco Controller) >*DHCP Socket Task: Jan 29 15:47:07.575: 00:0e:2e:ce:68:94 DHCP   server id: 11.11.11.11  rcvd
server id: 172.31.1.200
*apfMsConnTask_3: Jan 30 10:33:11.057: 00:0e:2e:ce:68:94 Association received from mobile on AP c4:7d:4f:46:4b:00
*apfMsConnTask_3: Jan 30 10:33:11.057: 00:0e:2e:ce:68:94 10.1.30.20 RUN (20) Changing IPv4 ACL 'none' (ACL ID 255)
===> 'none' (ACL ID 255) --- (caller apf_policy.c:1697)
*apfMsConnTask_3: Jan 30 10:33:11.057: 00:0e:2e:ce:68:94 10.1.30.20 RUN (20) Changing IPv6 ACL 'none' (ACL ID 255)
===> 'none' (ACL ID 255) --- (caller apf_policy.c:1864)
*apfMsConnTask_3: Jan 30 10:33:11.057: 00:0e:2e:ce:68:94 Applying site-specific Local Bridging override for station
00:0e:2e:ce:68:94 - vapId 1, site 'default-group', interface 'dmz_interface'
*apfMsConnTask_3: Jan 30 10:33:11.057: 00:0e:2e:ce:68:94 Applying Local Bridging Interface Policy for station
00:0e:2e:ce:68:94 - vlan 0, interface id 11, interface 'dmz_interface'
*apfMsConnTask_3: Jan 30 10:33:11.057: 00:0e:2e:ce:68:94 processSsidIE  statusCode is 0 and status is 0
*apfMsConnTask_3: Jan 30 10:33:11.057: 00:0e:2e:ce:68:94 processSsidIE  ssid_done_flag is 0 finish_flag is 0
*apfMsConnTask_3: Jan 30 10:33:11.057: 00:0e:2e:ce:68:94 STA - rates (8): 130 132 139 12 18 150 24 36 48 72 96 108 0
0 0 0
*apfMsConnTask_3: Jan 30 10:33:11.057: 00:0e:2e:ce:68:94 suppRates  statusCode is 0 and gotSuppRatesElement is 1
*apfMsConnTask_3: Jan 30 10:33:11.057: 00:0e:2e:ce:68:94 STA - rates (12): 130 132 139 12 18 150 24 36 48 72 96 108
0 0 0 0
*apfMsConnTask_3: Jan 30 10:33:11.057: 00:0e:2e:ce:68:94 extSuppRates  statusCode is 0 and gotExtSuppRatesElement is
1
*apfMsConnTask_3: Jan 30 10:33:11.057: 00:0e:2e:ce:68:94 Processing RSN IE type 48, length 20 for mobile
00:0e:2e:ce:68:94
*apfMsConnTask_3: Jan 30 10:33:11.057: 00:0e:2e:ce:68:94 Received RSN IE with 0 PMKIDs from mobile 00:0e:2e:ce:68:94
*apfMsConnTask_3: Jan 30 10:33:11.057: 00:0e:2e:ce:68:94 Found an cache entry for BSSID c4:7d:4f:46:4b:00 in PMKID
cache at index 0 of station 00:0e:2e:ce:68:94
*apfMsConnTask_3: Jan 30 10:33:11.057: 00:0e:2e:ce:68:94 Removing BSSID c4:7d:4f:46:4b:00 from PMKID cache of
station 00:0e:2e:ce:68:94
*apfMsConnTask_3: Jan 30 10:33:11.057: 00:0e:2e:ce:68:94 Resetting MSCB PMK Cache Entry 0 for station
00:0e:2e:ce:68:94
*apfMsConnTask_3: Jan 30 10:33:11.057: 00:0e:2e:ce:68:94 Setting active key cache index 0 ---> 8
*apfMsConnTask_3: Jan 30 10:33:11.057: 00:0e:2e:ce:68:94 unsetting PmkIdValidatedByAp
*apfMsConnTask_3: Jan 30 10:33:11.057: 00:0e:2e:ce:68:94 apfMsRunStateDec
*apfMsConnTask_3: Jan 30 10:33:11.058: 00:0e:2e:ce:68:94 apfMs1xStateDec
*apfMsConnTask_3: Jan 30 10:33:11.058: 00:0e:2e:ce:68:94 10.1.30.20 RUN (20) Change state to START (0) last state
RUN (20)

*apfMsConnTask_3: Jan 30 10:33:11.058: 00:0e:2e:ce:68:94 pemApfAddMobileStation2: APF_MS_PEM_WAIT_L2_AUTH_COMPLETE =
0.
*apfMsConnTask_3: Jan 30 10:33:11.058: 00:0e:2e:ce:68:94 10.1.30.20 START (0) Initializing policy
*apfMsConnTask_3: Jan 30 10:33:11.058: 00:0e:2e:ce:68:94 10.1.30.20 START (0) Change state to AUTHCHECK (2) last
state RUN (20)

*apfMsConnTask_3: Jan 30 10:33:11.058: 00:0e:2e:ce:68:94 10.1.30.20 AUTHCHECK (2) Change state to 8021X_REQD (3)
last state RUN (20)

*apfMsConnTask_3: Jan 30 10:33:11.058: 00:0e:2e:ce:68:94 10.1.30.20 8021X_REQD (3) DHCP required on AP
c4:7d:4f:46:4b:00 vapId 1 apVapId 1for this client
*apfMsConnTask_3: Jan 30 10:33:11.058: 00:0e:2e:ce:68:94 Not Using WMM Compliance code qosCap 00
*apfMsConnTask_3: Jan 30 10:33:11.058: 00:0e:2e:ce:68:94 10.1.30.20 8021X_REQD (3) Plumbed mobile LWAPP rule on AP
c4:7d:4f:46:4b:00 vapId 1 apVapId 1
*apfMsConnTask_3: Jan 30 10:33:11.058: 00:0e:2e:ce:68:94 apfPemAddUser2 (apf_policy.c:268) Changing state for mobile
00:0e:2e:ce:68:94 on AP c4:7d:4f:46:4b:00 from Associated to Associated

*apfMsConnTask_3: Jan 30 10:33:11.058: 00:0e:2e:ce:68:94 Stopping deletion of Mobile Station: (callerId: 48)
*apfMsConnTask_3: Jan 30 10:33:11.058: 00:0e:2e:ce:68:94 Sending Assoc Response to station on BSSID
c4:7d:4f:46:4b:00 (status 0) ApVapId 1 Slot 0
*apfMsConnTask_3: Jan 30 10:33:11.058: 00:0e:2e:ce:68:94 apfProcessAssocReq (apf_80211.c:6290) Changing state for
mobile 00:0e:2e:ce:68:94 on AP c4:7d:4f:46:4b:00 from Associated to Associated

*pemReceiveTask: Jan 30 10:33:11.061: 00:0e:2e:ce:68:94 10.1.30.20 Removed NPU entry.
*dot1xMsgTask: Jan 30 10:33:11.064: 00:0e:2e:ce:68:94 Disable re-auth, use PMK lifetime.

        // 802.1x is starting here. There are couple of Access-Challenge messages
        because there is PEAP negotiation and certificate authentication.
```

```
*dot1xMsgTask: Jan 30 10:33:11.064: 00:0e:2e:ce:68:94 dot1x - moving mobile 00:0e:2e:ce:68:94 into Connecting state
*dot1xMsgTask: Jan 30 10:33:11.064: 00:0e:2e:ce:68:94 Sending EAP-Request/Identity to mobile 00:0e:2e:ce:68:94 (EAP
Id 1)
*Dot1x_NW_MsgTask_4: Jan 30 10:33:11.088: 00:0e:2e:ce:68:94 Received EAPOL START from mobile 00:0e:2e:ce:68:94
*Dot1x_NW_MsgTask_4: Jan 30 10:33:11.088: 00:0e:2e:ce:68:94 dot1x - moving mobile 00:0e:2e:ce:68:94 into Connecting
state
*Dot1x_NW_MsgTask_4: Jan 30 10:33:11.088: 00:0e:2e:ce:68:94 Sending EAP-Request/Identity to mobile 00:0e:2e:ce:68:94
(EAP Id 2)
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.182: 00:0e:2e:ce:68:94 Received EAPOL EAPPKT from mobile 00:0e:2e:ce:68:94
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.182: 00:0e:2e:ce:68:94 Received Identity Response (count=2) from mobile
00:0e:2e:ce:68:94
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.182: 00:0e:2e:ce:68:94 EAP State update from Connecting to Authenticating for
mobile 00:0e:2e:ce:68:94
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.182: 00:0e:2e:ce:68:94 dot1x - moving mobile 00:0e:2e:ce:68:94 into
Authenticating state
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.182: 00:0e:2e:ce:68:94 Entering Backend Auth Response state for mobile
00:0e:2e:ce:68:94
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.194: 00:0e:2e:ce:68:94 Processing Access-Challenge for mobile 00:0e:2e:ce:68:94
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.194: 00:0e:2e:ce:68:94 Entering Backend Auth Req state (id=230) for mobile
00:0e:2e:ce:68:94
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.194: 00:0e:2e:ce:68:94 WARNING: updated EAP-Identifier 2 ===> 230 for STA
00:0e:2e:ce:68:94
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.194: 00:0e:2e:ce:68:94 Sending EAP Request from AAA to mobile 00:0e:2e:ce:68:94
(EAP Id 230)
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.229: 00:0e:2e:ce:68:94 Received EAPOL EAPPKT from mobile 00:0e:2e:ce:68:94
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.229: 00:0e:2e:ce:68:94 Received EAP Response from mobile 00:0e:2e:ce:68:94 (EAP
Id 230, EAP Type 3)
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.229: 00:0e:2e:ce:68:94 Entering Backend Auth Response state for mobile
00:0e:2e:ce:68:94
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.234: 00:0e:2e:ce:68:94 Processing Access-Challenge for mobile 00:0e:2e:ce:68:94
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.234: 00:0e:2e:ce:68:94 Entering Backend Auth Req state (id=231) for mobile
00:0e:2e:ce:68:94

<snip>

*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.424: 00:0e:2e:ce:68:94 Sending EAP Request from AAA to mobile 00:0e:2e:ce:68:94
(EAP Id 239)
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.438: 00:0e:2e:ce:68:94 Received EAPOL EAPPKT from mobile 00:0e:2e:ce:68:94
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.438: 00:0e:2e:ce:68:94 Received EAP Response from mobile 00:0e:2e:ce:68:94 (EAP
Id 239, EAP Type 25)
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.438: 00:0e:2e:ce:68:94 Entering Backend Auth Response state for mobile
00:0e:2e:ce:68:94
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.527: 00:0e:2e:ce:68:94 Processing Access-Accept for mobile 00:0e:2e:ce:68:94
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.527: 00:0e:2e:ce:68:94 Resetting web IPv4 acl from 255 to 255

*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.527: 00:0e:2e:ce:68:94 10.1.30.20 8021X_REQD (3) Changing IPv4 ACL 'none' (ACL
ID 255) ===> 'none' (ACL ID 255) --- (caller apf_policy.c:1697)
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.527: 00:0e:2e:ce:68:94 10.1.30.20 8021X_REQD (3) Changing IPv6 ACL 'none' (ACL
ID 255) ===> 'none' (ACL ID 255) --- (caller apf_policy.c:1864)
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.527: 00:0e:2e:ce:68:94 Inserting AAA Override struct for mobile
        MAC: 00:0e:2e:ce:68:94, source 4

          // access list is applied as per AAA server request.

*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.527: 00:0e:2e:ce:68:94 10.1.30.20 8021X_REQD (3) Changing IPv4 ACL 'none' (ACL
ID 255) ===> 'ACL_INTERNET_ONLY' (ACL ID 0) --- (caller apf_policy.c:1750)
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.527: 00:0e:2e:ce:68:94 Setting re-auth timeout to 1800 seconds, got from WLAN
config.
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.527: 00:0e:2e:ce:68:94 Station 00:0e:2e:ce:68:94 setting dot1x reauth timeout =
1800
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.527: 00:0e:2e:ce:68:94 Creating a PKC PMKID Cache entry for station
00:0e:2e:ce:68:94 (RSN 2)
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.527: 00:0e:2e:ce:68:94 Resetting MSCB PMK Cache Entry 0 for station
00:0e:2e:ce:68:94
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.527: 00:0e:2e:ce:68:94 Setting active key cache index 8 ---> 8
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.527: 00:0e:2e:ce:68:94 Setting active key cache index 8 ---> 0
```

```
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.528: 00:0e:2e:ce:68:94 Adding BSSID c4:7d:4f:46:4b:00 to PMKID cache at index 0
for station 00:0e:2e:ce:68:94
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.528: New PMKID: (16)

*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.528:      [0000] b5 ea 8f f1 2c 5c 67 90 f9 ab 6d 25 33 69 8b d7

*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.528: 00:0e:2e:ce:68:94 Disabling re-auth since PMK lifetime can take care of
same.
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.528: 00:0e:2e:ce:68:94 unsetting PmkIdValidatedByAp
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.528: 00:0e:2e:ce:68:94 PMK sent to mobility group
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.528: 00:0e:2e:ce:68:94 Sending EAP-Success to mobile 00:0e:2e:ce:68:94 (EAP Id
239)
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.528: 00:0e:2e:ce:68:94 Found an cache entry for BSSID c4:7d:4f:46:4b:00 in
PMKID cache at index 0 of station 00:0e:2e:ce:68:94
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.528: 00:0e:2e:ce:68:94 Found an cache entry for BSSID c4:7d:4f:46:4b:00 in
PMKID cache at index 0 of station 00:0e:2e:ce:68:94
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.528: Including PMKID in M1  (16)

*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.528:      [0000] b5 ea 8f f1 2c 5c 67 90 f9 ab 6d 25 33 69 8b d7

*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.528: 00:0e:2e:ce:68:94 Starting key exchange to mobile 00:0e:2e:ce:68:94, data
packets will be dropped
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.528: 00:0e:2e:ce:68:94 Sending EAPOL-Key Message to mobile 00:0e:2e:ce:68:94

state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.528: 00:0e:2e:ce:68:94 Entering Backend Auth Success state (id=239) for mobile
00:0e:2e:ce:68:94
```

```
        // authentication is successful. The client gets encryption keys from the WLC
        for its session.
```

```
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.528: 00:0e:2e:ce:68:94 Received Auth Success while in Authenticating state for
mobile 00:0e:2e:ce:68:94
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.528: 00:0e:2e:ce:68:94 dot1x - moving mobile 00:0e:2e:ce:68:94 into
Authenticated state
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.535: 00:0e:2e:ce:68:94 Received EAPOL-Key from mobile 00:0e:2e:ce:68:94
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.535: 00:0e:2e:ce:68:94 Ignoring invalid EAPOL version (1) in EAPOL-key message
from mobile 00:0e:2e:ce:68:94
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.535: 00:0e:2e:ce:68:94 Received EAPOL-key in PTK_START state (message 2) from
mobile 00:0e:2e:ce:68:94
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.536: 00:0e:2e:ce:68:94 PMK: Sending cache add
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.536: 00:0e:2e:ce:68:94 Stopping retransmission timer for mobile
00:0e:2e:ce:68:94
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.536: 00:0e:2e:ce:68:94 Sending the random GTK in M3 for WPA2 client
00:0e:2e:ce:68:94
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.536: 00:0e:2e:ce:68:94 Sending EAPOL-Key Message to mobile 00:0e:2e:ce:68:94

state PTKINITNEGOTIATING (message 3), replay counter 00.00.00.00.00.00.00.01
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.542: 00:0e:2e:ce:68:94 Received EAPOL-Key from mobile 00:0e:2e:ce:68:94
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.542: 00:0e:2e:ce:68:94 Ignoring invalid EAPOL version (1) in EAPOL-key message
from mobile 00:0e:2e:ce:68:94
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.542: 00:0e:2e:ce:68:94 Received EAPOL-key in PTKINITNEGOTIATING state (message
4) from mobile 00:0e:2e:ce:68:94
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.542: 00:0e:2e:ce:68:94 apfMs1xStateInc
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.542: 00:0e:2e:ce:68:94 10.1.30.20 8021X_REQD (3) Change state to L2AUTHCOMPLETE
(4) last state RUN (20)

*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.542: 00:0e:2e:ce:68:94 10.1.30.20 L2AUTHCOMPLETE (4) DHCP required on AP
c4:7d:4f:46:4b:00 vapId 1 apVapId 1for this client
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.542: 00:0e:2e:ce:68:94 Not Using WMM Compliance code qosCap 00
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.542: 00:0e:2e:ce:68:94 10.1.30.20 L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule
on AP c4:7d:4f:46:4b:00 vapId 1 apVapId 1
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.542: 00:0e:2e:ce:68:94 apfMsRunStateInc
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.542: 00:0e:2e:ce:68:94 10.1.30.20 L2AUTHCOMPLETE (4) Change state to RUN (20)
last state RUN (20)

*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.542: 00:0e:2e:ce:68:94 10.1.30.20 RUN (20) Reached PLUMBFASTPATH: from line
5362
```

```
*D: Jan 30 10:33:18.542: 00:0e:2e:ce:68:94 10.1.30.20 RUN (20) Adding Fast Path rule
  type = Airespace AP Client
  on AP c4:7d:4f:46:4b:00, slot 0, interface = 1, QOS = 0
  IPv4 ACL ID = 0, IPv6 ACL ID = 255,
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.542: 00:0e:2e:ce:68:94 10.1.30.20 RUN (20) Fast Path rule (contd...) 802.1P =
0, DSCP = 0, TokenID = 7006  Local Bridging Vlan = 0, Local Bridging intf id = 11
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.543: 00:0e:2e:ce:68:94 10.1.30.20 RUN (20) Successfully plumbed mobile rule
(IPv4 ACL ID 0, IPv6 ACL ID 255)
*Dot1x_NW_MsgTask_4: Jan 30 10:33:18.543: 00:0e:2e:ce:68:94 Stopping retransmission timer for mobile
00:0e:2e:ce:68:94
*pemReceiveTask: Jan 30 10:33:18.543: 00:0e:2e:ce:68:94 10.1.30.20 Added NPU entry of type 1, dtlFlags 0x0
```

// after authentication (which is done at Layer 2) the client asks for IP address. There must be path opened between WLC and DHCP server to get an IP address for the client.

```
*DHCP Socket Task: Jan 30 10:33:18.667: 00:0e:2e:ce:68:94 DHCP received op BOOTREQUEST (1) (len 326,vlan 10, port 1,
encap 0xec03)
*DHCP Socket Task: Jan 30 10:33:18.667: 00:0e:2e:ce:68:94 DHCP selecting relay 1 - control block settings:
                        dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,
                        dhcpGateway: 0.0.0.0, dhcpRelay: 0.0.0.0  VLAN: 0
*DHCP Socket Task: Jan 30 10:33:18.668: 00:0e:2e:ce:68:94 DHCP selected relay 1 - 172.31.1.200 (local address
10.1.30.5, gateway 10.1.30.10, VLAN 0, port 2)
*DHCP Socket Task: Jan 30 10:33:18.668: 00:0e:2e:ce:68:94 DHCP transmitting DHCP REQUEST (3)
*DHCP Socket Task: Jan 30 10:33:18.668: 00:0e:2e:ce:68:94 DHCP   op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1
*DHCP Socket Task: Jan 30 10:33:18.668: 00:0e:2e:ce:68:94 DHCP   xid: 0x4ae5f8a2 (1256585378), secs: 0, flags: 0
*DHCP Socket Task: Jan 30 10:33:18.668: 00:0e:2e:ce:68:94 DHCP   chaddr: 00:0e:2e:ce:68:94
*DHCP Socket Task: Jan 30 10:33:18.668: 00:0e:2e:ce:68:94 DHCP   ciaddr: 0.0.0.0,  yiaddr: 0.0.0.0
*DHCP Socket Task: Jan 30 10:33:18.668: 00:0e:2e:ce:68:94 DHCP   siaddr: 0.0.0.0,  giaddr: 10.1.30.5
*DHCP Socket Task: Jan 30 10:33:18.668: 00:0e:2e:ce:68:94 DHCP   requested ip: 10.1.30.20
*DHCP Socket Task: Jan 30 10:33:18.668: 00:0e:2e:ce:68:94 DHCP sending REQUEST to 10.1.30.10 (len 362, port 2, vlan
0)
*DHCP Socket Task: Jan 30 10:33:18.668: 00:0e:2e:ce:68:94 DHCP selecting relay 2 - control block settings:
                        dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,
                        dhcpGateway: 0.0.0.0, dhcpRelay: 10.1.30.5  VLAN: 0
*DHCP Socket Task: Jan 30 10:33:18.668: 00:0e:2e:ce:68:94 DHCP selected relay 2 - NONE
*DHCP Socket Task: Jan 30 10:33:18.754: 00:0e:2e:ce:68:94 DHCP received op BOOTREPLY (2) (len 312,vlan 0, port 2,
encap 0xec00)
*DHCP Socket Task: Jan 30 10:33:18.754: 00:0e:2e:ce:68:94 DHCP setting server from ACK (server 172.31.1.200, yiaddr
10.1.30.20)
*DHCP Socket Task: Jan 30 10:33:18.754: 00:0e:2e:ce:68:94 DHCP sending REPLY to STA (len 418, port 1, vlan 10)
*DHCP Socket Task: Jan 30 10:33:18.754: 00:0e:2e:ce:68:94 DHCP transmitting DHCP ACK (5)
*DHCP Socket Task: Jan 30 10:33:18.754: 00:0e:2e:ce:68:94 DHCP   op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0
*DHCP Socket Task: Jan 30 10:33:18.754: 00:0e:2e:ce:68:94 DHCP   xid: 0x4ae5f8a2 (1256585378), secs: 0, flags: 0
*DHCP Socket Task: Jan 30 10:33:18.755: 00:0e:2e:ce:68:94 DHCP   chaddr: 00:0e:2e:ce:68:94
*DHCP Socket Task: Jan 30 10:33:18.755: 00:0e:2e:ce:68:94 DHCP   ciaddr: 0.0.0.0,  yiaddr: 10.1.30.20
*DHCP Socket Task: Jan 30 10:33:18.755: 00:0e:2e:ce:68:94 DHCP   siaddr: 0.0.0.0,  giaddr: 0.0.0.0
*DHCP Socket Task: Jan 30 10:33:18.755: 00:0e:2e:ce:68:94 DHCP   server id: 11.11.11.11  rcvd server id:
172.31.1.200
*IPv6_Msg_Task: Jan 30 10:33:18.755: 00:0e:2e:ce:68:94 Pushing IPv6: fe80:0000:0000:0000: 7dff:670e:20ef:2045 , and
MAC: 00:0E:2E:CE:68:94 , Binding to Data Plane. SUCCESS !!
*DHCP Socket Task: Jan 30 10:33:21.850: 00:0e:2e:ce:68:94 DHCP received op BOOTREQUEST (1) (len 308,vlan 10, port 1,
encap 0xec03)
*DHCP Socket Task: Jan 30 10:33:21.850: 00:0e:2e:ce:68:94 DHCP selecting relay 1 - control block settings:
                        dhcpServer: 172.31.1.200, dhcpNetmask: 255.255.255.0,
                        dhcpGateway: 10.1.30.10, dhcpRelay: 10.1.30.5  VLAN: 0
*DHCP Socket Task: Jan 30 10:33:21.850: 00:0e:2e:ce:68:94 DHCP selected relay 1 - 172.31.1.200 (local address
10.1.30.5, gateway 10.1.30.10, VLAN 0, port 2)
```

// here's the DHCP INFORM (or OFFER if this is first attempt to get an IP address) with IP address for the client.

```
*DHCP Socket Task: Jan 30 10:33:21.850: 00:0e:2e:ce:68:94 DHCP transmitting DHCP INFORM (8)
*DHCP Socket Task: Jan 30 10:33:21.850: 00:0e:2e:ce:68:94 DHCP   op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1
*DHCP Socket Task: Jan 30 10:33:21.850: 00:0e:2e:ce:68:94 DHCP   xid: 0xbfbc6234 (3216794164), secs: 0, flags: 0
*DHCP Socket Task: Jan 30 10:33:21.850: 00:0e:2e:ce:68:94 DHCP   chaddr: 00:0e:2e:ce:68:94
*DHCP Socket Task: Jan 30 10:33:21.850: 00:0e:2e:ce:68:94 DHCP   ciaddr: 10.1.30.20,  yiaddr: 0.0.0.0
```

```
*DHCP Socket Task: Jan 30 10:33:21.850: 00:0e:2e:ce:68:94 DHCP   siaddr: 0.0.0.0,  giaddr: 10.1.30.5
*DHCP Socket Task: Jan 30 10:33:21.851: 00:0e:2e:ce:68:94 DHCP sending REQUEST to 10.1.30.10 (len 346, port 2, vlan 
0)
*DHCP Socket Task: Jan 30 10:33:21.851: 00:0e:2e:ce:68:94 DHCP selecting relay 2 - control block settings:
                        dhcpServer: 172.31.1.200, dhcpNetmask: 255.255.255.0,
                        dhcpGateway: 10.1.30.10, dhcpRelay: 10.1.30.5  VLAN: 0
*DHCP Socket Task: Jan 30 10:33:21.851: 00:0e:2e:ce:68:94 DHCP selected relay 2 - NONE
*DHCP Socket Task: Jan 30 10:33:21.923: 00:0e:2e:ce:68:94 DHCP received op BOOTREPLY (2) (len 308,vlan 0, port 2, 
encap 0xec00)
*DHCP Socket Task: Jan 30 10:33:21.923: 00:0e:2e:ce:68:94 DHCP sending REPLY to STA (len 418, port 1, vlan 10)
*DHCP Socket Task: Jan 30 10:33:21.923: 00:0e:2e:ce:68:94 DHCP transmitting DHCP ACK (5)
*DHCP Socket Task: Jan 30 10:33:21.923: 00:0e:2e:ce:68:94 DHCP   op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0
*DHCP Socket Task: Jan 30 10:33:21.923: 00:0e:2e:ce:68:94 DHCP   xid: 0xbfbc6234 (3216794164), secs: 0, flags: 0
*DHCP Socket Task: Jan 30 10:33:21.923: 00:0e:2e:ce:68:94 DHCP   chaddr: 00:0e:2e:ce:68:94
*DHCP Socket Task: Jan 30 10:33:21.923: 00:0e:2e:ce:68:94 DHCP   ciaddr: 10.1.30.20,  yiaddr: 0.0.0.0
*DHCP Socket Task: Jan 30 10:33:21.924: 00:0e:2e:ce:68:94 DHCP   siaddr: 0.0.0.0,  giaddr: 0.0.0.0
*DHCP Socket Task: Jan 30 10:33:21.924: 00:0e:2e:ce:68:94 DHCP   server id: 11.11.11.11  rcvd server id: 
172.31.1.200
```

LAB 3.12. Local Web Authentication (LWA) for Wired

Objectives

This lab shows how to configure Local WebAuth on switch.

IP Addressing and devices

Device	Interface	IP address
ISE	NIC	172.31.1.20
R1	Lo0	1.1.1.1/32
	E0/0	10.1.10.1/24
	E0/1	172.31.1.1/24
AD	NIC	172.31.1.200
WinXP	NIC	10.1.10.50/24
WLC	G0/0/1 (mgmt.)	10.1.10.5/24
	G0/0/2	10.1.30.5/24
ASA1	G0/0 (outside)	100.2.2.10/24
	G0/1 (inside)	10.1.10.10/24
	G0/2 (dmz)	10.1.30.10/24
Win7 PC	LAN NIC (LAB-Network)	DHCP-Assigned
	WLAN NIC	10.1.30.x (DHCP)

Task

Disable Win7 native supplicant and Wireless connection. Enable LAN connection and setup ISE to use WebAuth as a last resort authentication mechanism for members of AD group micronics.local/Users/students. The members of that group should have access to the following services after authentication:

DST IP	Protocol	DST Port	Service
172.31.1.200	TCP	80	WWW

Any	ICMP	-	Ping
172.31.1.200	UDP	53	DNS
Any	TCP	3389	RDP

Allow only DNS and DHCP packets before authentication. You can alter default authentication rule to first authenticate users against Internal Identity Store and then Active Directory. DO NOT use Downloadable ACL to accomplish this task.

Configuration

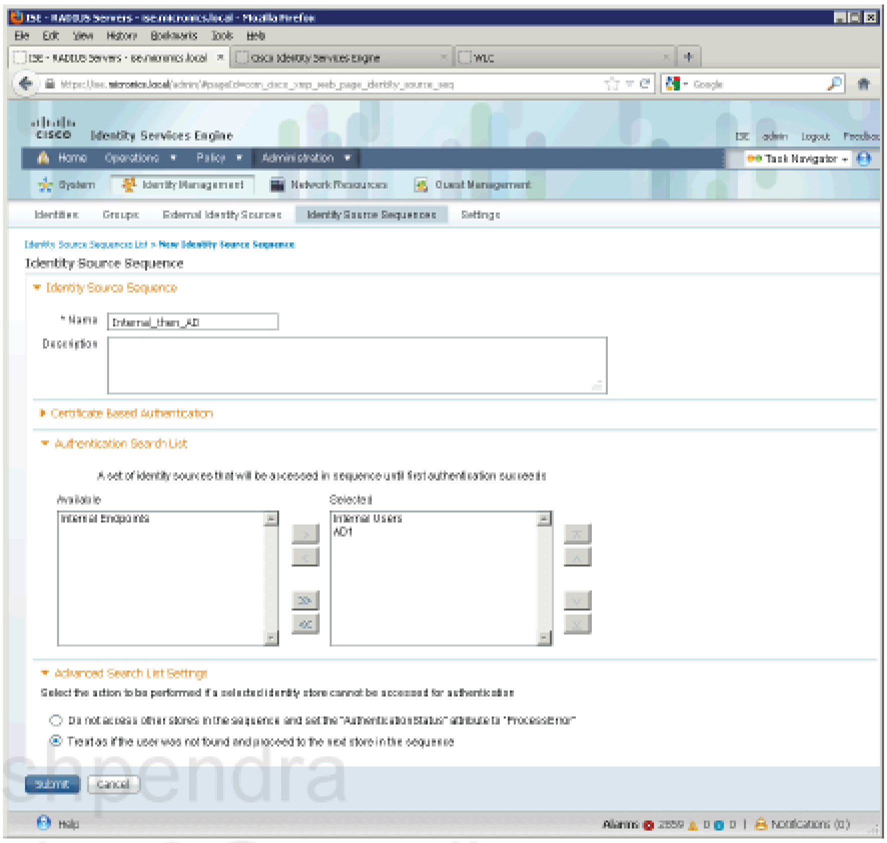
Complete these steps:

Step 1 Switch configuration.

```
!
aaa authentication login default group radius
aaa authorization auth-proxy default group radius
!
ip http server
ip http secure-server
ip admission name WEBAUTH proxy http
!
ip access-list extended PRE_AUTH_POLICY
 permit udp any any eq bootps
 permit udp any any eq domain
!
fallback profile WEBAUTH_PROFILE
 ip access-group PRE_AUTH_POLICY in
 ip admission WEBAUTH
!
interface GigabitEthernet0/7
 no ip access-group DEFAULT in
 authentication fallback WEBAUTH_PROFILE
 authentication order dot1x mab webauth
 authentication event fail action next-method
!
ip access-list extended ACL_WEBAUTH_STUDENTS
 permit tcp any host 172.31.1.200 eq www
 permit icmp any any
 permit tcp any any eq 3389
 permit udp any host 172.31.1.200 eq domain
!
```

Step 2 ISE configuration. Add Identity Source Sequence and change default authentication rule.

- Go to **Administration > Identity Management > Identity Source Sequences** and click **Add**. Enter a name for the object e.g. **Internal_then_AD** and move **Internal Users** & **AD1** identity stores to the right pane. Click **Submit**.



Identity Source Sequence List > New Identity Source Sequence

Identity Source Sequence

Identity Source Sequence

* Name: Internal_then_AD

Description:

Certificate Based Authentication

Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available: Internal Endpoints

Selected: Internal Users, AD1

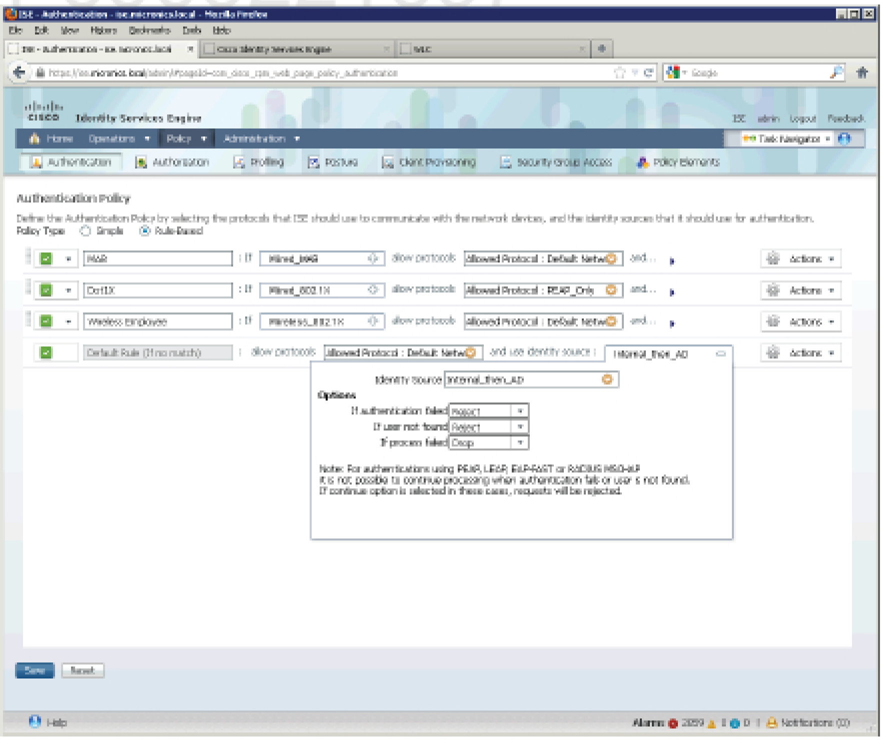
Advanced Search List Settings

Select the action to be performed if a selected identity store cannot be accessed for authentication

○ Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"

● Treat as if the user was not found and proceed to the next store in the sequence

- Go to **Policy > Authentication** and for default rule (the last one) change the identity source to **Internal_then_AD**.



Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

Policy Type ○ Simple ● Rule-Based

☑	MAB	: If Wired_MAB	allow protocols	Allowed Protocol : Default Netw	and ...
☑	Dot1X	: If Wired_802.1X	allow protocols	Allowed Protocol : PEAP_Only	and ...
☑	Wireless Employee	: If Wireless_802.1X	allow protocols	Allowed Protocol : Default Netw	and ...
☑	Default Rule (If no match)	:	allow protocols	Allowed Protocol : Default Netw	and use identity source : Internal_then_AD

Identity Source: Internal_then_AD

Options

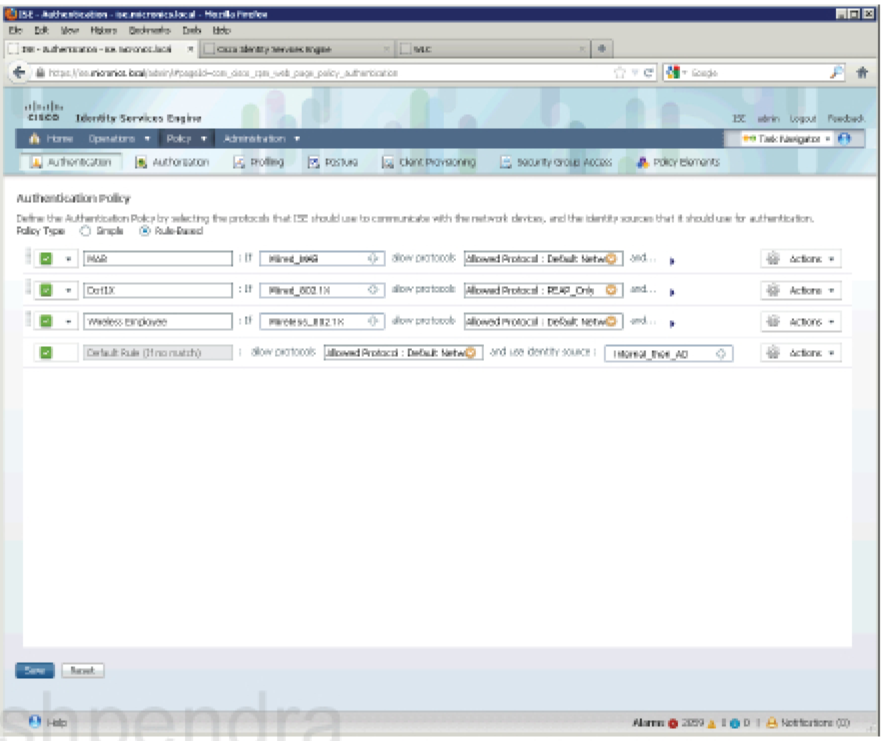
If authentication failed: Reject

If user not found: Reject

If process failed: Drop

Note: For authentications using PEAP, LEAP, EAP-FAST or RADIUS MSCHAP it is not possible to continue processing when authentication fails or user is not found. If continue option is selected in these cases, requests will be rejected.

- Click **Save** to apply changes.



ISE - Authentication - ise.micronics.local - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Identity Services Engine
ISE admin Logout Feedback
Home Operations ▾ Policy ▾ Administration ▾
Task Navigator ▾
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements
Save Reset
Help

Authentication Policy

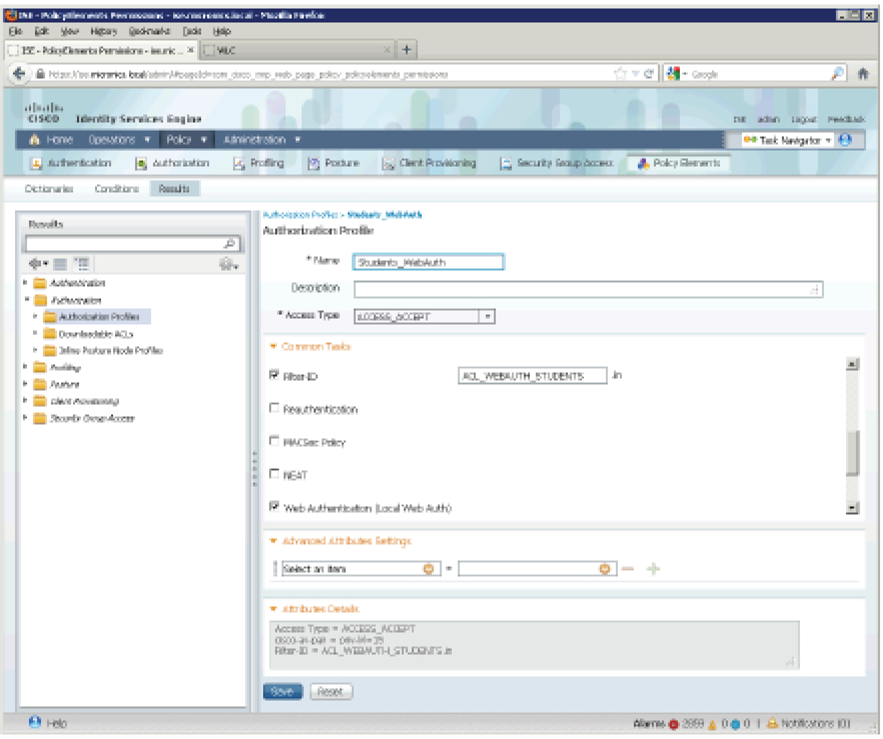
Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

Policy Type ○ Simple ● Rule-Based

☑ MAB	: If	Wired_MAB	allow protocols	Allowed Protocol : Default Netw	and ...	Actions ▾
☑ Dot1X	: If	Wired_802.1X	allow protocols	Allowed Protocol : PEAP_Only	and ...	Actions ▾
☑ Wireless Employee	: If	Wireless_802.1X	allow protocols	Allowed Protocol : Default Netw	and ...	Actions ▾
☑ Default Rule (If no match)	:	allow protocols	Allowed Protocol : Default Netw	and use identity source :	Internal_then_AD	Actions ▾

Step 3 Create new authorization profile for Students.

- Go to **Policy > Policy Elements > Results > Authorization > Authorization Profiles** and click **Add**. Enter a name for the object e.g. **Students_WebAuth**, select **Web Authentication (Local Web Auth)** and set **Filter-ID** to **ACL_WEBAUTH_STUDENTS** (the ACL name as it is configured on the switch). Click **Save**.



Authorization Profiles > Students_WebAuth

Authorization Profile

* Name: Students_WebAuth

Description:

* Access Type: ACCESS_ACCEPT

Common Tasks

☑ Filter-ID ACL_WEBAUTH_STUDENTS .in

□ Reauthentication

□ MACSec Policy

□ NEAT

☑ Web Authentication (Local Web Auth)

Advanced Attributes Settings

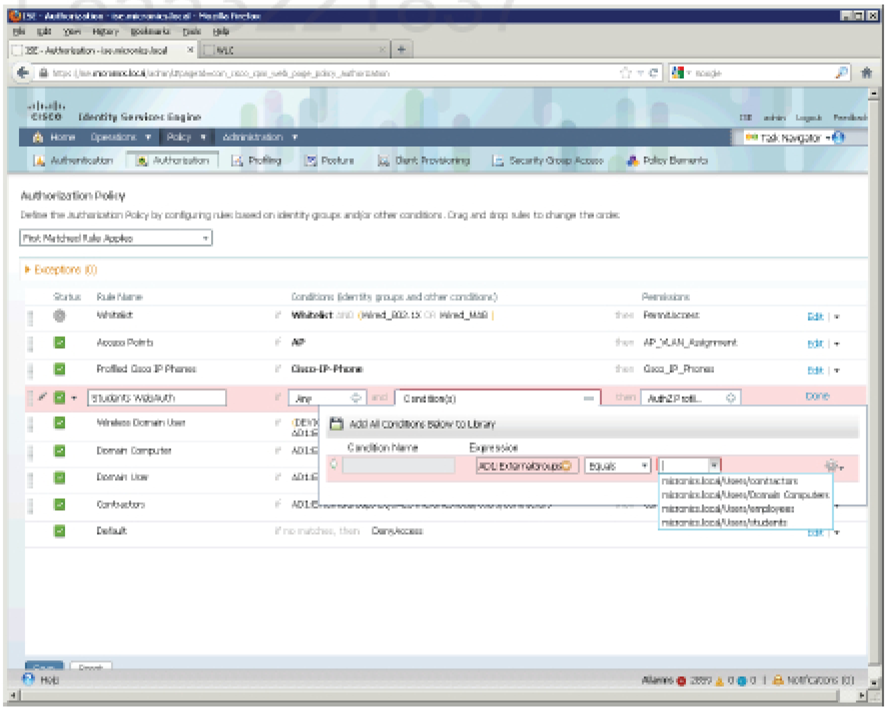
Select an item =

Attributes Details

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = priv-lvl=15
Filter-ID = ACL_WEBAUTH_STUDENTS.in
```

Step 4 Create new authorization rule for Students.

- Go to **Policy > Authorization** and add anew rule. Enter a name for the rule e.g. **Students WebAuth** and select compound condition that **AD1:ExternalGroups Equals micronics.local/Users/students**.



Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

Exceptions (0)

Status	Rule Name	Conditions (identity groups and other conditions)		Permissions
	Whitelist	Whitelist AND (Wired_802.1X OR Wired_MAB)	then	PermitAccess
	Access Points	AP	then	AP_VLAN_Assignment
	Profiled Cisco IP Phones	Cisco-IP-Phone	then	Cisco_IP_Phones
	Students WebAuth	Any and Condition(s)	then	AuthZ Profil...
	Wireless Domain User			
	Domain Computer			
	Domain User			
	Contractors			
	Default	If no matches, then DenyAccess		

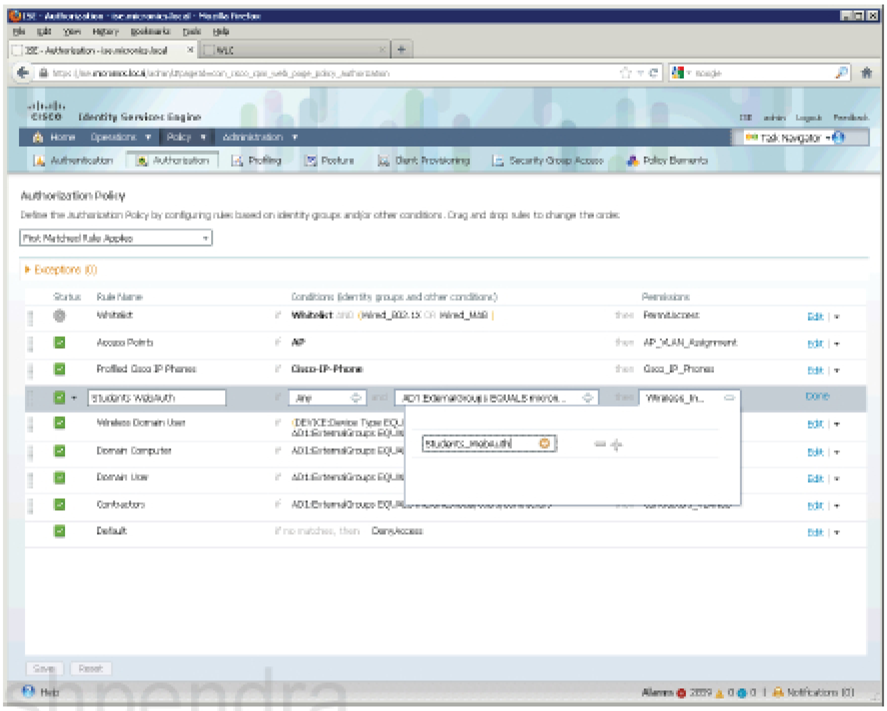
Add All Conditions Below to Library

Condition Name | Expression: AD1:ExternalGroups Equals

micronics.local/Users/contractors
micronics.local/Users/Domain Computers
micronics.local/Users/employees
micronics.local/Users/students

- For Permissions select **Students_WebAuth** authorization profile.

Click **Done** and **Save**.



Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

Exceptions (0)

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
	Whitelist	if	Whitelist AND (Wired_802.1X OR Wired_MAB)	then	PermitAccess	Edit ▾
✓	Access Points	if	AP	then	AP_VLAN_Assignment	Edit ▾
✓	Profiled Cisco IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phones	Edit ▾
✓	Students WebAuth	if	Any and AD1:ExternalGroups EQUALS microl...	then	Wireless_In...	Done
✓	Wireless Domain User	if	(DEVICE:Device Type EQU... AD1:ExternalGroups EQU...			Edit ▾
✓	Domain Computer	if	AD1:ExternalGroups EQU...			Edit ▾
✓	Domain User	if	AD1:ExternalGroups EQU...			Edit ▾
✓	Contractors	if	AD1:ExternalGroups EQU...			Edit ▾
✓	Default		if no matches, then DenyAccess			Edit ▾

Students_WebAuth

Step 5 Win7 PC configuration.

- Go to **Control Panel > Network and Internet > Network Connections** and disable wireless adapter.
- Go to **Services** (services.msc) and disable **Wired AutoConfig** service.
- Enable LAN interface (LAB-Network)

Verification

Enable debugging on the switch:

```
debug radius
debug dot1x events
```

Check settings on the switch.

```
SW1#sh run int g0/7
Building configuration...

Current configuration : 546 bytes
!
interface GigabitEthernet0/7
 description IPP + Win7
 switchport access vlan 10
 switchport mode access
 switchport nonegotiate
 switchport voice vlan 500
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication order dot1x mab webauth
 authentication port-control auto
 authentication periodic
 authentication timer reauthenticate server
 authentication violation protect
 authentication fallback WEBAUTH_PROFILE
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 5
 spanning-tree portfast
end

SW1#sh ip access-lists interface g0/7

       // there is no ACL applied to the port. There is only IP Phone authenticated
       (VOICE domain).

SW1#sh auth sess int g0/7
            Interface:  GigabitEthernet0/7
          MAC Address:  0021.a084.6ff4
           IP Address:  Unknown
            User-Name:  00-21-A0-84-6F-F4
               Status:  Authz Success
               Domain:  VOICE
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
              ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-4f57e406
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A010A070000002F00ED9839
      Acct Session ID:  0x00000034
               Handle:  0x3500002F

Runnable methods list:
       Method   State
       dot1x    Failed over
       mab      Authc Success
       webauth  Not run
```

Enable LAB-Network connection on the Win7 PC. Check out switch logs.

```
       // Dot1x is starting on the switch. It tries three times and fails.
```

```
dot1x-ev(Gi0/7): Couldn't find the supplicant in the list
dot1x-ev(Gi0/7): Sending create new context event to EAP for 0x980000E7 (0026.55d0.0d56)
dot1x-ev(Gi0/7): Created a client entry (0x980000E7)
dot1x-ev(Gi0/7): Dot1x authentication started for 0x980000E7 (0026.55d0.0d56)
%AUTHMGR-5-START: Starting 'dot1x' for client (0026.55d0.0d56) on Interface Gi0/7 AuditSessionID
0A010A07000000620AD3DF00

dot1x-ev(Gi0/7): Sending EAPOL packet to 0026.55d0.0d56
dot1x-ev(Gi0/7): Role determination not required
dot1x-ev(Gi0/7): Sending out EAPOL packet

dot1x-ev(Gi0/7): Sending EAPOL packet to 0026.55d0.0d56
dot1x-ev(Gi0/7): Role determination not required
dot1x-ev(Gi0/7): Sending out EAPOL packet

dot1x-ev(Gi0/7): Sending EAPOL packet to 0026.55d0.0d56
dot1x-ev(Gi0/7): Role determination not required
dot1x-ev(Gi0/7): Sending out EAPOL packet

dot1x-ev(Gi0/7): Received an EAP Timeout
%DOT1X-5-FAIL: Authentication failed for client (0026.55d0.0d56) on Interface Gi0/7 AuditSessionID
dot1x-ev(Gi0/7): Sending event (2) to Auth Mgr for 0026.55d0.0d56
%AUTHMGR-7-RESULT: Authentication result 'no-response' from 'dot1x' for client (0026.55d0.0d56) on Interface Gi0/7
AuditSessionID 0A010A07000000620AD3DF00
dot1x-ev(Gi0/7): Received Authz fail for the client  0x980000E7 (0026.55d0.0d56)
dot1x-ev(Gi0/7): Deleting client 0x980000E7 (0026.55d0.0d56)
```

// dot1x has failed, the next method is MAB.

```
%AUTHMGR-7-FAILOVER: Failing over from 'dot1x' for client (0026.55d0.0d56) on Interface Gi0/7 AuditSessionID
0A010A07000000620AD3DF00
%AUTHMGR-5-START: Starting 'mab' for client (0026.55d0.0d56) on Interface Gi0/7 AuditSessionID
0A010A07000000620AD3DF00
dot1x-ev:Delete auth client (0x980000E7) message
dot1x-ev:Auth client ctx destroyed
dot1x-ev:Aborted posting message to authenticator state machine: Invalid client
RADIUS/ENCODE(00000074):Orig. component type = DOT1X
RADIUS(00000074): Config NAS IP: 10.1.10.7
RADIUS/ENCODE(00000074): acct_session_id: 116
RADIUS(00000074): sending
```

// MAB never times out because there is no supplicat required on the client. So, the authentication based on MAC address is running.

```
RADIUS(00000074): Send Access-Request to 172.31.1.20:1812 id 1645/236, len 215
RADIUS:  authenticator 5F F3 35 47 99 D5 0F B7 - 1F BD 59 69 D9 91 47 A9
RADIUS:  User-Name           [1]   14  "002655d00d56"
RADIUS:  User-Password       [2]   18  *
RADIUS:  Service-Type        [6]   6   Call Check                [10]
RADIUS:  Framed-IP-Address   [8]   6   10.1.10.104
RADIUS:  Framed-MTU          [12]  6   1500
RADIUS:  Called-Station-Id   [30]  19  "C4-64-13-6C-E8-07"
RADIUS:  Calling-Station-Id  [31]  19  "00-26-55-D0-0D-56"
RADIUS:  Message-Authenticato[80]  18
RADIUS:   26 87 D2 19 10 C3 AE F5 22 F5 47 91 69 27 DF 8B             [ &"Gi']
RADIUS:  EAP-Key-Name        [102] 2   *
RADIUS:  Vendor, Cisco       [26]  49
RADIUS:   Cisco AVpair       [1]   43  "audit-session-id=0A010A07000000620AD3DF00"
RADIUS:  NAS-Port-Type       [61]  6   Ethernet                  [15]
RADIUS:  NAS-Port            [5]   6   50007
RADIUS:  NAS-Port-Id         [87]  20  "GigabitEthernet0/7"
RADIUS:  NAS-IP-Address      [4]   6   10.1.10.7
RADIUS(00000074): Started 5 sec timeout
```

// The ISE has no MAC address in the Endpoint Identity Store so it rejects the client.

```
RADIUS: Received from id 1645/236 172.31.1.20:1812, Access-Reject, len 38
RADIUS:  authenticator 74 78 74 54 CE 6D 62 ED - 4D C0 E6 7E 23 BF 16 FB
RADIUS:  Message-Authenticato[80]  18
RADIUS:   1B 5C B1 9B 26 F5 DB F6 15 C9 B1 64 0E 30 53 90            [ \εd0S]
RADIUS(00000074): Received from id 1645/236
%MAB-5-FAIL: Authentication failed for client (0026.55d0.0d56) on Interface Gi0/7 AuditSessionID
0A010A07000000620AD3DF00
%AUTHMGR-7-RESULT: Authentication result 'no-response' from 'mab' for client (0026.55d0.0d56) on Interface Gi0/7
AuditSessionID 0A010A07000000620AD3DF00
```

// since we have third method configured on the port the WebAuth is starting.

```
%AUTHMGR-7-FAILOVER: Failing over from 'mab' for client (0026.55d0.0d56) on Interface Gi0/7 AuditSessionID
0A010A07000000620AD3DF00
%AUTHMGR-5-START: Starting 'webauth' for client (0026.55d0.0d56) on Interface Gi0/7 AuditSessionID
0A010A07000000620AD3DF00
%EPM-6-POLICY_REQ: IP 0.0.0.0| MAC 0026.55d0.0d56| AuditSessionID 0A010A07000000620AD3DF00| AUTHTYPE AUTHPROXY|
EVENT APPLY
```

// EPM is assigning a Pre-Auth ACL configured in the fallback profile.

```
%EPM-6-POLICY_APP_SUCCESS: IP 10.1.10.104| MAC 0026.55d0.0d56| AuditSessionID 0A010A07000000620AD3DF00| AUTHTYPE
AUTHPROXY| POLICY_TYPE Named ACL| POLICY_NAME PRE_AUTH_POLICY| RESULT SUCCESS
%AUTHMGR-7-RESULT: Authentication result 'success' from 'webauth' for client (0026.55d0.0d56) on Interface Gi0/7
AuditSessionID 0A010A07000000620AD3DF00
%AUTHMGR-5-SUCCESS: Authorization succeeded for client (0026.55d0.0d56) on Interface Gi0/7 AuditSessionID
0A010A07000000620AD3DF00
```

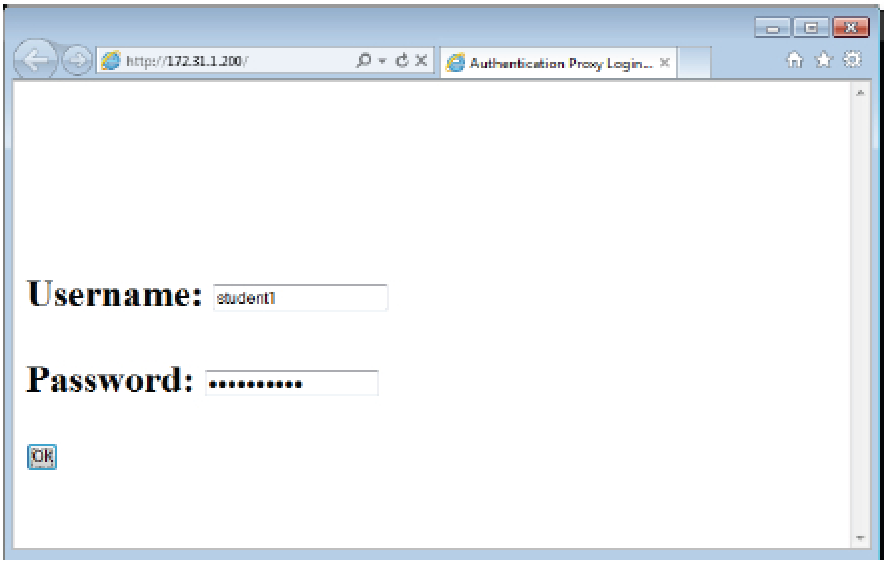
// Check the status on the switch. Now we should see authentication success on DATA domain.

```
SW1#sh auth sess int g0/7
            Interface:  GigabitEthernet0/7
          MAC Address:  0026.55d0.0d56
           IP Address:  10.1.10.104
            User-Name:  002655d00d56
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
           Vlan Group:  N/A
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A010A07000000620AD3DF00
      Acct Session ID:  0x00000074
               Handle:  0xAB000062

Runnable methods list:
       Method   State
       dot1x    Failed over
       mab      Failed over
       webauth  Authc Success

----------------------------------------
```

```
             Interface:  GigabitEthernet0/7
           MAC Address:  0021.a084.6ff4
            IP Address:  Unknown
             User-Name:  00-21-A0-84-6F-F4
                Status:  Authz Success
                Domain:  VOICE
       Security Policy:  Should Secure
       Security Status:  Unsecure
        Oper host mode:  multi-domain
      Oper control dir:  both
         Authorized By:  Authentication Server
               ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-4f57e406
       Session timeout:  N/A
          Idle timeout:  N/A
     Common Session ID:  0A010A070000002F00ED9839
       Acct Session ID:  0x00000034
                Handle:  0x3500002F

Runnable methods list:
       Method   State
       dot1x    Failed over
       mab      Authc Success
       webauth  Not run

       // There is pre-auth ACL applied to the port.

SW1#sh ip access-lists interface g0/7
     permit udp host 10.1.10.104 any eq bootps
     permit udp host 10.1.10.104 any eq domain
```

Now go to Win7 PC and open up web browser. Enter some IP address and hit enter.

- You should get a special webpage asking for authentication. Provide user credentials of student1/Micronics1 and click **OK**.

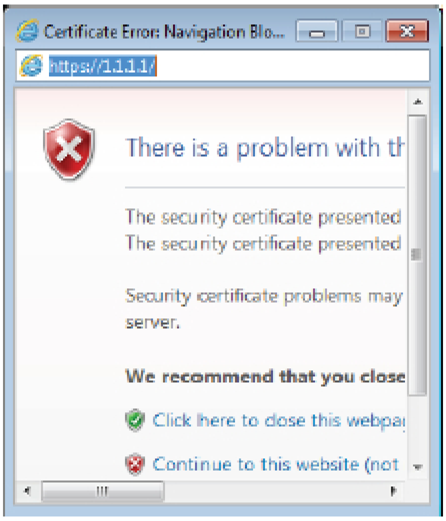


Username: student1

Password: ••••••••••

OK

- A pop-up window appears with certificate warning. Accept the connection.



Certificate Error: Navigation Blo...

https://1.1.1.1/

There is a problem with th

The security certificate presented
The security certificate presented

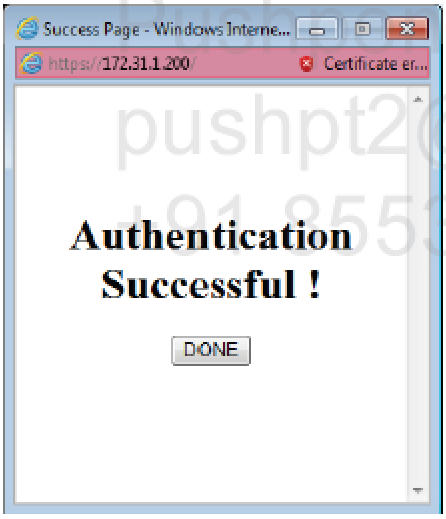
Security certificate problems may
server.

We recommend that you close

Click here to close this webpa

Continue to this website (not

- You should be successfully authenticated.

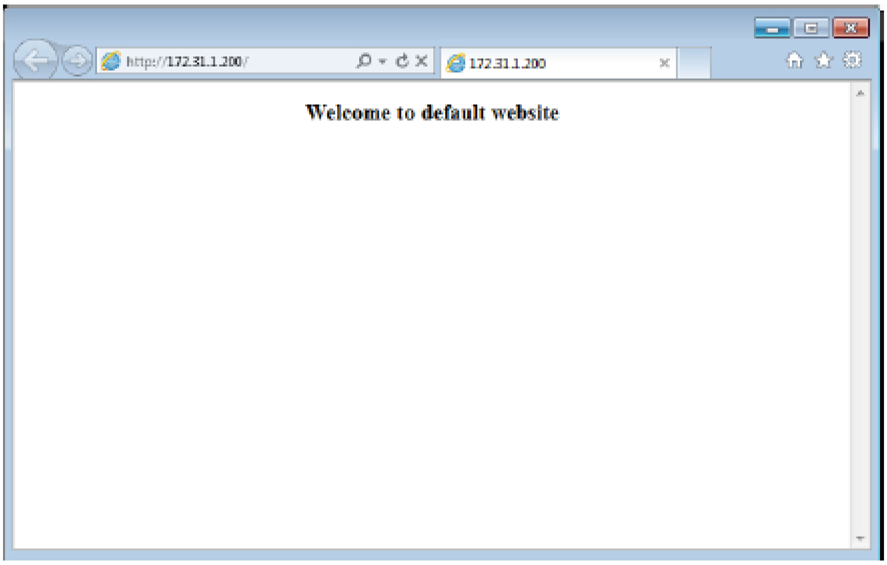


Success Page - Windows Interne...

https://172.31.1.200/ Certificate er...

Authentication Successful !

- Now you can access the web page.



Welcome to default website

Check logs on the switch.

```
RADIUS/ENCODE(00000075):Orig. component type = AUTH_PROXY
RADIUS(00000075): Config NAS IP: 10.1.10.7
RADIUS/ENCODE(00000075): acct_session_id: 117
RADIUS(00000075): sending

       // RADIUS request is sent to the ISE for username 'student1'

RADIUS(00000075): Send Access-Request to 172.31.1.20:1812 id 1645/237, len 165
RADIUS:  authenticator D6 23 03 51 BF E7 68 D2 - D7 DD A1 2A 8D F2 99 76
RADIUS:  User-Name           [1]   10  "student1"
RADIUS:  User-Password       [2]   18  *
RADIUS:  Framed-IP-Address   [8]   6   10.1.10.104
RADIUS:  Service-Type        [6]   6   Outbound                  [5]
RADIUS:  Message-Authenticato[80]  18
RADIUS:   36 AF D0 76 A0 2E 0C D0 28 3C EC A6 7C 6B BF 92           [ 6v.(<|k]
RADIUS:  Vendor, Cisco       [26]  49
RADIUS:   Cisco AVpair       [1]   43  "audit-session-id=0A010A0700000062 0AD3DF00"
RADIUS:  NAS-Port-Type       [61]  6   Ethernet                  [15]
RADIUS:  NAS-Port            [5]   6   50007
RADIUS:  NAS-Port-Id         [87]  20  "GigabitEthernet0/7"
RADIUS:  NAS-IP-Address      [4]   6   10.1.10.7
RADIUS(00000075): Started 5 sec timeout

       // ISE authenticates and authorizes the user because of modified default
       authentication rule (now the user can be search in two identity stores) and new
       authorization rule for Students_WebAuth.

RADIUS: Received from id 1645/237 172.31.1.20:1812, Access-Accept, len 188
RADIUS:  authenticator 8E AB 6C 50 EF F1 7F 9F - C8 12 87 CA D7 C3 C3 F1
RADIUS:  User-Name           [1]   10  "student1"
RADIUS:  Filter-Id           [11]  25
```

```
RADIUS:   41 43 4C 5F 57 45 42 41 55 54 48 5F 53 54 55 44  [ACL_WEBAUTH_STUD]
RADIUS:   45 4E 54 53 2E 69 6E            [ ENTS.in]
RADIUS:  State               [24]  40
RADIUS:   52 65 61 75 74 68 53 65 73 73 69 6F 6E 3A 30 41  [ReauthSession:0A]
RADIUS:   30 31 30 41 30 37 30 30 30 30 30 30 36 32 30 41  [010A07000000620A]
RADIUS:   44 33 44 46 30 30            [ D3DF00]
RADIUS:  Class               [25]  50
RADIUS:   43 41 43 53 3A 30 41 30 31 30 41 30 37 30 30 30  [CACS:0A010A07000]
RADIUS:   30 30 30 36 32 30 41 44 33 44 46 30 30 3A 49 53  [000620AD3DF00:IS]
RADIUS:   45 2F 31 34 33 35 35 38 35 35 33 2F 33 32 34 36  [ E/143558553/3246]
RADIUS:  Termination-Action  [29]  6   1
RADIUS:  Message-Authenticato[80]  18
RADIUS:   4F F4 1A 7C 9E EB C4 DF 48 FD 1C 4D E4 C4 63 C3            [ O|HMc]
RADIUS:  Vendor, Cisco       [26]  19
RADIUS:   Cisco AVpair       [1]   13  "priv-lvl=15"
RADIUS(00000075): Received from id 1645/237
```

```
       // EPM is changing ACL on port. Now the ACL sent from the ISE is applied.
```

```
%EPM-6-POLICY_REQ: IP 10.1.10.104| MAC 0026.55d0.0d56| AuditSessionID
0A010A07000000620AD3DF00| AUTHTYPE AUTHPROXY| EVENT APPLY
%EPM-6-POLICY_APP_SUCCESS: IP 10.1.10.104| MAC 0026.55d0.0d56| AuditSessionID
0A010A07000000620AD3DF00| AUTHTYPE AUTHPROXY| POLICY_TYPE Named ACL| POLICY_NAME
ACL_WEBAUTH_STUDENTS| RESULT SUCCESS
```

```
SW1#sh ip access-lists interface g0/7
     permit tcp host 10.1.10.104 host 172.31.1.200 eq www
     permit icmp host 10.1.10.104 any
     permit tcp host 10.1.10.104 any eq 3389
     permit udp host 10.1.10.104 host 172.31.1.200 eq domain
```

```
SW1#sh auth sess int g0/7
            Interface:  GigabitEthernet0/7
          MAC Address:  0026.55d0.0d56
           IP Address:  10.1.10.104
            User-Name:  002655d00d56
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
           Vlan Group:  N/A
            Filter-Id:  ACL_WEBAUTH_STUDENTS
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A010A07000000620AD3DF00
      Acct Session ID:  0x00000074
```

```
               Handle:  0xAB000062

Runnable methods list:
       Method   State
       dot1x    Failed over
       mab      Failed over
       webauth  Authc Success

----------------------------------------
            Interface:  GigabitEthernet0/7
          MAC Address:  0021.a084.6ff4
           IP Address:  Unknown
            User-Name:  00-21-A0-84-6F-F4
               Status:  Authz Success
               Domain:  VOICE
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
              ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-4f57e406
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A010A070000002F00ED9839
      Acct Session ID:  0x00000034
               Handle:  0x3500002F

Runnable methods list:
       Method   State
       dot1x    Failed over
       mab      Authc Success
       webauth  Not run
```

LAB 3.13. Central Web Authentication (CWA) for Wired

Objectives

This lab shows how to configure Centralized WebAuth on.

IP Addressing and devices

Device	Interface	IP address
ISE	NIC	172.31.1.20
R1	Lo0 E0/0 E0/1	1.1.1.1/32 10.1.10.1/24 172.31.1.1/24
AD	NIC	172.31.1.200
WinXP	NIC	10.1.10.50/24
WLC	G0/0/1 (mgmt.) G0/0/2	10.1.10.5/24 10.1.30.5/24
ASA1	G0/0 (outside) G0/1 (inside) G0/2 (dmz)	100.2.2.10/24 10.1.10.10/24 10.1.30.10/24
Win7 PC	LAN NIC (LAB-Network) WLAN NIC	DHCP-Assigned 10.1.30.x (DHCP)

Task

Reconfigure switch so that it uses ISE to perform Central WebAuth. All users without supplicant must be authenticated using WebAuth as a last resort method. Configure ISE so that users from AD group micronics.local/Users/employees get full access to the network after authenticating through the website.
Use 802.1x low impact mode on the port and allow only DHCP, DNS, TFTP and ICMP traffic without authentication.

Configuration

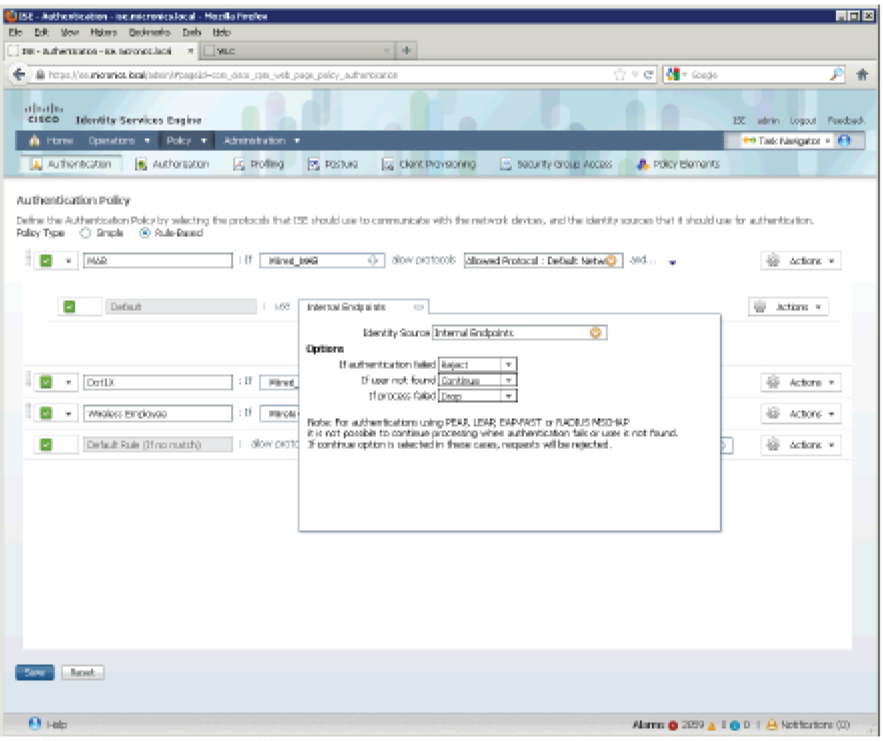
Complete these steps:

Step 1 Switch configuration.

```
!
no aaa authentication login default group radius
no aaa authorization auth-proxy default group radius
!
ip access-list extended DEFAULT
 remark DHCP
 permit udp any eq bootpc any eq bootps
 remark DNS
 permit udp any any eq domain
 remark TFTP
 permit udp any any eq tftp
 remark Ping
 permit icmp any any
!
interface GigabitEthernet0/7
 no authentication fallback WEBAUTH_PROFILE
 ip access-group DEFAULT in
 authentication order dot1x mab
 authentication event fail action next-method
!
ip access-list extended ACL_REDIRECT
 deny udp any any eq domain
 deny tcp any host 172.31.1.20 eq 8443
 permit ip any any
!
```

Step 2 ISE configuration. Change authentication rule for MAB.

- Go to **Policy > Authentication** and click black arrow for MAB rule to see more options. Click on orange arrow to see Identity Source (which should be Internal Endpoints) and change advanced option '**If user not found'** to **Continue**. Click **Save**.



Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

Policy Type ○ Simple ● Rule-Based

MAB : If Wired_MAB allow protocols Allowed Protocol : Default Netw and ...

Default : use Internal Endpoints

Identity Source Internal Endpoints

Options

If authentication failed Reject

If user not found Continue

If process failed Drop

Note: For authentications using PEAP, LEAP, EAP-FAST or RADIUS MSCHAP it is not possible to continue processing when authentication fails or user is not found. If continue option is selected in these cases, requests will be rejected.

Dot1X : If Wired_

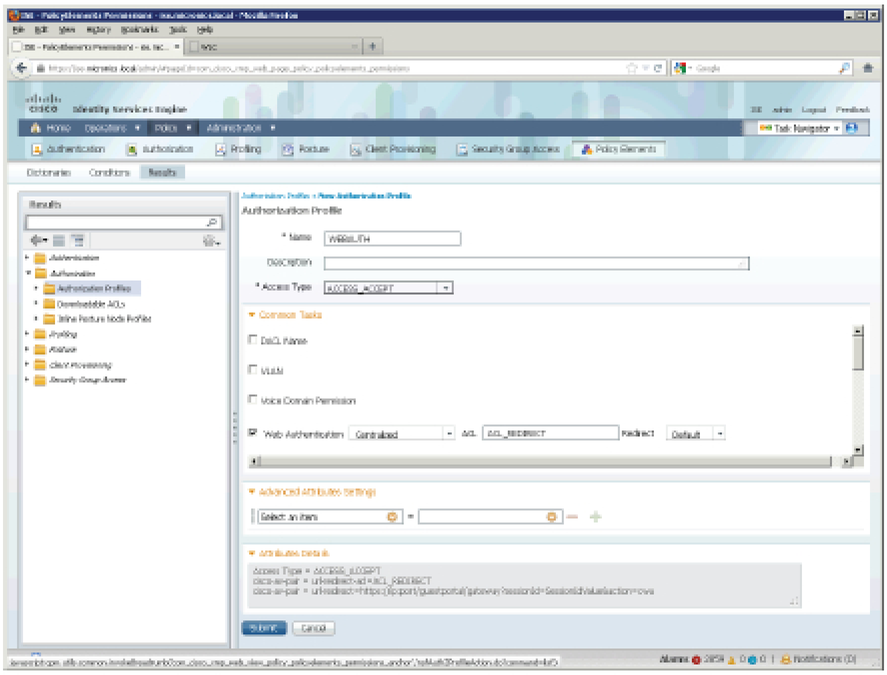
Wireless Employee : If Wirele

Default Rule (If no match) : allow proto

ISE - Authentication - ise.micronics.local - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Identity Services Engine
ISE admin Logout Feedback
Home Operations Policy Administration
Task Navigator
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements
Actions
Save Reset
Help
Alarms 2059 1 0 Notifications (0)

Step 3 Create authorization profile and reconfigure default authorization rule.

- Go to **Policy > Policy Elements > Results > Authorization > Authorization Profiles** and click **Add**. Enter a name for new profile e.g. **WEBAUTH** and select **Web Authentication** option. Additional options should show up. Provide ACL name for redirection e.g. **ACL_REDIRECT** (this ACL must be configured on the switch). Click **Submit**.



Authorization Profile

* Name: WEBAUTH

Description:

* Access Type: ACCESS_ACCEPT

Common Tasks

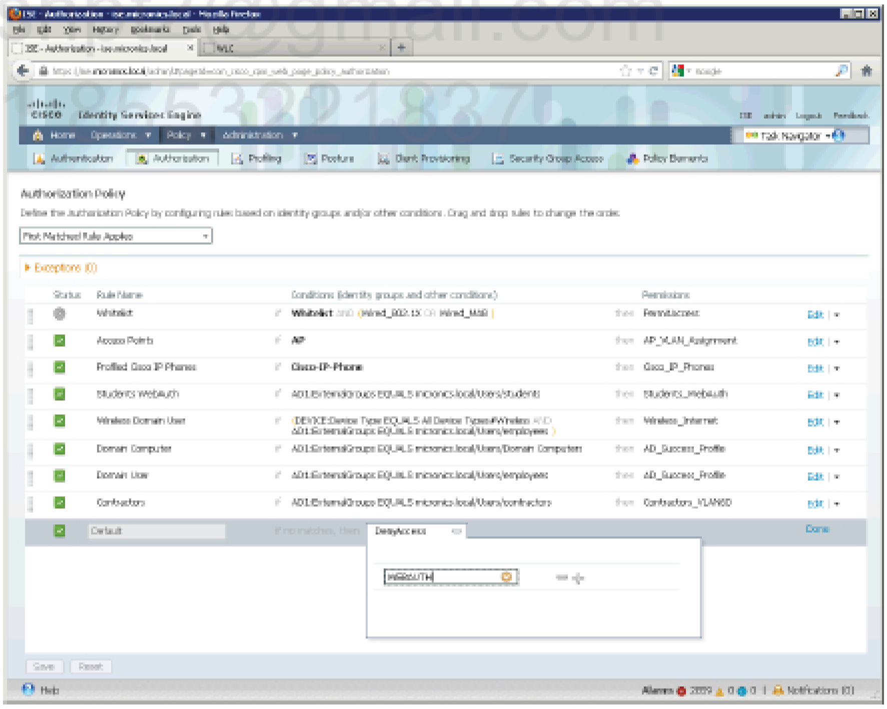
- ☐ DACL Name
- ☐ VLAN
- ☐ Voice Domain Permission
- ☑ Web Authentication: Centralized, ACL: ACL_REDIRECT, Redirect: Default

Advanced Attributes Settings

Attributes Details

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect-acl=ACL_REDIRECT
cisco-av-pair = url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=cwa
```

- Go to **Policy > Authorization** and change **Default** rule to use **WEBAUTH** authorization profile. Click **Done** and **Save**.



Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

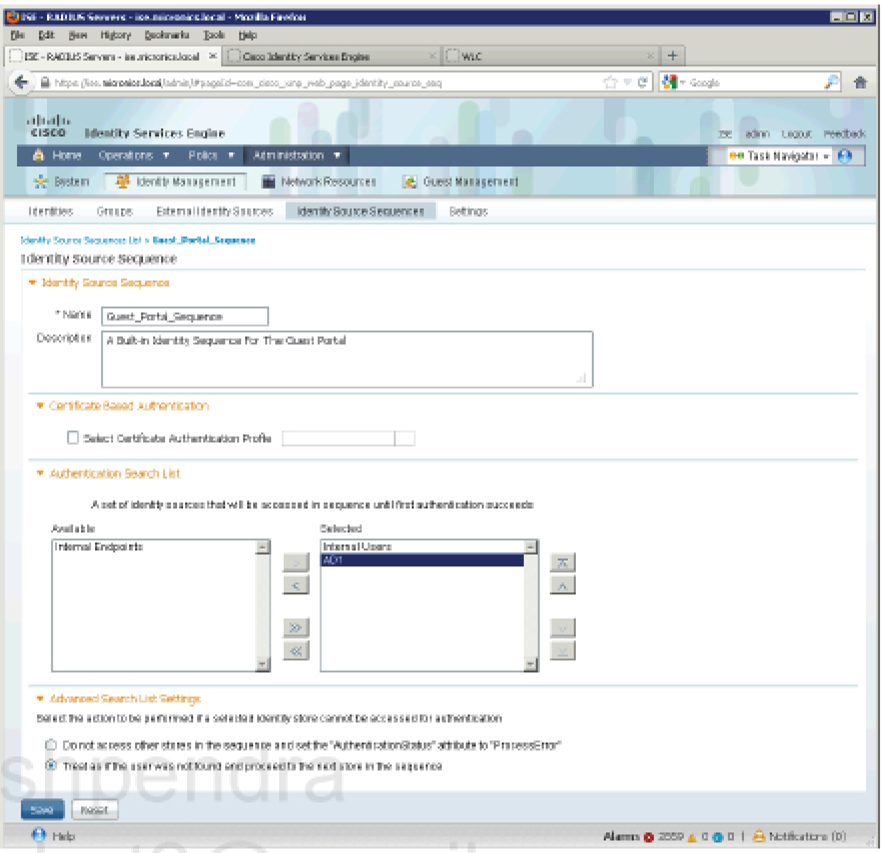
First Matched Rule Applies

Exceptions (0)

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
○	Whitelist	Whitelist AND (Wired_802.1X OR Wired_MAB)	then PermitAccess
☑	Access Points	AP	then AP_VLAN_Assignment
☑	Profiled Cisco IP Phones	Cisco-IP-Phone	then Cisco_IP_Phones
☑	Students WebAuth	AD1:ExternalGroups EQUALS micronics.local/Users/students	then Students_WebAuth
☑	Wireless Domain User	(DEVICE:Device Type EQUALS All Device Types#Wireless AND AD1:ExternalGroups EQUALS micronics.local/Users/employees)	then Wireless_Internet
☑	Domain Computer	AD1:ExternalGroups EQUALS micronics.local/Users/Domain Computers	then AD_Success_Profile
☑	Domain User	AD1:ExternalGroups EQUALS micronics.local/Users/employees	then AD_Success_Profile
☑	Contractors	AD1:ExternalGroups EQUALS micronics.local/Users/contractors	then Contractors_VLAN60
☑	Default	If no matches, then DenyAccess	WEBAUTH

Step 4 Configure ISE Guest portal to authenticate users against AD store.

- Go to **Administration > Identity Management >Identity Source Sequences** and click on **Guest_Portal_Sequence** on the list. For **Authentication Search List** move **AD1** to the right pane. Click **Save**.


ISE - RADIUS Servers - ise.micronics.local - Mozilla Firefox
File Edit View History Bookmarks Tools Help
ISE - RADIUS Servers - ise.micronics.local
Cisco Identity Services Engine
WLC
Identity Services Engine
ise admin Logout Feedback
Home Operations ▼ Policy ▼ Administration ▼
Task Navigator
System Identity Management Network Resources Guest Management
Identities Groups External Identity Sources Identity Source Sequences Settings
Identity Source Sequence List > Guest_Portal_Sequence
Save Reset
Help
Alarms 2559 0 0 | Notifications (0)

Identity Source Sequence

▼ Identity Source Sequence

* Name: Guest_Portal_Sequence

Description: A Built-in Identity Sequence For The Guest Portal

▼ Certificate Based Authentication

□ Select Certificate Authentication Profile

▼ Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available: Internal Endpoints

Selected: Internal Users, AD1

▼ Advanced Search List Settings

Select the action to be performed if a selected identity store cannot be accessed for authentication

○ Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"

● Treat as if the user was not found and proceed to the next store in the sequence

Verification

Enable debugging on the switch:

```
debug radius
debug dot1x events
```

Check settings on the switch.

```
SW1#sh auth sess int g0/7
           Interface:  GigabitEthernet0/7
         MAC Address:  0026.55d0.0d56
          IP Address:  10.1.10.104
              Status:  Running
              Domain:  UNKNOWN
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  multi-domain
    Oper control dir:  both
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A010A070000000770C26EF3D
     Acct Session ID:  0x0000008B
```

```
              Handle:  0x04000077

Runnable methods list:
       Method   State
       dot1x    Running
       mab      Not run

----------------------------------------
           Interface:  GigabitEthernet0/7
         MAC Address:  0021.a084.6ff4
          IP Address:  Unknown
           User-Name:  00-21-A0-84-6F-F4
              Status:  Authz Success
              Domain:  VOICE
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  multi-domain
    Oper control dir:  both
       Authorized By:  Authentication Server
             ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-4f57e406
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A010A070000002F00ED9839
     Acct Session ID:  0x00000034
              Handle:  0x3500002F

Runnable methods list:
       Method   State
       dot1x    Failed over
       mab      Authc Success
```

Enable LAB-Network connection on the Win7 PC. Check out switch logs.

```
       // Dot1x is starting and it times out after two retries.

%AUTHMGR-5-START: Starting 'dot1x' for client (0026.55d0.0d56) on Interface Gi0/7
AuditSessionID 0A010A07000000770C26EF3D
dot1x-ev(Gi0/7): Sending EAPOL packet to 0026.55d0.0d56
dot1x-ev(Gi0/7): Role determination not required
dot1x-ev(Gi0/7): Sending out EAPOL packet

dot1x-ev(Gi0/7): Sending EAPOL packet to 0026.55d0.0d56
dot1x-ev(Gi0/7): Role determination not required
dot1x-ev(Gi0/7): Sending out EAPOL packet

dot1x-ev(Gi0/7): Sending EAPOL packet to 0026.55d0.0d56
dot1x-ev(Gi0/7): Role determination not required
dot1x-ev(Gi0/7): Sending out EAPOL packet
```

```
dot1x-ev(Gi0/7): Received an EAP Timeout
%DOT1X-5-FAIL: Authentication failed for client (0026.55d0.0d56) on Interface Gi0/7
AuditSessionID
dot1x-ev(Gi0/7): Sending event (2) to Auth Mgr for 0026.55d0.0d56
%AUTHMGR-7-RESULT: Authentication result 'no-response' from 'dot1x' for client
(0026.55d0.0d56) on Interface Gi0/7 AuditSessionID 0A010A07000000770C26EF3D
dot1x-ev(Gi0/7): Received Authz fail for the client  0x770000FE (0026.55d0.0d56)
dot1x-ev(Gi0/7): Deleting client 0x770000FE (0026.55d0.0d56)

       // MAB is starting. RADIUS request is sent for MAC authentication.

%AUTHMGR-7-FAILOVER: Failing over from 'dot1x' for client (0026.55d0.0d56) on Interface
Gi0/7 AuditSessionID 0A010A07000000770C26EF3D
%AUTHMGR-5-START: Starting 'mab' for client (0026.55d0.0d56) on Interface Gi0/7
AuditSessionID 0A010A07000000770C26EF3D
dot1x-ev:Delete auth client (0x770000FE) message
dot1x-ev:Auth client ctx destroyed
dot1x-ev:Aborted posting message to authenticator state machine: Invalid client
RADIUS/ENCODE(0000008B):Orig. component type = DOT1X
RADIUS(0000008B): Config NAS IP: 10.1.10.7
RADIUS/ENCODE(0000008B): acct_session_id: 139
RADIUS(0000008B): sending
RADIUS(0000008B): Send Access-Request to 172.31.1.20:1812 id 1645/253, len 215
RADIUS:  authenticator 36 78 97 9D 8D 27 8B F8 - 8A C6 19 64 44 70 71 06
RADIUS:  User-Name           [1]   14  "002655d00d56"
RADIUS:  User-Password       [2]   18  *
RADIUS:  Service-Type        [6]   6   Call Check                [10]
RADIUS:  Framed-IP-Address   [8]   6   10.1.10.104
RADIUS:  Framed-MTU          [12]  6   1500
RADIUS:  Called-Station-Id   [30]  19  "C4-64-13-6C-E8-07"
RADIUS:  Calling-Station-Id  [31]  19  "00-26-55-D0-0D-56"
RADIUS:  Message-Authenticato[80]  18
RADIUS:   8F 5F BA 6F 62 03 22 17 CA A9 54 EC 55 91 E3 98           [ _ob"TU]
RADIUS:  EAP-Key-Name        [102] 2   *
RADIUS:  Vendor, Cisco       [26]  49
RADIUS:   Cisco AVpair       [1]   43  "audit-session-id=0A010A07000000770C26EF3D"
RADIUS:  NAS-Port-Type       [61]  6   Ethernet                  [15]
RADIUS:  NAS-Port            [5]   6   50007
RADIUS:  NAS-Port-Id         [87]  20  "GigabitEthernet0/7"
RADIUS:  NAS-IP-Address      [4]   6   10.1.10.7
RADIUS(0000008B): Started 5 sec timeout

       // RADIUS Access-Accept is received. This is because of advanced options in MAB
       rule on ISE. If user not found = Continue. The ideai behind that is to get
       Access-Accept message back and some attributes specified in authorization rule.
       Since we do not have any specific authorization rule for MAC address of our
       Win7PC the session is matched agains the default WEBAUTH rule. This
       authorization profile is configured to send Redirect URL and Redirect ACL name
       down to the switch.
```

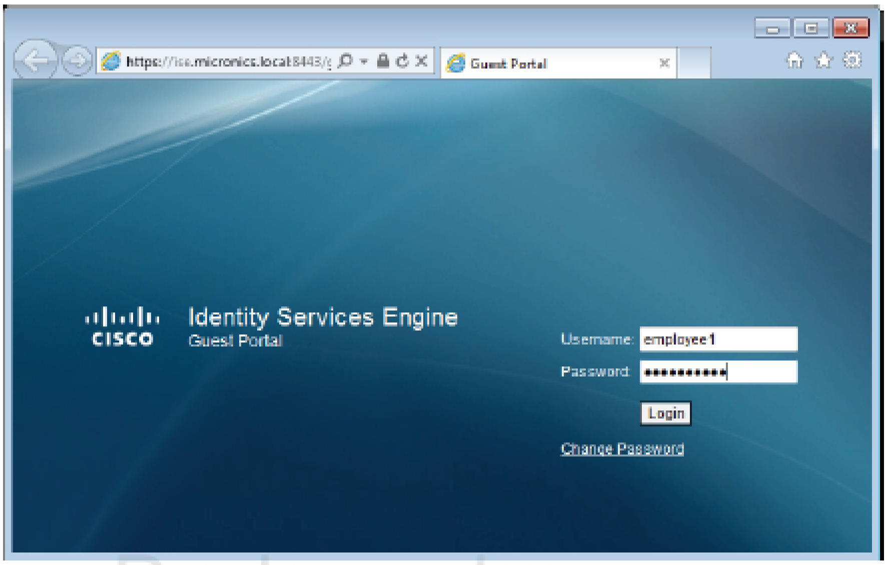
```
RADIUS: Received from id 1645/253 172.31.1.20:1812, Access-Accept, len 309
RADIUS:  authenticator 02 05 36 2F 9C C0 A2 52 - AC ED 56 B1 B0 F8 FE C3
RADIUS:  User-Name           [1]   19  "00-26-55-D0-0D-56"
RADIUS:  State               [24]  4
RADIUS:   52 65 61 75 74 68 53 65 73 73 69 6F 6E 3A 30 41  [ReauthSession:0A]
RADIUS:   30 31 30 41 30 37 30 30 30 30 30 30 37 37 30 43  [010A07000000770C]
RADIUS:   32 36 45 46 33 44            [ 26EF3D]
RADIUS:  Class               [25]  50
RADIUS:   43 41 43 53 3A 30 41 30 31 30 41 30 37 30 30 30  [CACS:0A010A07000]
RADIUS:   30 30 30 37 37 30 43 32 36 45 46 33 44 3A 49 53  [000770C26EF3D:IS]
RADIUS:   45 2F 31 34 33 35 35 38 35 35 33 2F 33 32 38 33  [ E/143558553/3283]
RADIUS:  Termination-Action  [29]  6   1
RADIUS:  Message-Authenticato[80]  18
RADIUS:   FC FB 13 D6 A1 82 84 9E 14 D6 B4 DC 54 A4 B5 0E                 [ T]
RADIUS:  Vendor, Cisco       [26]  37
RADIUS:   Cisco AVpair       [1]   31  "url-redirect-acl=ACL_REDIRECT"
RADIUS:  Vendor, Cisco       [26]  119
RADIUS:   Cisco AVpair       [1]   113 "url-
redirect=https://ise.micronics.local:8443/guestportal/gateway?sessionId=0A010A070000007
70C26EF3D&action=cwa"
RADIUS(0000008B): Received from id 1645/253

%MAB-5-SUCCESS: Authentication successful for client (0026.55d0.0d56) on Interface
Gi0/7 AuditSessionID 0A010A07000000770C26EF3D
%AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client
(0026.55d0.0d56) on Interface Gi0/7 AuditSessionID 0A010A07000000770C26EF3D
%EPM-6-POLICY_REQ: IP 0.0.0.0| MAC 0026.55d0.0d56| AuditSessionID
0A010A07000000770C26EF3D| AUTHTYPE DOT1X| EVENT APPLY
%EPM-6-POLICY_APP_SUCCESS: IP 10.1.10.104| MAC 0026.55d0.0d56| AuditSessionID
0A010A07000000770C26EF3D| AUTHTYPE DOT1X| POLICY_TYPE Named ACL| POLICY_NAME EPM-HOLE-
ACL| RESULT SUCCESS

       // EPM is applying Redirect URL to the port.

%EPM-6-POLICY_APP_SUCCESS: IP 10.1.10.104| MAC 0026.55d0.0d56| AuditSessionID
0A010A07000000770C26EF3D| AUTHTYPE DOT1X| POLICY_TYPE URL Redirect| POLICY_NAME
https://ise.micronics.local:8443/guestportal/gateway?sessionId=0A010A07000000770C26EF3D
&action=cwa| RESULT SUCCESS
%EPM-6-POLICY_APP_SUCCESS: IP 10.1.10.104| MAC 0026.55d0.0d56| AuditSessionID
0A010A07000000770C26EF3D| AUTHTYPE DOT1X| POLICY_TYPE URL Match ACL| POLICY_NAME
ACL_REDIRECT| RESULT SUCCESS
%AUTHMGR-5-SUCCESS: Authorization succeeded for client
(0026.55d0.0d56) on Interface Gi0/7 AuditSessionID 0A010A07000000770C26EF3D
```

Check commands on the switch.

```
SW1#sh auth sess int g0/7
            Interface:  GigabitEthernet0/7
          MAC Address:  0026.55d0.0d56
           IP Address:  10.1.10.104
            User-Name:  00-26-55-D0-0D-56
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
           Vlan Group:  N/A
     URL Redirect ACL:  ACL_REDIRECT
         URL Redirect:
https://ise.micronics.local:8443/guestportal/gateway?sessionId=0A010A07000000770C26EF3D
&action=cwa
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A010A07000000770C26EF3D
      Acct Session ID:  0x0000008B
               Handle:  0x04000077

Runnable methods list:
       Method   State
       dot1x    Failed over
       mab      Authc Success

----------------------------------------
            Interface:  GigabitEthernet0/7
          MAC Address:  0021.a084.6ff4
           IP Address:  Unknown
            User-Name:  00-21-A0-84-6F-F4
               Status:  Authz Success
               Domain:  VOICE
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
              ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-4f57e406
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A010A070000002F00ED9839
      Acct Session ID:  0x00000034
               Handle:  0x3500002F

Runnable methods list:
       Method   State
       dot1x    Failed over
       mab      Authc Success
```

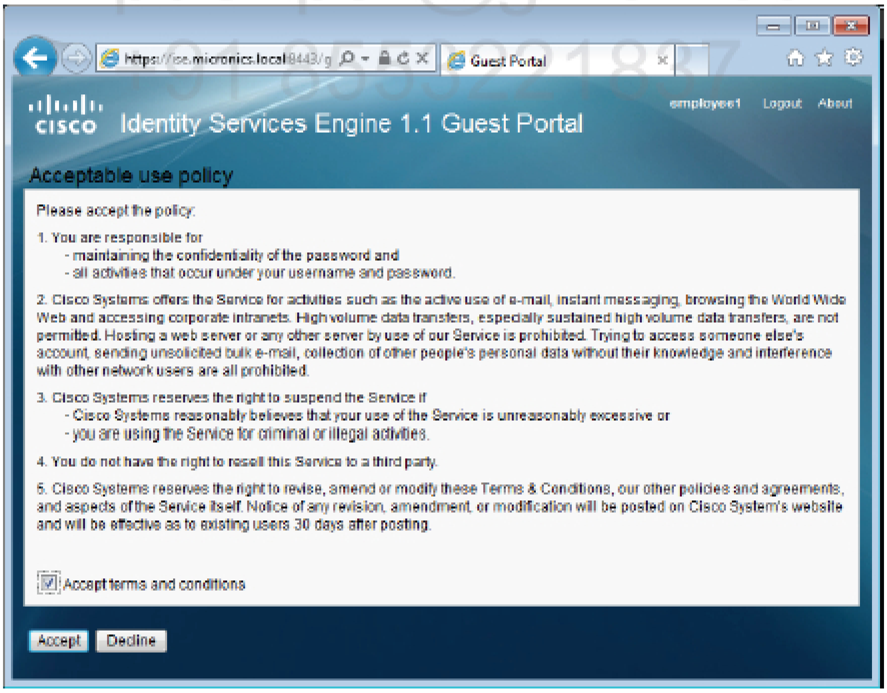
Now go to Win7 PC and open up web browser. Enter some IP address and hit enter.

- You should be redirected to ISE Guest Portal. Provide user credentials of employee1/Micronics1 and click **OK**.



Username: employee1
Password: ••••••••••

- After successful authentication you should be asked to read and accept default AUC (Acceptable Use Policy). Pick the checkbox and click **Accept**.


https://ise.micronics.local:8443/g
Guest Portal
Identity Services Engine 1.1 Guest Portal
employee1
Logout
About
Accept
Decline

Acceptable use policy

Please accept the policy:

1. You are responsible for
   - maintaining the confidentiality of the password and
   - all activities that occur under your username and password.

2. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited.

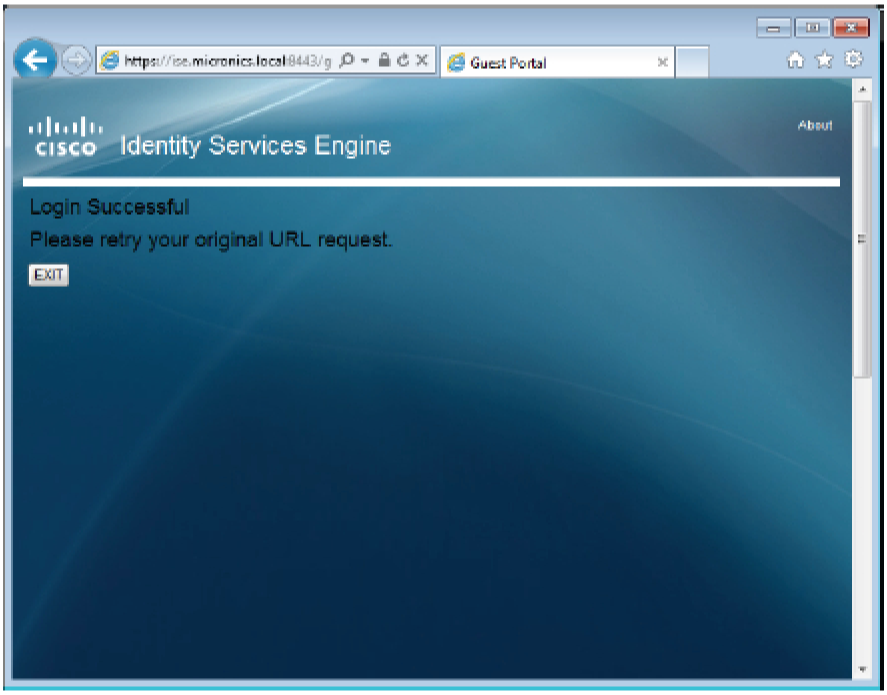
3. Cisco Systems reserves the right to suspend the Service if
   - Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or
   - you are using the Service for criminal or illegal activities.

4. You do not have the right to resell this Service to a third party.

5. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or modification will be posted on Cisco System's website and will be effective as to existing users 30 days after posting.

☑ Accept terms and conditions

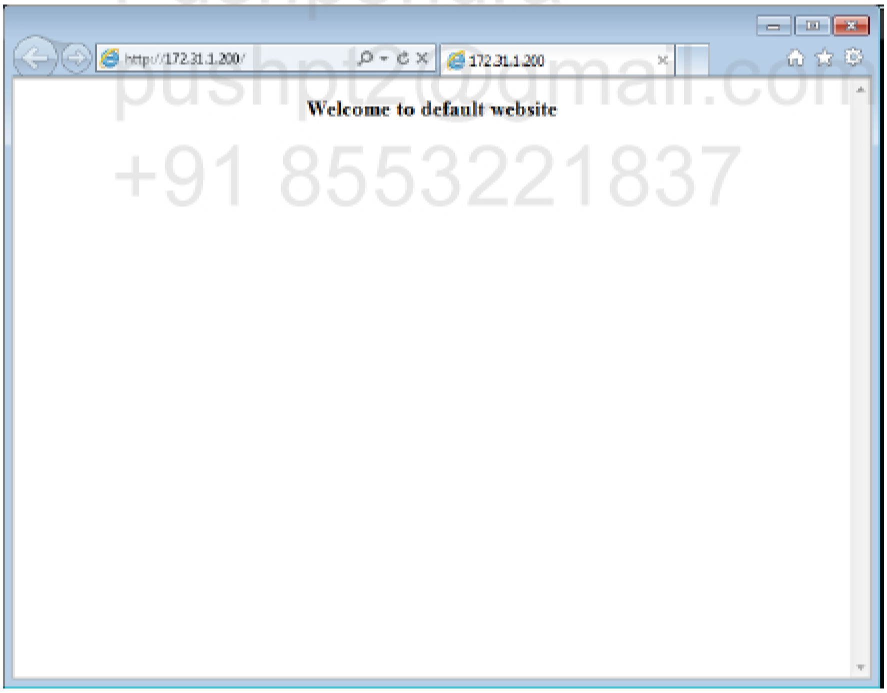
- You should get **Login Successful** message.



Login Successful

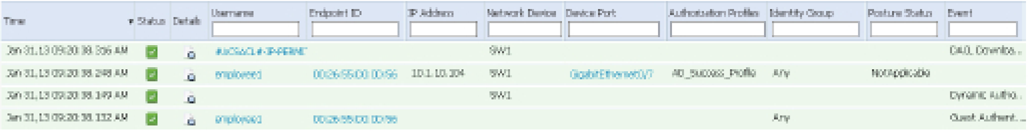
Please retry your original URL request.

- Now you can resend your original request to the website.



Welcome to default website

Check ISE log messages.



Time	Status	Details	Username	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Identity Group	Posture Status	Event
Jan 31,13 09:20:38.336 AM	✓		#ACSACL#-IP-PERMIT			SW1					DACL Downloa...
Jan 31,13 09:20:38.248 AM	✓		employee1	00:26:55:D0:D0:56	10.1.10.204	SW1	GigabitEthernet0/7	AD_Success_Profile	Any	NotApplicable	
Jan 31,13 09:20:38.149 AM	✓					SW1					Dynamic Autho...
Jan 31,13 09:20:38.132 AM	✓		employee1	00:26:55:D0:D0:56					Any		Guest Authent...

Check switch logs from user authentication.

```
        // RADIUS CoA message should be received to trigger the switch to re-
        authenticate the session. That's why it is so important to have CoA enabled on
        the switch.

RADIUS: COA  received from id 1 172.31.1.20:27981, CoA Request, len 183
RADIUS/DECODE: parse unknown cisco vsa "reauthenticate-type" - IGNORE
RADIUS/ENCODE(00000000):Orig. component type = INVALID
RADIUS(00000000): sending
RADIUS(00000000): Send CoA Ack Response to 172.31.1.20:27981 id 1, len 20
RADIUS:  authenticator 3B 48 8D 65 E4 2B 36 BA - 33 7B 54 B0 46 AD 0C E4
RADIUS/ENCODE(0000008B):Orig. component type = DOT1X
RADIUS(0000008B): Config NAS IP: 10.1.10.7
RADIUS/ENCODE(0000008B): acct_session_id: 139
RADIUS(0000008B): sending

        // dot1x reauthentication is sending another RADIUS request to the ISE. Notice
        that the switch has no idea of username, so it uses MAC address of the client
        and Session-ID to identify the session on the ISE.

RADIUS(0000008B): Send Access-Request to 172.31.1.20:1812 id 1645/254, len 253
RADIUS:  authenticator 1A D3 BA C8 CC 83 9B 00 - E5 3E 4B 8B D0 EF 8E 08
RADIUS:  User-Name           [1]   14  "002655d00d56"
RADIUS:  User-Password       [2]   18  *
RADIUS:  Service-Type        [6]   6   Call Check                [10]
RADIUS:  Framed-IP-Address   [8]   6   10.1.10.104
RADIUS:  Framed-MTU          [12]  6   1500
RADIUS:  Called-Station-Id   [30]  19  "C4-64-13-6C-E8-07"
RADIUS:  Calling-Station-Id  [31]  19  "00-26-55-D0-0D-56"
RADIUS:  Message-Authenticato[80]  18
RADIUS:   0F 27 F3 FE 92 4F E1 95 B9 AE E6 FC 5D 65 0C 8B              [ 'O]e]
RADIUS:  EAP-Key-Name        [102] 2   *
RADIUS:  Vendor, Cisco       [26]  49
RADIUS:   Cisco AVpair       [1]   43  "audit-session-id=0A010A07000000770C26EF3D"
RADIUS:  NAS-Port-Type       [61]  6   Ethernet                  [15]
RADIUS:  NAS-Port            [5]   6   50007
RADIUS:  NAS-Port-Id         [87]  20  "GigabitEthernet0/7"
RADIUS:  Called-Station-Id   [30]  19  "C4-64-13-6C-E8-07"
RADIUS:  Calling-Station-Id  [31]  19  "00-26-55-D0-0D-56"
RADIUS:  NAS-IP-Address      [4]   6   10.1.10.7
RADIUS(0000008B): Started 5 sec timeout

        // RADIUS Access-Accept is having correct username now and provides additionall
        attributes for that user such as dACL.

RADIUS: Received from id 1645/254 172.31.1.20:1812, Access-Accept, len 220
RADIUS:  authenticator 25 D8 C6 0A 44 BB 54 A6 - CF 26 A9 63 A7 5E 6D CA
RADIUS:  User-Name           [1]   11  "employee1"
RADIUS:  State               [24]  40
RADIUS:   52 65 61 75 74 68 53 65 73 73 69 6F 6E 3A 30 41  [ReauthSession:0A]
```

```
RADIUS:   30 31 30 41 30 37 30 30 30 30 30 30 37 37 30 43  [010A07000000770C]
RADIUS:   32 36 45 46 33 44            [ 26EF3D]
RADIUS:  Class               [25]  50
RADIUS:   43 41 43 53 3A 30 41 30 31 30 41 30 37 30 30 30  [CACS:0A010A07000]
RADIUS:   30 30 30 37 37 30 43 32 36 45 46 33 44 3A 49 53  [000770C26EF3D:IS]
RADIUS:   45 2F 31 34 33 35 35 38 35 35 33 2F 33 32 38 35  [ E/143558553/3285]
RADIUS:  Termination-Action  [29]  6   1
RADIUS:  Message-Authenticato[80]  18
RADIUS:   E4 EE 8B 92 1D 51 C3 4A 9F 35 7F 02 A0 AF E8 97               [ QJ5]
RADIUS:  Vendor, Cisco       [26]  75
RADIUS:   Cisco AVpair       [1]   69  "ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-
PERMIT_ALL_TRAFFIC-4f57e406"
RADIUS(0000008B): Received from id 1645/254

%MAB-5-SUCCESS: Authentication successful for client (0026.55d0.0d56) on Interface
Gi0/7 AuditSessionID 0A010A07000000770C26EF3D
%AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client
(0026.55d0.0d56) on Interface Gi0/7 AuditSessionID 0A010A07000000770C26EF3D
%EPM-6-POLICY_REQ: IP 10.1.10.104| MAC 0026.55d0.0d56| AuditSessionID
0A010A07000000770C26EF3D| AUTHTYPE DOT1X| EVENT APPLY
%EPM-6-AAA: POLICY xACSACLx-IP-PERMIT_ALL_TRAFFIC-4f57e406| EVENT DOWNLOAD-REQUEST
```

// Another RADIUS request message is sent to download the ACL.

```
RADIUS/ENCODE(00000000):Orig. component type = INVALID
RADIUS(00000000): Config NAS IP: 10.1.10.7
RADIUS(00000000): sending
RADIUS(00000000): Send Access-Request to 172.31.1.20:1812 id 1645/255, len 147
RADIUS:  authenticator B2 85 44 71 1C 7B 7D 64 - 2C 85 D0 53 D3 DF 63 57
RADIUS:  NAS-IP-Address      [4]   6   10.1.10.7
RADIUS:  User-Name           [1]   41  "#ACSACL#-IP-PERMIT_ALL_TRAFFIC-4f57e406"
RADIUS:  Vendor, Cisco       [26]  32
RADIUS:   Cisco AVpair       [1]   26  "aaa:service=ip_admission"
RADIUS:  Vendor, Cisco       [26]  30
RADIUS:   Cisco AVpair       [1]   24  "aaa:event=acl-download"
RADIUS:  Message-Authenticato[80]  18
RADIUS:   E7 62 82 14 A3 B7 A2 BB 17 0F 9C B1 9D 6D C4 0C               [ bm]
RADIUS(00000000): Started 5 sec timeout
```

// Here are ACEs.

```
RADIUS: Received from id 1645/255 172.31.1.20:1812, Access-Accept, len 211
RADIUS:  authenticator B2 DD 86 61 D8 52 C0 6F - 8D B3 0B F2 7B 57 1A 1B
RADIUS:  User-Name           [1]   41  "#ACSACL#-IP-PERMIT_ALL_TRAFFIC-4f57e406"
RADIUS:  State               [24]  40
RADIUS:   52 65 61 75 74 68 53 65 73 73 69 6F 6E 3A 61 63  [ReauthSession:ac]
RADIUS:   31 66 30 31 31 34 30 30 30 30 30 42 39 41 35 31  [1f011400000B9A51]
RADIUS:   30 41 33 37 36 36            [ 0A3766]
RADIUS:  Class               [25]  50
RADIUS:   43 41 43 53 3A 61 63 31 66 30 31 31 34 30 30 30  [CACS:ac1f0114000]
RADIUS:   30 30 42 39 41 35 31 30 41 33 37 36 36 3A 49 53  [00B9A510A3766:IS]
```

```
RADIUS:    45 2F 31 34 33 35 35 38 35 35 33 2F 33 32 38 36  [ E/143558553/3286]
RADIUS:  Termination-Action  [29]   6   1
RADIUS:  Message-Authenticato[80]   18
RADIUS:   9E CE 34 A5 C8 AF F5 C0 68 90 A6 37 EA 0A 83 53              [ 4h7S]
RADIUS:  Vendor, Cisco       [26]   36
RADIUS:   Cisco AVpair       [1]    30  "ip:inacl#1=permit ip any any"
RADIUS(00000000): Received from id 1645/255

       // the authorization is successful and EPM applies the dACL to the user.

%EPM-6-AAA: POLICY xACSACLx-IP-PERMIT_ALL_TRAFFIC-4f57e406| EVENT DOWNLOAD-SUCCESS
%EPM-6-POLICY_APP_SUCCESS: IP 10.1.10.104| MAC 0026.55d0.0d56| AuditSessionID
0A010A07000000770C26EF3D| AUTHTYPE DOT1X| POLICY_TYPE Named ACL| POLICY_NAME xACSACLx-
IP-PERMIT_ALL_TRAFFIC-4f57e406| RESULT SUCCESS
%AUTHMGR-5-SUCCESS: Authorization succeeded for client (0026.55d0.0d56) on Interface
Gi0/7 AuditSessionID 0A010A07000000770C26EF3D


SW1#sh authentication sessions interface g0/7
            Interface:  GigabitEthernet0/7
          MAC Address:  0026.55d0.0d56
           IP Address:  10.1.10.104
            User-Name:  employee1
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
           Vlan Group:  N/A
              ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-4f57e406
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A010A07000000770C26EF3D
      Acct Session ID:  0x0000008B
               Handle:  0x04000077

Runnable methods list:
       Method   State
       dot1x    Failed over
       mab      Authc Success

----------------------------------------
            Interface:  GigabitEthernet0/7
          MAC Address:  0021.a084.6ff4
           IP Address:  Unknown
            User-Name:  00-21-A0-84-6F-F4
               Status:  Authz Success
               Domain:  VOICE
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
              ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-4f57e406
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A010A070000002F00ED9839
      Acct Session ID:  0x00000034
               Handle:  0x3500002F

Runnable methods list:
       Method   State
       dot1x    Failed over
       mab      Authc Success
```

LAB 3.14. Central Web Authentication (CWA) for Wireless

Objectives

This lab shows how to configure Centralized WebAuth on wireless controller.

IP Addressing and devices

Device	Interface	IP address
ISE	NIC	172.31.1.20
R1	Lo0	1.1.1.1/32
	E0/0	10.1.10.1/24
	E0/1	172.31.1.1/24
AD	NIC	172.31.1.200
WinXP	NIC	10.1.10.50/24
WLC	G0/0/1 (mgmt.)	10.1.10.5/24
	G0/0/2	10.1.30.5/24
ASA1	G0/0 (outside)	100.2.2.10/24
	G0/1 (inside)	10.1.10.10/24
	G0/2 (dmz)	10.1.30.10/24
Win7 PC	LAN NIC (LAB-Network)	DHCP-Assigned
	WLAN NIC	10.1.30.x (DHCP)

Task

Based on the previous task, configure WLC to perform CWA for all clients without supplicant. Configure Authentication Open on MICRONICS SSID. Allow only DNS and ICMP traffic without authentication. You can alter default MAB authentication rule to work also for Wireless clients. After authentication users from AD employees group should get access to the Internet (all tcp/80).

Configuration

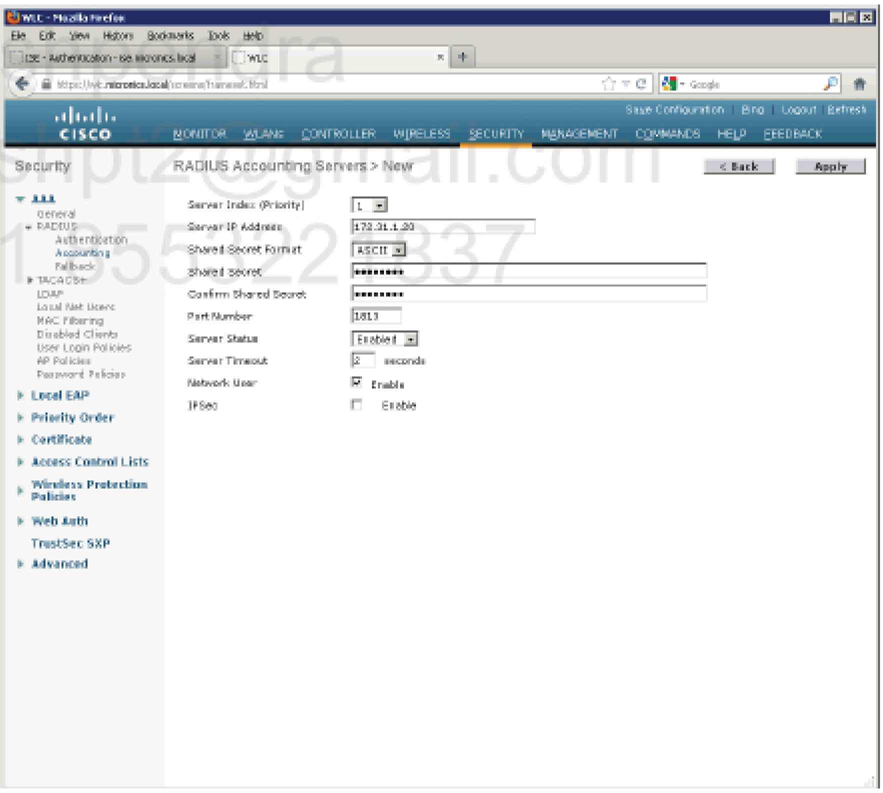
Complete these steps:

Step 1 ASA configuration changes. New required lines are highlighted.

```
!
access-list DMZ_IN permit icmp any any
access-list DMZ_IN permit udp host 10.1.30.5 eq bootps host
172.31.1.200 eq bootps
access-list DMZ_IN permit tcp any any eq www
access-list DMZ_IN permit udp any host 172.31.1.200 eq domain
access-list DMZ_IN permit tcp any host 172.31.1.20 eq 8443
!
```

Step 2 WLC configuration. Make changes to MICRONICS SSID.

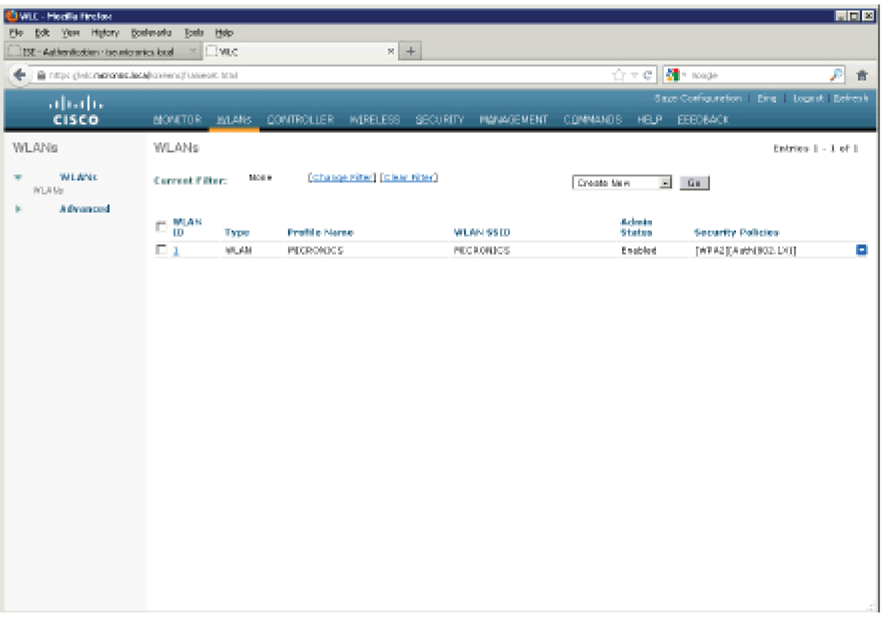
- Go to **SECURITY > AAA > RADIUS > Accounting** and click **New…** Configure ISE as RADIUS Accounting server with 'cisco123' as shared secret. Click **Apply**.


WLC - Mozilla Firefox
File Edit View History Bookmarks Tools Help
ISE - Authentication - ise.micronics.local
WLC
https://wlc.micronics.local/screens/frameset.html
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Security
AAA
General
RADIUS
Authentication
Accounting
Fallback
TACACS+
LDAP
Local Net Users
MAC Filtering
Disabled Clients
User Login Policies
AP Policies
Password Policies
Local EAP
Priority Order
Certificate
Access Control Lists
Wireless Protection Policies
Web Auth
TrustSec SXP
Advanced
< Back
Apply

RADIUS Accounting Servers > New

Server Index (Priority) 1
Server IP Address 172.31.1.20
Shared Secret Format ASCII
Shared Secret •••••••••
Confirm Shared Secret •••••••••
Port Number 1813
Server Status Enabled
Server Timeout 2 seconds
Network User ☑ Enable
IPSec □ Enable

- Go to **WLANs** and click on **1** to edit MICRONICS SSID.



WLC - Mozilla Firefox
File Edit View History Bookmarks Tools Help
ISE - Authentication - ise.micronics.local
WLC
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
Advanced
Create New
Go

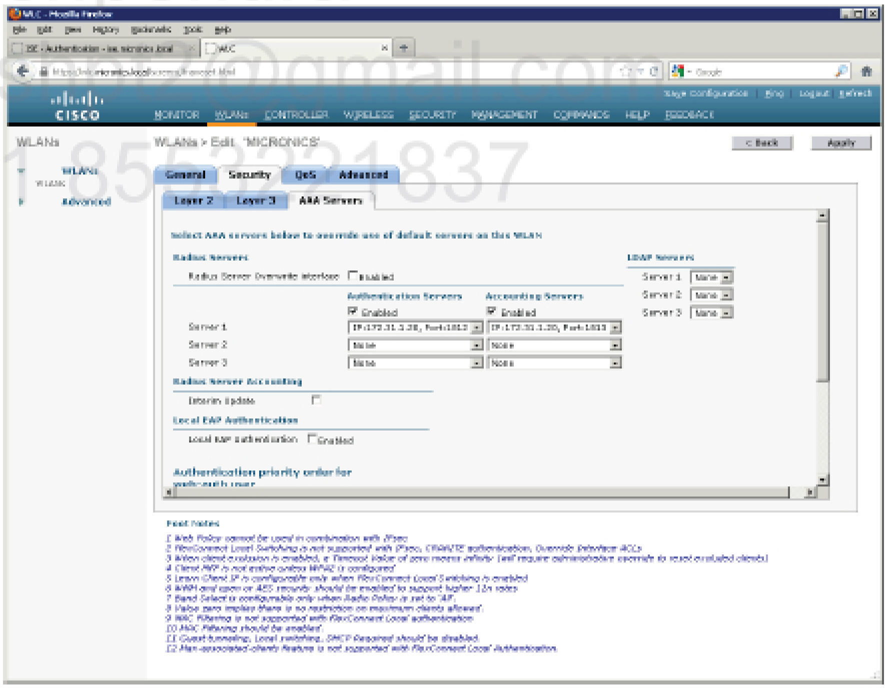
WLANs

Entries 1 - 1 of 1

Current Filter: None [Change Filter] [Clear Filter]

	WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
□	1	WLAN	MICRONICS	MICRONICS	Enabled	[WPA2][Auth(802.1X)]

- Go to **Security > AAA Servers** tab and pick already defined RADIUS Accounting server from the drop-down list.



WLC - Mozilla Firefox
File Edit View History Bookmarks Tools Help
ISE - Authentication - ise.micronics.local
WLC
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
Advanced
< Back
Apply
General
Security
QoS
Advanced
Layer 2
Layer 3
AAA Servers

WLANs > Edit 'MICRONICS'

Select AAA servers below to override use of default servers on this WLAN

Radius Servers

Radius Server Overwrite interface □ Enabled

	Authentication Servers	Accounting Servers
	☑ Enabled	☑ Enabled
Server 1	IP:172.31.1.20, Port:1812	IP:172.31.1.20, Port:1813
Server 2	None	None
Server 3	None	None

LDAP Servers

Server 1	None
Server 2	None
Server 3	None

Radius Server Accounting

Interim Update □

Local EAP Authentication

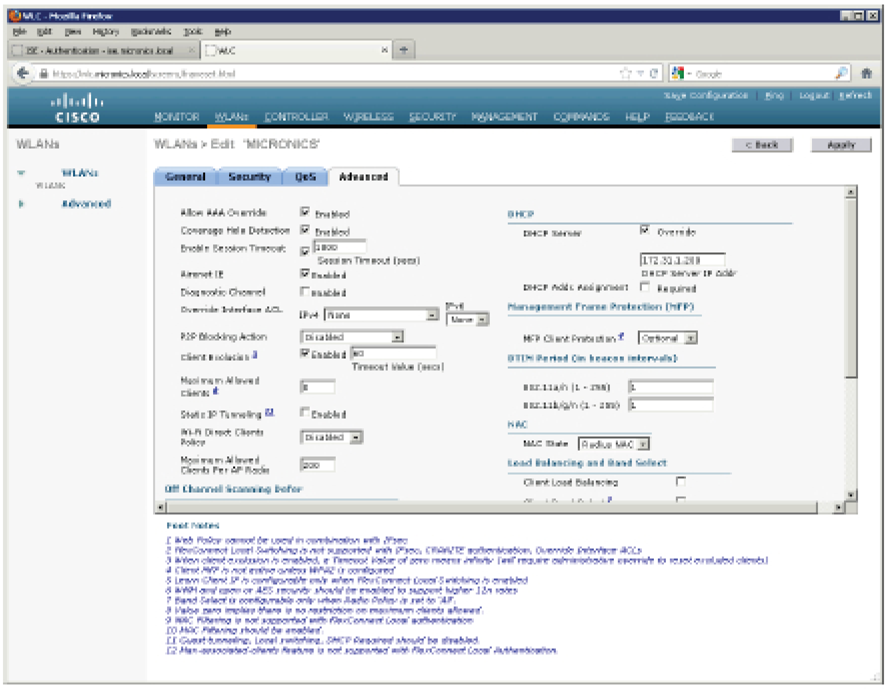
Local EAP Authentication □ Enabled

Authentication priority order for web-auth user

Foot Notes

1 Web Policy cannot be used in combination with IPsec
2 FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs
3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
4 Client MFP is not active unless WPA2 is configured
5 Learn Client IP is configurable only when FlexConnect Local Switching is enabled
6 WMM and open or AES security should be enabled to support higher 11n rates
7 Band Select is configurable only when Radio Policy is set to 'All'.
8 Value zero implies there is no restriction on maximum clients allowed.
9 MAC Filtering is not supported with FlexConnect Local authentication
10 MAC Filtering should be enabled.
11 Guest tunneling, Local switching, DHCP Required should be disabled.
12 Max-associated-clients feature is not supported with FlexConnect Local Authentication.

- Go to **Advanced** tab and select **Radius NAC** for **NAC State** option. Ensure that **Allow AAA Override** option is enabled.



WLANs > Edit 'MICRONICS'

Allow AAA Override ☑ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout ☑ 1800 Session Timeout (secs)
Aironet IE ☑ Enabled
Diagnostic Channel □ Enabled
Override Interface ACL IPv4 None IPv6 None
P2P Blocking Action Disabled
Client Exclusion[3] ☑ Enabled 60 Timeout Value (secs)
Maximum Allowed Clients[8] 0
Static IP Tunneling[11] □ Enabled
Wi-Fi Direct Clients Policy Disabled
Maximum Allowed Clients Per AP Radio 200
Off Channel Scanning Defer

DHCP
DHCP Server ☑ Override
172.30.1.200 DHCP Server IP Addr
DHCP Addr. Assignment □ Required

Management Frame Protection (MFP)
MFP Client Protection[4] Optional

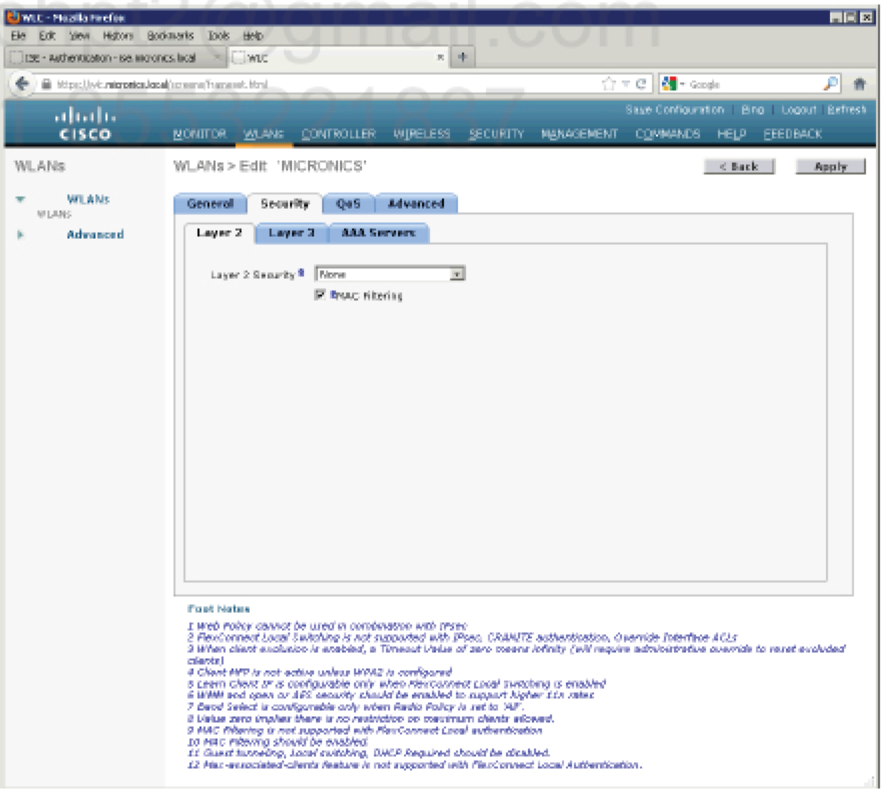
DTIM Period (in beacon intervals)
802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1

NAC
NAC State Radius NAC

Load Balancing and Band Select
Client Load Balancing □

Foot Notes
1 Web Policy cannot be used in combination with IPsec
2 FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs
3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
4 Client MFP is not active unless WPA2 is configured
5 Learn Client IP is configurable only when FlexConnect Local Switching is enabled
6 WMM and open or AES security should be enabled to support higher 11n rates
7 Band Select is configurable only when Radio Policy is set to 'All'.
8 Value zero implies there is no restriction on maximum clients allowed.
9 MAC Filtering is not supported with FlexConnect Local authentication
10 MAC Filtering should be enabled.
11 Guest tunneling, Local switching, DHCP Required should be disabled.
12 Max-associated-clients feature is not supported with FlexConnect Local Authentication.

Go to **Security > Layer 2** tab and change **Layer 2 Security** to **None**. Pick **MAC Filtering** checkbox. Click **Apply**.



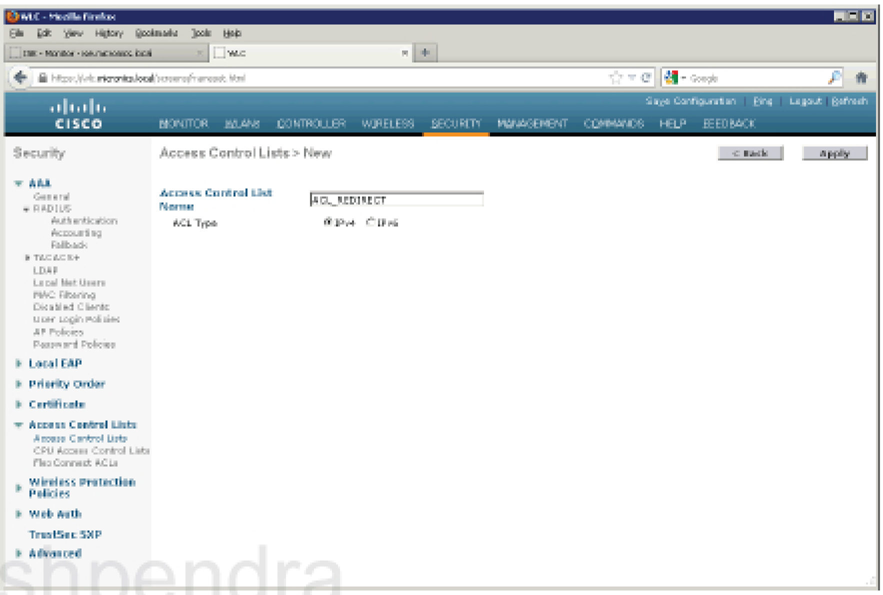
WLANs > Edit 'MICRONICS'

Layer 2 Security[6] None
☑ [9]MAC Filtering

Foot Notes
1 Web Policy cannot be used in combination with IPsec
2 FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs
3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
4 Client MFP is not active unless WPA2 is configured
5 Learn Client IP is configurable only when FlexConnect Local Switching is enabled
6 WMM and open or AES security should be enabled to support higher 11n rates
7 Band Select is configurable only when Radio Policy is set to 'All'.
8 Value zero implies there is no restriction on maximum clients allowed.
9 MAC Filtering is not supported with FlexConnect Local authentication
10 MAC Filtering should be enabled.
11 Guest tunneling, Local switching, DHCP Required should be disabled.
12 Max-associated-clients feature is not supported with FlexConnect Local Authentication.

Step 3 Redirect ACL on WLC.

- Go to **SECURITY > Access Control Lists > Access Control Lists** and click **New…** Enter a name for ACL e.g. **ACL_REDIRECT** (this name must be the same as it is configured on ISE for WEBAUTH authorization policy). Click **Apply** to create ACL.

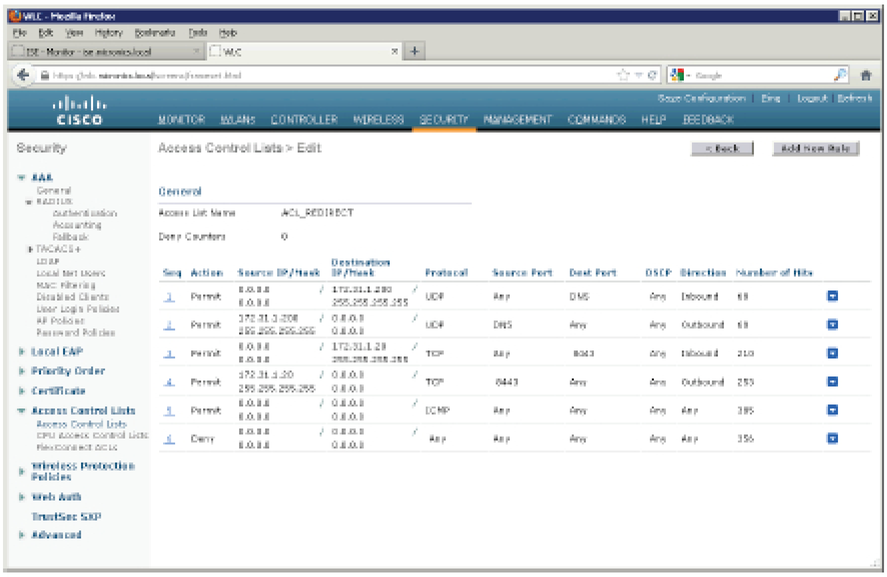


Access Control Lists > New

Access Control List Name: ACL_REDIRECT

ACL Type: ● IPv4 ○ IPv6

- Click on newly created **ACL_REDIRECT** to edit it. Enter the following entries. Remember that redirect ACL works differently on WLC than on IOS. Here, permit statements are those that NOT trigger redirection. Click **< Back** and **Apply** to save the changes.



Access Control Lists > Edit

General

Access List Name: ACL_REDIRECT

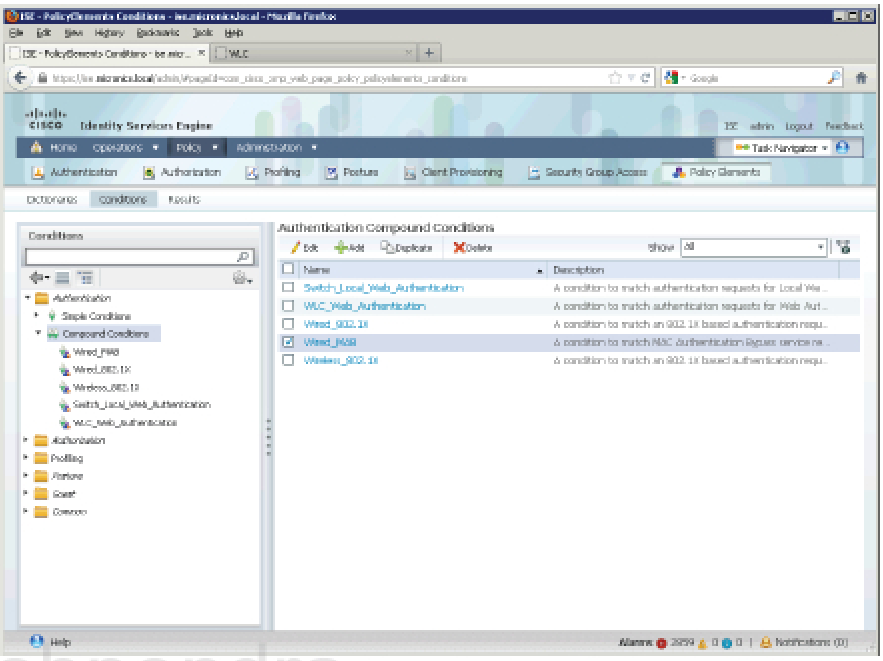
Deny Counters: 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	172.31.1.200 / 255.255.255.255	UDP	Any	DNS	Any	Inbound	68
2	Permit	172.31.1.200 / 255.255.255.255	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Outbound	68
3	Permit	0.0.0.0 / 0.0.0.0	172.31.1.20 / 255.255.255.255	TCP	Any	8443	Any	Inbound	210
4	Permit	172.31.1.20 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	8443	Any	Any	Outbound	253
5	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Any	395
6	Deny	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	356

Step 4 ISE configuration. Change authentication rule for MAB to work for both Wired and Wireless MAB.

- Go to **Policy > Policy Elements > Conditions > Authentication >**

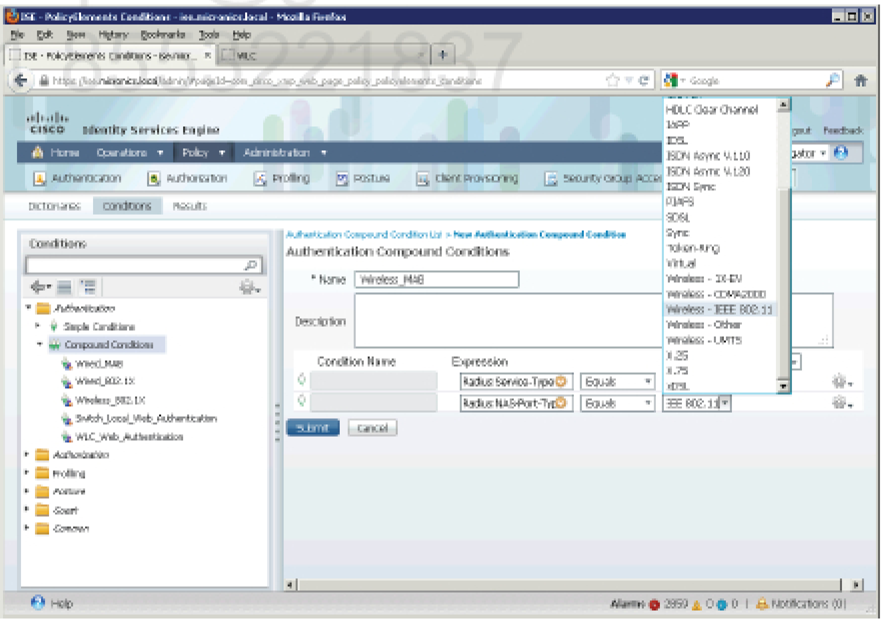
Compound Conditions and pick **Wired_MAB** condition on the list. Click **Duplicate** button.



Authentication Compound Conditions

□	Name	Description
□	Switch_Local_Web_Authentication	A condition to match authentication requests for Local We...
□	WLC_Web_Authentication	A condition to match authentication requests for Web Aut...
□	Wired_802.1X	A condition to match an 802.1X based authentication requ...
☑	Wired_MAB	A condition to match MAC Authentication Bypass service re...
□	Wireless_802.1X	A condition to match an 802.1X based authentication requ...

- Change the default name to **Wireless_MAB** and change second rule to match against **Wireless – IEEE 802.11**. Click **Submit**.



Authentication Compound Condition List > New Authentication Compound Condition

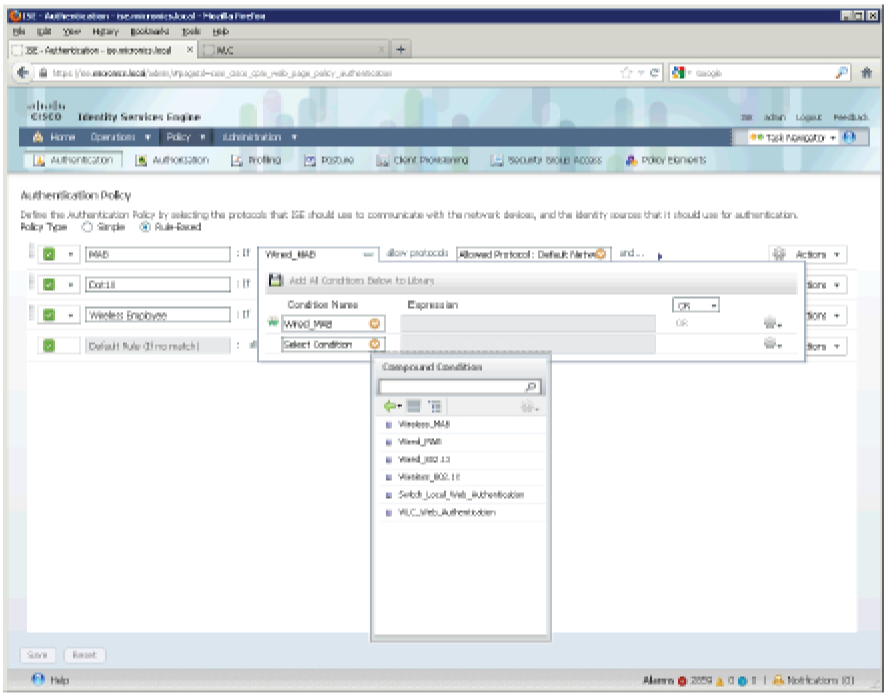
Authentication Compound Conditions

* Name: Wireless_MAB

Description:

Condition Name	Expression		
	Radius:Service-Type	Equals	
	Radius:NAS-Port-Type	Equals	IEEE 802.11

- Go to **Policy > Authentication** and click **Wired_MAB** condition. Add **Wireless_MAB** condition with **OR** in between.



Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

Policy Type ○ Simple ● Rule-Based

☑ MAB	: If	Wired_MAB	allow protocols Allowed Protocol : Default Netw... and ...
☑ Dot1X	: If		
☑ Wireless Employee	: If		
☑ Default Rule (If no match)	:		

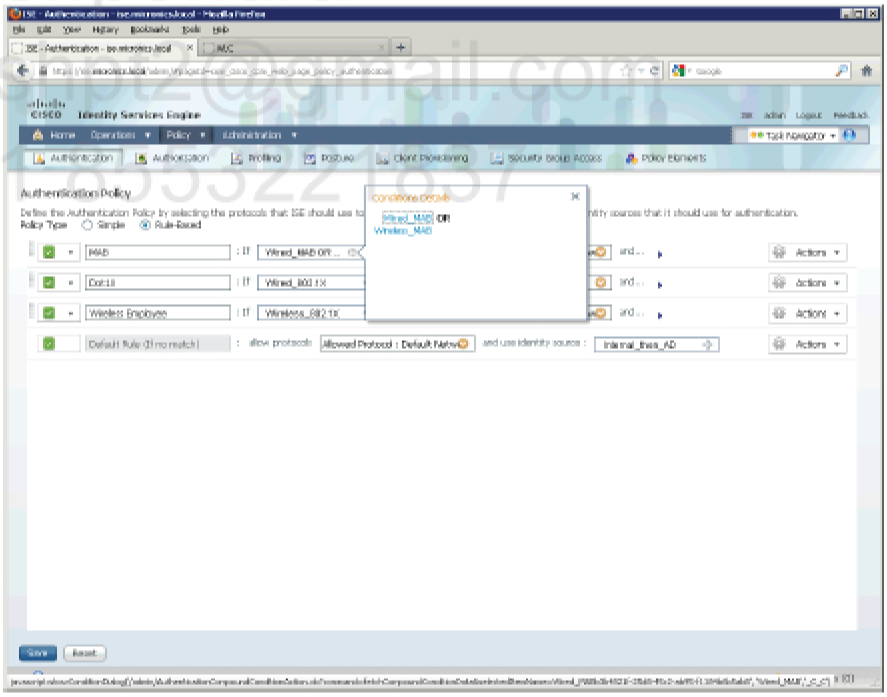
Add All Conditions Below to Library

Condition Name	Expression	OR
Wired_MAB		OR
Select Condition		

Compound Condition

- Wireless_MAB
- Wired_MAB
- Wired_802.1X
- Wireless_802.1X
- Switch_Local_Web_Authentication
- WLC_Web_Authentication

- Click **Save** to apply the changes.



Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to ... ...tity sources that it should use for authentication.

Policy Type ○ Simple ● Rule-Based

☑ MAB	: If	Wired_MAB OR ...	and ...
☑ Dot1X	: If	Wired_802.1X	and ...
☑ Wireless Employee	: If	Wireless_802.1X	and ...
☑ Default Rule (If no match)	:	allow protocols Allowed Protocol : Default Netw...	and use identity source : Internal_then_AD

Conditions Details

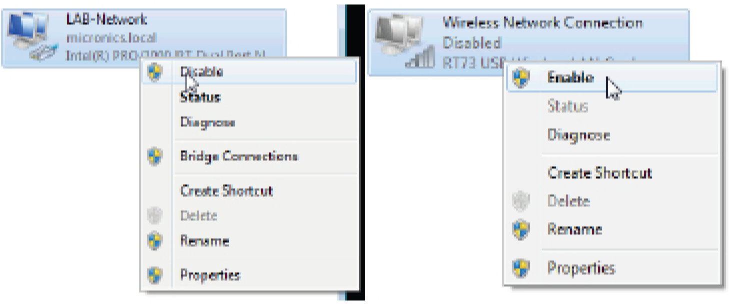
Wired_MAB OR
Wireless_MAB

Verification

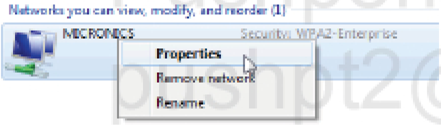
Enable debugging on the WLC:

```
debug client <client-MAC-address>
```

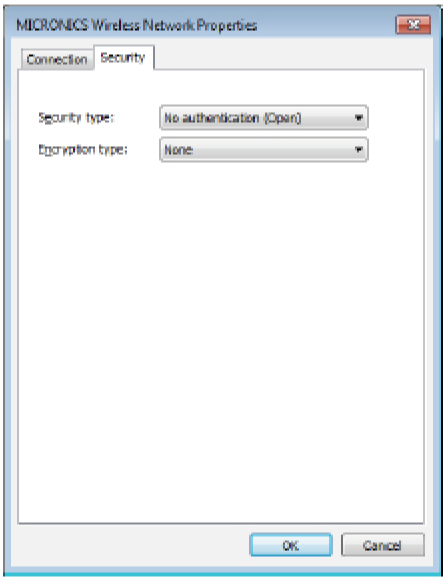
On Win7 PC disable LAN NIC and enable Wireless NIC.



- Go to **Control Panel > Network and Internet > Manage Wireless Networks** and display Properties of MICRONICS connection.


Networks you can view, modify, and reorder (1)
MICRONICS
Security: WPA2-Enterprise
Properties
Remove network
Rename

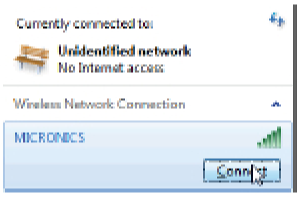
- On the **Security** tab select options as follows and click **OK**.



Security type: No authentication (Open)

Encryption type: None

- Click on network connection icon on the Windows tray and select **MICRONICS** network. Click **Connect**.



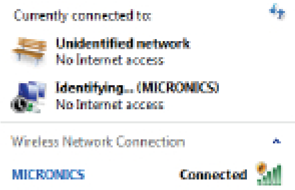
Currently connected to:

Unidentified network
No Internet access

Wireless Network Connection

MICRONICS

- You should see **Connected** status.



Currently connected to:

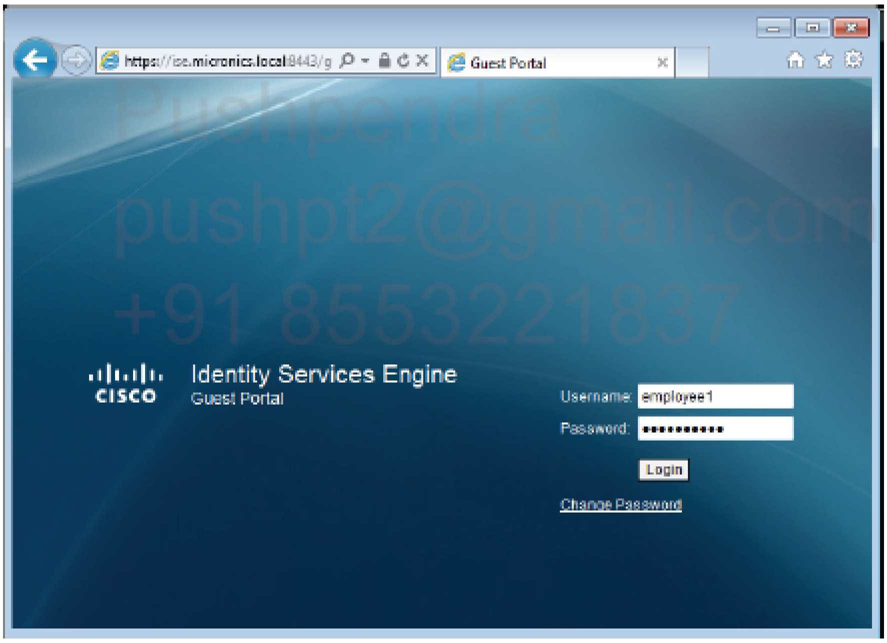
Unidentified network
No Internet access

Identifying... (MICRONICS)
No Internet access

Wireless Network Connection

MICRONICS Connected

- Open up web browser and enter some IP address or FQDN. You should be redirected to ISE for CWA. Provide user credentials and hit **Login**.



https://ise.micronics.local:8443/g

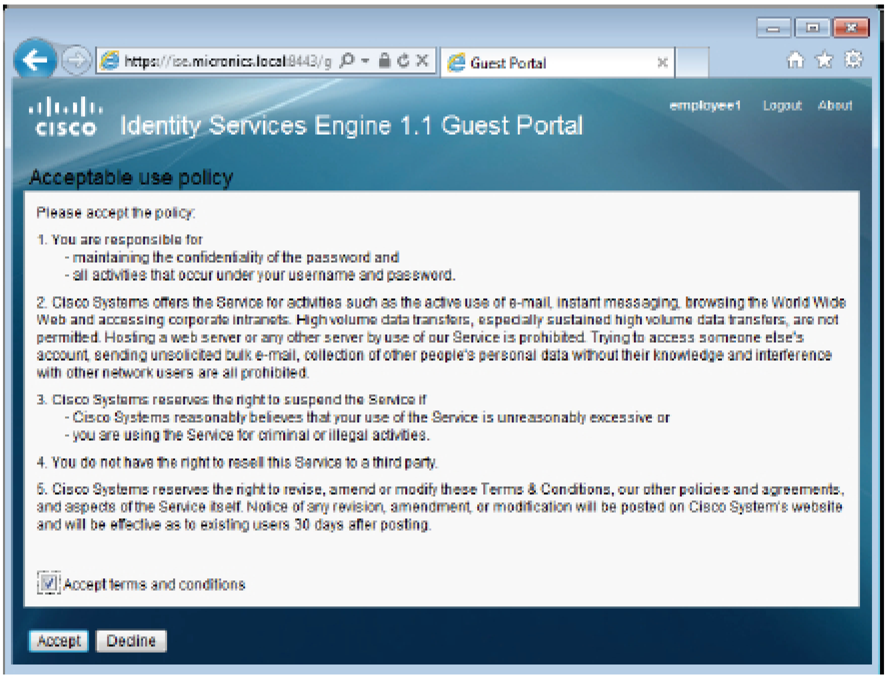
Guest Portal

Identity Services Engine
Guest Portal

Username: employee1

Password: ••••••••••

- Accept the policy.



https://ise.micronics.local:8443/g
Guest Portal
employee1
Logout
About
Identity Services Engine 1.1 Guest Portal

Acceptable use policy

Please accept the policy:

1. You are responsible for
   - maintaining the confidentiality of the password and
   - all activities that occur under your username and password.

2. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited.

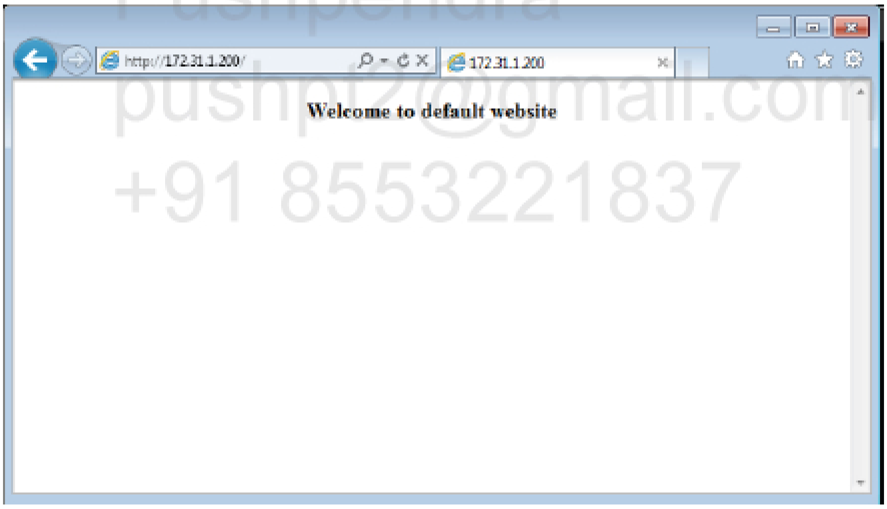
3. Cisco Systems reserves the right to suspend the Service if
   - Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or
   - you are using the Service for criminal or illegal activities.

4. You do not have the right to resell this Service to a third party.

5. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or modification will be posted on Cisco System's website and will be effective as to existing users 30 days after posting.

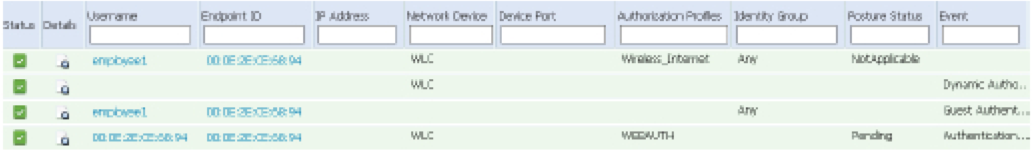
☑ Accept terms and conditions

- Now you should be able to access all web servers.



Welcome to default website

Log on ISE.



Status	Details	Username	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Identity Group	Posture Status	Event
✓		employee1	00:0E:2E:CE:68:94		WLC		Wireless_Internet	Any	NotApplicable	
✓					WLC					Dynamic Autho...
✓		employee1	00:0E:2E:CE:68:94					Any		Guest Authent...
✓		00:0E:2E:CE:68:94	00:0E:2E:CE:68:94		WLC		WEBAUTH		Pending	Authentication...

WLC debug while connecting the client.

```
(Cisco Controller) >debug client 00:0e:2e:ce:68:94

        // client debug is enabled. There is a new client discovered on AP with the following MAC address.

*apfMsConnTask_3: Jan 31 13:12:13.094: 00:0e:2e:ce:68:94 Association received from mobile on AP c4:7d:4f:46:4b:00
```

```
*apfMsConnTask_3: Jan 31 13:12:13.094: 00:0e:2e:ce:68:94 10.1.30.20 WEBAUTH_REQD (8) Changing IPv4 ACL 'none' (ACL
ID 255) ===> 'none' (ACL ID 255) --- (caller apf_policy.c:1697)
*apfMsConnTask_3: Jan 31 13:12:13.094: 00:0e:2e:ce:68:94 10.1.30.20 WEBAUTH_REQD (8) Changing IPv6 ACL 'none' (ACL
ID 255) ===> 'none' (ACL ID 255) --- (caller apf_policy.c:1864)
*apfMsConnTask_3: Jan 31 13:12:13.094: 00:0e:2e:ce:68:94 apfApplyWlanPolicy: Retaining the ACL recieved in AAA
attributes 2 on mobile
*apfMsConnTask_3: Jan 31 13:12:13.094: 00:0e:2e:ce:68:94 Applying site-specific Local Bridging override for station
00:0e:2e:ce:68:94 - vapId 1, site 'default-group', interface 'dmz_interface'
*apfMsConnTask_3: Jan 31 13:12:13.094: 00:0e:2e:ce:68:94 Applying Local Bridging Interface Policy for station
00:0e:2e:ce:68:94 - vlan 0, interface id 11, interface 'dmz_interface'
*apfMsConnTask_3: Jan 31 13:12:13.094: 00:0e:2e:ce:68:94 processSsidIE  statusCode is 0 and status is 0
*apfMsConnTask_3: Jan 31 13:12:13.094: 00:0e:2e:ce:68:94 processSsidIE  ssid_done_flag is 0 finish_flag is 0
*apfMsConnTask_3: Jan 31 13:12:13.094: 00:0e:2e:ce:68:94 STA - rates (8): 130 132 139 12 18 150 24 36 48 72 96 108 0
0 0 0
*apfMsConnTask_3: Jan 31 13:12:13.094: 00:0e:2e:ce:68:94 suppRates  statusCode is 0 and gotSuppRatesElement is 1
*apfMsConnTask_3: Jan 31 13:12:13.094: 00:0e:2e:ce:68:94 STA - rates (12): 130 132 139 12 18 150 24 36 48 72 96 108
0 0 0 0
*apfMsConnTask_3: Jan 31 13:12:13.095: 00:0e:2e:ce:68:94 extSuppRates  statusCode is 0 and gotExtSuppRatesElement is
1
*apfMsConnTask_3: Jan 31 13:12:13.095: 00:0e:2e:ce:68:94 apfMsAssoStateDec
*apfMsConnTask_3: Jan 31 13:12:13.095: 00:0e:2e:ce:68:94 apfProcessAssocReq (apf_80211.c:6171) Changing state for
mobile 00:0e:2e:ce:68:94 on AP c4:7d:4f:46:4b:00 from Associated to AAA Pending

*apfMsConnTask_3: Jan 31 13:12:13.095: 00:0e:2e:ce:68:94 Scheduling deletion of Mobile Station:  (callerId: 20) in
10 seconds

          // Redirect ACL name has been received from ISE.

*apfReceiveTask: Jan 31 13:12:13.225: 00:0e:2e:ce:68:94 Received SGT for this Client.
*apfReceiveTask: Jan 31 13:12:13.225: 00:0e:2e:ce:68:94 Redirect URL received for client from RADIUS. Client will be
moved to WebAuth_Reqd state to facilitate redirection.
*apfReceiveTask: Jan 31 13:12:13.226: 00:0e:2e:ce:68:94 10.1.30.20 WEBAUTH_REQD (8) Changing IPv4 ACL 'none' (ACL ID
255) ===> 'none' (ACL ID 255) --- (caller apf_policy.c:1697)
*apfReceiveTask: Jan 31 13:12:13.226: 00:0e:2e:ce:68:94 10.1.30.20 WEBAUTH_REQD (8) Changing IPv6 ACL 'none' (ACL ID
255) ===> 'none' (ACL ID 255) --- (caller apf_policy.c:1864)
*apfReceiveTask: Jan 31 13:12:13.226: 00:0e:2e:ce:68:94 apfApplyWlanPolicy: Retaining the ACL recieved in AAA
attributes 2 on mobile
*apfReceiveTask: Jan 31 13:12:13.226: 00:0e:2e:ce:68:94 Inserting AAA Override struct for mobile
        MAC: 00:0e:2e:ce:68:94, source 2

*apfReceiveTask: Jan 31 13:12:13.226: 00:0e:2e:ce:68:94 apfMs1xStateDec
*apfReceiveTask: Jan 31 13:12:13.226: 00:0e:2e:ce:68:94 10.1.30.20 WEBAUTH_REQD (8) Change state to START (0) last
state WEBAUTH_REQD (8)

*apfReceiveTask: Jan 31 13:12:13.226: 00:0e:2e:ce:68:94 pemApfAddMobileStation2: APF_MS_PEM_WAIT_L2_AUTH_COMPLETE =
0.
*apfReceiveTask: Jan 31 13:12:13.226: 00:0e:2e:ce:68:94 10.1.30.20 START (0) Initializing policy
*apfReceiveTask: Jan 31 13:12:13.226: 00:0e:2e:ce:68:94 10.1.30.20 START (0) Change state to AUTHCHECK (2) last
state WEBAUTH_REQD (8)

*apfReceiveTask: Jan 31 13:12:13.226: 00:0e:2e:ce:68:94 10.1.30.20 AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4)
last state WEBAUTH_REQD (8)

*apfReceiveTask: Jan 31 13:12:13.226: 00:0e:2e:ce:68:94 10.1.30.20 L2AUTHCOMPLETE (4) DHCP Not required on AP
c4:7d:4f:46:4b:00 vapId 1 apVapId 1for this client
*apfReceiveTask: Jan 31 13:12:13.226: 00:0e:2e:ce:68:94 Not Using WMM Compliance code qosCap 00
*apfReceiveTask: Jan 31 13:12:13.226: 00:0e:2e:ce:68:94 10.1.30.20 L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on
AP c4:7d:4f:46:4b:00 vapId 1 apVapId 1
*apfReceiveTask: Jan 31 13:12:13.226: 00:0e:2e:ce:68:94 10.1.30.20 L2AUTHCOMPLETE (4) Change state to WEBAUTH_REQD
(8) last state WEBAUTH_REQD (8)

*apfReceiveTask: Jan 31 13:12:13.226: 00:0e:2e:ce:68:94 10.1.30.20 WEBAUTH_REQD (8) pemApfAddMobileStation2 3121,
Adding TMP rule
*apfReceiveTask: Jan 31 13:12:13.226: 00:0e:2e:ce:68:94 10.1.30.20 WEBAUTH_REQD (8) Adding Fast Path rule
  type = Airespace AP Client - ACL passthru
  on AP c4:7d:4f:46:4b:00, slot 0, interface = 1, QOS = 0
  IPv4 ACL ID =
*apfReceiveTask: Jan 31 13:12:13.226: 00:0e:2e:ce:68:94 10.1.30.20 WEBAUTH_REQD (8) Fast Path rule (contd...) 802.1P
= 0, DSCP = 0, TokenID = 7006  Local Bridging Vlan = 0, Local Bridging intf id = 11
```

```
*apfReceiveTask: Jan 31 13:12:13.226: 00:0e:2e:ce:68:94 10.1.30.20 WEBAUTH_REQD (8) Successfully plumbed mobile rule
(IPv4 ACL ID 2, IPv6 ACL ID 255)
*apfReceiveTask: Jan 31 13:12:13.226: 00:0e:2e:ce:68:94 10.1.30.20 WEBAUTH_REQD (8) pemApfAddMobileStation2 3219,
Adding TMP rule
*apfReceiveTask: Jan 31 13:12:13.226: 00:0e:2e:ce:68:94 10.1.30.20 WEBAUTH_REQD (8) Replacing Fast Path rule
  type = Airespace AP Client - ACL passthru
  on AP c4:7d:4f:46:4b:00, slot 0, interface = 1, QOS = 0
  IPv4 ACL I
*apfReceiveTask: Jan 31 13:12:13.226: 00:0e:2e:ce:68:94 10.1.30.20 WEBAUTH_REQD (8) Fast Path rule (contd...) 802.1P
= 0, DSCP = 0, TokenID = 7006  Local Bridging Vlan = 0, Local Bridging intf id = 11
*apfReceiveTask: Jan 31 13:12:13.226: 00:0e:2e:ce:68:94 10.1.30.20 WEBAUTH_REQD (8) Successfully plumbed mobile rule
(IPv4 ACL ID 2, IPv6 ACL ID 255)
*apfReceiveTask: Jan 31 13:12:13.226: 00:0e:2e:ce:68:94 apfMsAssoStateInc
*apfReceiveTask: Jan 31 13:12:13.226: 00:0e:2e:ce:68:94 apfPemAddUser2 (apf_policy.c:268) Changing state for mobile
00:0e:2e:ce:68:94 on AP c4:7d:4f:46:4b:00 from AAA Pending to Associated

*apfReceiveTask: Jan 31 13:12:13.226: 00:0e:2e:ce:68:94 Scheduling deletion of Mobile Station:  (callerId: 49) in
1800 seconds
*apfReceiveTask: Jan 31 13:12:13.226: 00:0e:2e:ce:68:94 Sending Assoc Response to station on BSSID c4:7d:4f:46:4b:00
(status 0) ApVapId 1 Slot 0
*apfReceiveTask: Jan 31 13:12:13.226: 00:0e:2e:ce:68:94 apfProcessRadiusAssocResp (apf_80211.c:2504) Changing state
for mobile 00:0e:2e:ce:68:94 on AP c4:7d:4f:46:4b:00 from Associated to Associated

*pemReceiveTask: Jan 31 13:12:13.227: 00:0e:2e:ce:68:94 10.1.30.20 Removed NPU entry.
*pemReceiveTask: Jan 31 13:12:13.227: 00:0e:2e:ce:68:94 10.1.30.20 Added NPU entry of type 2, dtlFlags 0x0
*pemReceiveTask: Jan 31 13:12:13.227: 00:0e:2e:ce:68:94 Pushing IPv6: fe80:0000:0000:0000: 7dff:670e:20ef:2045 , and
MAC: 00:0E:2E:CE:68:94 , Binding to Data Plane. SUCCESS !!
*pemReceiveTask: Jan 31 13:12:13.227: 00:0e:2e:ce:68:94 Sent an XID frame
*pemReceiveTask: Jan 31 13:12:13.227: 00:0e:2e:ce:68:94 10.1.30.20 Added NPU entry of type 2, dtlFlags 0x0
*pemReceiveTask: Jan 31 13:12:13.227: 00:0e:2e:ce:68:94 Pushing IPv6: fe80:0000:0000:0000: 7dff:670e:20ef:2045 , and
MAC: 00:0E:2E:CE:68:94 , Binding to Data Plane. SUCCESS !!
*pemReceiveTask: Jan 31 13:12:13.227: 00:0e:2e:ce:68:94 Sent an XID frame
*IPv6_Msg_Task: Jan 31 13:12:13.372: 00:0e:2e:ce:68:94 10.1.30.20 WEBAUTH_REQD (8) DHCP Address Re-established
*IPv6_Msg_Task: Jan 31 13:12:13.372: 00:0e:2e:ce:68:94 10.1.30.20 WEBAUTH_REQD (8) Reached PLUMBFASTPATH: from line
5373
*IPv6_Msg_Task: Jan 31 13:12:13.372: 00:0e:2e:ce:68:94 10.1.30.20 WEBAUTH_REQD (8) Replacing Fast Path rule
  type = Airespace AP Client - ACL passthru
  on AP c4:7d:4f:46:4b:00, slot 0, interface = 1, QOS = 0
  IPv4 ACL I
*IPv6_Msg_Task: Jan 31 13:12:13.372: 00:0e:2e:ce:68:94 10.1.30.20 WEBAUTH_REQD (8) Fast Path rule (contd...) 802.1P
= 0, DSCP = 0, TokenID = 7006  Local Bridging Vlan = 0, Local Bridging intf id = 11
*IPv6_Msg_Task: Jan 31 13:12:13.372: 00:0e:2e:ce:68:94 10.1.30.20 WEBAUTH_REQD (8) Successfully plumbed mobile rule
(IPv4 ACL ID 2, IPv6 ACL ID 255)
*pemReceiveTask: Jan 31 13:12:13.373: 00:0e:2e:ce:68:94 10.1.30.20 Added NPU entry of type 2, dtlFlags 0x0
*pemReceiveTask: Jan 31 13:12:13.373: 00:0e:2e:ce:68:94 Pushing IPv6: fe80:0000:0000:0000: 7dff:670e:20ef:2045 , and
MAC: 00:0E:2E:CE:68:94 , Binding to Data Plane. SUCCESS !!
*pemReceiveTask: Jan 31 13:12:13.373: 00:0e:2e:ce:68:94 Sent an XID frame
*DHCP Socket Task: Jan 31 13:12:13.468: 00:0e:2e:ce:68:94 DHCP received op BOOTREQUEST (1) (len 326,vlan 10, port 1,
encap 0xec03)
*DHCP Socket Task: Jan 31 13:12:13.468: 00:0e:2e:ce:68:94 DHCP selecting relay 1 - control block settings:
                        dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,
                        dhcpGateway: 0.0.0.0, dhcpRelay: 0.0.0.0  VLAN: 0

          // WLC relies DHCP Request to the server and gets IP address to the client.

*DHCP Socket Task: Jan 31 13:12:13.468: 00:0e:2e:ce:68:94 DHCP selected relay 1 - 172.31.1.200 (local address
10.1.30.5, gateway 10.1.30.10, VLAN 0, port 2)
*DHCP Socket Task: Jan 31 13:12:13.468: 00:0e:2e:ce:68:94 DHCP transmitting DHCP REQUEST (3)
*DHCP Socket Task: Jan 31 13:12:13.468: 00:0e:2e:ce:68:94 DHCP   op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1
*DHCP Socket Task: Jan 31 13:12:13.468: 00:0e:2e:ce:68:94 DHCP   xid: 0x399cb961 (966572385), secs: 0, flags: 0
*DHCP Socket Task: Jan 31 13:12:13.468: 00:0e:2e:ce:68:94 DHCP   chaddr: 00:0e:2e:ce:68:94
*DHCP Socket Task: Jan 31 13:12:13.468: 00:0e:2e:ce:68:94 DHCP   ciaddr: 0.0.0.0,  yiaddr: 0.0.0.0
*DHCP Socket Task: Jan 31 13:12:13.468: 00:0e:2e:ce:68:94 DHCP   siaddr: 0.0.0.0,  giaddr: 10.1.30.5
*DHCP Socket Task: Jan 31 13:12:13.468: 00:0e:2e:ce:68:94 DHCP   requested ip: 10.1.30.20
*DHCP Socket Task: Jan 31 13:12:13.468: 00:0e:2e:ce:68:94 DHCP sending REQUEST to 10.1.30.10 (len 362, port 2, vlan
0)
*DHCP Socket Task: Jan 31 13:12:13.468: 00:0e:2e:ce:68:94 DHCP selecting relay 2 - control block settings:
                        dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,
                        dhcpGateway: 0.0.0.0, dhcpRelay: 10.1.30.5  VLAN: 0
```

```
*DHCP Socket Task: Jan 31 13:12:13.468: 00:0e:2e:ce:68:94 DHCP selected relay 2 - NONE
*DHCP Socket Task: Jan 31 13:12:13.471: 00:0e:2e:ce:68:94 DHCP received op BOOTREPLY (2) (len 312,vlan 0, port 2,
encap 0xec00)
*DHCP Socket Task: Jan 31 13:12:13.471: 00:0e:2e:ce:68:94 DHCP setting server from ACK (server 172.31.1.200, yiaddr
10.1.30.20)
*DHCP Socket Task: Jan 31 13:12:13.471: 00:0e:2e:ce:68:94 DHCP sending REPLY to STA (len 418, port 1, vlan 10)
*DHCP Socket Task: Jan 31 13:12:13.471: 00:0e:2e:ce:68:94 DHCP transmitting DHCP ACK (5)
*DHCP Socket Task: Jan 31 13:12:13.471: 00:0e:2e:ce:68:94 DHCP   op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0
*DHCP Socket Task: Jan 31 13:12:13.471: 00:0e:2e:ce:68:94 DHCP   xid: 0x399cb961 (966572385), secs: 0, flags: 0
*DHCP Socket Task: Jan 31 13:12:13.471: 00:0e:2e:ce:68:94 DHCP   chaddr: 00:0e:2e:ce:68:94
*DHCP Socket Task: Jan 31 13:12:13.471: 00:0e:2e:ce:68:94 DHCP   ciaddr: 0.0.0.0,  yiaddr: 10.1.30.20
*DHCP Socket Task: Jan 31 13:12:13.471: 00:0e:2e:ce:68:94 DHCP   siaddr: 0.0.0.0,  giaddr: 0.0.0.0
*DHCP Socket Task: Jan 31 13:12:13.471: 00:0e:2e:ce:68:94 DHCP   server id: 11.11.11.11  rcvd server id:
172.31.1.200
*DHCP Socket Task: Jan 31 13:12:16.400: 00:0e:2e:ce:68:94 DHCP received op BOOTREQUEST (1) (len 308,vlan 10, port 1,
encap 0xec03)
*DHCP Socket Task: Jan 31 13:12:16.400: 00:0e:2e:ce:68:94 DHCP selecting relay 1 - control block settings:
                        dhcpServer: 172.31.1.200, dhcpNetmask: 255.255.255.0,
                        dhcpGateway: 10.1.30.10, dhcpRelay: 10.1.30.5  VLAN: 0
*DHCP Socket Task: Jan 31 13:12:16.400: 00:0e:2e:ce:68:94 DHCP selected relay 1 - 172.31.1.200 (local address
10.1.30.5, gateway 10.1.30.10, VLAN 0, port 2)
*DHCP Socket Task: Jan 31 13:12:16.400: 00:0e:2e:ce:68:94 DHCP transmitting DHCP INFORM (8)
*DHCP Socket Task: Jan 31 13:12:16.400: 00:0e:2e:ce:68:94 DHCP   op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1
*DHCP Socket Task: Jan 31 13:12:16.401: 00:0e:2e:ce:68:94 DHCP   xid: 0x45e3106d (1172508781), secs: 0, flags: 0
*DHCP Socket Task: Jan 31 13:12:16.401: 00:0e:2e:ce:68:94 DHCP   chaddr: 00:0e:2e:ce:68:94
*DHCP Socket Task: Jan 31 13:12:16.401: 00:0e:2e:ce:68:94 DHCP   ciaddr: 10.1.30.20,  yiaddr: 0.0.0.0
*DHCP Socket Task: Jan 31 13:12:16.401: 00:0e:2e:ce:68:94 DHCP   siaddr: 0.0.0.0,  giaddr: 10.1.30.5
*DHCP Socket Task: Jan 31 13:12:16.401: 00:0e:2e:ce:68:94 DHCP sending REQUEST to 10.1.30.10 (len 346, port 2, vlan
0)
*DHCP Socket Task: Jan 31 13:12:16.401: 00:0e:2e:ce:68:94 DHCP selecting relay 2 - control block settings:
                        dhcpServer: 172.31.1.200, dhcpNetmask: 255.255.255.0,
                        dhcpGateway: 10.1.30.10, dhcpRelay: 10.1.30.5  VLAN: 0
*DHCP Socket Task: Jan 31 13:12:16.401: 00:0e:2e:ce:68:94 DHCP selected relay 2 - NONE
*DHCP Socket Task: Jan 31 13:12:16.409: 00:0e:2e:ce:68:94 DHCP received op BOOTREPLY (2) (len 308,vlan 0, port 2,
encap 0xec00)
*DHCP Socket Task: Jan 31 13:12:16.410: 00:0e:2e:ce:68:94 DHCP sending REPLY to STA (len 418, port 1, vlan 10)
*DHCP Socket Task: Jan 31 13:12:16.410: 00:0e:2e:ce:68:94 DHCP transmitting DHCP ACK (5)
*DHCP Socket Task: Jan 31 13:12:16.410: 00:0e:2e:ce:68:94 DHCP   op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0
*DHCP Socket Task: Jan 31 13:12:16.410: 00:0e:2e:ce:68:94 DHCP   xid: 0x45e3106d (1172508781), secs: 0, flags: 0
*DHCP Socket Task: Jan 31 13:12:16.410: 00:0e:2e:ce:68:94 DHCP   chaddr: 00:0e:2e:ce:68:94
*DHCP Socket Task: Jan 31 13:12:16.410: 00:0e:2e:ce:68:94 DHCP   ciaddr: 10.1.30.20,  yiaddr: 0.0.0.0
*DHCP Socket Task: Jan 31 13:12:16.410: 00:0e:2e:ce:68:94 DHCP   siaddr: 0.0.0.0,  giaddr: 0.0.0.0
*DHCP Socket Task: Jan 31 13:12:16.410: 00:0e:2e:ce:68:94 DHCP   server id: 11.11.11.11  rcvd server id:
172.31.1.200
*dot11b: Jan 31 13:12:28.221: 00:0e:2e:ce:68:94 Client stats update: Time now in sec 1359637948, Last Acct Msg Sent
at 0 sec
*dot11b: Jan 31 13:12:28.221: 00:0e:2e:ce:68:94 Requested to send acct interim update request msg to APF task for
client 0:e:2e:ce:68:94

*DHCP Socket Task: Jan 31 13:13:32.852: 00:0e:2e:ce:68:94 DHCP received op BOOTREQUEST (1) (len 308,vlan 10, port 1,
encap 0xec03)
*DHCP Socket Task: Jan 31 13:13:32.852: 00:0e:2e:ce:68:94 DHCP selecting relay 1 - control block settings:
                        dhcpServer: 172.31.1.200, dhcpNetmask: 255.255.255.0,
                        dhcpGateway: 10.1.30.10, dhcpRelay: 10.1.30.5  VLAN: 0
*DHCP Socket Task: Jan 31 13:13:32.852: 00:0e:2e:ce:68:94 DHCP selected relay 1 - 172.31.1.200 (local address
10.1.30.5, gateway 10.1.30.10, VLAN 0, port 2)
*DHCP Socket Task: Jan 31 13:13:32.852: 00:0e:2e:ce:68:94 DHCP transmitting DHCP INFORM (8)
*DHCP Socket Task: Jan 31 13:13:32.852: 00:0e:2e:ce:68:94 DHCP   op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1
*DHCP Socket Task: Jan 31 13:13:32.852: 00:0e:2e:ce:68:94 DHCP   xid: 0xefd1ec8d (4023512205), secs: 0, flags: 0
*DHCP Socket Task: Jan 31 13:13:32.852: 00:0e:2e:ce:68:94 DHCP   chaddr: 00:0e:2e:ce:68:94
*DHCP Socket Task: Jan 31 13:13:32.853: 00:0e:2e:ce:68:94 DHCP   ciaddr: 10.1.30.20,  yiaddr: 0.0.0.0
*DHCP Socket Task: Jan 31 13:13:32.853: 00:0e:2e:ce:68:94 DHCP   siaddr: 0.0.0.0,  giaddr: 10.1.30.5
*DHCP Socket Task: Jan 31 13:13:32.853: 00:0e:2e:ce:68:94 DHCP sending REQUEST to 10.1.30.10 (len 346, port 2, vlan
0)
*DHCP Socket Task: Jan 31 13:13:32.853: 00:0e:2e:ce:68:94 DHCP selecting relay 2 - control block settings:
                        dhcpServer: 172.31.1.200, dhcpNetmask: 255.255.255.0,
                        dhcpGateway: 10.1.30.10, dhcpRelay: 10.1.30.5  VLAN: 0
*DHCP Socket Task: Jan 31 13:13:32.853: 00:0e:2e:ce:68:94 DHCP selected relay 2 - NONE
```

```
*DHCP Socket Task: Jan 31 13:13:32.933: 00:0e:2e:ce:68:94 DHCP received op BOOTREPLY (2) (len 308,vlan 0, port 2,
encap 0xec00)
*DHCP Socket Task: Jan 31 13:13:32.933: 00:0e:2e:ce:68:94 DHCP sending REPLY to STA (len 418, port 1, vlan 10)
*DHCP Socket Task: Jan 31 13:13:32.933: 00:0e:2e:ce:68:94 DHCP transmitting DHCP ACK (5)
*DHCP Socket Task: Jan 31 13:13:32.934: 00:0e:2e:ce:68:94 DHCP   op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0
*DHCP Socket Task: Jan 31 13:13:32.934: 00:0e:2e:ce:68:94 DHCP   xid: 0xefd1ec8d (4023512205), secs: 0, flags: 0
*DHCP Socket Task: Jan 31 13:13:32.934: 00:0e:2e:ce:68:94 DHCP   chaddr: 00:0e:2e:ce:68:94
*DHCP Socket Task: Jan 31 13:13:32.934: 00:0e:2e:ce:68:94 DHCP   ciaddr: 10.1.30.20,  yiaddr: 0.0.0.0
*DHCP Socket Task: Jan 31 13:13:32.934: 00:0e:2e:ce:68:94 DHCP   siaddr: 0.0.0.0,  giaddr: 0.0.0.0
*DHCP Socket Task: Jan 31 13:13:32.934: 00:0e:2e:ce:68:94 DHCP   server id: 11.11.11.11  rcvd server id:
172.31.1.200

          // the client authenticates with web browser. The WLC applies new ACL for that client.

*apfReceiveTask: Jan 31 13:13:56.112: 00:0e:2e:ce:68:94 Received SGT for this Client.
*apfReceiveTask: Jan 31 13:13:56.112: 00:0e:2e:ce:68:94 AAA redirect is NULL. Skipping Web-auth for Radius NAC
enabled WLAN.
*apfReceiveTask: Jan 31 13:13:56.112: 00:0e:2e:ce:68:94 10.1.30.20 WEBAUTH_REQD (8) Changing IPv4 ACL 'none' (ACL ID
255) ===> 'none' (ACL ID 255) --- (caller apf_policy.c:1697)
*apfReceiveTask: Jan 31 13:13:56.112: 00:0e:2e:ce:68:94 10.1.30.20 WEBAUTH_REQD (8) Changing IPv6 ACL 'none' (ACL ID
255) ===> 'none' (ACL ID 255) --- (caller apf_policy.c:1864)
*apfReceiveTask: Jan 31 13:13:56.112: 00:0e:2e:ce:68:94 apfApplyWlanPolicy: Retaining the ACL recieved in AAA
attributes 255 on mobile
*apfReceiveTask: Jan 31 13:13:56.112: 00:0e:2e:ce:68:94 Inserting AAA Override struct for mobile
        MAC: 00:0e:2e:ce:68:94, source 2

*apfReceiveTask: Jan 31 13:13:56.112: 00:0e:2e:ce:68:94 10.1.30.20 WEBAUTH_REQD (8) Changing IPv4 ACL 'none' (ACL ID
255) ===> 'ACL_INTERNET_ONLY' (ACL ID 0) --- (caller apf_policy.c:1750)
*apfReceiveTask: Jan 31 13:13:56.112: 00:0e:2e:ce:68:94 apfMs1xStateDec
*apfReceiveTask: Jan 31 13:13:56.112: 00:0e:2e:ce:68:94 10.1.30.20 WEBAUTH_REQD (8) Change state to START (0) last
state WEBAUTH_REQD (8)

<snip>
```

LAB 3.15. Configure ISE for Guest Access

Objectives

This lab shows how to configure guest access on ISE and wireless controller.

IP Addressing and devices

Device	Interface	IP address
ISE	NIC	172.31.1.20
R1	Lo0 E0/0 E0/1	1.1.1.1/32 10.1.10.1/24 172.31.1.1/24
AD	NIC	172.31.1.200
WinXP	NIC	10.1.10.50/24
WLC	G0/0/1 (mgmt.) G0/0/2	10.1.10.5/24 10.1.30.5/24
ASA1	G0/0 (outside) G0/1 (inside) G0/2 (dmz)	100.2.2.10/24 10.1.10.10/24 10.1.30.10/24
Win7 PC	LAN NIC (LAB-Network) WLAN NIC	DHCP-Assigned 10.1.30.x (DHCP)

Task

Configure Guest Portal at http://guest.micronics.local with the following properties:

- no Acceptable Use Policy (AUC) is displayed for guests
- Guest users can create accounts for themselves
- new account have the following attributes:
    - account is valid for 8 hours staring from the first login
    - default timezone is set to UTC
    - account is valid only Mon-Fri
    - account belongs to Guest role
    - login name is an email of the user

- guest user must provide at least First Name, Company Name and his email to create an account
- password must be auto-generated based on at least 4 alphabetic characters and 2 numbers and not contain any special characters

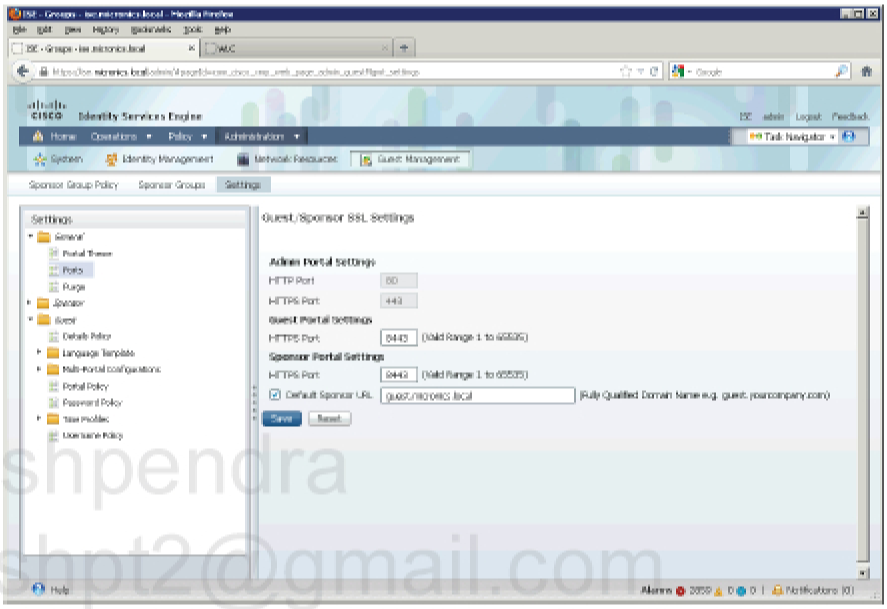
Guest users should get access to Internet only after successful authentication.

Configuration

Complete these steps:

Step 1 ISE configuration. Configure Guest Portal settings.

- Go to **Administration > Guest Management > Settings > General > Ports** and enter **guest.micronics.local** into **Default Sponsor URL** field. Click **Save**.



Guest/Sponsor SSL Settings

Admin Portal Settings

HTTP Port 80

HTTPS Port 443

Guest Portal Settings

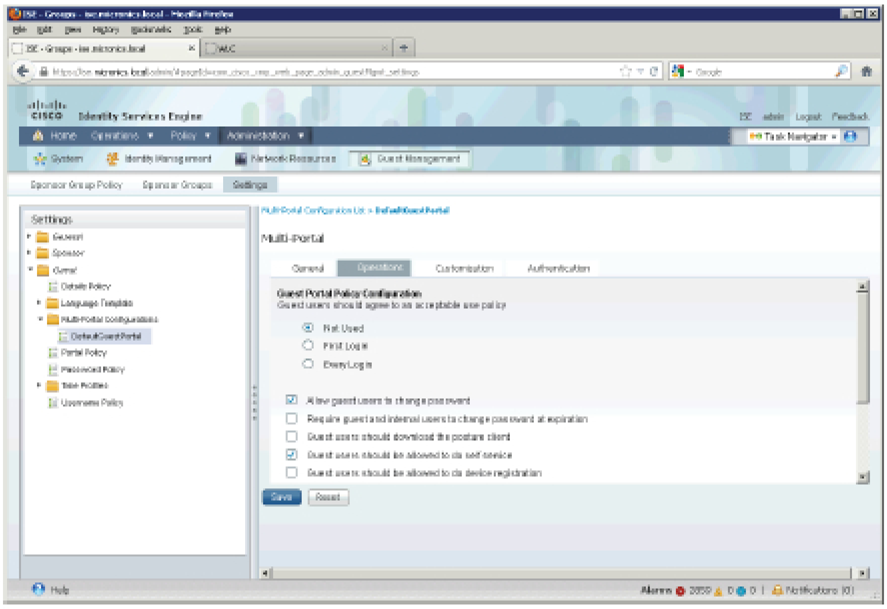
HTTPS Port 8443 (Valid Range 1 to 65535)

Sponsor Portal Settings

HTTPS Port 8443 (Valid Range 1 to 65535)

☑ Default Sponsor URL guest.micronics.local (Fully Qualified Domain Name e.g. guest.yourcompany.com)

- Go to **Administration > Guest Management > Settings > Guest > Multi-Portal Configuration > DefaultGuestPortal > Operations (tab)** and disable AUC on that portal. Enable **Guest users should be allowed to do self service** option. Click **Save**.



Multi-Portal Configuration List > DefaultGuestPortal

Multi-Portal

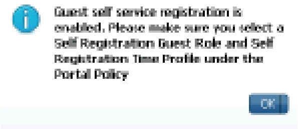
Guest Portal Policy Configuration

Guest users should agree to an acceptable use policy

● Not Used
○ First Login
○ Every Login

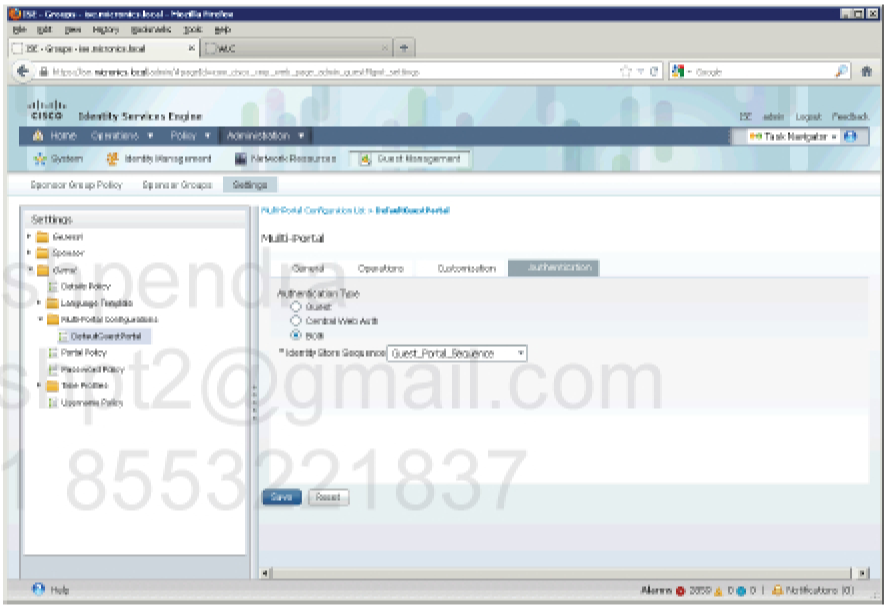
☑ Allow guest users to change password
☐ Require guest and internal users to change password at expiration
☐ Guest users should download the posture client
☑ Guest users should be allowed to do self service
☐ Guest users should be allowed to do device registration

- If self-service registration is enabled there must be two other options correctly configured. There is a message about that.



Guest self service registration is enabled. Please make sure you select a Self Registration Guest Role and Self Registration Time Profile under the Portal Policy

- Go to **Authentication** tab and check below settings. The **Guest_Portal_Sequence** defines Internal Users and AD users and was reconfigured in one of previous tasks.



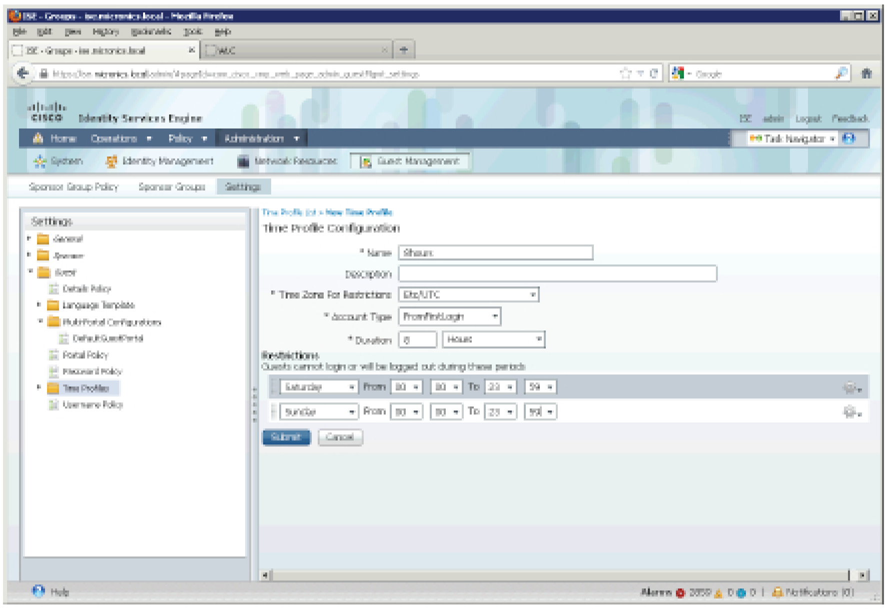
Multi-Portal Configuration List > DefaultGuestPortal

Multi-Portal

Authentication Type
○ Guest
○ Central Web Auth
● Both

* Identity Store Sequence: Guest_Portal_Sequence

- Go to **Administration > Guest Management > Settings > Guest > Time Profiles** and click **Add**. Enter a name for the profile e.g. **8hours** and specify settings as follows:



Time Profile List > New Time Profile

Time Profile Configuration

* Name: 8hours

Description:

* Time Zone For Restrictions: Etc/UTC

* Account Type: FromFirstLogin

* Duration: 8 Hours

Restrictions

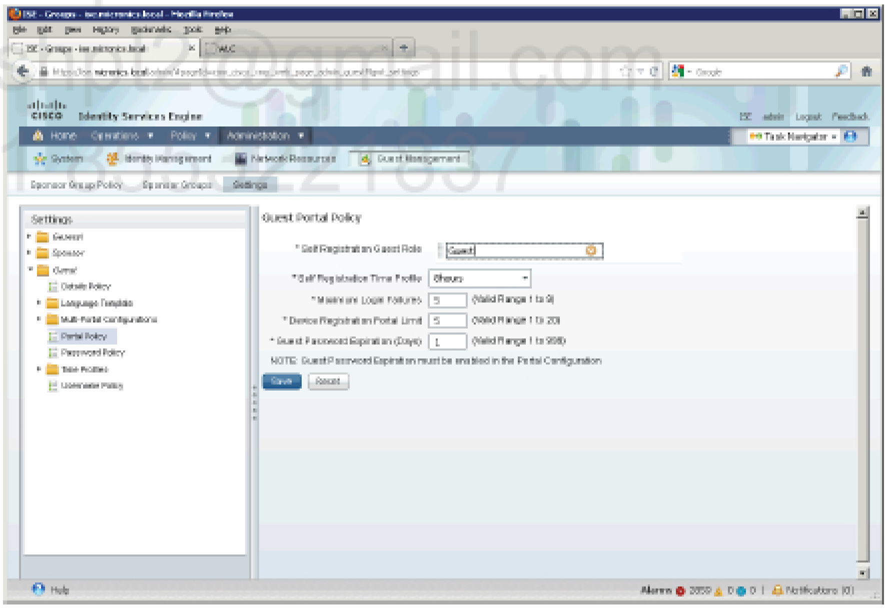
Guests cannot login or will be logged out during these periods

Saturday From 00 00 To 23 59

Sunday From 00 00 To 23 59

Submit Cancel

- Go to **Administration > Guest Management > Settings > Guest > Portal Policy** and set **Self Registration Guest Role** to **Guest** and assign **8hours** as **Self Registration Time Profile**. Click **Save**.



Guest Portal Policy

* Self Registration Guest Role: Guest

* Self Registration Time Profile: 8hours

* Maximum Login Failures: 5 (Valid Range 1 to 9)

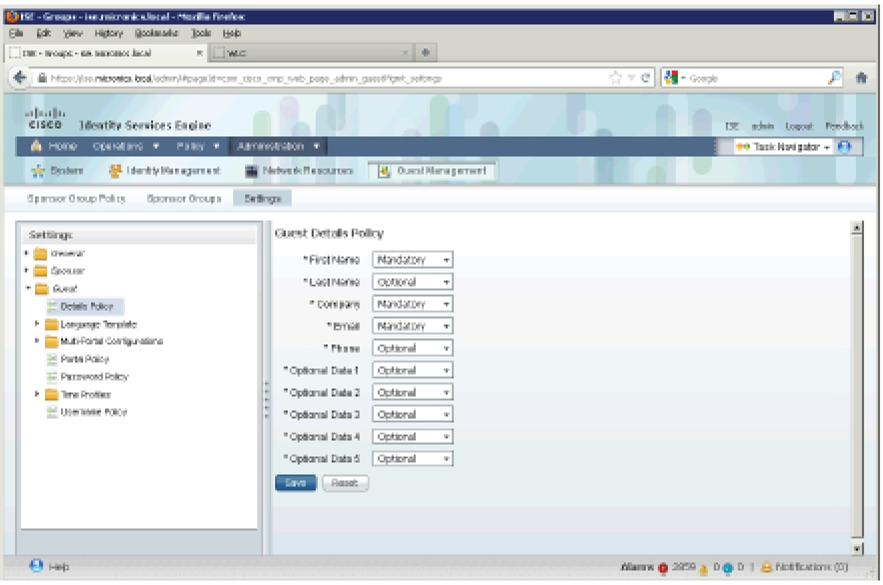
* Device Registration Portal Limit: 5 (Valid Range 1 to 20)

* Guest Password Expiration (Days): 1 (Valid Range 1 to 999)

NOTE: Guest Password Expiration must be enabled in the Portal Configuration

Save Reset

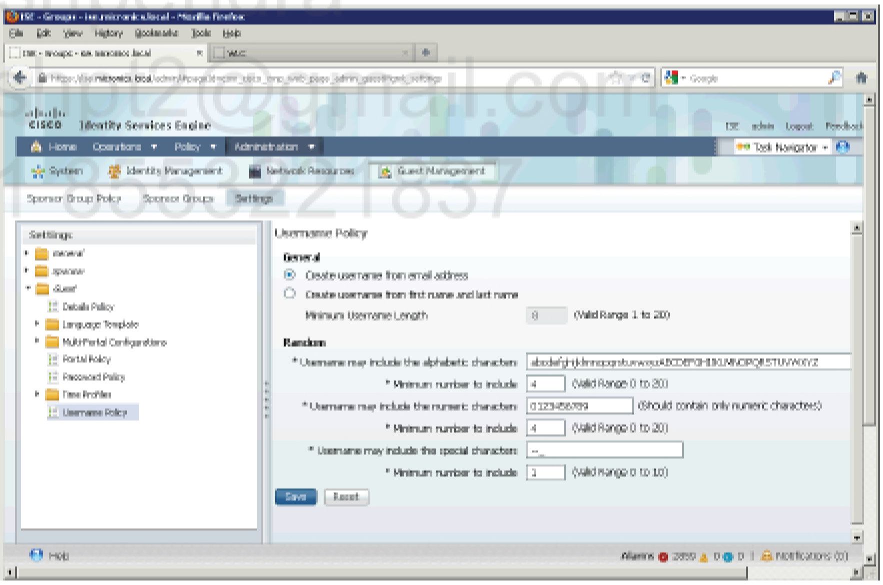
- Go to **Administration > Guest Management > Settings > Guest > Details Policy** and set **First Name, Company** and **Email** as **Mandatory** settings. Click **Save**.



Guest Details Policy

* First Name	Mandatory
* Last Name	Optional
* Company	Mandatory
* Email	Mandatory
* Phone	Optional
* Optional Data 1	Optional
* Optional Data 2	Optional
* Optional Data 3	Optional
* Optional Data 4	Optional
* Optional Data 5	Optional

- Go to **Administration > Guest Management > Settings > Guest > Username Policy** and check **Create username from email address** option. Click **Save.**



Username Policy

General

● Create username from email address

○ Create username from first name and last name

Minimum Username Length 8 (Valid Range 1 to 20)

Random

* Username may include the alphabetic characters: abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ

* Minimum number to include 4 (Valid Range 0 to 20)

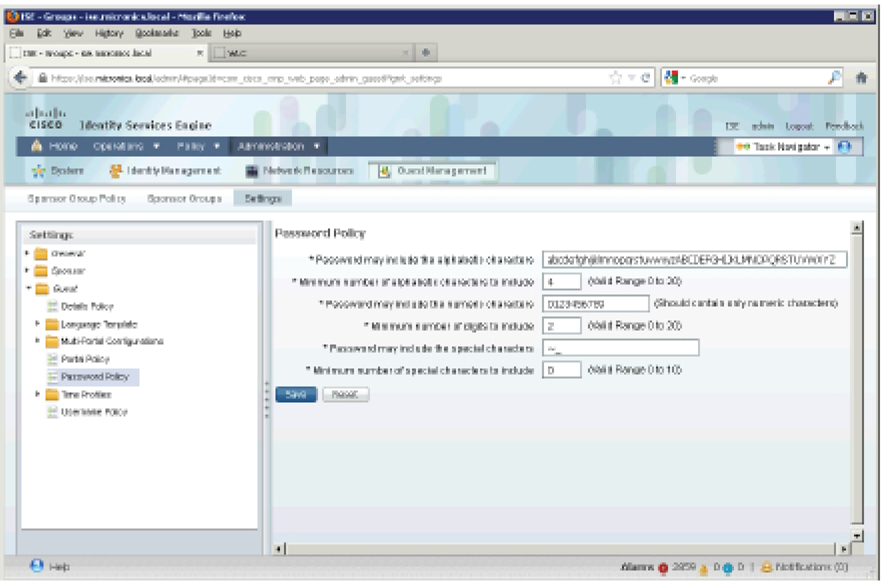
* Username may include the numeric characters: 0123456789 (Should contain only numeric characters)

* Minimum number to include 4 (Valid Range 0 to 20)

* Username may include the special characters: -_

* Minimum number to include 1 (Valid Range 0 to 10)

- Go to **Administration > Guest Management > Settings > Guest > Password Policy** and set **Minimum number of special characters to include** to **0** and **Minimum number of digits to include** to **2**. Click **Save**.



Password Policy

* Password may include the alphabetic characters: abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ

* Minimum number of alphabetic characters to include: 4 (Valid Range 0 to 20)

* Password may include the numeric characters: 0123456789 (Should contain only numeric characters)

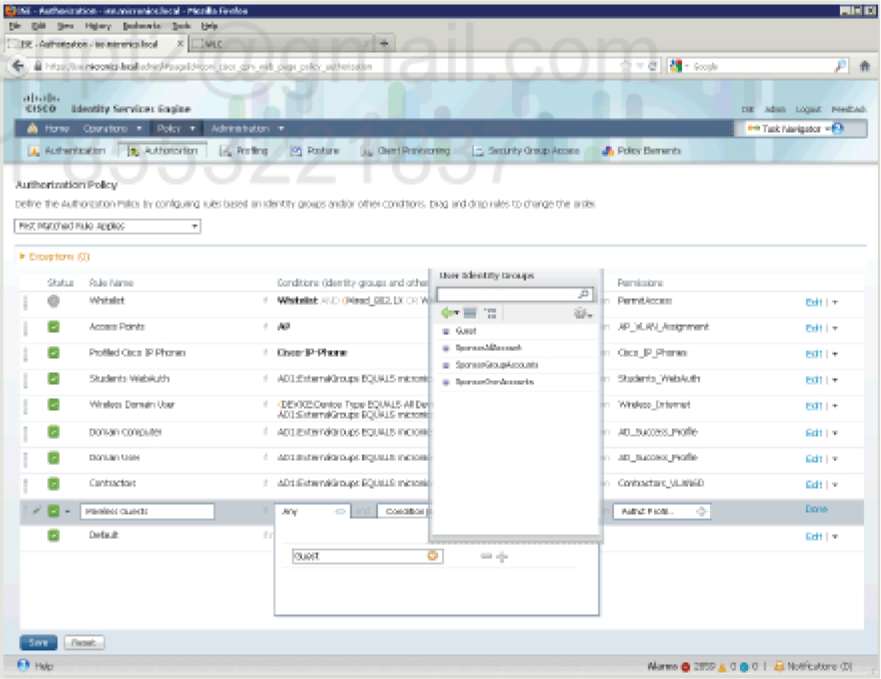
* Minimum number of digits to include: 2 (Valid Range 0 to 20)

* Password may include the special characters: ~_

* Minimum number of special characters to include: 0 (Valid Range 0 to 10)

Step 2 Create new authorization rule for Guests.

- Go to **Policy > Authorization** and add new rule at the end. Enter a name for the rule e.g. **Wireless Guests** and set identity groups condition to **Guest**.



Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

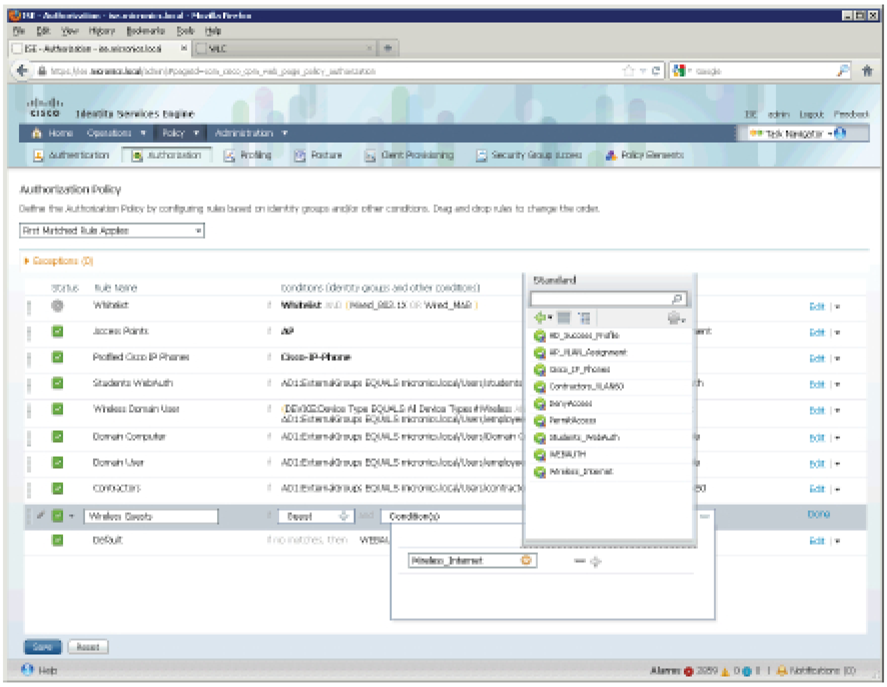
Exceptions (0)

Status	Rule Name	Conditions (identity groups and other	Permissions
	Whitelist	Whitelist AND (Wired_802.1X OR W	PermitAccess
✓	Access Points	AP	AP_VLAN_Assignment
✓	Profiled Cisco IP Phones	Cisco-IP-Phone	Cisco_IP_Phones
✓	Students WebAuth	AD1:ExternalGroups EQUALS microni	Students_WebAuth
✓	Wireless Domain User	(DEVICE:Device Type EQUALS All De AD1:ExternalGroups EQUALS microni	Wireless_Internet
✓	Domain Computer	AD1:ExternalGroups EQUALS microni	AD_Success_Profile
✓	Domain User	AD1:ExternalGroups EQUALS microni	AD_Success_Profile
✓	Contractors	AD1:ExternalGroups EQUALS microni	Contractors_VLAN60
✓	Wireless Guests	Any and Condition(s)	AuthZ Profil...
✓	Default		

User Identity Groups: Guest, SponsorAllAccount, SponsorGroupAccounts, SponsorOwnAccounts

Selected: Guest

- Set permissions to **Wireless_Internet** authorization profile. This profile has ACL_REDIRECT for WLC configured.


ISE - Authorization - ise.micronics.local - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Identity Services Engine
Home Operations Policy Administration
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements
Standard
AD_Success_Profile
AP_VLAN_Assignment
Cisco_IP_Phones
Contractors_VLAN50
DenyAccess
PermitAccess
Students_WebAuth
WEBAUTH
Wireless_Internet
Save
Reset
Help

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

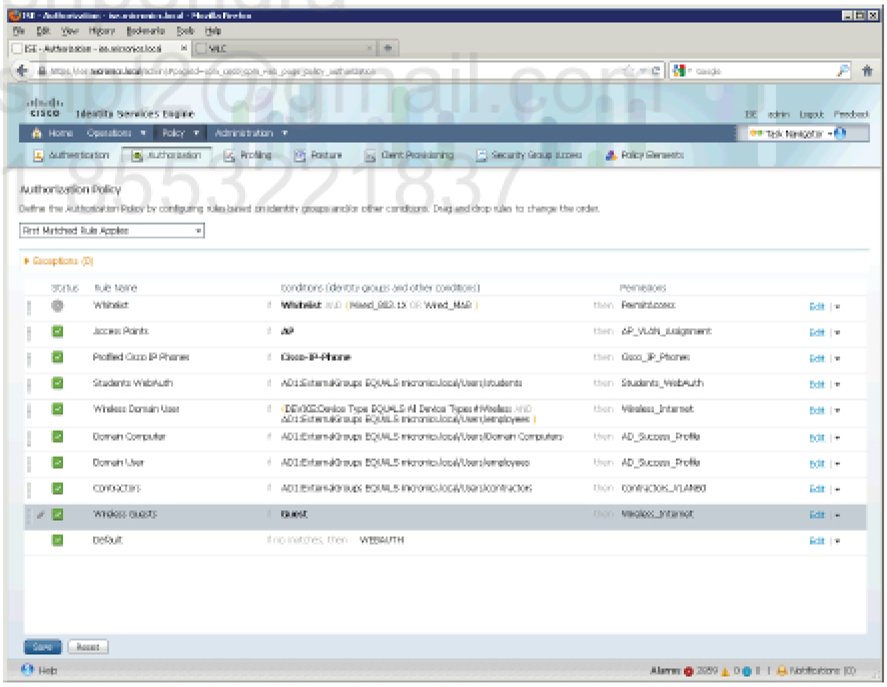
Exceptions (0)

Status	Rule Name		Conditions (identity groups and other conditions)
	Whitelist	if	Whitelist AND (Wired_802.1X OR Wired_MAB)
✓	Access Points	if	AP
✓	Profiled Cisco IP Phones	if	Cisco-IP-Phone
✓	Students WebAuth	if	AD1:ExternalGroups EQUALS micronics.local/Users/students
✓	Wireless Domain User	if	(DEVICE:Device Type EQUALS All Device Types#Wireless AND AD1:ExternalGroups EQUALS micronics.local/Users/employees
✓	Domain Computer	if	AD1:ExternalGroups EQUALS micronics.local/Users/Domain C
✓	Domain User	if	AD1:ExternalGroups EQUALS micronics.local/Users/employee
✓	Contractors	if	AD1:ExternalGroups EQUALS micronics.local/Users/contracto
✓	Wireless Guests	if	Guest and Condition(s)
✓	Default		if no matches, then WEBAU

Wireless_Internet

Done

- Click **Done** and **Save** to apply the changes.


ISE - Authorization - ise.micronics.local - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Identity Services Engine
Home Operations Policy Administration
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements
Save
Reset
Help

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

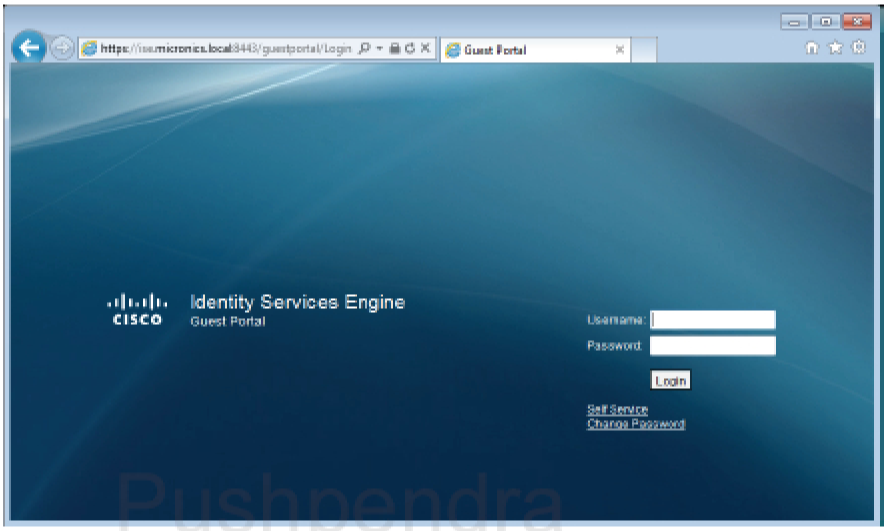
Exceptions (0)

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
	Whitelist	if	Whitelist AND (Wired_802.1X OR Wired_MAB)	then	PermitAccess
✓	Access Points	if	AP	then	AP_VLAN_Assignment
✓	Profiled Cisco IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phones
✓	Students WebAuth	if	AD1:ExternalGroups EQUALS micronics.local/Users/students	then	Students_WebAuth
✓	Wireless Domain User	if	(DEVICE:Device Type EQUALS All Device Types#Wireless AND AD1:ExternalGroups EQUALS micronics.local/Users/employees)	then	Wireless_Internet
✓	Domain Computer	if	AD1:ExternalGroups EQUALS micronics.local/Users/Domain Computers	then	AD_Success_Profile
✓	Domain User	if	AD1:ExternalGroups EQUALS micronics.local/Users/employees	then	AD_Success_Profile
✓	Contractors	if	AD1:ExternalGroups EQUALS micronics.local/Users/contractors	then	Contractors_VLAN50
✓	Wireless Guests	if	Guest	then	Wireless_Internet
✓	Default		if no matches, then WEBAUTH		

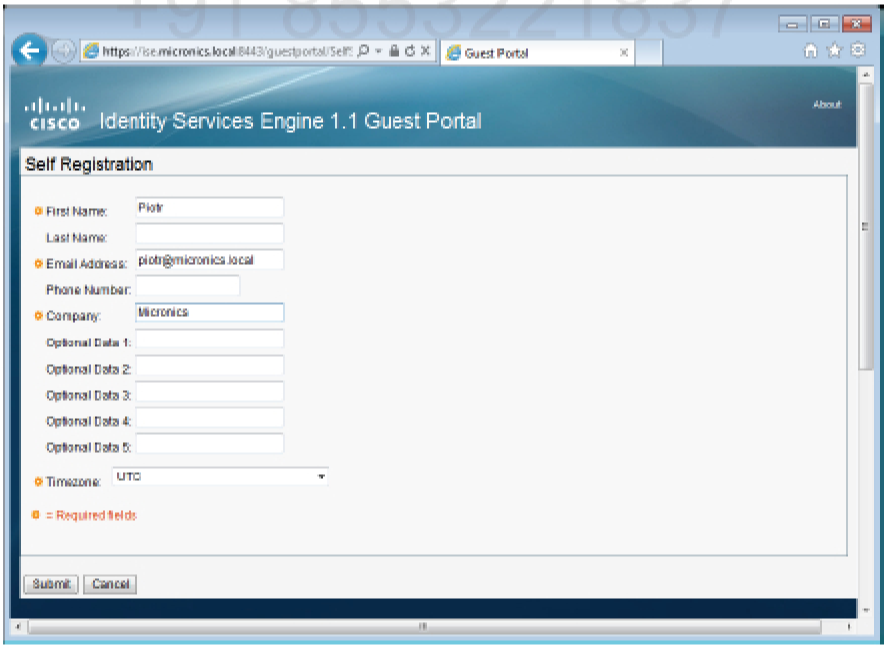
Verification

Go to Win7 PC and bounce Wireless NIC. Then connect to MICRONICS SSID. The connection should be successful as the network is open.

Open up web browser and enter http://guest.micronics.local



Click on **Self Service** link. You should be moved to **Self Registration** portal. Fill up all required fields and click **Submit**.

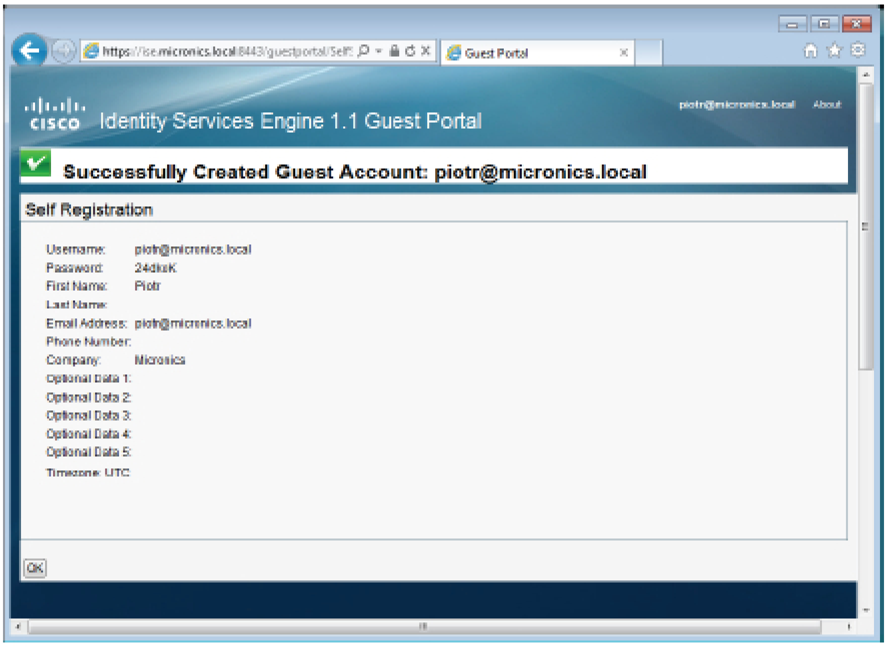

https://ise.micronics.local:8443/guestportal/Self
Guest Portal
cisco
Identity Services Engine 1.1 Guest Portal
About
Submit
Cancel

Self Registration

- First Name: Piotr
- Last Name:
- Email Address: piotr@micronics.local
- Phone Number:
- Company: Micronics
- Optional Data 1:
- Optional Data 2:
- Optional Data 3:
- Optional Data 4:
- Optional Data 5:
- Timezone: UTC

= Required fields

You should get details of new auto-generated account. Check if this suffices all task requirements. Write down user credentials and click **OK**.



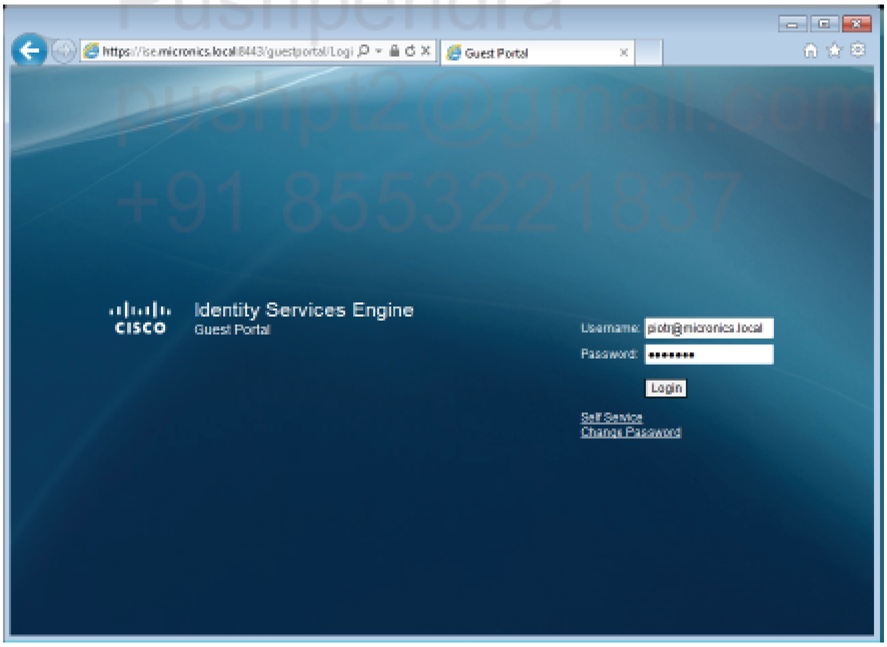
Identity Services Engine 1.1 Guest Portal

Successfully Created Guest Account: piotr@micronics.local

Self Registration

Username:	piotr@micronics.local
Password:	24dkzK
First Name:	Piotr
Last Name:	
Email Address:	piotr@micronics.local
Phone Number:	
Company:	Micronics
Optional Data 1:	
Optional Data 2:	
Optional Data 3:	
Optional Data 4:	
Optional Data 5:	
Timezone: UTC	

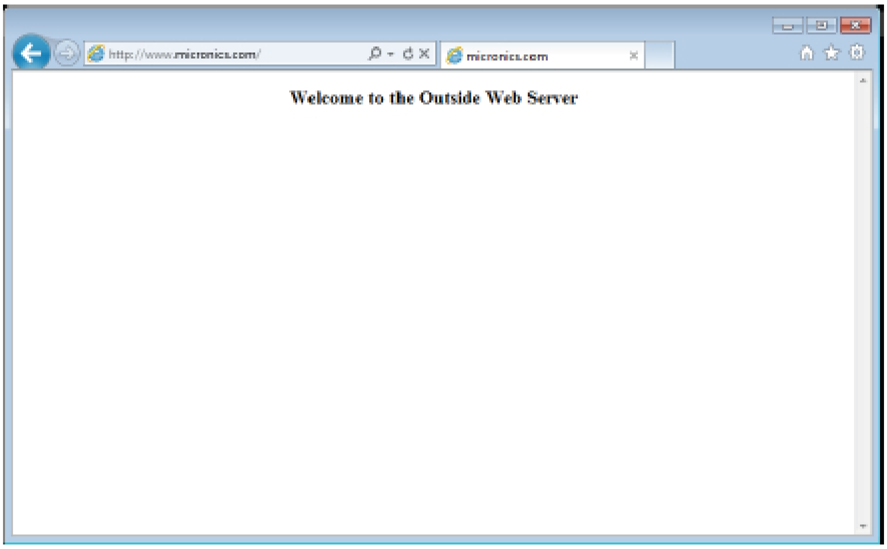
Provide new user credentials and log in to the Guest Portal.



Identity Services Engine
Guest Portal

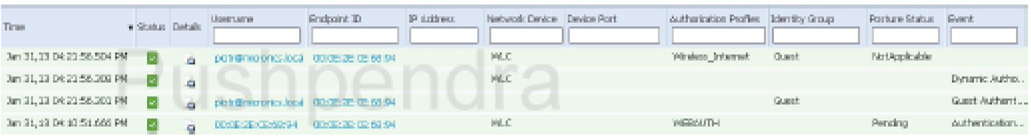
Username: piotr@micronics.local
Password: ••••••••

Now you should be able to connect to any Website without being redirected to the Guest Portal.



Welcome to the Outside Web Server

Check ISE logs.



Time	Status	Details	Username	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Identity Group	Posture Status	Event
Jan 31,13 04:23:56.504 PM	✓		pod1@micronics.local	00:0E:2E:C2:68:94		WLC		Wireless_Internet	Guest	NotApplicable	
Jan 31,13 04:23:56.208 PM	✓					WLC					Dynamic Autho...
Jan 31,13 04:23:56.201 PM	✓		pod1@micronics.local	00:0E:2E:C2:68:94					Guest		Guest Authent...
Jan 31,13 04:10:51.666 PM	✓		00:0E:2E:C2:68:94	00:0E:2E:C2:68:94		WLC		WEBAUTH		Pending	Authentication...

LAB 3.16. Configure ISE Profiler

Objectives

This lab shows how to configure profiling services on ISE.

IP Addressing and devices

Device	Interface	IP address
ISE	NIC	172.31.1.20
WinXP	NIC	10.1.10.50/24
Win7 PC	LAN NIC (LAB-Network) WLAN NIC	DHCP-Assigned 10.1.30.x (DHCP)

Task

Configure ISE profiling services to discover Win7 PC. Use DHCP, RADIUS and SNMP services on SW1. Configure SNMP v2c on the switch with read-only community string of 'cisco123' and polling interval of 600 seconds. The Windows client should be recognized based on its hostname carried in DHCP packets. Configure new profiling policy so that WIN7-PC endpoint profile will be created and use it in Domain Computers authorization rule.

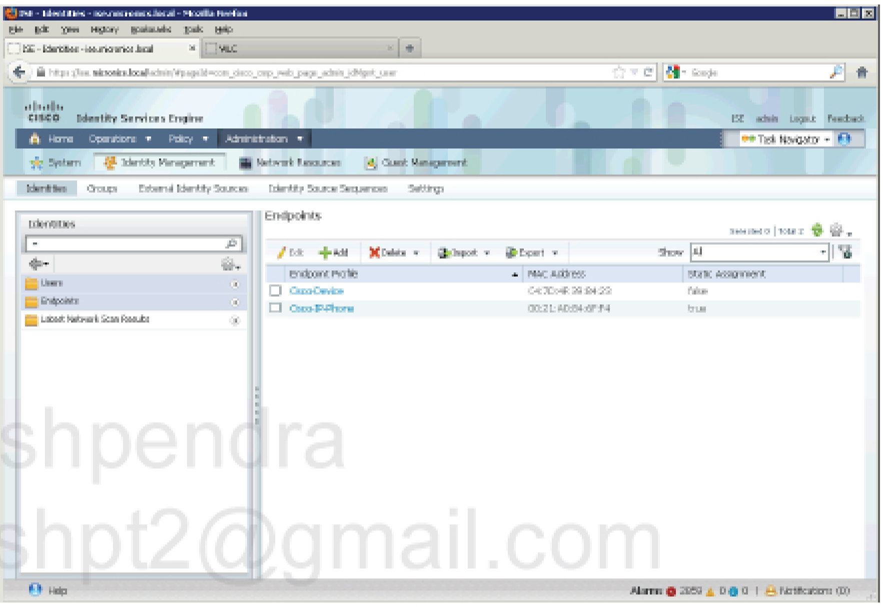
Configuration

Complete these steps:

Step 0 Check what devices ISE knows about (Internal Endpoint list).

(opt.)

- Go to **Administration > Identity Management > Identities > Endpoints**. There are only two devices: **Cisco-Device** (which is AP) ad **Cisco-IP-Phone** (which is IP Phone). There is no Win7 PC.



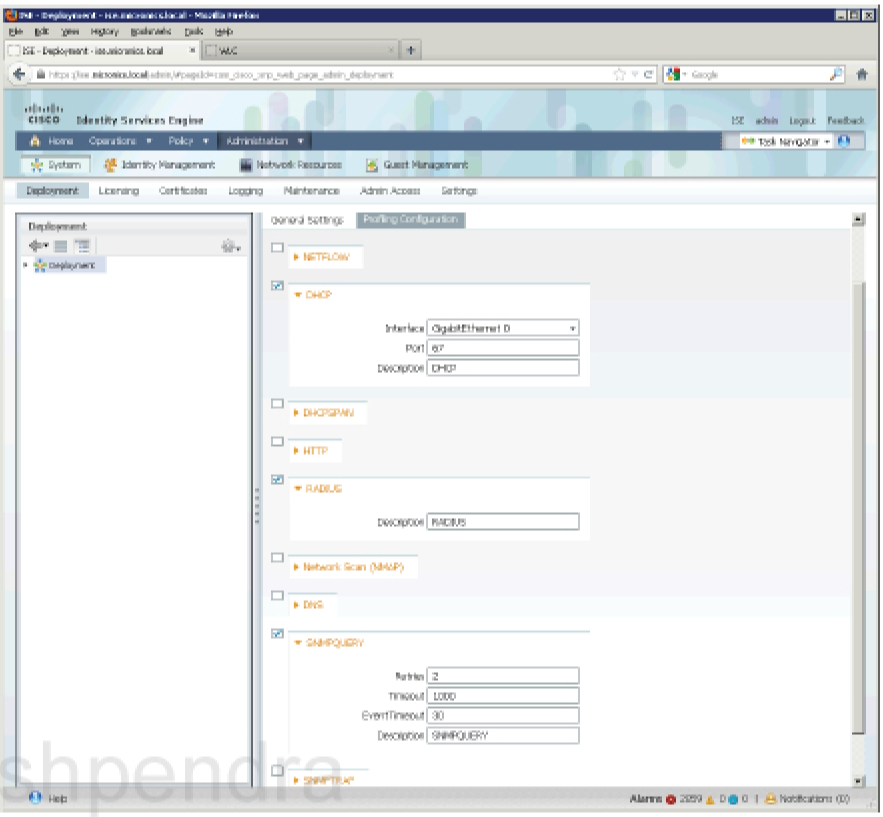
Endpoint Profile	MAC Address	Static Assignment
Cisco-Device	C4:7D:4F:39:B4:22	false
Cisco-IP-Phone	00:21:A0:B4:6F:F4	true

Step 1 Switch configuration.

```
!
snmp-server community cisco123 RO
snmp-server enable traps snmp linkdown linkup
snmp-server enable traps mac-notification change move
snmp-server host 172.31.1.20 version 2c cisco123
!
interface Vlan10
 ip helper-address 172.31.1.20
!
```

Step 2 ISE configuration. Enable Profiling services.

- Go to **Administration > System > Deployment** and click **ISE** on the list. Go to **Profiling Configuration** and check **DHCP, RADIUS** and **SNMPQUERY** options. Leave default settings for profiling services. Click **Save**.



☐ NETFLOW

☑ DHCP

Interface: GigabitEthernet 0
Port: 67
Description: DHCP

☐ DHCPSPAN

☐ HTTP

☑ RADIUS

Description: RADIUS

☐ Network Scan (NMAP)

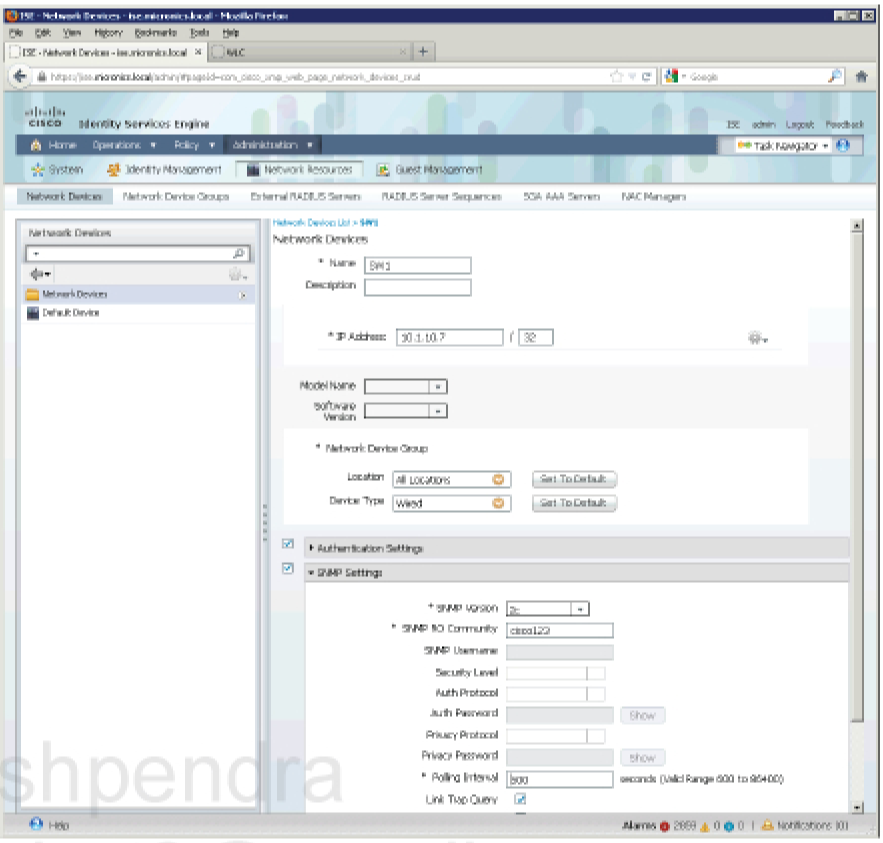
☐ DNS

☑ SNMPQUERY

Retries: 2
Timeout: 1000
EventTimeout: 30
Description: SNMPQUERY

☐ SNMPTRAP

- Go to **Administration > Network Resources > Network Devices** and click **SW1** on the list to edit it. Pick **SNMP Settings** checkbox and configure SNMP v2c with community string of 'cisco123' for that device. Set **Polling Interval** to **600**. Click **Save**.


ISE - Network Devices - ise.micronics.local - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Identity Services Engine
Home Operations Policy Administration
Task Navigator
System Identity Management Network Resources Guest Management
Network Devices Network Device Groups External RADIUS Servers RADIUS Server Sequences SGA AAA Servers NAC Managers
Network Devices
Default Device
Network Device List > SW1
Help
Alarms 2859 0 0 Notifications (0)

Network Devices

* Name: SW1

Description:

* IP Address: 10.1.10.7 / 32

Model Name:

Software Version:

* Network Device Group

Location: All Locations Set To Default

Device Type: Wired Set To Default

☑ ▸ Authentication Settings

☑ ▾ SNMP Settings

* SNMP Version: 2c

* SNMP RO Community: cisco123

SNMP Username:

Security Level:

Auth Protocol:

Auth Password: Show

Privacy Protocol:

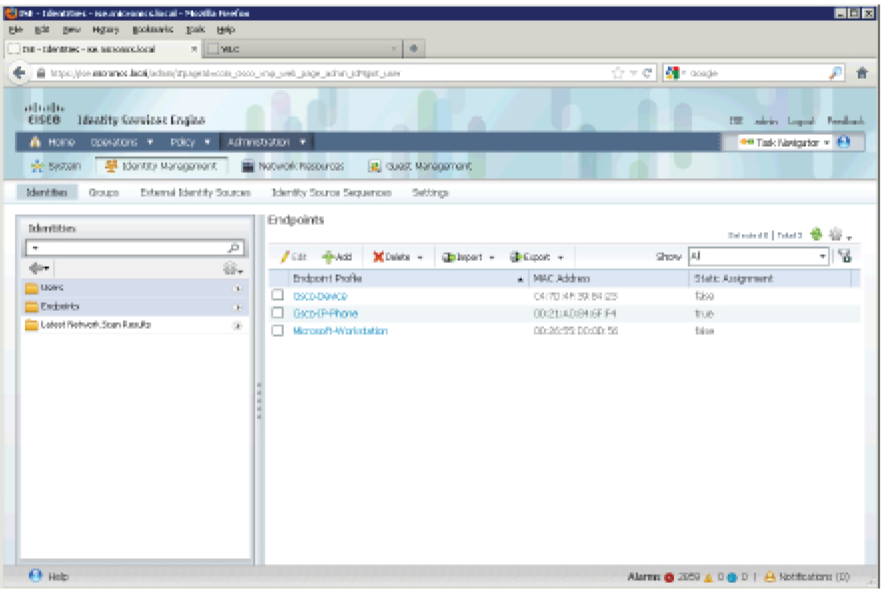
Privacy Password: Show

* Polling Interval: 600 seconds (Valid Range 600 to 86400)

Link Trap Query: ☑

Step 3 Check if ISE profiled other devices.

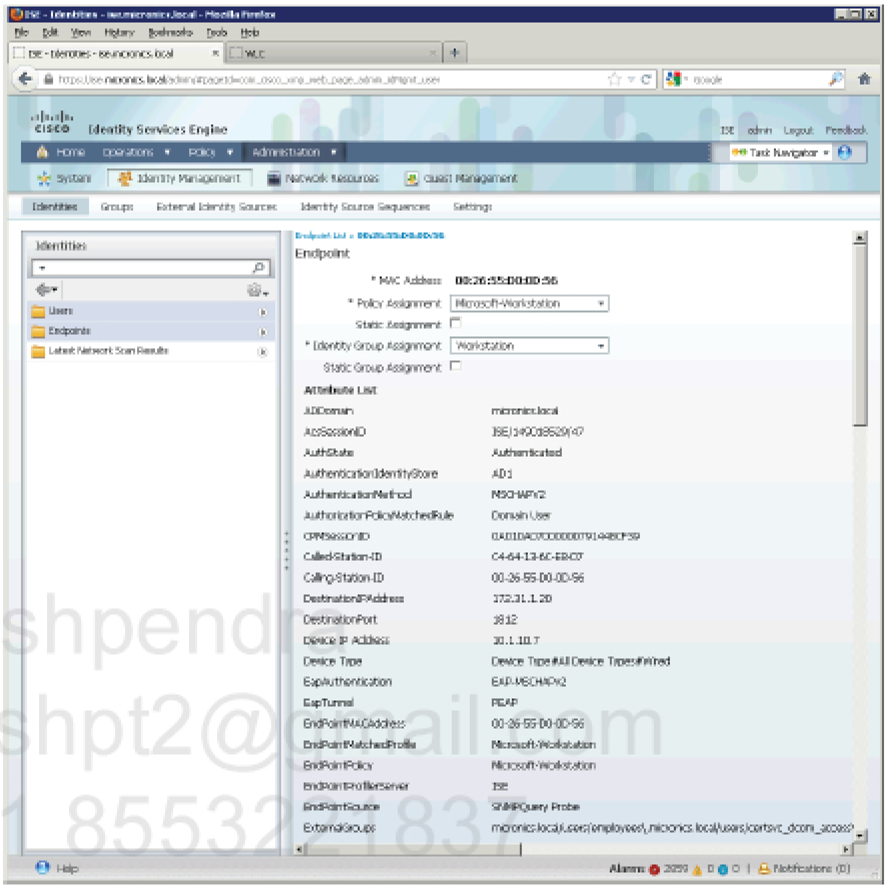
- Go to **Administration > Identity Management > Identities > Endpoints**. There are only two devices: **Cisco-Device** (which is AP) ad **Cisco-IP-Phone** (which is IP Phone). Now you should see **Microsoft-Workstation** on the list. This is our Win7 PC.


ISE - Identities - ise.micronics.local - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Identity Services Engine
Home Operations Policy Administration
Task Navigator
System Identity Management Network Resources Guest Management
Identities Groups External Identity Sources Identity Source Sequences Settings
Identities
Users
Endpoints
Latest Network Scan Results
Edit Add Delete Import Export
Show All
Help
Alarms 2859 0 0 Notifications (0)

Endpoints

	Endpoint Profile	MAC Address	Static Assignment
□	Cisco-Device	C4:7D:4F:39:B4:23	false
□	Cisco-IP-Phone	00:21:A0:84:6F:F4	true
□	Microsoft-Workstation	00:26:55:DD:0D:56	false

- Click on the new device to see more details. There are attributes from different sources. First we see attributes taken from RADIUS messages.


ISE - Identities - ise.micronics.local - Mozilla Firefox
File Edit View History Bookmarks Tools Help
ISE - Identities - ise.micronics.local
WLC
https://ise.micronics.local/admin/#pageId=com_cisco_xmp_web_page_admin_idmgmt_user
Google
Identity Services Engine
ISE admin Logout Feedback
Home Operations Policy Administration
Task Navigator
System Identity Management Network Resources Guest Management
Identities Groups External Identity Sources Identity Source Sequences Settings
Identities
Users
Endpoints
Latest Network Scan Results
Endpoint List » 00:26:55:D0:0D:56
Endpoint
Help
Alarms 2059 0 0 Notifications (0)

* MAC Address 00:26:55:D0:0D:56

* Policy Assignment Microsoft-Workstation

Static Assignment ☐

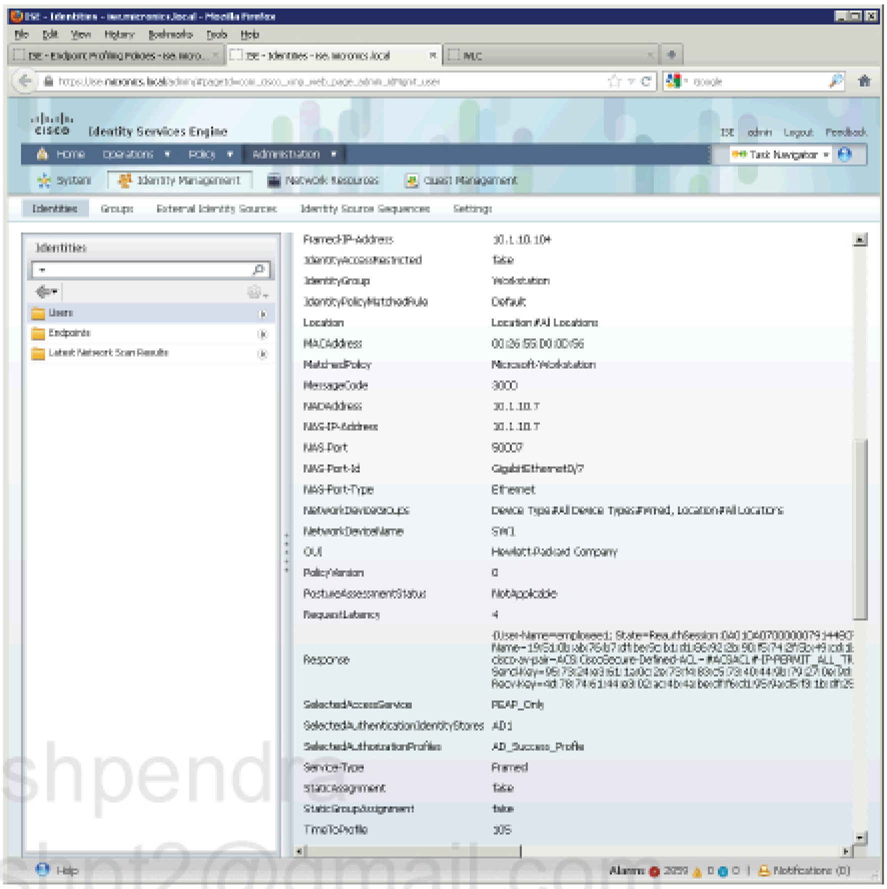
* Identity Group Assignment Workstation

Static Group Assignment ☐

Attribute List

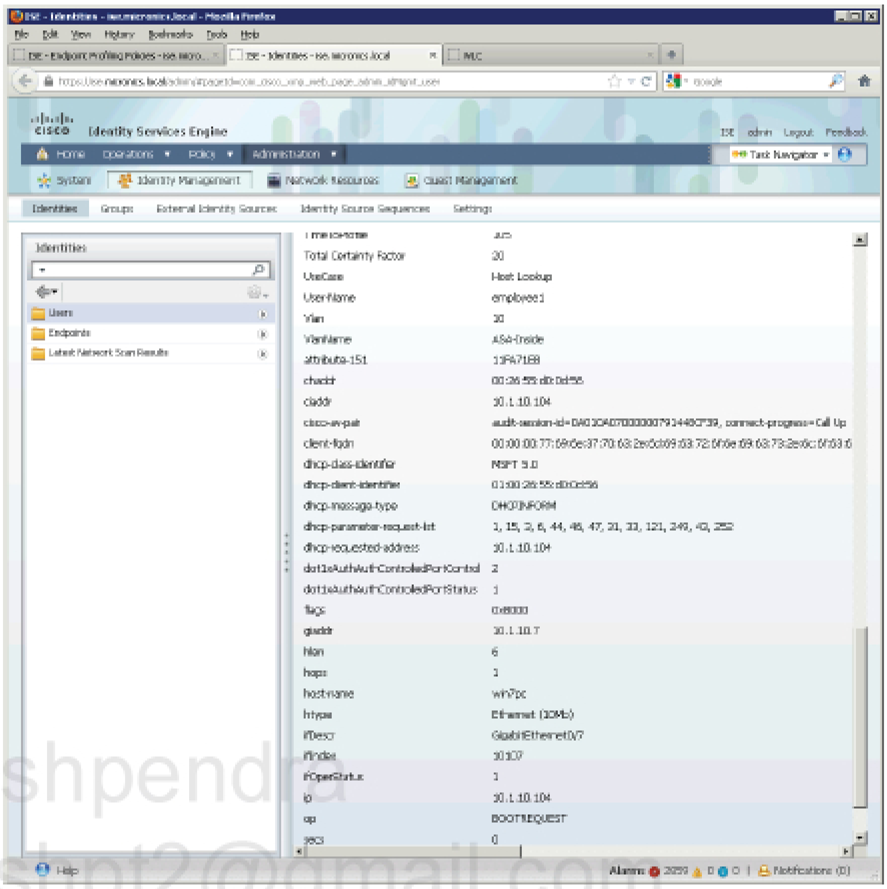
ADDomain	micronics.local
AcsSessionID	ISE/149018529/47
AuthState	Authenticated
AuthenticationIdentityStore	AD1
AuthenticationMethod	MSCHAPV2
AuthorizationPolicyMatchedRule	Domain User
CPMSessionID	0A010A07000000791448CF59
Called-Station-ID	C4-64-13-6C-E8-07
Calling-Station-ID	00-26-55-D0-0D-56
DestinationIPAddress	172.31.1.20
DestinationPort	1812
Device IP Address	10.1.10.7
Device Type	Device Type#All Device Types#Wired
EapAuthentication	EAP-MSCHAPV2
EapTunnel	PEAP
EndPointMACAddress	00-26-55-D0-0D-56
EndPointMatchedProfile	Microsoft-Workstation
EndPointPolicy	Microsoft-Workstation
EndPointProfilerServer	ISE
EndPointSource	SNMPQuery Probe
ExternalGroups	micronics.local/Users/employees\,micronics.local/users/certsvc_dcom_access

- Scroll down to see more. There are more attributes from RADIUS.



Framed-IP-Address	10.1.10.104
IdentityAccessRestricted	false
IdentityGroup	Workstation
IdentityPolicyMatchedRule	Default
Location	Location#All Locations
MACAddress	00:26:55:D0:0D:56
MatchedPolicy	Microsoft-Workstation
MessageCode	3000
NADAddress	10.1.10.7
NAS-IP-Address	10.1.10.7
NAS-Port	50007
NAS-Port-Id	GigabitEthernet0/7
NAS-Port-Type	Ethernet
NetworkDeviceGroups	Device Type#All Device Types#Wired, Location#All Locations
NetworkDeviceName	SW1
OUI	Hewlett-Packard Company
PolicyVersion	0
PostureAssessmentStatus	NotApplicable
RequestLatency	4
Response	{User-Name=employee1; State=ReauthSession:0A010A0700000079 ... Name=19:51:0b:ab:76:b7:df:be:9c:b1:d1:86:92:2b:90:f5:74:2f:3c:49:cd:... cisco-av-pair=ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-PERMIT_ALL_TR... Send-Key=95:73:24:a3:61:1a:0c:2e:73:f4:83:c5:73:40:44:9b:79:27:0e:9d:... Recv-Key=4d:78:74:61:44:a3:02:ac:4b:4a:be:df:f6:d1:95:9a:d5:f3:1b:df:2...
SelectedAccessService	PEAP_Only
SelectedAuthenticationIdentityStores	AD1
SelectedAuthorizationProfiles	AD_Success_Profile
Service-Type	Framed
StaticAssignment	false
StaticGroupAssignment	false
TimeToProfile	105

- Scroll down. There are attributes taken from DHCP messages. There is an attribute **host-name** based on which we can create our profiling rule.

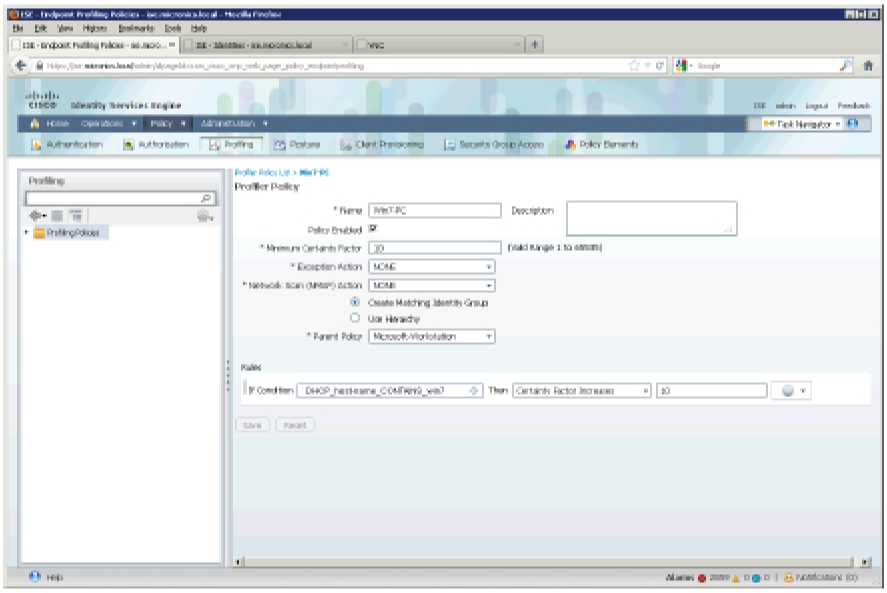


TimeToProfile	[illegible]
Total Certainty Factor	20
UseCase	Host Lookup
UserName	employee1
Vlan	10
VlanName	ASA-Inside
attribute-151	11FA71E8
chaddr	00:26:55:d0:0d:56
ciaddr	10.1.10.104
cisco-av-pair	audit-session-id=0A010A070000007914480739, connect-progress=Call Up
client-fqdn	00:00:00:77:69:6e:37:70:63:2e:6d:69:63:72:6f:6e:69:63:73:2e:6c:6f:63:6
dhcp-class-identifier	MSFT 5.0
dhcp-client-identifier	01:00:26:55:d0:0d:56
dhcp-message-type	DHCPINFORM
dhcp-parameter-request-list	1, 15, 3, 6, 44, 46, 47, 31, 33, 121, 249, 43, 252
dhcp-requested-address	10.1.10.104
dot1xAuthAuthControlledPortControl	2
dot1xAuthAuthControlledPortStatus	1
flags	0x8000
giaddr	10.1.10.7
hlen	6
hops	1
host-name	win7pc
htype	Ethernet (10Mb)
ifDescr	GigabitEthernet0/7
ifIndex	10107
ifOperStatus	1
ip	10.1.10.104
op	BOOTREQUEST
secs	0

ISE - Identities - ise.micronics.local - Mozilla Firefox
File Edit View History Bookmarks Tools Help
ISE - Endpoint Profiling Policies - ise.micro...
ISE - Identities - ise.micronics.local
WLC
https://ise.micronics.local/admin/#pageId=com_cisco_xmp_web_page_admin_idmgmt_user
Google
Identity Services Engine
ISE admin Logout Feedback
Home Operations Policy Administration
Task Navigator
System Identity Management Network Resources Guest Management
Identities Groups External Identity Sources Identity Source Sequences Settings
Identities
Users
Endpoints
Latest Network Scan Results
Help
Alarms 2059 0 0 Notifications (0)

Step 4 Create profiler policy to match 'win7' keyword and categorize Windows client.

- Go to **Policy > Profiling > Profiling Policies** and click **Add**. Enter **Win7-PC** as a name for new policy (this name will be used to create respective Endpoint Identity Group). Set **Minimum Certainty Factor** to **10** and pick **Windows-Workstation** as a **Parent Policy**. Add new rule at the bottom that **DHCP:host-name** attribute must contain keyword 'win7'. If this is true, increase the certainty factor by 10. Click **Save**.



Profiler Policy List > Win7-PC

Profiler Policy

* Name: Win7-PC

Description:

Policy Enabled: ☑

* Minimum Certainty Factor: 10 (Valid Range 1 to 65535)

* Exception Action: NONE

* Network Scan (NMAP) Action: NONE

● Create Matching Identity Group

○ Use Hierarchy

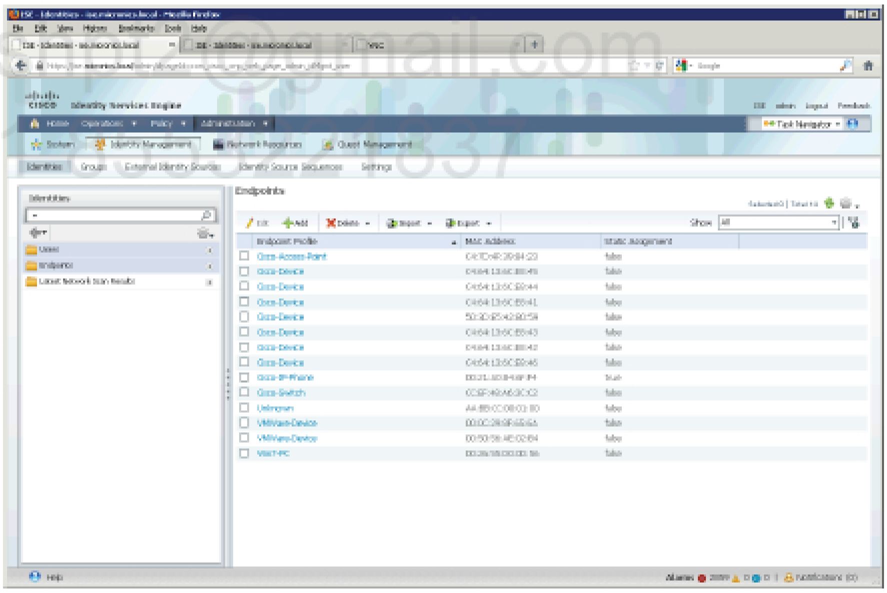
* Parent Policy: Microsoft-Workstation

Rules

If Condition: DHCP_hostname_CONTAINS_win7 Then: Certainty Factor Increases 10

Step 5 Check is profiling works.

- Go to **Administration > Identity Management > Identities > Endpoints**. There are now more devices on the list. You should see **Win7-PC** on the list.

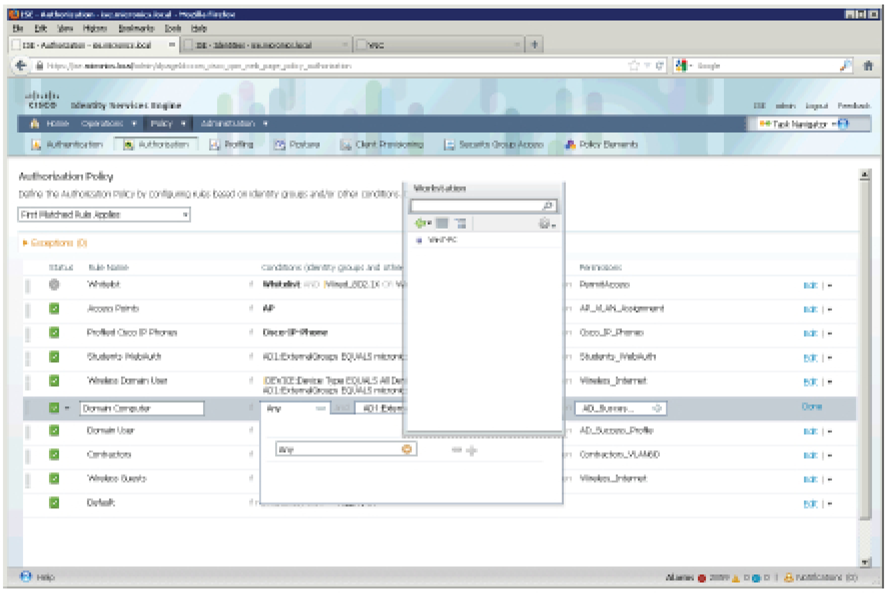


Endpoints

	Endpoint Profile	MAC Address	Static Assignment
□	Cisco-Access-Point	C4:7D:4F:39:B4:23	false
□	Cisco-Device	C4:64:13:6C:B0:45	false
□	Cisco-Device	C4:64:13:6C:B0:44	false
□	Cisco-Device	C4:64:13:6C:B5:41	false
□	Cisco-Device	50:3D:E5:42:B0:59	false
□	Cisco-Device	C4:64:13:6C:B5:43	false
□	Cisco-Device	C4:64:13:6C:B0:42	false
□	Cisco-Device	C4:64:13:6C:B0:46	false
□	Cisco-IP-Phone	00:21:A0:B4:6F:F4	true
□	Cisco-Switch	CC:EF:48:A6:3C:C2	false
□	Unknown	A4:BB:CC:08:C0:E0	false
□	VMWare-Device	00:0C:29:9F:65:6A	false
□	VMWare-Device	00:50:56:AE:02:B4	false
□	Win7-PC	00:26:55:DD:DD:56	false

Step 6 Based on above Endpoint Profile, change authorization rule.

- Go to **Policy > Authorization** and click **Edit** button next to **Domain Computer** rule. Click identity group condition list and pick **Win7-PC** from the profiled devices.



Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions.

First Matched Rule Applies

Exceptions (0)

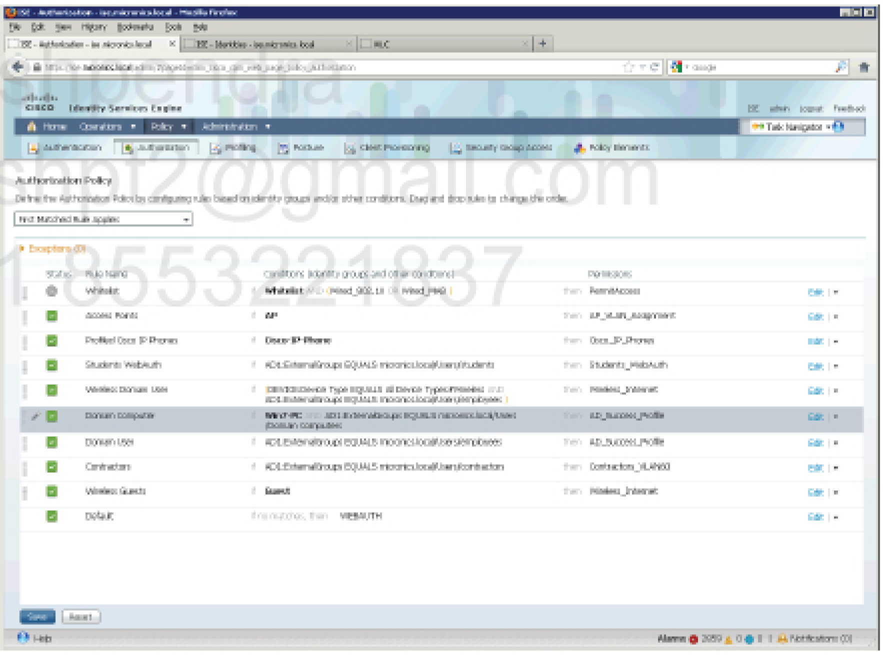
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
	Whitelist	if Whitelist AND (Wired_802.1X OR W	then PermitAccess
	Access Points	if AP	then AP_VLAN_Assignment
	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones
	Students WebAuth	if AD1:ExternalGroups EQUALS micronic	then Students_WebAuth
	Wireless Domain User	if (DEVICE:Device Type EQUALS All Dev AD1:ExternalGroups EQUALS micronic	then Wireless_Internet
	Domain Computer	if Any AND AD1:Extern	then AD_Success...
	Domain User	if	then AD_Success_Profile
	Contractors	if	then Contractors_VLAN60
	Wireless Guests	if	then Wireless_Internet
	Default	if	

Workstation

Win7-PC

Any

- Click **Done** and **Save**.



Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

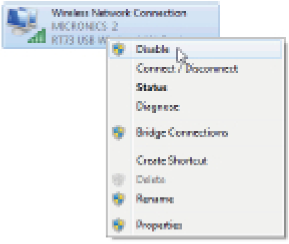
Exceptions (0)

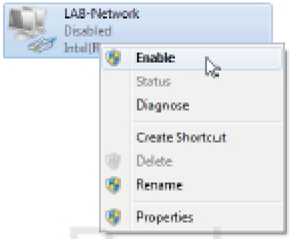
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
	Whitelist	if Whitelist AND (Wired_802.1X OR Wired_MAB)	then PermitAccess
	Access Points	if AP	then AP_VLAN_Assignment
	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones
	Students WebAuth	if AD1:ExternalGroups EQUALS micronics.local/Users/students	then Students_WebAuth
	Wireless Domain User	if (DEVICE:Device Type EQUALS All Device Types#Wireless AND AD1:ExternalGroups EQUALS micronics.local/Users/employees)	then Wireless_Internet
	Domain Computer	if Win7-PC AND AD1:ExternalGroups EQUALS micronics.local/Users/Domain computers	then AD_Success_Profile
	Domain User	if AD1:ExternalGroups EQUALS micronics.local/Users/employees	then AD_Success_Profile
	Contractors	if AD1:ExternalGroups EQUALS micronics.local/Users/contractors	then Contractors_VLAN60
	Wireless Guests	if Guest	then Wireless_Internet
	Default	if no matches, then WEBAUTH	

Verification

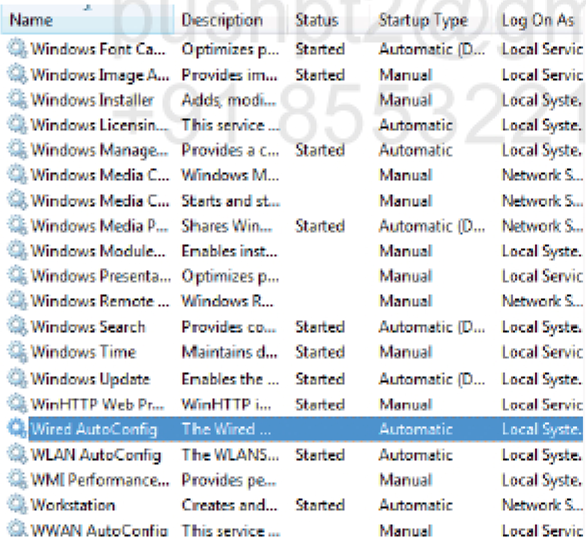
Some of verification steps have been done during the configuration.

Disable Wireless adapter and enable LAN NIC to trigger authentication.



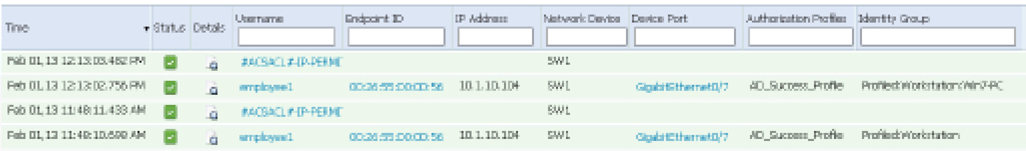


Enable **Wired AutoConfig** service. Authenticate using employee1 user.



Name	Description	Status	Startup Type	Log On As
Windows Font Ca...	Optimizes p...	Started	Automatic (D...	Local Servic
Windows Image A...	Provides im...	Started	Manual	Local Servic
Windows Installer	Adds, modi...		Manual	Local Syste.
Windows Licensin...	This service ...		Automatic	Local Syste.
Windows Manage...	Provides a c...	Started	Automatic	Local Syste.
Windows Media C...	Windows M...		Manual	Network S...
Windows Media C...	Starts and st...		Manual	Network S...
Windows Media P...	Shares Win...	Started	Automatic (D...	Network S...
Windows Module...	Enables inst...		Manual	Local Syste.
Windows Presenta...	Optimizes p...		Manual	Local Servic
Windows Remote ...	Windows R...		Manual	Network S...
Windows Search	Provides co...	Started	Automatic (D...	Local Syste.
Windows Time	Maintains d...	Started	Manual	Local Servic
Windows Update	Enables the ...	Started	Automatic (D...	Local Syste.
WinHTTP Web Pr...	WinHTTP i...	Started	Manual	Local Servic
Wired AutoConfig	The Wired ...		Automatic	Local Syste.
WLAN AutoConfig	The WLANS...	Started	Automatic	Local Syste.
WMI Performance...	Provides pe...		Manual	Local Syste.
Workstation	Creates and...	Started	Automatic	Network S...
WWAN AutoConfig	This service ...		Manual	Local Servic

Check ISE logs.



Time	Status	Details	Username	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Identity Group
Feb 01,13 12:13:03.482 PM	✓		#ACSACL#-IP-PERMI			SW1			
Feb 01,13 12:13:02.756 PM	✓		employee1	00:26:55:D0:CD:56	10.1.10.104	SW1	GigabitEthernet0/7	AD_Success_Profile	Profiled:Workstation:Win7-PC
Feb 01,13 11:48:11.433 AM	✓		#ACSACL#-IP-PERMI			SW1			
Feb 01,13 11:48:10.699 AM	✓		employee1	00:26:55:D0:CD:56	10.1.10.104	SW1	GigabitEthernet0/7	AD_Success_Profile	Profiled:Workstation

LAB 3.17. AnyConnect NAM

Objectives

This lab shows how to configure and use AnyConnect Network Access Manager instead of Win7 native supplicant.

IP Addressing and devices

Device	Interface	IP address
ISE	NIC	172.31.1.20
WinXP	NIC	10.1.10.50/24
Win7 PC	LAN NIC (LAB-Network) WLAN NIC	DHCP-Assigned 10.1.30.x (DHCP)

Task

Configure Win7 client PC to use Cisco AnyConnect Network Access Manager (NAM) as dot1x supplicant instead of native Windows 7 supplicant. The NAM must provide to the user a new network connection profile 'wired-peap' with PEAP/MS-CHAPv2 secure authentication method. Enable user and machine authentication with open mode. Do not cache user's credentials.

Configuration

Complete these steps:

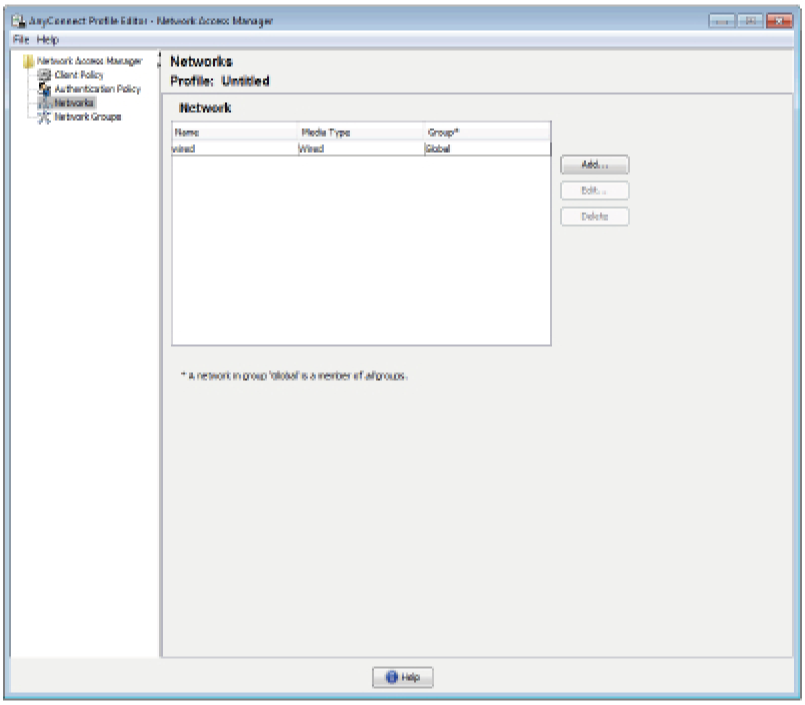
Step 0 Check switch configuration.

(opt.)

```
!
interface GigabitEthernet0/7
 description IPP + Win7
 switchport access vlan 10
 switchport mode access
 switchport nonegotiate
 switchport voice vlan 500
 ip access-group DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication port-control auto
 authentication violation protect
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 5
 spanning-tree portfast
!
```

Step 1 Run NAM Profile Editor and create configuration file.

- Run **Network Access Manager Profile Editor** and click **Networks** option in the left pane. Click **Add...**



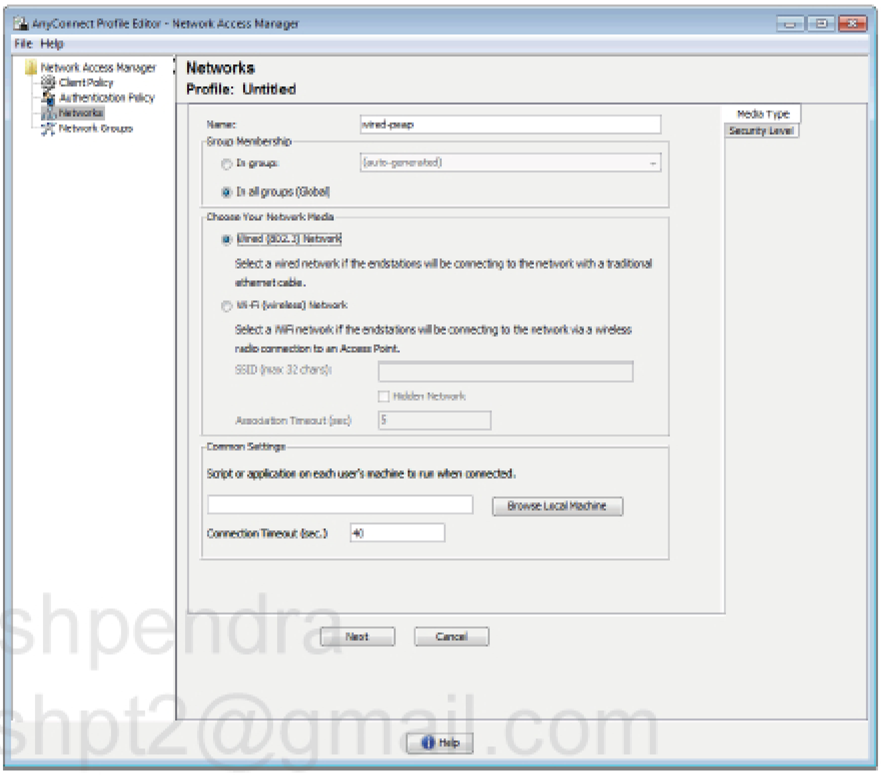
Networks
Profile: Untitled

Network

Name	Media Type	Group*
wired	Wired	Global

* A network in group 'Global' is a member of all groups.

- Enter a name for new profile e.g. **wired-peap** and specify network media as **Wired (802.3) Network**. Click **Next**.



Networks
Profile: Untitled

Name: wired-peap

Group Membership

○ In group: (auto-generated)

● In all groups (Global)

Choose Your Network Media

● Wired (802.3) Network

Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable.

○ Wi-Fi (wireless) Network

Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point.

SSID (max 32 chars):

□ Hidden Network

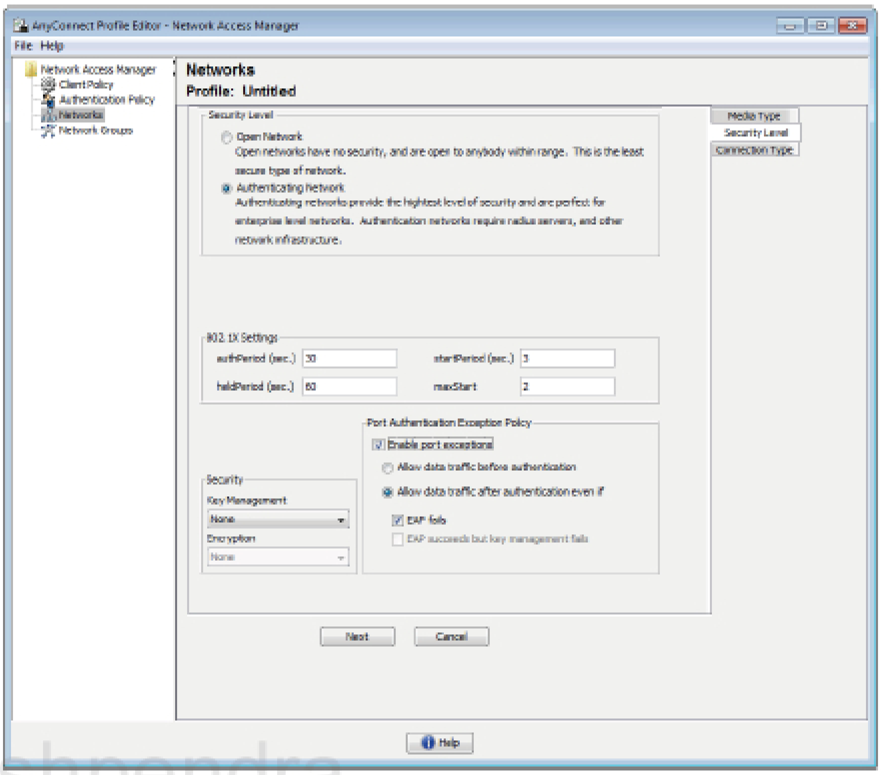
Association Timeout (sec) 5

Common Settings

Script or application on each user's machine to run when connected.

Connection Timeout (sec.) 40

- Select **Authenticating Network** for **Security Level** and tick **Enable port exceptions** checkbox. Select **Allow data traffic after authentication even if** radio button and tick **EAP fails** checkbox. Click **Next**.



AnyConnect Profile Editor - Network Access Manager

File Help

Network Access Manager
- Client Policy
- Authentication Policy
- Networks
- Network Groups

Networks

Profile: Untitled

Security Level

○ Open Network
Open networks have no security, and are open to anybody within range. This is the least secure type of network.

● Authenticating Network
Authenticating networks provide the hightest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure.

802.1X Settings

authPeriod (sec.) 30 startPeriod (sec.) 3

heldPeriod (sec.) 60 maxStart 2

Port Authentication Exception Policy

☑ Enable port exceptions

○ Allow data traffic before authentication

● Allow data traffic after authentication even if

☑ EAP fails

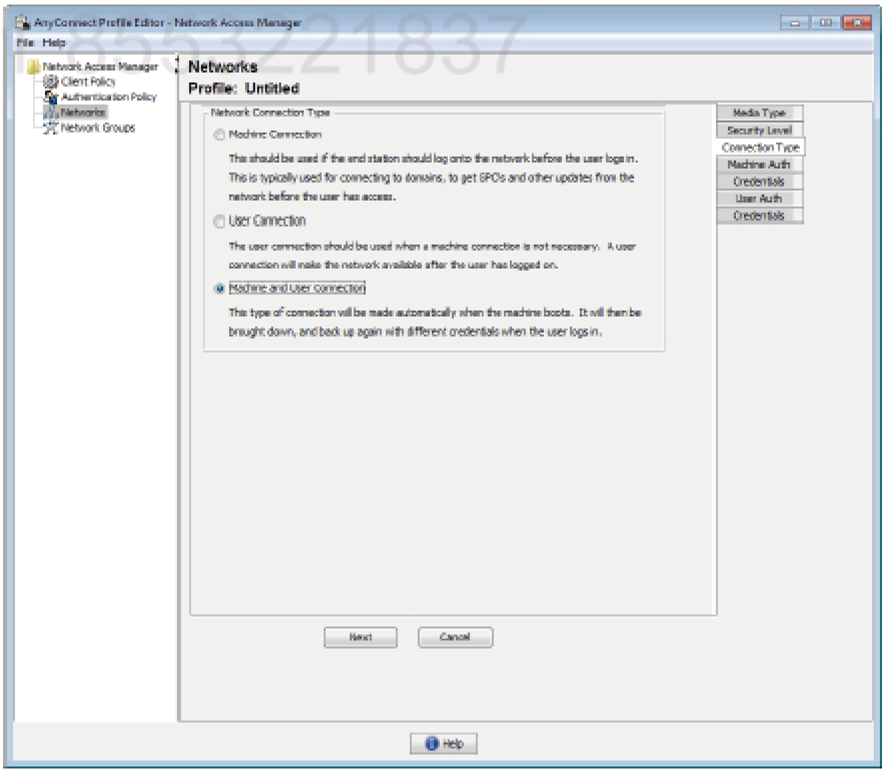
☐ EAP succeeds but key management fails

Security

Key Management: None

Encryption: None

- Select **Machine and User Connection** option to authenticate machine and user. Click **Next**.



AnyConnect Profile Editor - Network Access Manager

File Help

Network Access Manager
- Client Policy
- Authentication Policy
- Networks
- Network Groups

Networks

Profile: Untitled

Network Connection Type

○ Machine Connection

This should be used if the end station should log onto the network before the user logs in. This is typically used for connecting to domains, to get GPOs and other updates from the network before the user has access.

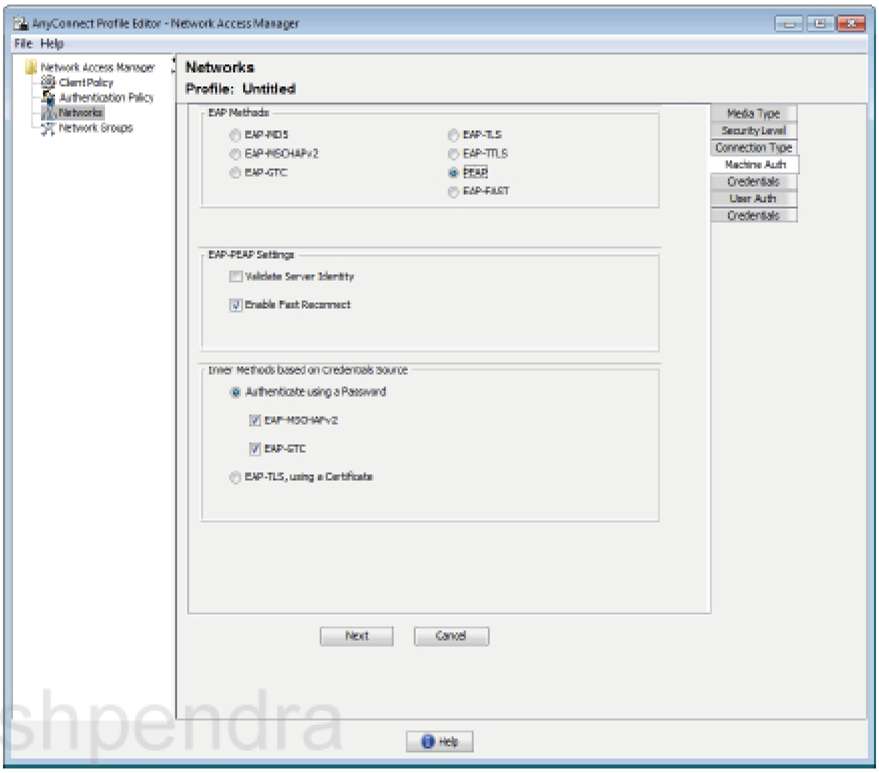
○ User Connection

The user connection should be used when a machine connection is not necessary. A user connection will make the network available after the user has logged on.

● Machine and User connection

This type of connection will be made automatically when the machine boots. It will then be brought down, and back up again with different credentials when the user logs in.

- For **Machine Auth** select **PEAP** as EAP method. Click **Next**.



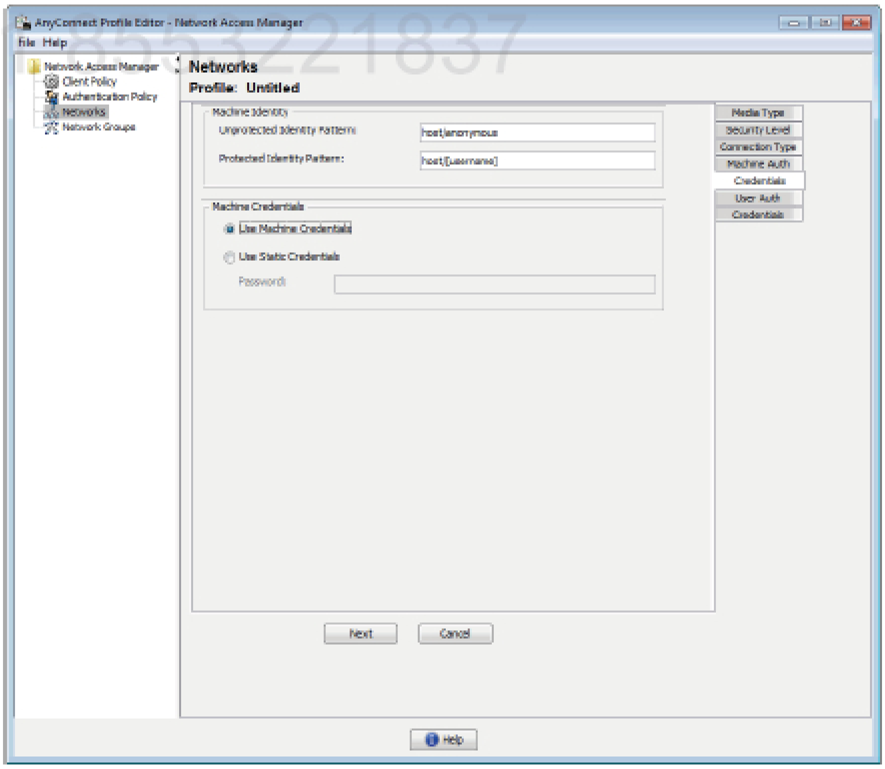
Networks
Profile: Untitled

EAP Methods
○ EAP-MD5 ○ EAP-TLS
○ EAP-MSCHAPv2 ○ EAP-TTLS
○ EAP-GTC ● PEAP
○ EAP-FAST

EAP-PEAP Settings
□ Validate Server Identity
☑ Enable Fast Reconnect

Inner Methods based on Credentials Source
● Authenticate using a Password
☑ EAP-MSCHAPv2
☑ EAP-GTC
○ EAP-TLS, using a Certificate

- For machine credentials leave all default settings. Click **Next**.

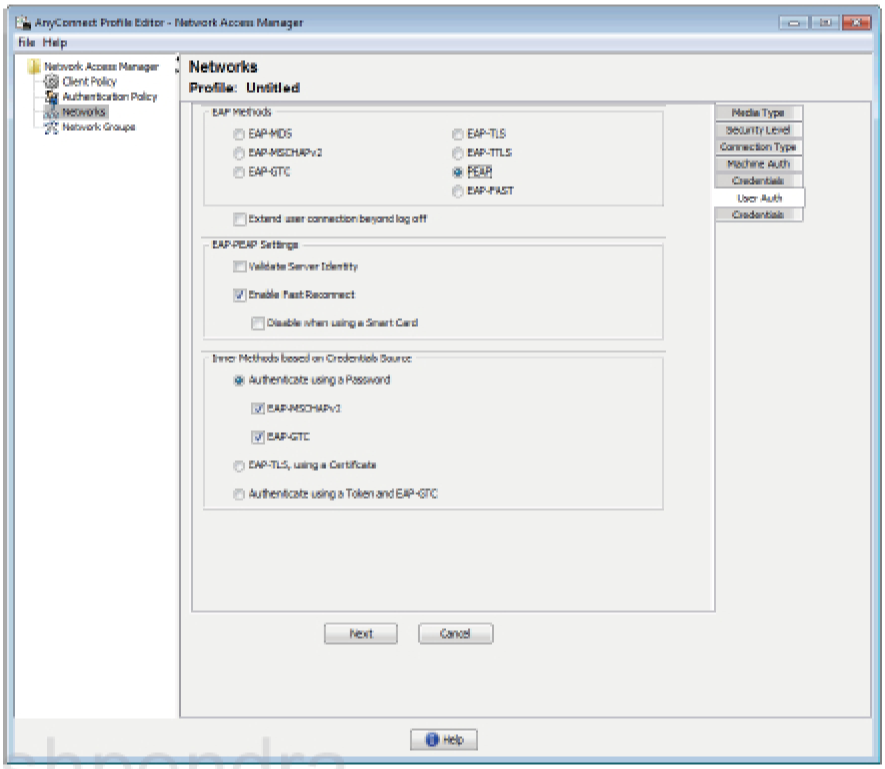


Networks
Profile: Untitled

Machine Identity
Unprotected Identity Pattern: host/anonymous
Protected Identity Pattern: host/[username]

Machine Credentials
● Use Machine Credentials
○ Use Static Credentials
Password:

- For **User Auth** select **PEAP** as EAP method. Click **Next**.



Networks
Profile: Untitled

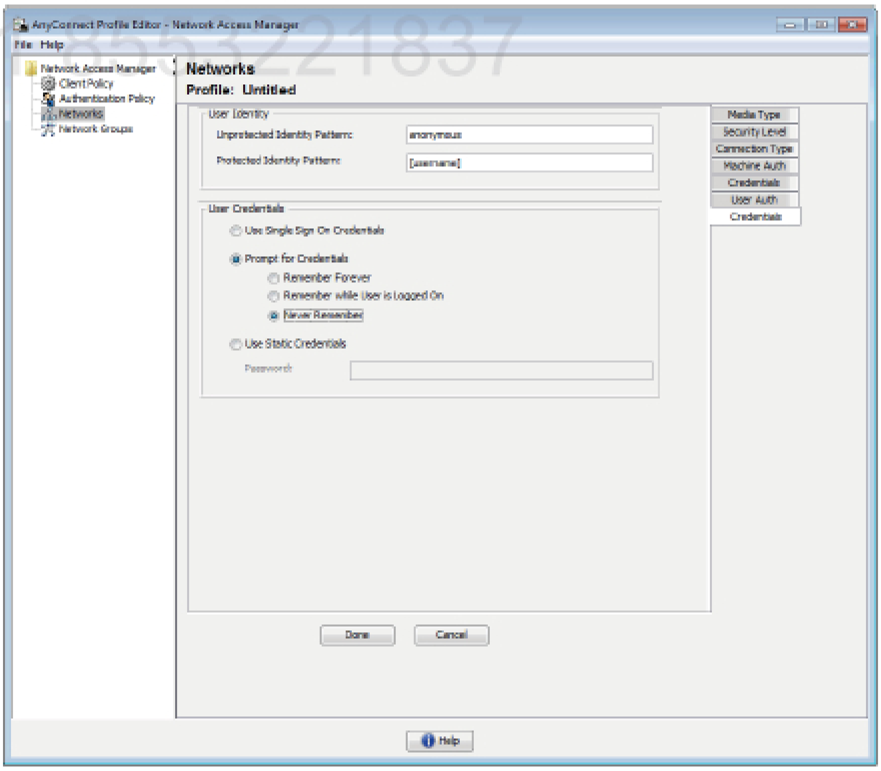
EAP Methods
○ EAP-MD5 ○ EAP-TLS
○ EAP-MSCHAPv2 ○ EAP-TTLS
○ EAP-GTC ● PEAP
○ EAP-FAST

□ Extend user connection beyond log off

EAP-PEAP Settings
□ Validate Server Identity
☑ Enable Fast Reconnect
□ Disable when using a Smart Card

Inner Methods based on Credentials Source
● Authenticate using a Password
☑ EAP-MSCHAPv2
☑ EAP-GTC
○ EAP-TLS, using a Certificate
○ Authenticate using a Token and EAP-GTC

For user credentials select **Prompt for Credentials** optiona and then select **Never Remember**. Click **Done**.

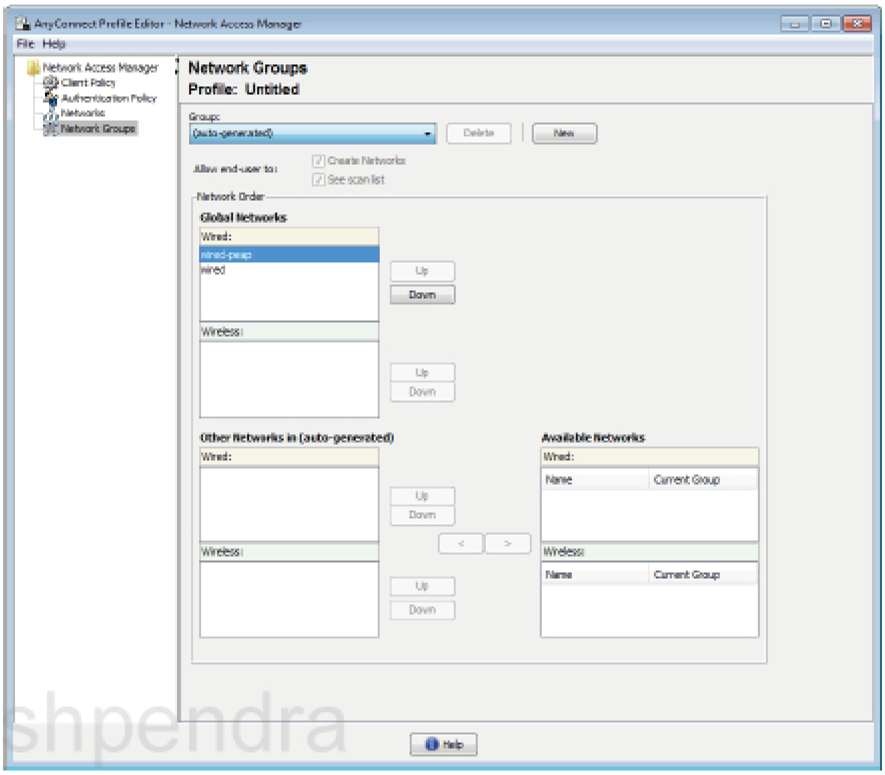


Networks
Profile: Untitled

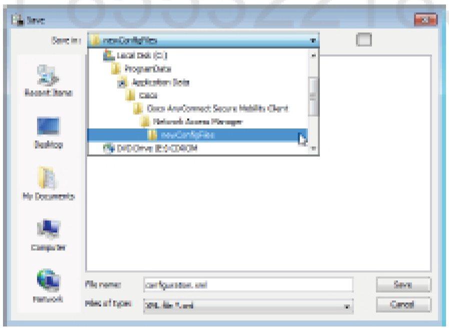
User Identity
Unprotected Identity Pattern: anonymous
Protected Identity Pattern: [username]

User Credentials
○ Use Single Sign On Credentials
● Prompt for Credentials
○ Remember Forever
○ Remember while User is Logged On
● Never Remember
○ Use Static Credentials
Password:

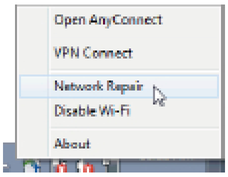
Go to **Network Groups** menu on the left pane and move **wired-peap** network to the top of the list.



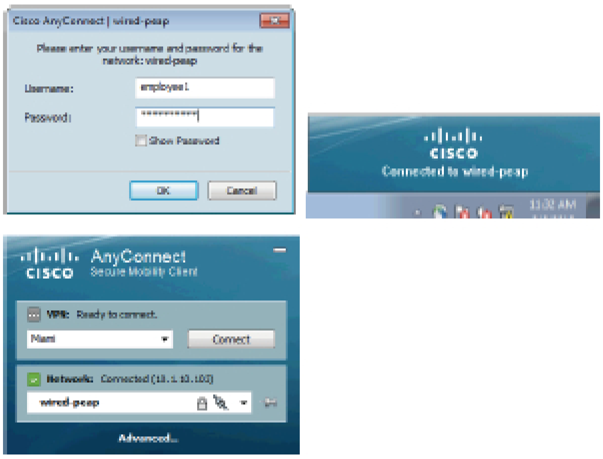
- From the top menu select **File > Save As…** Enter **configuration.xml** as file name and select the following directory. Click **Save**.



- Right click AnyConnect icon on the windows taskbar and select **Network Repair** option.



- Authenticate to the network as employee1 user. You should see a message from AnyConnect.



Cisco AnyConnect | wired-peap

Please enter your username and password for the network: wired-peap

Username: employee1

Password: ***********

□ Show Password

VPN: Ready to connect.

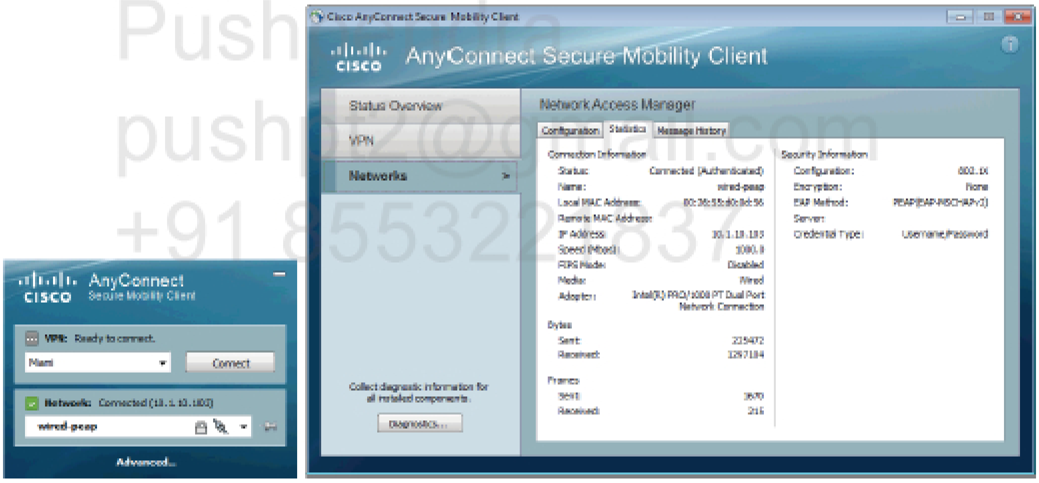
Miami

Network: Connected (10.1.10.103)

wired-peap

Verification

Show advanced options for AnyConnect NAM connection.



Connection Information

Status:	Connected (Authenticated)
Name:	wired-peap
Local MAC Address:	00:26:55:d0:0d:56
Remote MAC Address:	
IP Address:	10.1.10.103
Speed (Mbps):	1000.0
FIPS Mode:	Disabled
Media:	Wired
Adapter:	Intel(R) PRO/1000 PT Dual Port Network Connection

Bytes

Sent:	215472
Received:	1297184

Frames

Sent:	1670
Received:	216

Security Information

Configuration:	802.1X
Encryption:	None
EAP Method:	PEAP(EAP-MSCHAPv2)
Server:	
Credential Type:	Username/Password

Collect diagnostic information for all installed components.

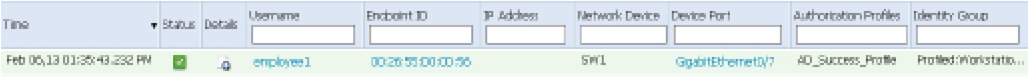
VPN: Ready to connect.

Miami

Network: Connected (10.1.10.103)

wired-peap

Check logs on ISE.



Time	Status	Details	Username	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Identity Group
Feb 06,13 01:35:43.232 PM	☑		employee1	00:26:55:D0:0D:56		SW1	GigabitEthernet0/7	AD_Success_Profile	Profiled:Workstatio...

Check commands on the switch.

```
SW1#sh authentication sessions interface g0/7
            Interface:  GigabitEthernet0/7
          MAC Address:  0026.55d0.0d56
           IP Address:  10.1.10.103
            User-Name:  employee1
               Status:  Authz Success
               Domain:  DATA
```

```
         Security Policy:  Should Secure
         Security Status:  Unsecure
          Oper host mode:  multi-domain
        Oper control dir:  both
           Authorized By:  Authentication Server
              Vlan Group:  N/A
                 ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-4f57e406
         Session timeout:  N/A
            Idle timeout:  N/A
       Common Session ID:  0A010A070000001A007ED78C
         Acct Session ID:  0x0000001F
                  Handle:  0xF600001B

Runnable methods list:
       Method   State
       dot1x    Authc Success
       mab      Not run

----------------------------------------
               Interface:  GigabitEthernet0/7
             MAC Address:  0021.a084.6ff4
              IP Address:  Unknown
               User-Name:  00-21-A0-84-6F-F4
                  Status:  Authz Success
                  Domain:  VOICE
         Security Policy:  Should Secure
         Security Status:  Unsecure
          Oper host mode:  multi-domain
        Oper control dir:  both
           Authorized By:  Authentication Server
                 ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-4f57e406
         Session timeout:  N/A
            Idle timeout:  N/A
       Common Session ID:  0A010A0700000018007D0EBA
         Acct Session ID:  0x0000001C
                  Handle:  0x18000019

Runnable methods list:
       Method   State
       dot1x    Failed over
       mab      Authc Success
```

LAB 3.18. MACSec Switch-to-Host

Objectives

This lab shows how to configure AnyConnect NAM to encrypt data at Layer 2 between the client PC and the switch.

IP Addressing and devices

Device	Interface	IP address
ISE	NIC	172.31.1.20
WinXP	NIC	10.1.10.50/24
Win7 PC	LAN NIC (LAB-Network) WLAN NIC	DHCP-Assigned 10.1.30.x (DHCP)
SW1	Vlan10	10.1.10.7/24

Task

Configure AnyConnect NAM to encrypt user data at Layer 2 using strong AES-GCM-128 algorithm. The link must be secured all the time. If EAP negotiation fails the user shouldn’t be able to send traffic unencrypted. Disable machine authentication. You can edit wired-peap connection profile to accomplish this task.

Configuration

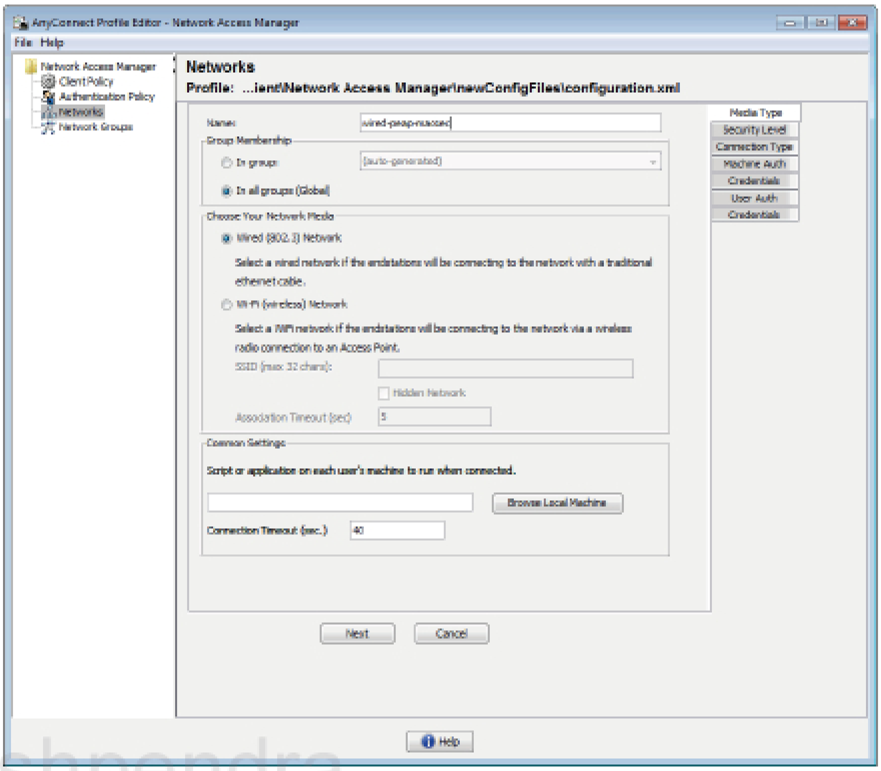
Complete these steps:

Step 1 Switch configuration (commands required in this lab are highlighted).

```
!
interface GigabitEthernet0/7
 description IPP + Win7
 switchport access vlan 10
 switchport mode access
 switchport nonegotiate
 switchport voice vlan 500
 ip access-group DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication linksec policy must-secure
 authentication order dot1x mab
 authentication port-control auto
 authentication violation protect
 macsec
 mka default-policy
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 5
 spanning-tree portfast
!
```

Step 2 Run NAM Profile Editor and re-configure network profile.

- Run **Network Access Manager Profile Editor** and **Open configuration.xml** file. Click **Networks** option on the left pane, select **wired-peap** profile from the list and click **Edit…** Change the profile name to **wired-peap-macsec** and click **Next**.



Networks

Profile: ...ient\Network Access Manager\newConfigFiles\configuration.xml

Name: wired-peap-macsec

Group Membership

○ In group: (auto-generated)

● In all groups (Global)

Choose Your Network Media

● Wired (802.1) Network

Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable.

○ Wi-Fi (wireless) Network

Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point.

SSID (max 32 chars):

□ Hidden Network

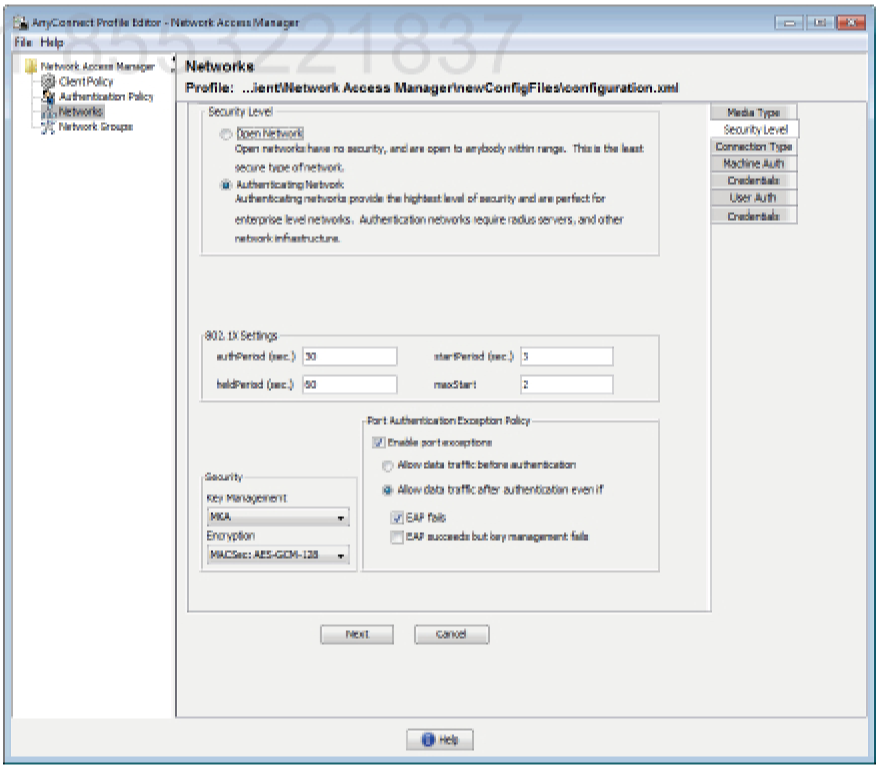
Association Timeout (sec) 5

Common Settings

Script or application on each user's machine to run when connected.

Connection Timeout (sec.) 40

- In **Security** section select **MKA** as **Key Management** and **MACSec: AES-GCM-128** for **Encryption**. Click **Next**.



Networks

Profile: ...ient\Network Access Manager\newConfigFiles\configuration.xml

Security Level

○ Open Network

Open networks have no security, and are open to anybody within range. This is the least secure type of network.

● Authenticating Network

Authenticating networks provide the highest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure.

802.1X Settings

authPeriod (sec.) 30 startPeriod (sec.) 3

heldPeriod (sec.) 60 maxStart 2

Security

Key Management: MKA

Encryption: MACSec: AES-GCM-128

Port Authentication Exception Policy

☑ Enable port exceptions

○ Allow data traffic before authentication

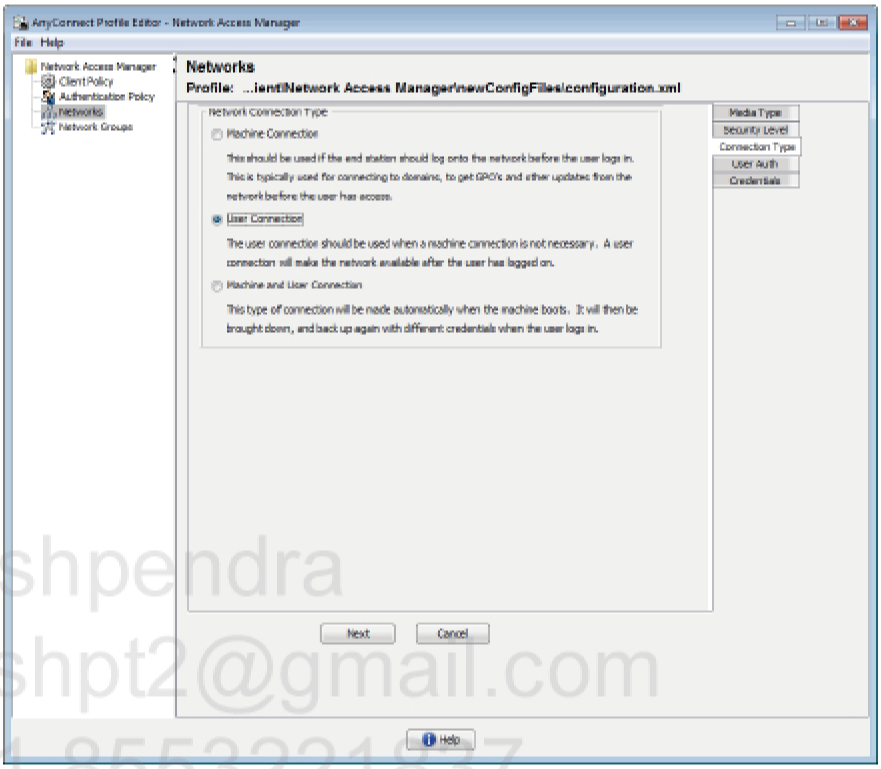
● Allow data traffic after authentication even if

☑ EAP fails

□ EAP succeeds but key management fails

The requirement is to set Port Authentication Exception Policy to 'must-secure' then we must enable 'EAP succeeds but key management fails' option. 'Should-secure' is the default policy set on Cisco X-series switches. To accommodate for a macsec policy set to 'must-secure', uncheck 'EAP succeeds by key management fails'.

- Select **User Connection** option to authenticate user only. Click **Next**.



Networks

Profile: ...ient\Network Access Manager\newConfigFiles\configuration.xml

Network Connection Type

○ Machine Connection

This should be used if the end station should log onto the network before the user logs in. This is typically used for connecting to domains, to get GPO's and other updates from the network before the user has access.

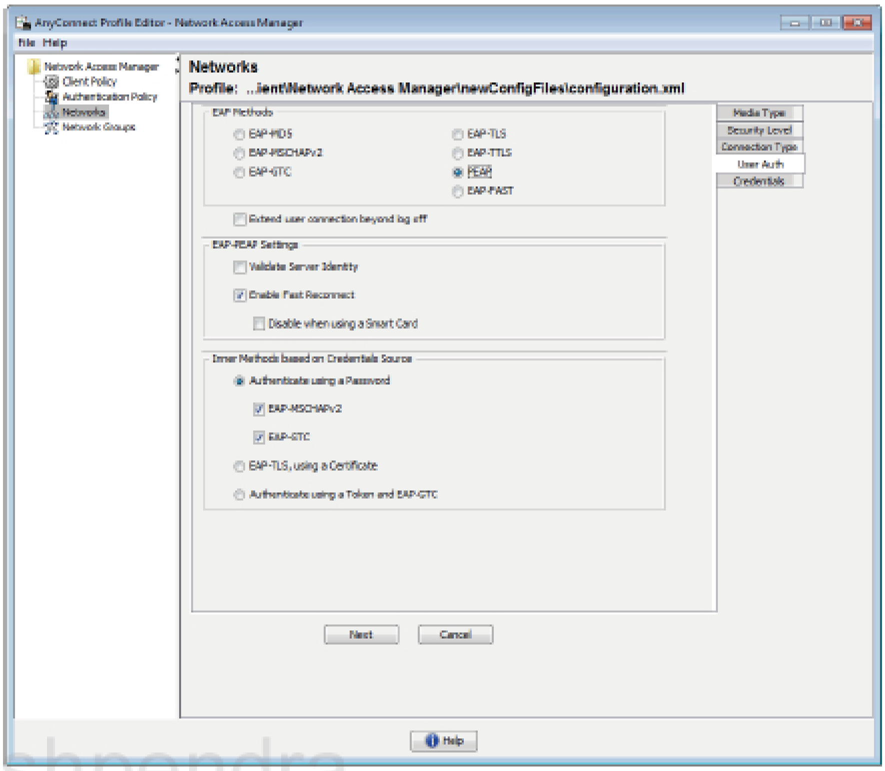
● User Connection

The user connection should be used when a machine connection is not necessary. A user connection will make the network available after the user has logged on.

○ Machine and User Connection

This type of connection will be made automatically when the machine boots. It will then be brought down, and back up again with different credentials when the user logs in.

- For **User Auth** select **PEAP** as EAP method. Click **Next**.



AnyConnect Profile Editor - Network Access Manager

Networks

Profile: ...ient\Network Access Manager\newConfigFiles\configuration.xml

EAP Methods

- ○ EAP-MD5
- ○ EAP-MSCHAPv2
- ○ EAP-GTC
- ○ EAP-TLS
- ○ EAP-TTLS
- ● PEAP
- ○ EAP-FAST

□ Extend user connection beyond log off

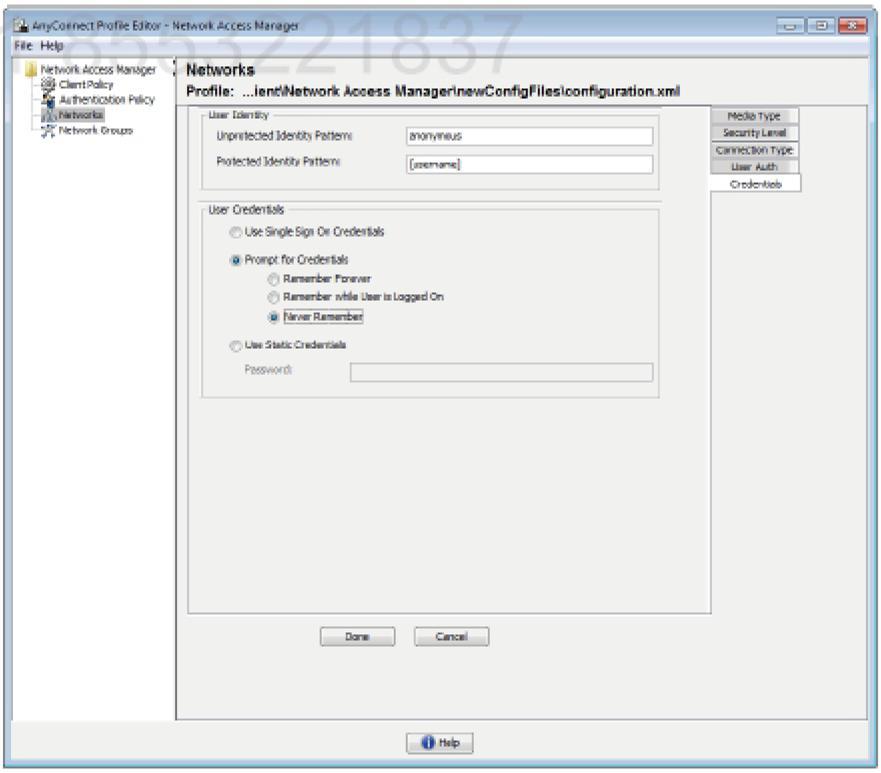
EAP-PEAP Settings

- □ Validate Server Identity
- ☑ Enable Fast Reconnect
  - □ Disable when using a Smart Card

Inner Methods based on Credentials Source

- ● Authenticate using a Password
  - ☑ EAP-MSCHAPv2
  - ☑ EAP-GTC
- ○ EAP-TLS, using a Certificate
- ○ Authenticate using a Token and EAP-GTC

For user credentials select **Prompt for Credentials** optiona and then select **Never Remember**. Click **Done**.



AnyConnect Profile Editor - Network Access Manager

Networks

Profile: ...ient\Network Access Manager\newConfigFiles\configuration.xml

User Identity

Unprotected Identity Pattern: anonymous

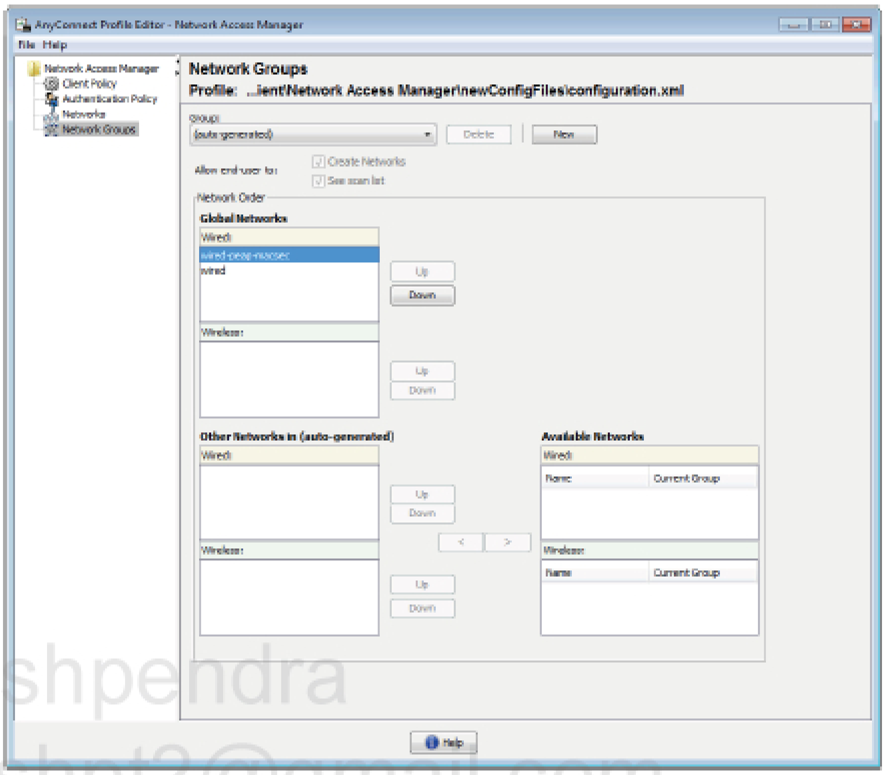
Protected Identity Pattern: [username]

User Credentials

- ○ Use Single Sign On Credentials
- ● Prompt for Credentials
  - ○ Remember Forever
  - ○ Remember while User is Logged On
  - ● Never Remember
- ○ Use Static Credentials

Password:

Go to **Network Groups** menu on the left pane and move **wired-peap-macsec** network to the top of the list.



Network Groups

Profile: ...ient\Network Access Manager\newConfigFiles\configuration.xml

Group: (auto-generated)

Allow end user to: ☑ Create Networks ☑ See scan list

Network Order

Global Networks

Wired:
wired-peap-macsec
wired

Wireless:

Other Networks in (auto-generated)

Wired:

Wireless:

Available Networks

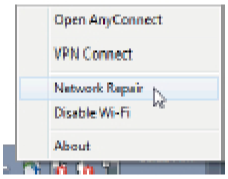
Wired:

Name	Current Group

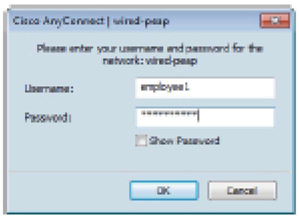
Wireless:

Name	Current Group

- From the top menu select **File > Save**. Right click AnyConnect icon on the windows taskbar and select **Network Repair** option.



- Authenticate to the network as employee1 user. You should see a message from AnyConnect.

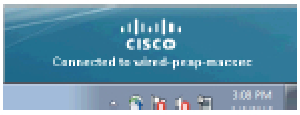


Please enter your username and password for the network: wired-peap

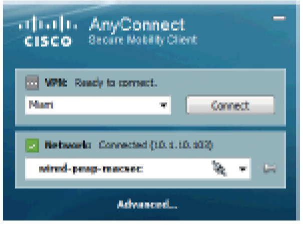
Username: employee1

Password: ***********

□ Show Password



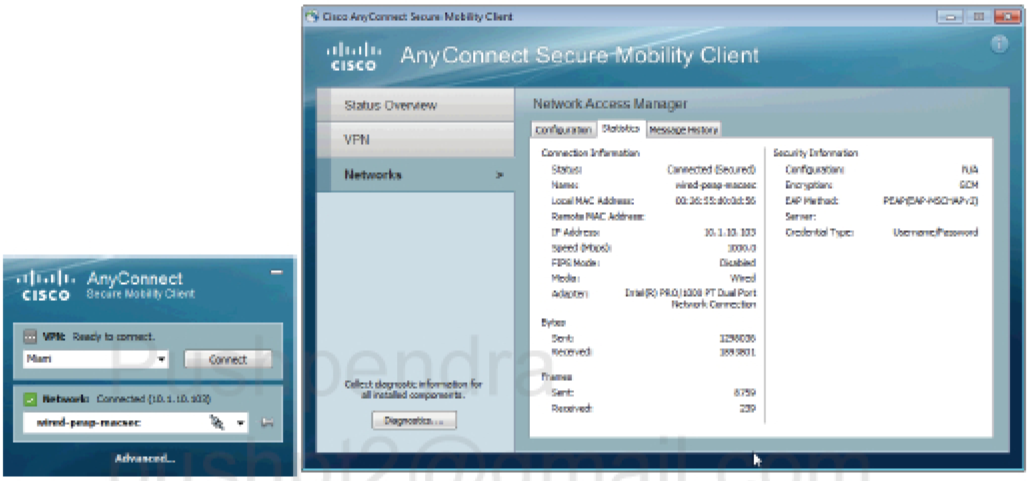
Connected to wired-peap-macsec



VPN: Ready to connect.
Miami
Network: Connected (10.1.10.103)
wired-peap-macsec

Verification

Show advanced options for AnyConnect NAM connection.



Connection Information
Status: Connected (Secured)
Name: wired-peap-macsec
Local MAC Address: 00:26:55:d0:0d:56
Remote MAC Address:
IP Address: 10.1.10.103
Speed (Mbps): 1000.0
FIPS Mode: Disabled
Media: Wired
Adapter: Intel(R) PRO/1000 PT Dual Port Network Connection

Bytes
Sent: 1298036
Received: 1893801

Frames
Sent: 8759
Received: 239

Security Information
Configuration: N/A
Encryption: GCM
EAP Method: PEAP(EAP-MSCHAPv2)
Server:
Credential Type: Username/Password

Collect diagnostic information for all installed components.

VPN: Ready to connect.
Miami
Network: Connected (10.1.10.103)
wired-peap-macsec

Check commands on the switch.

```
SW1#sh macsec summary
Interface                    Transmit SC          Receive SC
GigabitEthernet0/7                1                    1


SW1#sh macsec interface g0/7
 MACsec is enabled
  Replay protect : enabled
  Replay window : 0
  Include SCI : yes
  Cipher : GCM-AES-128
  Confidentiality Offset : 0
 Capabilities
  Max. Rx SA : 16
  Max. Tx SA : 16
  Validate Frames : strict
  PN threshold notification support : Yes
  Ciphers supported : GCM-AES-128
 Transmit Secure Channels
  SCI : C464136CE8070002
```

```
   Elapsed time : 00:01:20
   Current AN: 0   Previous AN: -
   SC Statistics
    Auth-only (0 / 0)
    Encrypt (1263 / 0)
 Receive Secure Channels
  SCI : 002655D00D560000
   Elapsed time : 00:01:20
   Current AN: 0   Previous AN: -
   SC Statistics
    Notvalid pkts 0      Invalid pkts 0
    Valid pkts 64         Late pkts 0
    Uncheck pkts 0       Delay pkts 0
  Port Statistics
   Ingress untag pkts  0        Ingress notag pkts 25567
   Ingress badtag pkts 0        Ingress unknownSCI pkts 0
   Ingress noSCI pkts 0         Unused pkts 0
   Notusing pkts 0              Decrypt bytes 89423
   Ingress miss pkts 25488

SW1#sh authentication sessions interface g0/7
            Interface:  GigabitEthernet0/7
          MAC Address:  0026.55d0.0d56
           IP Address:  10.1.10.103
            User-Name:  employee1
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Must Secure
      Security Status:  Secured
       Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
           Vlan Group:  N/A
              ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-4f57e406
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A010A070000002F0142B428
      Acct Session ID:  0x00000079
               Handle:  0xA6000030

Runnable methods list:
       Method   State
       dot1x    Authc Success
       mab      Not run


SW1#sh ip access-lists interface g0/7
     permit ip host 10.1.10.103 any
```

LAB 3.19. MACSec Switch-to-Switch

Objectives

This lab shows how to configure MACSec between two switches with manual keyring.

IP Addressing and devices

Device	Interface	IP address
ISE	NIC	172.31.1.20
WinXP	NIC	10.1.10.50/24
Win7 PC	LAN NIC (LAB-Network) WLAN NIC	DHCP-Assigned 10.1.30.x (DHCP)
SW1	G0/24	Trunk
SW2	G0/24	Trunk

Task

Enable link encryption between SW1 and SW2. Do not use authorization server. Instead, configure encryption key of '987654321' manually and use GCM-AES-128 encryption algorithm.

Configuration

Complete these steps:

Step 1 Switch 1 configuration.

```
!
interface GigabitEthernet0/24
 description To SWITCH2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 cts manual
  no propagate sgt
  sap pmk 987654321 mode-list gcm-encrypt
!
```

Step 2 Switch 2 configuration.

```
!
interface GigabitEthernet0/24
 description To SWITCH1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 cts manual
  no propagate sgt
  sap pmk 987654321 mode-list gcm-encrypt
!
```

Verification

Check commands on both switches.

```
SW1#sh cts interface
Global Dot1x feature is Enabled
Interface GigabitEthernet0/24:
    CTS is enabled, mode:    MANUAL
    IFC state:               OPEN
    Authentication Status:   NOT APPLICABLE
        Peer identity:       "unknown"
        Peer's advertised capabilities: "sap"
    Authorization Status:    NOT APPLICABLE
    SAP Status:              SUCCEEDED
        Version:             2
        Configured pairwise ciphers:
            gcm-encrypt

        Replay protection:      enabled
        Replay protection mode: STRICT

        Selected cipher:        gcm-encrypt
    Propagate SGT:           Disabled
    Cache Info:
        Cache applied to link : NONE

    Statistics:
        authc success:              0
        authc reject:               0
        authc failure:              0
        authc no response:          0
        authc logoff:               0
        sap success:                1
        sap fail:                   9
        authz success:              0
        authz fail:                 0
        port auth fail:             0
        Ingress:
            control frame bypassed: 0
            sap frame bypassed:     0
            esp packets:            0
            unknown sa:             0
            invalid sa:             0
            inverse binding failed: 0
            auth failed:            0
            replay error:           0
        Egress:
            control frame bypassed: 0
            esp packets:            0
            sgt filtered:           0
            sap frame bypassed:     0
            unknown sa dropped:     0
            unknown sa bypassed:    0
```

```
SW1#sh macsec interface g0/24
 MACsec is enabled
  Replay protect : enabled
  Replay window : 0
  Include SCI : yes
  Cipher : GCM-AES-128
  Confidentiality Offset : 0
 Capabilities
  Max. Rx SA : 16
  Max. Tx SA : 16
  Validate Frames : strict
  PN threshold notification support : Yes
  Ciphers supported : GCM-AES-128
 Transmit Secure Channels
  SCI : C464136CE8180000
   Elapsed time : 7w0d
   Current AN: 0   Previous AN: 1
   SC Statistics
```

```
    Auth-only (0 / 0)
    Encrypt (38040 / 0)
 Receive Secure Channels
  SCI : CCEF48A63C980000
   Elapsed time : 7w0d
   Current AN: 0   Previous AN: 1
   SC Statistics
    Notvalid pkts 0      Invalid pkts 0
    Valid pkts 165125         Late pkts 0
    Uncheck pkts 0       Delay pkts 0
  Port Statistics
   Ingress untag pkts  0        Ingress notag pkts 19165
   Ingress badtag pkts 0        Ingress unknownSCI pkts 0
   Ingress noSCI pkts 0         Unused pkts 0
   Notusing pkts 0              Decrypt bytes 43163117
   Ingress miss pkts 19153

       // same commands on other switch. Note that Dot1x is NOT necessary to be
       enabled in order to make manual MACSec work. It is only important wen we use
       'cts dot1x' command on the interface.

SW2#sh cts interface
Global Dot1x feature is Disabled
Interface GigabitEthernet0/24:
    CTS is enabled, mode:    MANUAL
    IFC state:               OPEN
    Authentication Status:   NOT APPLICABLE
        Peer identity:       "unknown"
        Peer's advertised capabilities: "sap"
    Authorization Status:    NOT APPLICABLE
    SAP Status:              SUCCEEDED
        Version:             2
        Configured pairwise ciphers:
            gcm-encrypt

        Replay protection:      enabled
        Replay protection mode: STRICT

        Selected cipher:        gcm-encrypt

    Propagate SGT:           Disabled
    Cache Info:
        Cache applied to link : NONE

    Statistics:
        authc success:              0
        authc reject:               0
        authc failure:              0
        authc no response:          0
        authc logoff:               0
        sap success:                1
        sap fail:                   0
        authz success:              0
        authz fail:                 0
        port auth fail:             0
        Ingress:
            control frame bypassed: 0
            sap frame bypassed:     0
            esp packets:            0
            unknown sa:             0
            invalid sa:             0
            inverse binding failed: 0
            auth failed:            0
            replay error:           0
        Egress:
            control frame bypassed: 0
            esp packets:            0
            sgt filtered:           0
            sap frame bypassed:     0
            unknown sa dropped:     0
            unknown sa bypassed:    0


SW2#sh macsec interface g0/24
 MACsec is enabled
  Replay protect : enabled
  Replay window : 0
  Include SCI : yes
  Cipher : GCM-AES-128
  Confidentiality Offset : 0
 Capabilities
  Max. Rx SA : 16
  Max. Tx SA : 16
  Validate Frames : strict
  PN threshold notification support : Yes
  Ciphers supported : GCM-AES-128
 Transmit Secure Channels
  SCI : CCEF48A63C980000
   Elapsed time : 05:24:03
   Current AN: 0   Previous AN: 1
   SC Statistics
    Auth-only (0 / 0)
    Encrypt (165971 / 0)
 Receive Secure Channels
  SCI : C464136CE8180000
   Elapsed time : 05:24:03
   Current AN: 0   Previous AN: 1
   SC Statistics
    Notvalid pkts 0      Invalid pkts 0
    Valid pkts 38131         Late pkts 0
    Uncheck pkts 0       Delay pkts 0
  Port Statistics
```

```
Ingress untag pkts  0        Ingress notag pkts 23
Ingress badtag pkts 0        Ingress unknownSCI pkts 0
Ingress noSCI pkts 0         Unused pkts 0
Notusing pkts 0              Decrypt bytes 5441050
Ingress miss pkts 23
```

This page is intentionally left blank.

Advanced
CCIE SECURTY v4
LAB WORKBOOK

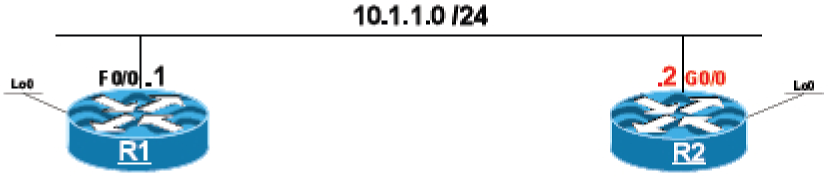
Advanced IOS Security

Narbik Kocharians
CCIE #12410 (R&S, Security, SP)
CCSI #30832

Piotr Matusiak
CCIE #19860 (R&S, Security)
C|EH, CCSI #33705

www.MicronicsTraining.com

LAB 3.20. Basic Router Security



Lab Setup

- Ensure that R1's F0/0 and R2's G0/0 interface is configured in VLAN 12.
- Assign the IP addressing using the chart below.

IP Addressing

Router	Interface	IP address
R1	Lo0 F0/0	1.1.1.1/8 10.1.1.1/24
R2	Lo0 G0/0	2.2.2.2/8 10.1.1.2/24

Task 1

Ensure that R1 is configured with the following policy:

- Configure this router such that the user needs to enter a password of "Cisco07" before the user is allowed access to the privilege mode
- The password must be at least seven characters in length
- Use the strongest hashing method based on MD5
- No recovery of the passwords are allowed on this routers

Configuration

Complete these steps:

Step 1 R1 configuration.

```
R1(config)#security passwords min-length 7
R1(config)#no service password-recovery

WARNING:
Executing this command will disable password recovery me
chanism.
Do not execute this command without another plan for
password recovery.

Are you sure you want to continue? [yes/no]: yes

R1(config)#enable secret Cisco

% Invalid Password length - must contain 7 to 25 characters.
Password configuration failed

        Note above message is saying that the length of the
password must be 7 characters.

R1(config)#enable secret Cisco07

        Note the "Security passwords min-length 7" command effects
        all the passwords on this router.
```

Task 2

Ensure that all the passwords on both routers are unreadable if a “show run” command is issued.

Configuration

Complete these steps:

Step 1 On both routers.

```
(config)#service password-encryption

        Note a "no service password-encryption" command will not
        decrypt the passwords, but all the passwords configured
```

after this command is entered will be displayed in the running configuration as unencrypted.

Task 3

Ensure that if the console port of any of these routers stops functioning, the administrator has another way to connect to the routers locally. DO NOT configure telnet or modems for to accomplish this task. The password for this task should be "Cisc@??07"

Configuration

Complete these steps:

Step 1 On both routers.

```
(config)#line aux 0
(config-line)#login
(config-line)#password Cisc@??07
```

Note in order to configure the password of these routers to be "Cisc@??07", you must enter the "Esc and then Q" before typing each "?", in this task, the "Esc and then Q" needs to be done twice one for each "?", but to enter the password when a login attempt is made, you MUST NOT use the "Esc and then Q" for entering the "?".

Task 4

On R1 configure the number of allowable unsuccessful login attempts to 3 within one minute, if this policy is violated, the router should generate a syslog message.

Configuration

Complete these steps:

Step 1 R1 configuration.

```
R1(config)#security authentication failure rate 3 log
```

```
When the number of failed login attempts reaches the
configured threshold, the router will send a
"TOOMANY_AUTHFAILS" event message to the configured SYSLOG
server. The router will also start a 15 second delay timer,
once this delay timer expires, the user can try to login
again.
```

Task 5

Configure both Routers to terminate an unattended console connection after 4 minutes and 30 seconds

Configuration

Complete these steps:

Step 1 On both routers.

```
(config)#line con 0
(config-line)#exec-timeout 4 30
```

```
Note that a command "exec-timeout 0 0" should be used to
disable console timeout at all.
```

Task 6

Create the following users on R2 using the chart below and ensure that ONLY the assigned commands are available to these users via the console:

User name	Password	Available commands:
U2	Cisco2	Show interface G0/0, Show ip int brief, ping and

		Traceroute.
U3	Cisco3	All the User level commands, The user should be able to assign an IP addresses and shut and no shut the interfaces.
Admin	Cisco	All levels and commands.

Configuration

Complete these steps:

Step 1 R2 configuration.

To configure the privilege level for User U2:

```
R2(config)#privilege EXEC level 2 Show interface F0/0
R2(config)#privilege EXEC level 2 Show ip int brie
R2(config)#privilege EXEC level 2 ping
R2(config)#privilege EXEC level 2 Traceroute

R2(config)#username U2 privilege 2 password cisco2
```

Note that user U2, has access to all privilege level 1 commands also. For example:

```
R2#sh privilege
Current privilege level is 2
R2#sh ip route | inc 10.1.1.0
C       10.1.1.0 is directly connected, FastEthernet0/0
R2#
```

To configure the privilege level for User U3:

```
R2(config)#privilege EXEC level 3 configure terminal
R2(config)#privilege configure level 3 interface
R2(config)#privilege interface level 3 shutdown
R2(config)#privilege interface level 3 ip address

R2(config)#username U3 privilege 3 password cisco3
```

To configure the privilege level for User Admin:

```
R2(config)#username admin privilege 15 password cisco
```

Lastly force the users to login using the local user account database:

```
R2(config)#line con 0
R2(config-line)#login local
```

Task 7

Create a message of the day banner on R1 using the following policy:

The banner should state the router, line and it should also state that you are connected to www.MicronicsTraining.com

Configuration

Complete these steps:

Step 1 R1 configuration.

```
R1(config)#banner motd #You are connected to $(hostname) on line
$(line) on domain $(domain)#
R1(config)#ip domain-name www.MicronicsTraining.com
```

Verification

```
R1#logout

        You should see the following message on the console:

You are connected to R1 on line 0 on domain www.MicronicsTraining.com
```

Task 8

Router R1 should be configured such that when user U2 logs in to the router the following menu is displayed. The following policy must be configured for the menu: The screen must be cleared prior in displaying the menu, the menu should allow the user to type the desired number and then press the enter key to select that option,

option 3 should logout the user whereas, option 4 should exit the menu and into privilege exec mode (enable mode)

```
This is the menu for CCIE candidates

    1          Display all the interfaces and their assigned IP addresses

    2          Display the configuration of F0/0 interface

    3          Logout

    4          Exit out of the menu

Please Choose an option and press Enter :
```

Configuration

Complete these steps:

Step 1 R1 configuration.

```
R1(config)#menu U2 title # This is the menu for CCIE candidates #


R1(config)#menu U2 text 1 Display the interfaces and their assigned
IP addresses
R1(config)#menu U2 command 1 Show ip int brie
R1(config)#menu U2 options 1 pause
```

If the pause is not configured, the user will not see the output.

```
R1(config)#menu U2 text 2 Display the configuration of F0/0
interface
R1(config)#menu U2 command 2 Show run int f0/0

R1(config)#menu U2 options 2 pause

R1(config)#menu U2 text 3 Logout
R1(config)#menu U2 command 3 logout

R1(config)#menu U2 text 4 Exit out of the menu
R1(config)#menu U2 command 4 menu-exit
```

```
R1(config)#menu U2 clear-screen
R1(config)#menu U2 line-mode
R1(config)#menu U2 prompt # Please Choose an option and press Enter
:  #

R1(config)#username U2 privilege 15 password user2009
R1(config)#username U2 autocommand menu U2
R1(config)#username Admin password Cisco2009

        Always create another user so you won't lock yourself out
        of the con port, once tested you can always remove that
        username.

R1(config)#line con 0
R1(config-line)#login local
```

Task 9

Configure R2 using the following policy:

- Disable the service that when a wrong command is entered the router performs a broadcast looking for a DNS server to resolve the bad command to an IP address. This search should be restricted to 10.1.1.5 IP address.

- Disable the service that can be used to find out which users are logged into a network device. Although this information is considered not sensitive by many administrators, the information can be used by a hacker for reconnaissance attack.

- Disable the service that instructs an end node to use another and more efficient path to a particular destination.

Configuration

Complete these steps:

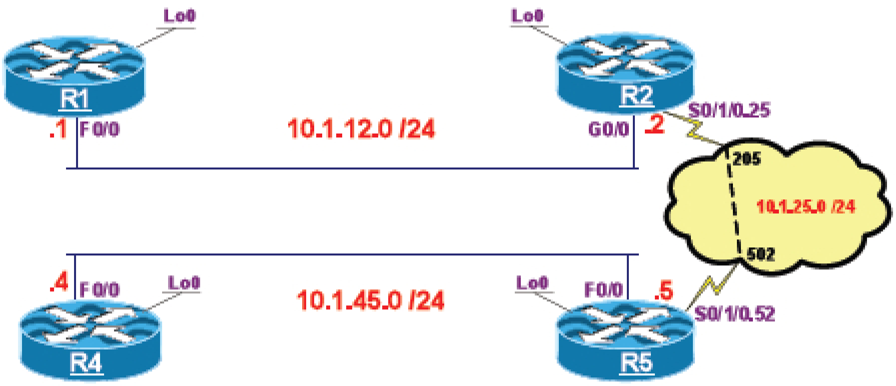
Step 1 R2 configuration.

```
R2(config)#ip name-server 10.1.1.5
R2(config)#no ip finger
R2(config)#no ip icmp redirect
```

Task 10

Erase the startup config and reload the routers before proceeding to the next lab.

LAB 3.21. Standard Named Access List



Lab Setup

- R1 and R2's G0/0 interface should be configured in VLAN 12
- R2 and R5's S0/1/0 interface should be configured in a frame-relay point-to-point manner.
- R5 and R4's F0/0 interface should be configured in VLAN 45
- Configure telnet on all routers using password "cisco"
- Run RIPv2 on the routers and advertise their directly connected networks

IP Addressing

Router	Interface	IP address
R1	Lo0 F0/0	1.1.1.1/24 10.1.12.1/24
R2	Lo0 G0/0 S0/1/0.25	2.2.2.2/24 10.1.12.2/24 10.1.25.2/24
R4	Lo0 F0/0	4.4.4.4/24 10.1.45.4/24
R5	Lo0 F0/0 S0/1/0.52	5.5.5.5/24 10.1.45.5/24 10.1.25.5/24

Task 1

Configure a standard numbered access-list on R1 to block host 4.4.4.4 from accessing any of its interfaces.

Configuration

Complete these steps:

Step 1 R1 configuration.

```
R1(config)#access-list 1 deny 4.4.4.4
R1(config)#access-list 1 permit any

R1(config)#int f0/0
R1(config-if)#ip access-group 1 in
```

Verification

```
R1#debug ip packet


R4#ping 1.1.1.1 source lo0
 Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 4.4.4.4
U.U.U
Success rate is 0 percent (0/5)

       You should see the following debug output on R1:

IP: s=4.4.4.4 (FastEthernet0/0), d=1.1.1.1, len 100, access denied
IP: tableid=0, s=10.1.12.1 (local), d=4.4.4.4 (FastEthernet0/0), routed via FIB
IP: s=10.1.12.1 (local), d=4.4.4.4 (FastEthernet0/0), len 56, sending

       Note the ping fails.
```

Task 2

Replace the previous task using a standard named access-list.

Configuration

Complete these steps:

Step 1 R1 configuration.

```
R1(config)#NO access-list 1

R1(config)#ip access-list standard TEST

R1(config-std-nacl)#deny host 4.4.4.4

R1(config-std-nacl)#permit any

R1(config)#int f0/0
R1(config-if)#ip access-group TEST in
```

Task 3

Remove the access-list from the previous step before proceeding to the next Lab.

Configuration

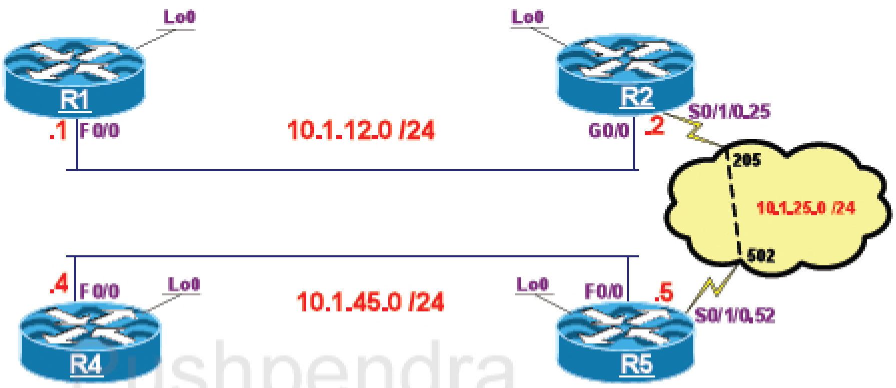
Complete these steps:

Step 1 R1 configuration.

```
R1(config)#no ip access-list standard TEST

R1(config)#int f0/0
R1(config-if)#no ip access-group TEST in
```

LAB 3.22. Controlling telnet access and SSH

Based on the previous Lab's IP addressing, topology and Lab setup



Task 1

Configure an access-list on R2 such that only 1.1.1.1/24 is allowed to telnet in, other packets should NOT be subject to inspection by this access-list.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#access-list 1 permit host 1.1.1.1

R2(config)#line vty 0 ?
R2(config-line)#access-class 1 in
```

The reason a question mark was used in the "line vty 0 ?" command is because different routers with different IOSes have different number of telnet ports. Most switches have 15 VTYs by default.

Verification

```
R1#telnet 10.1.12.2

Trying 10.1.12.2 ...
% Connection refused by remote host

R1#telnet 10.1.12.2 /source-interface lo0

Trying 10.1.12.2 ... Open
User Access Verification

Password:
```

Note the first time R1 telnet using its 10.1.12.1 IP address and the telnet was refused by R2. The second telnet was successful, because the source IP address of the telnet was 1.1.1.1.

```
R5#telnet 10.1.25.2

Trying 10.1.25.2 ...

% Connection refused by remote host

R5#telnet 10.1.25.2 /source-interface lo0

Trying 10.1.25.2 ...
% Connection refused by remote host
```

Note R5 is NOT successful.

```
R4#telnet 10.1.25.2

Trying 10.1.25.2 ...
% Connection refused by remote host

R4#telnet 2.2.2.2

Trying 2.2.2.2 ...
% Connection refused by remote host

R4#telnet 2.2.2.2 /source-interface Lo0

Trying 2.2.2.2 ...
% Connection refused by remote host
```

Note R4 is NOT successful.

Task 2

Configure R2 such that when host 1.1.1.1/24 telnets into any of its interfaces, from the telnet session, this host can only telnet to R4 and no other router. This access-list should not be applied to any of the routers interface.

Configuration

Complete these steps:

Step 1 Before configuring the task, you should test to ensure that the telnet works properly.

```
R1#telnet 10.1.12.2 /source-interface lo0

Trying 10.1.12.2 ... Open

User Access Verification

Password:
       Enter "cisco" as the password

R2>telnet 10.1.25.5

Trying 10.1.25.5 ... Open

User Access Verification

Password:

       Note R1 can successfully telnet into R5

R2>telnet 10.1.45.4

Trying 10.1.45.4 ... Open

User Access Verification

Password:

       Note R1 can successfully telnet into R4.
```

Step 2 R2 confguration.

```
R2(config)#line vty 0 871
R2(config-line)#access-class 2 out

R2(config)#access-list 2 permit host 4.4.4.4
```

Verification

Note R1 has successfuly telnet to R2

```
R1#telnet 10.1.12.2 /source-interface lo0
Trying 10.1.12.2 ... Open

User Access Verification

Password:
```

Note R1 can NOT telnet to R5

```
R2>telnet 5.5.5.5

Trying 5.5.5.5 ...
% Connections to that host not permitted from this terminal
```

Note R1 can ONLY telnet to R4

```
R2>telnet 4.4.4.4
Trying 4.4.4.4 ... Open

User Access Verification

Password:
R4>quit

[Connection to 4.4.4.4 closed by foreign host]
R2>quit
[Connection to 10.1.12.2 closed by foreign host]
```

Note that this solution works only for telnet connections originated from R2 VTYs (for users already connected to the router via telnet). It does not work for regular telnet originated from R2 (i.e. where user is connected via console and issue telnet command).

Task 3

Configure SSH on R4 using the following policy:

Domain name: MicronicsTraining.com

Key: 512 bit

Authentication: The authentication should be performed based on the local database.

Username: User1

Password: Cisco

Authentication Ports:

Local authentication should be configured on VTY.

No authentication should be done on the AUX or the CON lines.

You should only allow SSH connection to the VTY lines.

SSH (Secure Shell) is a protocol that enables a SSH client to make a secure and encrypted connection to Cisco Devices.

Configuration

Complete these steps:

Step 1 R4 configuration.

The following command configures a host domain for this router:

```
R4(config)#ip domain name MicronicsTraining.com
```

The following command generates an RSA key pair for your router, which automatically enables SSH, the last line of this message states that. Remember if you need to delete the RSA key pair, use the "crypto key zeroize rsa" command, once the key pair is deleted, SSH is automatically disabled.

```
R4(config)#crypto key generate rsa usage-keys
```

Once the above command is entered, the following message should appear on the console:

```
The name for the keys will be: R4.MicronicsTraining.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  Signature Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:
Choose the size of the key modulus in the range of 360 to 2048 for your
  Encryption Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]

%SSH-5-ENABLED: SSH 1.99 has been enabled
       Note that in order to use SSHv2 a key of at least 768 bits must
       be generated.

       The following command enables the AAA services

R4(config)#aaa new-model

       To create the requested username and password:

R4(config)#username User1 password Cisco

       The following command is created so it can be applied to all VTY
       ports.

R4(config)#aaa authentication login LOCAL-AUTH local

       The following commands will apply the "LOCAL-AUTH" policy to the
       vty ports:

R4(config)#line vty 0 181
R4(config-line)#login authentication LOCAL-AUTH
R4(config-line)#transport input ssh

       Note that there is no need to create "no authentication" policy
       for AUX and CON. This is because a named authentication list is
       used and it is only applied to the VTY ports.
```

Verification

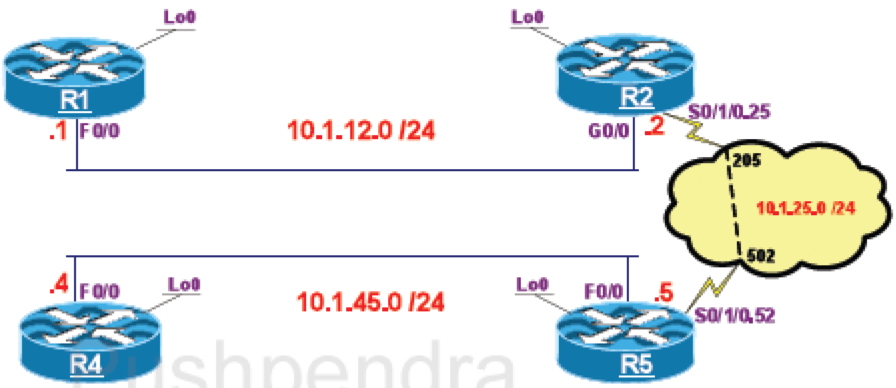
```
R5#ssh -l User1 -c 3des -v 1 10.1.45.4
Password:
R4>exit
[Connection to 10.1.45.4 closed by foreign host]
R5#
```

Task 4

Remove the configuration commands from the previous four steps before proceeding to the next lab.

LAB 3.23. Extended Access List IP and ICMP

Based on lab 2's IP addressing, topology and Lab setup



Task 1

Deny communication between hosts 1.1.1.1 and 4.4.4.4. This must be configured on R2. If these hosts attempt to communicate their packets should not reach their destination.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#access-list 100 deny ip host 4.4.4.4 host 1.1.1.1
R2(config)#access-list 100 permit ip any any

R2(config)#access-list 101 deny ip host 1.1.1.1 host 4.4.4.4
R2(config)#access-list 101 permit ip any any

R2(config)#int s0/1/0.25
R2(config-subif)#ip access-group 100 in

R2(config)#int g0/0
R2(config-subif)#ip access-group 101 in
```

Verification

```
R1#ping 2.2.2.2 source 1.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R1#ping 5.5.5.5 source 1.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.5.5.5, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/60 ms

R1#ping 4.4.4.4 source 1.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
U.U.U
Success rate is 0 percent (0/5)

R1#sh ip ro rip
     2.0.0.0/24 is subnetted, 1 subnets
R       2.2.2.0 [120/1] via 10.1.12.2, 00:00:21, FastEthernet0/0
     4.0.0.0/24 is subnetted, 1 subnets
R       4.4.4.0 [120/3] via 10.1.12.2, 00:00:21, FastEthernet0/0
     5.0.0.0/24 is subnetted, 1 subnets
R       5.5.5.0 [120/2] via 10.1.12.2, 00:00:21, FastEthernet0/0
     10.0.0.0/24 is subnetted, 3 subnets
R       10.1.25.0 [120/1] via 10.1.12.2, 00:00:21, FastEthernet0/0
R       10.1.45.0 [120/2] via 10.1.12.2, 00:00:21, FastEthernet0/0
```

Note even though network 4.4.4.0/24 is in R1's routing table, R1 can't ping 4.4.4.4 IP address, because of the inbound access-list 101 configured on R2's G0/0 interface.

```
R4#ping 5.5.5.5 source 4.4.4.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.5.5.5, timeout is 2 seconds:
Packet sent with a source address of 4.4.4.4
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R4#ping 2.2.2.2 source 4.4.4.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 4.4.4.4
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/57/60 ms

R4#ping 1.1.1.1 source 4.4.4.4


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 4.4.4.4
U.U.U
Success rate is 0 percent (0/5)

R4#ping 1.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/57/60 ms

        Note R4 can ping any IP address except 1.1.1.1 IP address using its Lo0 as the
        source, this is because of the inbound access-list configured on R2's S0/1/0.25
        interface.
```

Task 2

Configure R1 based on the following policy:

- R1 should successfully be able to ping R2 and receive the replies, but R2 should not be able to ping R1.

Configuration

Complete these steps:

Step 1 R1 configuration.

```
R1(config)#access-list 100 deny icmp host 10.1.12.2 any echo
R1(config)#access-list 100 deny icmp host 2.2.2.2 any echo
R1(config)#access-list 100 deny icmp host 10.1.25.2 any echo
R1(config)#access-list 100 permit ip any any

R1(config)#int f0/0
```

```
            R1(config-if)#ip access-group 100 in
```

Verification

```
R1#ping 10.1.12.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

R1#ping 2.2.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R1#ping 10.1.25.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.25.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Note R1 can successfully ping every IP address on R2.

```
R2#ping 10.1.12.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.12.1, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)

R2#ping 1.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
```

Note R2 cannot ping any IP address configured on R1.

```
R5#ping 10.1.12.1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.12.1, timeout is 2 seconds:
!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 56/57/60 ms

       Note R5 can successfully ping any IP address configured on R1


R4#ping 1.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/57/60 ms

       Note R4 can also successfully ping any IP address configured on R1
```

Task 3

R5 should be configured such that if R2 pings a host that is not reachable, R5 does NOT send ICMP host unreachable messages back to R2

Configuration

Complete these steps:

Step 1 Before configuring this task, you should test to see the host unreachable messages. In order to test you must configure the following on R2:

```
R2(config)#ip route 0.0.0.0 0.0.0.0 10.1.25.5

       This static route is needed on R2 so R2 uses R5 for any
       destination/s that it is not aware of.

R2#debug ip icmp

ICMP packet debugging is on

R2#ping 6.6.6.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 6.6.6.6, timeout is 2 seconds:
U.U.U
ICMP: dst (10.1.25.2) host unreachable rcv from 10.1.25.5.U
ICMP: dst (10.1.25.2) host unreachable rcv from 10.1.25.5.U
```

```
Success rate is 0 percent (0/5)

ICMP: dst (10.1.25.2) host unreachable rcv from 10.1.25.5

       Note the default route was needed for testing this
       scenario. Once 6.6.6.6 is pinged, the local router (R2)
       will perform a route table lookup and the closest match to
       that destination is the default gateway which is pointing
       to R5. Since R5 is not aware of this IP address, it sends
       icmp host unreachables back to the source (R2).
```

Step 2 R5 configuration.

```
R5(config)#int S0/1/0.52
R5(config-subif)#no ip unreachables
```

Verification

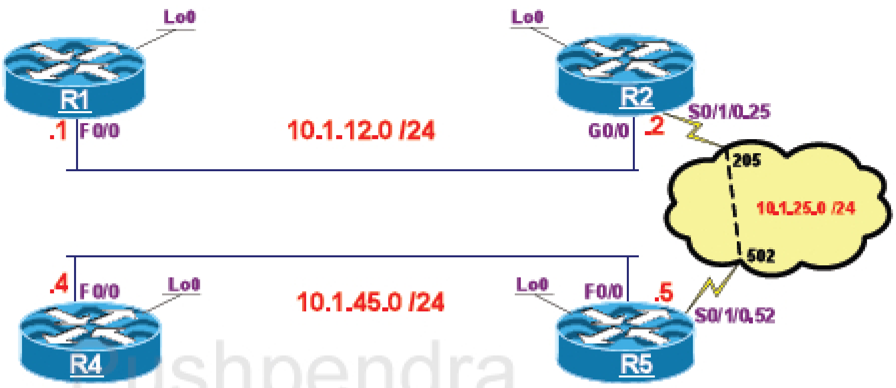
```
R2#ping 6.6.6.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 6.6.6.6, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

       Note R2 is no longer receiving the ICMP unreachables.
```

Task 4

Erase the startup config and reload the routers before proceeding to the next lab.

LAB 3.24. Extended Access List OSPF & EIGRP

Based on Lab 2's IP addressing and Topology



Task 0 - Preconfiguration

- Configure OSPF Area 0 and EIGRP 100 on all routers and advertise every interface in both routing protocols
- Ensure that "no auto-summary" command is used when configuring EIGRP 100
- In OSPF routing protocol, the loopback interfaces should be advertised with their correct mask

Configuration

Complete these steps:

Step 1 On all routers.

```
(config)#router ospf 1
(config-router)#network 0.0.0.0 0.0.0.0 area 0
(config-router)#exi

(config)#router eigrp 100
(config-router)#no auto
```

```
(config-router)#network 0.0.0.0 0.0.0.0
(config-router)#exi

(config)#int lo0
(config-if)#ip ospf network point-to-point
(config-if)#exi
```

Task 1

Configure an access-list on R1 to block EIGRP routing protocol and allow the rest of the IP protocol stack, if this configuration is performed successfully router R1 should only have OSPF routes in its routing table.

Configuration

Complete these steps:

Step 1 Before you configure this task, you should display the existing routing table:

```
R1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/24 is subnetted, 1 subnets
C       1.1.1.0 is directly connected, Loopback0
     2.0.0.0/24 is subnetted, 1 subnets
D       2.2.2.0 [90/156160] via 10.1.12.2, 00:01:47, FastEthernet0/0
     4.0.0.0/24 is subnetted, 1 subnets
D       4.4.4.0 [90/2302976] via 10.1.12.2, 00:01:35, FastEthernet0/0
     5.0.0.0/24 is subnetted, 1 subnets
D       5.5.5.0 [90/2300416] via 10.1.12.2, 00:01:35, FastEthernet0/0
     10.0.0.0/24 is subnetted, 3 subnets
C       10.1.12.0 is directly connected, FastEthernet0/0
D       10.1.25.0 [90/2172416] via 10.1.12.2, 00:01:49, FastEthernet0/0
D       10.1.45.0 [90/2174976] via 10.1.12.2, 00:01:37, FastEthernet0/0
```

```
Note you only see the EIGRP advertised routes because EIGRP has a
lower administrative distance - 90 versus 110.
```

Step 2 R1 configuration.

```
R1(config)#access-list 100 deny eigrp any any
R1(config)#access-list 100 permit ip any any

R1(config)#int f0/0
R1(config-if)#ip access-group 100 in
```

Verification

```
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 10.1.12.2 (FastEthernet0/0) is down:
holding time expired

R1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/24 is subnetted, 1 subnets
C       1.1.1.0 is directly connected, Loopback0
     2.0.0.0/24 is subnetted, 1 subnets
O       2.2.2.0 [110/2] via 10.1.12.2, 00:00:08, FastEthernet0/0
     4.0.0.0/24 is subnetted, 1 subnets
O       4.4.4.0 [110/67] via 10.1.12.2, 00:00:08, FastEthernet0/0
     5.0.0.0/24 is subnetted, 1 subnets
O       5.5.5.0 [110/66] via 10.1.12.2, 00:00:08, FastEthernet0/0
     10.0.0.0/24 is subnetted, 3 subnets
C       10.1.12.0 is directly connected, FastEthernet0/0
O       10.1.25.0 [110/65] via 10.1.12.2, 00:00:09, FastEthernet0/0
O       10.1.45.0 [110/66] via 10.1.12.2, 00:00:09, FastEthernet0/0
```

```
Note when the access-list is configured, the EIGRP neighbor adjacency between
R1 and R2 fails, and OSPF is allowed in the routing table.
```

Task 2

Remove the configuration command from the previous step (Task 1), erase the startup config and reload the routers before proceeding to the next lab.

Configuration

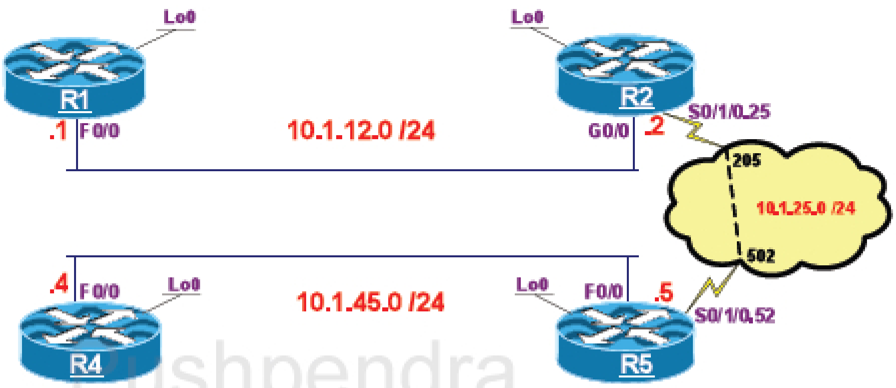
Complete these steps:

Step 1 R1 configuration.

```
R1(config)#NO access-list 100

R1(config)#int f0/0
R1(config-if)#NO ip access-group 100 in
```

LAB 3.25. Extended Access List With Established

Based on Lab 2s IP addressing and Topology



Task 0 - Preconfiguration

- Configure OSPF routing protocol on all routers and advertise every interface in OSPF Area 0.

Configuration

Complete these steps:

Step 1 On all routers.

```
(config)#router ospf 1
(config-router)#network 0.0.0.0 0.0.0.0 area 0
(config-router)#exi
```

Task 1

R1, R4 and R5 are offering telnet and HTTP services. R1 and R2 are the routers in your company; your company's policy is as follows:

R2 is the border router that connects R1 to the other routers. R2 should be configured with an inbound access-list such that it ONLY allows traffic that was initiated locally and by R1 to be returned. Ensure that the appropriate traffic is allowed. No other traffic should be allowed in.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#access-list 100 permit ospf any any
R2(config)#access-list 100 permit tcp any any established

R2(config)#int S0/1/0.25
R2(config-subif)#ip access-group 100 in
```

Verification

```
R1#telnet 10.1.45.4


Trying 10.1.45.4 ... Open

Password required, but none set


R2#sh access-list

Extended IP access list 100
    10 permit ospf any any (5 matches)
    20 permit tcp any any established (6 matches)
```

To test the configuration using ICMP and UDP

```
R4#sh flash | in bin
8      59455672 Feb 03 2010 13:34:44 c2800nm-adventerprisek9-mz.124-24.T2.bin

R4(config)#tftp-server flash:c2800nm-adventerprisek9-mz.124-24.T2.bin


R1#copy tftp flash
Address or name of remote host [10.1.45.4]?
Source filename [c2800nm-adventerprisek9-mz.124-24.T2.bin]?
Destination filename [c2800nm-adventerprisek9-mz.124-24.T2.bin]? test.bin
```

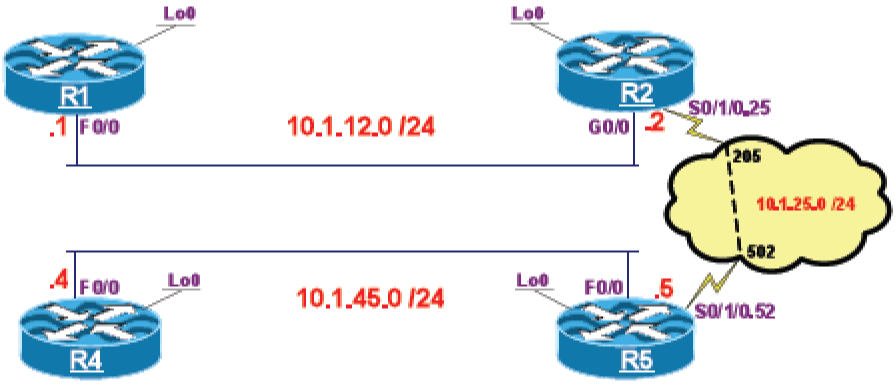
```
Accessing tftp://10.1.45.4/c2800nm-adventerprisek9-mz.124-24.T2.bin...
%Error opening tftp://10.1.45.4/c2800nm-adventerprisek9-mz.124-24.T2.bin (Timed out)

        Note “Established” only works on TCP based application and TFTP in this case
failed.

R1#ping 10.1.45.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.45.4, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

        Note ICMP will not be allowed back in, even though the traffic was initiated
        from R1, because the “Established” keyword only works on TCP based
        applications.

R1#sh ip route ospf
     2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O       2.2.2.2/32 [110/2] via 10.1.12.2, 00:09:14, FastEthernet0/0
     4.0.0.0/32 is subnetted, 1 subnets
O       4.4.4.4 [110/67] via 10.1.12.2, 00:09:14, FastEthernet0/0
     5.0.0.0/32 is subnetted, 1 subnets
O       5.5.5.5 [110/66] via 10.1.12.2, 00:09:04, FastEthernet0/0
     10.0.0.0/24 is subnetted, 3 subnets
O       10.1.25.0 [110/65] via 10.1.12.2, 00:09:14, FastEthernet0/0
O       10.1.45.0 [110/66] via 10.1.12.2, 00:09:14, FastEthernet0/0

        Note the routing protocol was NOT affected because it was specifically allowed
        in the access-list.
```

Task 2

Erase the startup config and reload the routers before proceeding to the next lab.

LAB 3.26. Dynamic Access List

Based on Lab 2s IP addressing and Topology



Task 0 - Preconfiguration

- Configure OSPF routing protocol on all routers and advertise their directly connected interfaces in OSPF Area 0
- The loopback interfaces should be advertised with their correct mask
- Create the following users on R2:

  First user name: U3, password: U3

  Second user name: U4, password U4

Configuration

Complete these steps:

Step 1 On all routers.

```
(config)#router ospf 1
(config-router)#network 0.0.0.0 0.0.0.0 area 0
(config-router)#exi

(config)#int lo0
(config-if)#ip ospf network point-to-point
(config-if)#exi
```

Step 2 R2 configuration.

```
R2(config)#username U3 password U3
R2(config)#username U4 password U4
```

Task 1

R1 and R2 belong to the same company; R2 is the border router connecting their company (consisting of R1 and R2) to the other routers belonging to another company (consisting of R4 and R5). Create a dynamic access-list on R2 using the following policy:

- Only the authenticated users are allowed to have access to R1
- Allow R5 and/or R4 to telnet into R2's S0/1/0.25 interface to get authenticated (using the usernames created in the lab setup) before they can access any of the services offered by R1
- This policy should NOT affect the routing protocol
- R1 or R2 should be able to have access to R5 and R4, without authentication

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#access-list 100 permit tcp any host 10.1.25.2 eq 23

        This access-list is needed so R5 and R4 can telnet to, in order to
get authenticated.


R2(config)#access-list 100 permit ospf any any

        This statement is required to allow OSPF through.

R2(config)#access-list 100 permit tcp any any established

        This statement allows the return traffic in the network that was
        initiated by any of the users within the company (R1 and/or R2 in
        this case).

R2(config)#access-list 100 dynamic TEST permit ip any any

        Note the above statement in the access-list tells the router to
```

create a dynamic access-list called TEST. This named access-list will be created when U3 and/or U4 telnet to this router and get authenticated.

```
R2(config)#int S0/1/0.25
R2(config-subif)#ip access-group 100 in
```

The above command is applying the access-list inbound to S0/1/0.25 interface.

Lastly the telnet ports must be configured for the dynamic access-list:

```
R2(config-subif)#line vty 0 871
R2(config-line)#autocommand access-enable host
R2(config-line)#login local
```

Note the access-enable may not show when a question mark is entered, because it's a hidden command. The "autocommand" command links the dynamic access-list to the telnet authentication. It creates an entry in the dynamic access-list using the source IP address of the host. If the "autocommand" is NOT used, the dynamic entry will not be created.
The second line specifies that authentication should be done using the local user account database.

Verification

```
R4#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/24 is subnetted, 1 subnets
O       1.1.1.0 [110/67] via 10.1.45.5, 00:04:01, FastEthernet0/0
     2.0.0.0/24 is subnetted, 1 subnets
O       2.2.2.0 [110/66] via 10.1.45.5, 00:04:01, FastEthernet0/0
     4.0.0.0/24 is subnetted, 1 subnets
C       4.4.4.0 is directly connected, Loopback0
     5.0.0.0/24 is subnetted, 1 subnets
O       5.5.5.0 [110/2] via 10.1.45.5, 00:03:51, FastEthernet0/0
```

```
     10.0.0.0/24 is subnetted, 3 subnets
O       10.1.12.0 [110/66] via 10.1.45.5, 00:04:01, FastEthernet0/0
O       10.1.25.0 [110/65] via 10.1.45.5, 00:04:02, FastEthernet0/0
C       10.1.45.0 is directly connected, FastEthernet0/0
```

Note the routing table contains all the networks.

```
R4#ping 1.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
```

The ping failed because R4 is not an authenticated user.

In the following steps, R4 will telnet to R2 in order to get authenticated. Note R4's telnet session is closed right after the authentication.

```
R4#telnet 10.1.25.2

Trying 10.1.25.2 ... Open

User Access Verification

Username: U3          Entering the username U3

Password:          Entering the password "U3" to get authenticated
[Connection to 10.1.25.2 closed by foreign host]
```

Note once the user gets authenticated, the telnet session is closed by 10.1.25.2.

To test connectivity:

```
R4#ping 1.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/58/60 ms

R4#telnet 1.1.1.1

Trying 1.1.1.1 ... Open

User Access Verification

Password:
```

Note both telnet and ping commands are successful after a successful authentication.

```
R2#show access-list
```

Note the dynamically created ACL

```
Extended IP access list 100
    10 permit tcp any host 10.1.25.2 eq telnet (60 matches)
    20 permit ospf any any (77 matches)
    30 permit tcp any any established (10 matches)
    40 Dynamic TEST permit ip any any
       permit ip host 10.1.45.4 any (6 matches)
```

Task 2

Clear the dynamically created access-list entry from R2, do not remove and reenter the access-list to accomplish this task. Configure an idle timeout on R2 for the dynamic access-list such that if an authenticated user is idle for 2 minutes the entry is removed.

Note a password was not entered, the telnet session expired, but the dynamic access-list is still on R2 allowing IP to any source going to any destination.

```
R4#telnet 1.1.1.1
Trying 1.1.1.1 ... Open

User Access Verification

Password:
% Password:  timeout expired!
Password:
% Password:  timeout expired!
Password:
% Password:  timeout expired!
% Bad passwords
[Connection to 1.1.1.1 closed by foreign host]
```

Check the dynamically created access-list:

```
R2#show access-list

Extended IP access list 100
    10 permit tcp any host 10.1.25.2 eq telnet (60 matches)
    20 permit ospf any any (98 matches)
    30 permit tcp any any established (13 matches)
    40 Dynamic TEST permit ip any any
       permit ip host 10.1.45.4 any (6 matches)
```

Configuration

To clear the dynamically created access-list:

```
R2#clear ip access-template 100 TEST host 10.1.45.4 any
```

To verify the configuration:

```
R2#show ip access-list

Extended IP access list 100
    10 permit tcp any host 10.1.25.2 eq telnet (60 matches)
    20 permit ospf any any (125 matches)
    30 permit tcp any any established (13 matches)
    40 Dynamic TEST permit ip any any
```

Note the dynamic entry is purged. Enter the following commands to setup the requested timeout value:

```
R2(config)#line vty 0 871
R2(config-line)#autocommand access-enable host timeout 2
```

The timeout here defines the idle timeout and it is in minutes.

To test the configuration:

```
R4#telnet 10.1.25.2

Trying 10.1.25.2 ... Open

User Access Verification

Username: U4
Password:
[Connection to 10.1.25.2 closed by foreign host]

R4#telnet 1.1.1.1

Trying 1.1.1.1 ... Open

User Access Verification

Password:
R1>
```

```
R2#sh access-list

Extended IP access list 100
    10 permit tcp any host 10.1.25.2 eq telnet (120 matches)
    20 permit ospf any any (175 matches)
    30 permit tcp any any established (26 matches)
    40 Dynamic TEST permit ip any any
       permit ip host 10.1.45.4 any (1 match) (time left 107)

R2#sh access-list

Extended IP access list 100

    10 permit tcp any host 10.1.25.2 eq telnet (120 matches)
    20 permit ospf any any (176 matches)
    30 permit tcp any any established (26 matches)
    40 Dynamic TEST permit ip any any
       permit ip host 10.1.45.4 any (1 match) (time left 97)

R2#sh access-list

Extended IP access list 100
    10 permit tcp any host 10.1.25.2 eq telnet (120 matches)
    20 permit ospf any any (185 matches)
    30 permit tcp any any established (26 matches)
    40 Dynamic TEST permit ip any any
       permit ip host 10.1.45.4 any (1 match) (time left 26)

R2#sh access-list

Extended IP access list 100
    10 permit tcp any host 10.1.25.2 eq telnet (120 matches)
    20 permit ospf any any (187 matches)
    30 permit tcp any any established (26 matches)
    40 Dynamic TEST permit ip any any
       permit ip host 10.1.45.4 any (1 match) (time left 1)

R2#sh access-list

Extended IP access list 100
    10 permit tcp any host 10.1.25.2 eq telnet (120 matches)
    20 permit ospf any any (187 matches)
    30 permit tcp any any established (26 matches)
    40 Dynamic TEST permit ip any any
       permit ip host 10.1.45.4 any (1 match)
```

Note the (time left) counter starts counting down from 120 seconds and once it reaches zero, the dynamically created access-list is purged.

Task 3

Re-configure this access-list such that the maximum time limit for each entry regardless of activity within this dynamic access-list is set to 3 minutes.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
        This command removes the access-list.

R2(config)#no access-list 100

        This command removes the "autocommand" command with an idle timeout
        value configured.

R2(config)#line vty 0 871
R2(config-line)#no autocommand access-enable host timeout 2
R2(config-line)#autocommand access-enable host


R2(config)#access-list 100 permit tcp any host 10.1.25.2 eq 23
R2(config)#access-list 100 permit ospf any any
R2(config)#access-list 100 permit tcp any any established
R2(config)#access-list 100 dynamic TEST timeout 3 permit ip any any

        This timeout is the absolute or time to live timeout, which defines
        the amount of time in minutes a dynamically created access-list, can
        exist.
        Since the access-list is already applied to the S0/1/0.25 sub-
        interface of R2, there is no need to re-apply the access-list.
```

Task 4

After configuring the dynamic access-list you realized that from time to time the administrator needs to telnet into R2 for trouble shooting and management purposes. Re-configure R2 such that the administrators can telnet into this router successfully to perform their day to day management tasks.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#line vty 0 870
R2(config-line)#login local
R2(config-line)#autocommand access-enable host

R2(config)#line vty 871
R2(config-line)#login local
R2(config-line)#rotary 5
R2(config-line)#no autocommand access-enable host
```

Note only one session is reserved for administration purposes, more ports can be used for this purpose. The "rotary 5" command allows telnet access to port 3005 instead of 23, this port number should be allowed in the access-list and therefore, it must be added to the existing access-list.

```
R2(config)#access-list 100 permit tcp any any eq 3005
```

Remember that "autocommand" can also be used for a specific user configuration by configuring "username.... autocommand access-enable host"; therefore, another solution in configuring this task is to move the autocommand to the other users and remove it from the vty line.

See that telnet to R1 loopback fails without authentication against R2.

Note that telnet to the port 3005 is successful and it allows administrator to issue commands on R2.

Verification

```
R4#telnet 1.1.1.1
Trying 1.1.1.1 ...
% Destination unreachable; gateway or host down

R4#telnet 10.1.25.2
Trying 10.1.23.2 ... Open

User Access Verification

Username: U3
Password:
[Connection to 10.1.25.2 closed by foreign host]
```

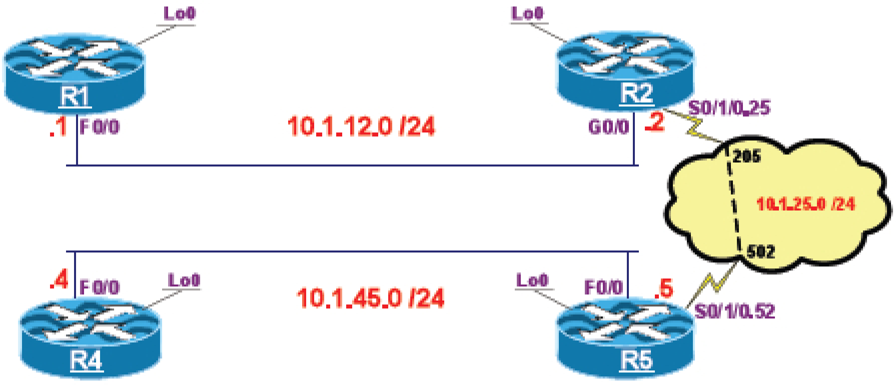
```
R4#telnet 1.1.1.1
Trying 1.1.1.1 ... Open

User Access Verification

Password:
[Connection to 1.1.1.1 closed by foreign host]

R4#telnet 10.1.25.2 3005
Trying 10.1.25.2, 3005 ... Open

User Access Verification

Username: U4
Password:
R2>exit

[Connection to 10.1.25.2 closed by foreign host]
R4#
```

Task 5

Erase the startup config and reload the router before proceeding to the next lab.

LAB 3.27. Reflexive Access-lists

Based on Lab 2s IP addressing and Topology



Task 0: Preconfiguration

- Configure the routers according to LAB 2's IP addressing and topology
- Configure OSPF routing protocol on all routers and advertise every interface in OSPF Area 0.
- The loopback interfaces should be advertised with their correct mask.

Configuration

Complete these steps:

Step 1 On all routers.

```
(config)#router ospf 1
(config-router)#network 0.0.0.0 0.0.0.0 area 0
(config-router)#exi

(config)#int lo0
(config-if)#ip ospf network point-to-point
(config-if)#exi
```

Task 1

R1 and R2 belong to Company-A. R4 and R5 belong to Company-B. R2 is the border router that connects these companies to each other; R2 should be configured such that it allows the return traffic for the following protocols:

- R2 should allow the return HTTP traffic that is originated locally or by R1.
- R2 should allow the return telnet traffic that is originated locally or by R1.
- R2 should allow the return TFTP traffic that is originated locally or by R1.
- R2 should allow the OSPF traffic into the network.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#ip access-list extended outbound
R2(config-ext-nacl)#permit tcp any any eq 80 reflect TEST
R2(config-ext-nacl)#permit tcp any any eq 23 reflect TEST
R2(config-ext-nacl)#permit udp any any eq 69 reflect TEST
R2(config-ext-nacl)#permit ospf any any

R2(config)#ip access-list extended inbound
R2(config-ext-nacl)#permit ospf any any

R2(config-ext-nacl)#evaluate TEST

R2(config)#int S0/1/0.25
R2(config-subif)#ip access-group inbound in
R2(config-subif)#ip access-group outbound out
```

Verification

```
R4#sh ip route ospf
     1.0.0.0/24 is subnetted, 1 subnets
O       1.1.1.0 [110/67] via 10.1.45.5, 00:23:24, FastEthernet0/0
     2.0.0.0/24 is subnetted, 1 subnets
O       2.2.2.0 [110/66] via 10.1.45.5, 00:23:24, FastEthernet0/0
     5.0.0.0/24 is subnetted, 1 subnets
O       5.5.5.0 [110/2] via 10.1.45.5, 00:23:24, FastEthernet0/0
     10.0.0.0/24 is subnetted, 3 subnets
O       10.1.12.0 [110/66] via 10.1.45.5, 00:23:24, FastEthernet0/0
O       10.1.25.0 [110/65] via 10.1.45.5, 00:23:24, FastEthernet0/0
```

Note R4 has network 1.1.1.0 /24 in its routing table, because OSPF is allowed through.

```
R4#ping 1.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
```

```
R4#telnet 1.1.1.1

Trying 1.1.1.1 ...
% Destination unreachable; gateway or host down
```

Note even though network 1.1.1.0 /24 is in R4's routing table no traffic is allowed in that network.

```
R1#telnet 4.4.4.4

Trying 4.4.4.4 ... Open

User Access Verification

Password:
R4>
```

Note R1 has established a telnet session with R4. To see the dynamically added lines in the ACL that allows this traffic to return do not close this connection and go to R2:

```
R2#show access-list
Reflexive IP access list TEST
     permit tcp host 4.4.4.4 eq telnet host 10.1.12.1 eq 22887 (28 matches) (time left
287)
Extended IP access list inbound
    10 permit ospf any any (15 matches)
    20 evaluate TEST
Extended IP access list outbound
    10 permit tcp any any eq www reflect TEST
    20 permit tcp any any eq telnet reflect TEST (39 matches)
    30 permit udp any any eq tftp reflect TEST
    40 permit ospf any any
```

Note an access-list is created dynamically called TEST. This access-list was created as a result of R1s telnet to R4's 4.4.4.4 IP address using port 22887 as the source and 23 as the destination port, therefore, this is created so the return traffic can be permitted back in.

Task 2

Re-configure the RACL on R2 using the following parameters:

- R2 should allow the return HTTP traffic that is originated locally or by R1. The temporary access-list should be set with an idle timeout of 120 seconds.
- R2 should allow the return telnet traffic that is originated locally or by R1. The temporary access-list should be set with an idle timeout of 60 seconds.
- R2 should allow the return TFTP traffic that is originated locally or by R1. The temporary access-list should be set with an idle timeout of 30 seconds.
- R2 should allow the return ICMP and DNS traffic that is originated locally or by R1. The temporary access-list should be set with an idle timeout of 10 seconds.
- R2 should allow the OSPF traffic into the network.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#no ip access-list extended outbound

R2(config)#ip access-list extended outbound
R2(config-ext-nacl)#permit ospf any any
R2(config-ext-nacl)#permit tcp any any eq 80 reflect TEST timeout 120
R2(config-ext-nacl)#permit tcp any any eq 23 reflect TEST timeout 60
R2(config-ext-nacl)#permit udp any any eq 69 reflect TEST timeout 30
R2(config-ext-nacl)#permit icmp any any reflect TEST timeout 10
R2(config-ext-nacl)#permit udp any any eq 53 reflect TEST timeout 10
```

Verification

To generate some ICMP traffic:

```
R1#ping 4.4.4.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/58/60 ms
```

To see the dynamically created access-list:

```
R2#sh access-list

Reflexive IP access list TEST
     permit icmp host 4.4.4.4 host 10.1.12.1  (10 matches) (time left 1)
Extended IP access list inbound
    10 permit ospf any any (85 matches)
    20 evaluate TEST
Extended IP access list outbound
    10 permit ospf any any
    20 permit tcp any any eq www reflect TEST
    30 permit tcp any any eq telnet reflect TEST

    40 permit udp any any eq tftp reflect TEST
    50 permit icmp any any reflect TEST (5 matches)
    60 permit udp any any eq domain reflect TEST
```

To generate telnet traffic:

```
R1#telnet 4.4.4.4

Trying 4.4.4.4 ... Open

User Access Verification

Password:
R4>
```

To see the dynamically added access-list:

```
R2#Sh access-list

Reflexive IP access list TEST
     permit tcp host 4.4.4.4 eq telnet host 10.1.12.1 eq 41142 (33 matches) (time left
54)
Extended IP access list inbound
    10 permit ospf any any (102 matches)
    20 evaluate TEST
Extended IP access list outbound
    10 permit ospf any any
    20 permit tcp any any eq www reflect TEST
    30 permit tcp any any eq telnet reflect TEST (19 matches)
    40 permit udp any any eq tftp reflect TEST
    50 permit icmp any any reflect TEST (5 matches)
    60 permit udp any any eq domain reflect TEST
```

Task 3

Re-configure the timeout parameter of the extended “outbound” access-list such that all the dynamically created entries have a time to live of 120 seconds, DO NOT use the timeout argument in the access-list to accomplish this task.

Configuration

Complete these steps:

Step 1 R2 configuration.

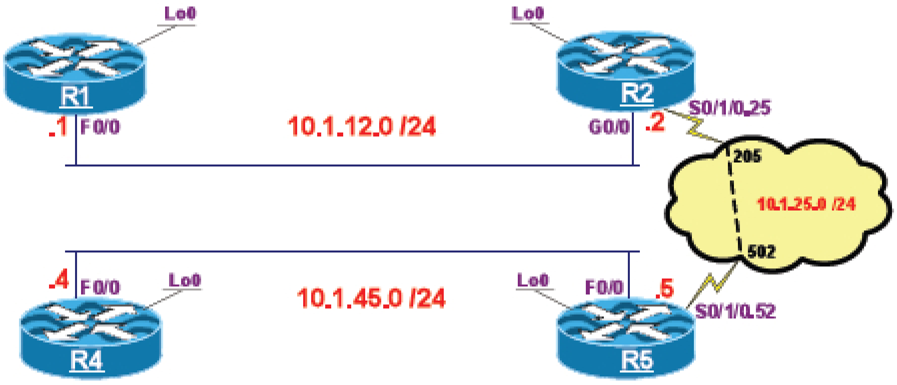
```
R2(config)#no ip access-list extended outbound

R2(config)#ip access-list extended outbound
R2(config-ext-nacl)#permit ospf any any
R2(config-ext-nacl)#permit tcp any any eq 80 reflect TEST
R2(config-ext-nacl)#permit tcp any any eq 23 reflect TEST
R2(config-ext-nacl)#permit udp any any eq 69 reflect TEST
R2(config-ext-nacl)#permit icmp any any reflect TEST
R2(config-ext-nacl)#permit udp any any eq 53 reflect TEST

R2(config)#ip reflexive-list timeout 120

        The above command specifies the length of time that reflexive access
        list entries will continue to exist when no packets in the session
        are detected, by default the timeout value is set to 300 seconds.
        Note if you have configured a timeout for each RACL entry and you
        have also configured the global timeout command, the more specific
        ones that are configured for each entry will take precedence over
        the global command.
```

Task 4

Erase the startup config and reload the routers before proceeding to the next lab.

LAB 3.28. Access-list and Time-range

Based on Lab 2' IP addressing and Topology



Task 0: Preconfiguration

- Configure the routers according to LAB 2's IP addressing and topology
- Configure OSPF routing protocol on all routers and advertise every interface in OSPF Area 0.
- The loopback interfaces should be advertised with their correct mask.

Configuration

Complete these steps:

Step 1 On all routers.

```
(config)#router ospf 1
(config-router)#network 0.0.0.0 0.0.0.0 area 0
(config-router)#exi

(config)#int lo0
(config-if)#ip ospf network point-to-point
(config-if)#exi
```

Task 1

Configure R1 to allow its internal users to have the ability to browse the Internet during the weekdays ONLY. R4 should be configured such that its internal users can only browse the Internet in weekends. The access-list should be applied outbound on their F0/0 interface, since this is the interface that connects these routers to the Internet.

Configuration

Complete these steps:

Step 1 R1 configuration.

```
R1(config)#time-range WEEKDAYS
R1(config-time-range)#periodic weekdays 00:00 to 23:59

R1(config)#access-list 100 permit tcp any any eq 80 time-range WEEKDAYS

R1(config)#int f0/0
R1(config-if)#ip access-group 100 out
```

Step 3 R4 configuration.

```
R4(config)#time-range WEEKENDS
R4(config-time-range)#periodic weekend 00:00 to 23:59

R4(config)#access-list 100 permit tcp any any eq 80 time-range WEEKENDS

R4(config)#int f0/0
R4(config-if)#ip access-group 100 out
```

The first step in configuring this policy is to configure the time-range and define the allowed time range. The second step is to configure the access-list referencing the time-range and lastly applying the access-list using the "access-group" command to the interface.

Task 2

Configure R5 to allow its internal users to browse the Internet using the following policy:

- This should ONLY be allowed Weekdays (Mon – Fri) between the hours of 2:00 PM and 6:30 PM.
- Because of unusual work load and special projects, this should NOT be allowed starting July 20th through Nov 26th 9:00 AM to 5:00 PM during the week days.
- The access-list should be applied outbound on their F0/0 interface, since this is the interface that connects to the Internet.

Configuration

Complete these steps:

Step 1 R5 configuration.

```
R5(config)#time-range ALLOW
R5(config-time-range)#periodic weekdays 14:00 to 18:30

R5(config)#time-range DENIED
R5(config-time-range)#absolute start 00:00 20 July 2010 end 23:59 26
November 2010
      Note that the above line may be different depends on the year.

R5(config-time-range)#periodic weekdays 9:00 to 17:00

R5(config)#access-list 100 deny tcp any any eq 80 time-range DENIED
R5(config)#access-list 100 permit tcp any any eq 80 time-range ALLOW

R5(config)#int f0/0
R5(config-if)#ip access-group 100 out
```

Verification

```
R5#sh access-lists
Extended IP access list 100
    10 deny tcp any any eq www time-range DENIED (inactive)
    20 permit tcp any any eq www time-range ALLOW (inactive)

R5#sh clock
*01:18:33.819 UTC Fri Sep 3 2010

R5#clock set 10:00:00 Sep 3 2010
```

```
R5#
%SYS-6-CLOCKUPDATE: System clock has been updated from 01:19:35 UTC Fri Sep 3 2010 to
10:00:00 UTC Fri Sep 3 2010, configured from console by console.

R5#sh clock
10:00:07.023 UTC Fri Sep 3 2010

R5#sh access-lists
Extended IP access list 100
    10 deny tcp any any eq www time-range DENIED (active)
    20 permit tcp any any eq www time-range ALLOW (inactive)
```

Task 3

Configure R2 using the following policy:

- Outgoing telnet traffic should only be denied between the hours of 11:00 AM and 2:00 PM, Monday to Friday.
- Outbound HTTP calls should be denied Monday to Friday, between the hours of 9:00 AM and 2:00 PM starting Feb 19th 2010 to April 24th 2010.
- Any other traffic should be denied. Ensure that the access-list is applied outbound on their G0/0 interface, since this is the interface that connects to the Internet.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#time-range TELNET
R2(config-time-range)#periodic weekdays 11:00 to 14:00

R2(config)#time-range HTTP
R2(config-time-range)#absolute start 00:00 19 Feb 2010 end 23:59 24 Apr 2010
R2(config-time-range)#periodic weekdays 9:00 to 14:00

R2(config)#access-list 100 deny tcp any any eq 23 time-range TELNET
R2(config)#access-list 100 permit tcp any any eq 23
R2(config)#access-list 100 deny tcp any any eq 80 time-range HTTP
R2(config)#access-list 100 permit tcp any any eq 80

R2(config)#int g0/0
R2(config-if)#ip access-group 100 out
```

Verification

```
R2#sh access-lists
Extended IP access list 100
    10 deny tcp any any eq telnet time-range TELNET (inactive)
    20 permit tcp any any eq telnet
    30 deny tcp any any eq www time-range HTTP (inactive)
    40 permit tcp any any eq www

R2#sh clock
*05:27:20.087 UTC Fri Sep 3 2010

R2#clock set 10:00:00 May 3 2010
R2#
%SYS-6-CLOCKUPDATE: System clock has been updated from 05:27:49 UTC Fri Sep 3 2010 to
10:00:00 UTC Mon May 3 2010, configured from console by console.

R2#sh clock
10:00:04.303 UTC Mon May 3 2010

R2#sh access-lists
Extended IP access list 100
    10 deny tcp any any eq telnet time-range TELNET (inactive)
    20 permit tcp any any eq telnet
    30 deny tcp any any eq www time-range HTTP (inactive)
    40 permit tcp any any eq www
```

The HTTP ACE is inactive because the clock is out of scope (we should be between Feb and Apr).

```
R2#clock set 10:00:00 Apr 3 2010
%SYS-6-CLOCKUPDATE: System clock has been updated from 10:02:30 UTC Mon May 3 2010 to
10:00:00 UTC Sat Apr 3 2010, configured from console by console.

R2#sh clock
10:00:02.963 UTC Sat Apr 3 2010

R2#sh access-lists
Extended IP access list 100
    10 deny tcp any any eq telnet time-range TELNET (inactive)
    20 permit tcp any any eq telnet
    30 deny tcp any any eq www time-range HTTP (inactive)
    40 permit tcp any any eq www
```

Again, the HTTP ACE is inactive because the clock is out of scope (we are in April but the day is Saturday).

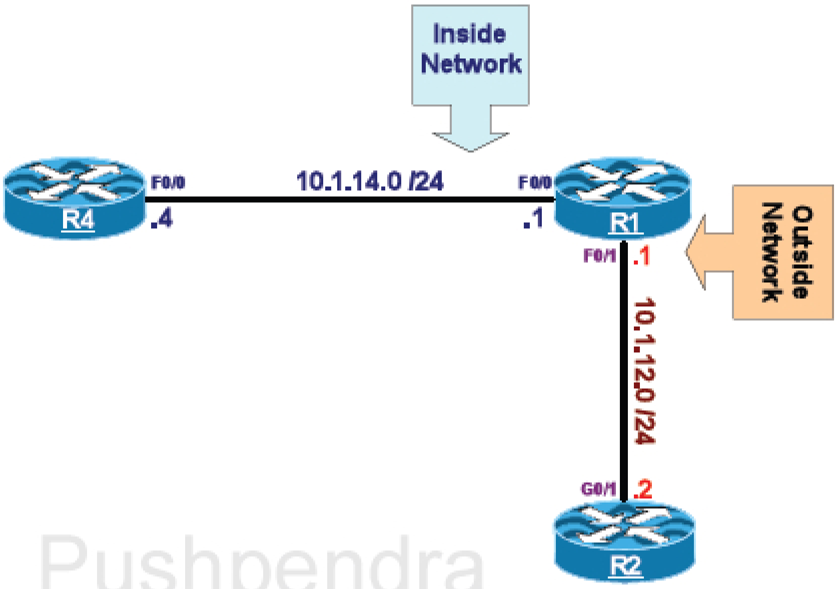
```
R2#clock set 10:00:00 Apr 5 2010
%SYS-6-CLOCKUPDATE: System clock has been updated from 10:00:26 UTC Sat Apr 3 2010 to
10:00:00 UTC Mon Apr 5 2010, configured from console by console.
```

```
R2#sh clock
10:00:03.967 UTC Mon Apr 5 2010

R2#sh access-lists
Extended IP access list 100
    10 deny tcp any any eq telnet time-range TELNET (inactive)
    20 permit tcp any any eq telnet
    30 deny tcp any any eq www time-range HTTP (active)
    40 permit tcp any any eq www
```

Task 4

Erase the startup config and reload the routers before proceeding to the next lab.

LAB 3.29. Configuring Basic CBAC



Lab Setup

- The F0/1 interface of R1 and R2's G0/1 interface should be configured in VLAN 12.
- The F0/0 interface of R1 and R4 should be configured in VLAN 14.
- Configure RIPv2 on all routers and advertise their directly connected interfaces in this routing protocol.

IP Addressing

Router	Interface	IP address
R1	F0/0	10.1.14.1/24
	F0/1	10.1.12.1/24
R2	G0/1	10.1.12.2/24
R4	F0/0	10.1.14.4/24

Task 1

Configure R1 to perform a generic TCP, UDP and ICMP inspection, ensure that only the traffic that was initiated from inside is allowed back in. You should also allow the appropriate traffic through.

Configuration

Complete these steps:

Step 1 R1 configuration.

```
R1(config)#access-list 100 permit udp any any eq 520
R1(config)#access-list 100 deny ip any any log

R1(config)#ip inspect name FW TCP
R1(config)#ip inspect name FW UDP
R1(config)#ip inspect name FW ICMP

R1(config)#interface f0/1
R1(config-if)#ip access-group 100 in
R1(config-if)#ip inspect FW out
```

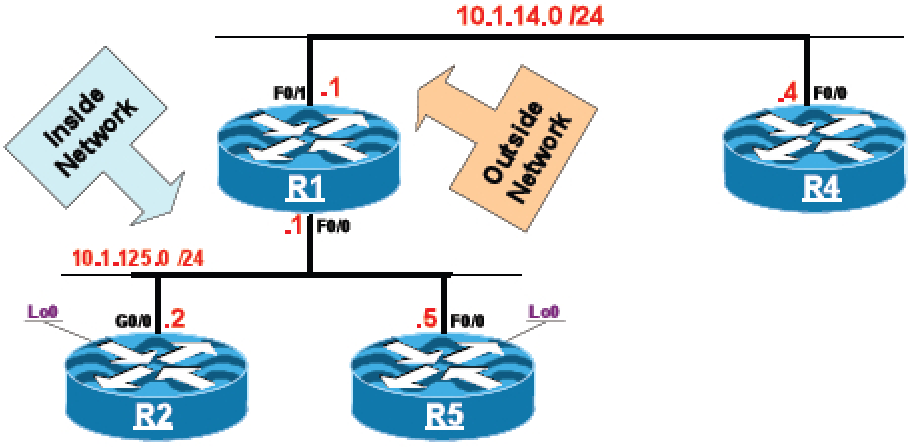
Verification

```
R4#telnet 10.1.12.2
Trying 10.1.12.2 ... Open


User Access Verification

Password:
R2>

R1#sh ip inspect session
Established Sessions
 Session 48E194C8 (10.1.14.4:11577)=>(10.1.12.2:23) tcp SIS_OPEN

        Note this entry was added to the state table for the telnet session.
```

Task 2

Erase the startup configuration and reload the routers before proceeding to the next lab.

LAB 3.30. Configuring Advanced CBAC



Lab Setup

- The F0/1 interface of R1 and R4's F0/0 interface should be configured in VLAN 14.
- The F0/0 interface of R1, R2 (G0/0), and R5 should be configured in VLAN 125.
- Configure RIPv2 on all routers and advertise their directly connected interfaces in this routing protocol.

IP Addressing

Router	Interface	IP address
R1	F0/0 F0/1	10.1.125.1/24 10.1.14.1/24
R2	G0/0 Lo0	10.1.125.2/24 2.2.2.2/24
R4	F0/0	10.1.14.4/24
R5	F0/0 Lo0	10.1.125.5/24 5.5.5.5/24

Task 1

Configure R1 to ONLY allow TCP, UDP and ICMP traffic initiated from the inside network (10.1.125.0 /24) to access the outside network/s. The traffic initiated from the outside networks should ONLY be allowed if it's ICMP or telnet destined for host 10.1.125.5/24. Ensure that any other traffic NOT initiated from inside network is denied.

Configuration

Complete these steps:

Step 1 In this case we have two security policies, one from inside to outside and the second one from outside to inside.

To allow inspection of the traffic from inside to outside:

```
R1(config)#ip inspect name OUT tcp
R1(config)#ip inspect name OUT udp
R1(config)#ip inspect name OUT icmp
```

The above three lines are the rules for inspection. Basically they tell the IOS to inspect the generic traffic for TCP, UDP and ICMP. Remember that with generic inspection CBAC ONLY performs connection inspection; it also adds new connections to the state table, add dynamic ACL and checks the sequence numbers in the returning traffic. With generic inspection, CBAC does NOT monitor what actually is occurring on the connection, such as the commands that are being executed or if a secondary connection is being negotiated, if these are required, then a specific inspection of the desired application can be configured, once this is configured, it will take precedence over the generic TCP or UDP inspection.

```
R1(config)#access-list 100 permit ip 10.1.125.0 0.0.0.255 any
R1(config)#access-list 100 permit udp any any eq rip
```

The above access-list permits any traffic from 10.1.125.0/24 to any network and it also allows RIP to operate.

```
R1(config)#int f0/0
R1(config-if)#ip inspect OUT in
R1(config-if)#ip access-group 100 in
```

The above commands apply the inspection rules and the access-lists to the F0/0 interface (the inside interface) in the ingress direction.

Step 2 For the ingress traffic from outside to inside:

In this policy telnet and ICMP traffic is allowed for host 10.1.125.5/24

```
R1(config)#access-list 101 permit icmp any host 10.1.125.5
R1(config)#access-list 101 permit tcp any host 10.1.125.5 eq 23
R1(config)#access-list 101 permit udp any any eq rip

R1(config)#int f0/1
R1(config-if)#ip access-group 101 in
```

Verification

```
R4#telnet 10.1.125.2
Trying 10.1.125.2 ...
% Destination unreachable; gateway or host down
```

Note the telnet is NOT successful

```
R4#telnet 10.1.125.5
Trying 10.1.125.5 ... Open

User Access Verification

Password:
R5>
```

Note the telnet is successful.

```
R2#telnet 10.1.14.4
Trying 10.1.14.4 ... Open

User Access Verification

Password:
R4>

R1#sh ip inspect session
Established Sessions
 Session 48E194C8 (10.1.125.2:35593)=>(10.1.14.4:23) tcp SIS_OPEN
```

Task 2

Configure R1 based on the following policy:

1. R1 should wait 20 seconds for all the TCP connections to be established, if any of the connections are not established with 20 seconds, they should be dropped.

2. R1 should wait 8 seconds before it removes an entry from its state table when either the source or the destination begins the tear down process of a TCP session.

3. R1 should maintain an idle TCP connection in its state table for 15 minutes ONLY.

4. R1 should maintain a DNS query connection in its state table for 8 seconds.

5. R1 should begin deleting half-open sessions if they reach 800, R1 should stop deleting these sessions once they fall below 600.

6. R1 should be also use the previous two policies for the connection made in the last one minute.

7. The maximum number of half-sessions to a specific host should NOT exceed 80, if this policy is violated, the IOS should delete all half-opened sessions and block all new connection requests for 8 minutes.

CBAC's global timeouts:

Ip inspect tcp synwait-time:
This command specifies how long the IOS waits for a TCP connection to be established. The default is 30 seconds, if the connection is not established, it will be dropped.

Ip inspect tcp finwait-time:

This command specifies how long the IOS waits to remove an entry from its table when the source or the destination begins the teardown process of a TCP session. The default is 5 seconds. Basically this is the wait time after receiving or exchanging the FIN packets.

Ip inspect tcp idle-time:

This command specifies how long the IOS maintains an idle TCP connection in its table. The default is 3600 seconds (1 hour).

Ip inspect udp idle-time:

This command specifies how long the IOS maintains an idle UDP connection in its table. The default is 30 seconds.

Ip inspect dns-timeout:

This command specifies how long the IOS maintains a DNS query connection in its state table. The default is 5 seconds.

Ip inspect max-incomplete high:

Once the number of half-open sessions reaches this threshold, the IOS will start deleting them. Default is 500

Ip inspect max-incomplete low:

Once the threshold is reached, the IOS will stop deleting the half-open sessions. Default is 400

Ip inspect one-minute high:

If the number of half-open sessions exceeds the configured threshold, the IOS will begin to delete them. Default is 500 per minute.

Ip inspect one-minute low:

Once it falls below this threshold within a minute, the IOS will stop to delete the half-open sessions.

Ip inspect tcp max-incomplete host number block-time minutes

The number of existing half-open sessions with the same destination host address that will cause the IOS to start deleting them. Default is 50.
If the block-time is set to 0 = This is the default, the IOS deletes the oldest existing half-opened session for the host for every new connection request to the host.

If the block-time is NOT set to 0 = the IOS deletes all half-opened sessions for the host and then blocks all new connection requests to the host.

Configuration

Complete these steps:

Step 1 Check CBAC configuration.

```
R1#show ip inspect config

Session audit trail is disabled
Session alert is enabled
one-minute (sampling period) thresholds are [unlimited : unlimited]
connections
max-incomplete sessions thresholds are [unlimited : unlimited]
max-incomplete tcp connections per host is unlimited. Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec

tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
Inspection Rule Configuration
 Inspection name FW
    tcp alert is on audit-trail is off timeout 3600
    udp alert is on audit-trail is off timeout 30
    icmp alert is on audit-trail is off timeout 10
```

Step 2 R1 configuration.

```
R1(config)#ip inspect TCP synwait-time 20
R1(config)#ip inspect TCP finwait-time 8
R1(config)#ip inspect TCP idle-time 900
R1(config)#ip inspect DNS-timeout 8
R1(config)#ip inspect max-incomplete high 800
%Also resetting low threshold from [unlimited] to [800]

R1(config)#ip inspect max-incomplete low 600
R1(config)#ip inspect one-minute high 800
%Also resetting low threshold from [unlimited] to [800]

R1(config)#ip inspect one-minute low 600
R1(config)#ip inspect TCP max-incomplete host 80 block-time 8
```

Verification

```
R1#show ip inspect config
Session audit trail is disabled
Session alert is enabled
one-minute (sampling period) thresholds are [600 : 800] connections
max-incomplete sessions thresholds are [600 : 800]
max-incomplete tcp connections per host is 80. Block-time 8 minutes.
tcp synwait-time is 20 sec -- tcp finwait-time is 8 sec
tcp idle-time is 900 sec -- udp idle-time is 30 sec
tcp reassembly queue length 16; timeout 5 sec; memory-limit 1024 kilo bytes
dns-timeout is 8 sec
Inspection Rule Configuration
 Inspection name OUT
    tcp alert is on audit-trail is off timeout 900
    udp alert is on audit-trail is off timeout 30
    icmp alert is on audit-trail is off timeout 10
```

Task 3

Enable audit trail logging and real-time alerts to provide a record of network access through R1, this should include illegitimate access attempts. These should be logged to the SYSLOG server located at 10.1.1.100

Configuration

Complete these steps:

Step 1 R1 configuration.

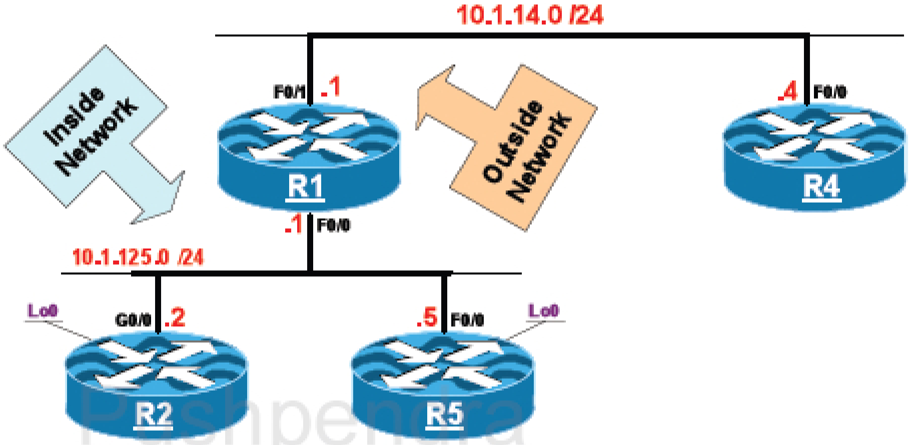
```
R1(config)#ip inspect audit-trail
R1(config)#no ip inspect alert-off

R1(config)#logging on
R1(config)#logging 10.1.1.100
```

Task 4

Erase the startup configuration and reload the routers before proceeding to the next lab.

LAB 3.31. Configuring CBAC & Java Blocking

The topology and the IP addressing is based on the previous lab



Task 1

R1 should be configured to ONLY allow the following traffic through its F0/1 (Outside) interface:

1. SMTP traffic that originates from the inside networks
2. ONLY Java applets from network 4.4.4.0/24 should be downloaded. Ensure that audit trail logging and real-time alerts are enabled for this inspection.
3. Netmeeting traffic that originated from the inside networks
4. Routing traffic for RIPv2 and ICMP should function properly

Remember the following:

- ***The access-list for the Java applets must be standard***
- ***If the access-list does not exist, all Java applets from all addresses will be blocked***
- ***CBAC does not detect or block encapsulated Java applets such as applets in ".zip" format.***
- ***CBAC DOES NOT detect or block applets loaded via FTP, Gopher or HTTP on a non-standard port***

Configuration

Complete these steps:

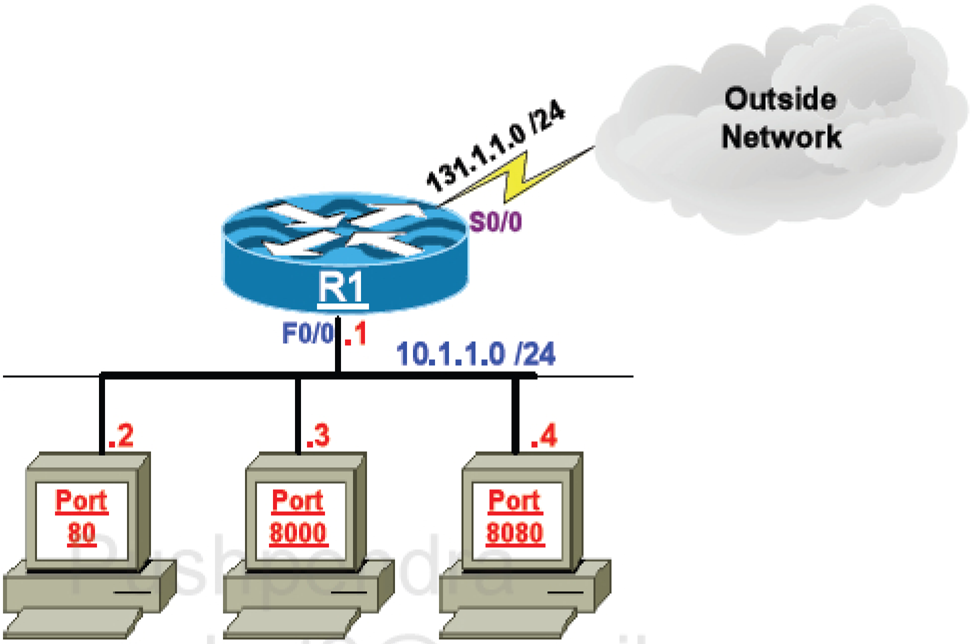
Step 1 R1 configuration.

```
R1(config)#access-list 1 permit 4.4.4.0 0.0.0.255

R1(config)#access-list 100 permit icmp any any
R1(config)#access-list 100 permit udp any any eq 520

R1(config)#ip inspect name FW http java-list 1 alert on audit-trail
on
R1(config)#ip inspect name FW SMTP
R1(config)#ip inspect name FW H323

R1(config)#int F0/1
R1(config-if)#ip inspect FW out
R1(config-if)#ip access-group 100 in
```

Task 2

Erase the startup configuration and reload the routers before proceeding to the next lab.

LAB 3.32. Configuring PAM



Task 1

There are three web servers connected to the F0/0 interface of R1. Configure R1 such that it can inspect the traffic for these web servers using the ports identified in the above diagram.

Configuration

Complete these steps:

Step 1 Before this change, you should display the default port mapping:

```
R1#sh ip port-map http

Default mapping:   http       tcp port 80    system defined
```

Step 2 R1 configuration.

```
R1(config)#ip port-map HTTP port 8000 list 1
R1(config)#access-list 1 permit 10.1.1.3

R1(config)#ip port-map HTTP port 8080 list 2

R1(config)#access-list 2 permit 10.1.1.4
```

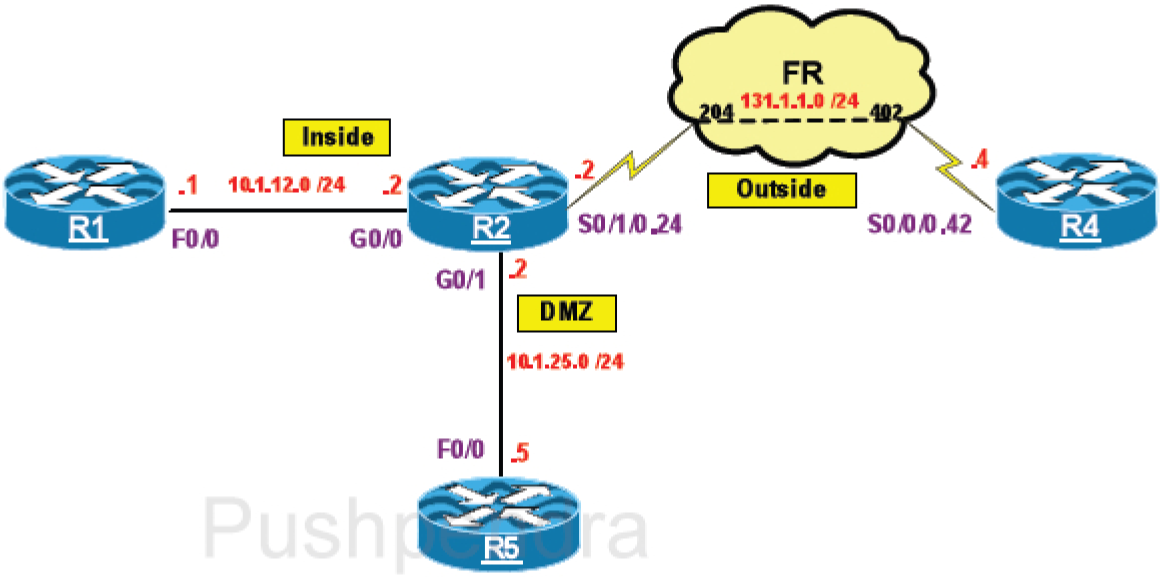
Verification

```
R1#sh ip port-map http

Default mapping:      http          tcp port 80                 system defined
Host specific:        http          tcp port 8000  in list 1      user defined
Host specific:        http          tcp port 8080  in list 2      user defined
```

Task 2

Erase the startup configuration and reload the routers before proceeding to the next lab.

LAB 3.33. Zone Based Policy Firewall (ZFW)



Lab Setup

- Configure the rack according to the diagram
- Use the IP addressing chart below for IP addressing scheme
- Run RIPv2 on the routers and advertise their directly connected networks.

IP addressing

Router	Interface	IP addressing
R1	F0/0	10.1.12.1/24
R2	G0/0 G0/1 S0/1/0.24	10.1.12.2/24 10.1.25.2/24 131.1.1.2/24
R4	S0/0/0.42	131.1.1.4/24
R5	F0/0	10.1.25.5/24

A previous version of IOS firewall was called Class-based Access Control (CBAC in short) and was offered interface-based firewall service only. What does it mean "interface-based"?
It means that traffic entering or leaving a particular interface is inspected for service conformance; if traffic matches requirements, the return traffic is allowed back through the firewall.

The CBAC inspection was sufficient for a small network with edge router with only two interfaces. However, multiple inspection policies and ACLs on several interfaces in a router make it difficult to correlate the policies that will be applied to traffic between multiple interfaces. As CBAC relies too heavily on ACLs it is not very flexible and has limited inspection granularity.

In addition to that, all traffic through a given interface was subjected to the same inspection. This was enough to start thinking about a new IOS firewall solution which gives more flexibility and can meet today's users expectations.
A Zone-Based Policy Firewall has been developed which uses completely different firewall configuration model. Instead relying on interfaces and ACLs it brings a term of ZONE. What is a zone? A zone defines a boundary where traffic is subjected to policy restrictions.
To make migration off of CBAC easier, we can configure ZFW and CBAC concurrently on the same router but not on the same interface.

ZFW configuration

First of all we need to configure zones. This is accomplished in router's global config mode by using command of "zone security <zone name>".
After creating the Zones, we need to configure something called a zone-pair, which is a pair of two zones where one zone is a source and second zone is a destination. Be careful because order of zones in the zone-pair is important and will dictate router the packet flow direction which will be subjected to inspection.
For example, if we want to inspect traffic from the Inside to the Outside the Inside must be source zone and the Outside must be a destination. However, for traffic originated on the outside zone, the Outside-Zone must be a source zone. Firewall policies are unidirectional and this must be considered at the beginning of zones creation.
Next is a policy creation process described in more details below.
The last step is making router interfaces members of an appropriate zone. This should be done as a very last step because if we could assign interface to the

zone before creating policy – all traffic will be denied by default. So it is much better to first create zones and policy and then assign the policy to the zone-pair and assign interface to the zone. This will effectively enable ZFW on the router.

ZFW basic rules

A policy applied between zones is Unidirectional. The ZFW is a stateful firewall which means all returning traffic will be allowed automatically on the returning interface. There is no need for ACL. However, if we want to allow traffic to flow in opposite direction we will need a new zone-pair to be created and a new policy attached to it.

The default policy for traffic between zones is DENY ALL. Once we create zones and zone-pair, the traffic stops going thru the router. This is because there is no policy attached to the zone-pair and NO POLICY equals DENY ALL. Only traffic explicitly allowed can be passed thru the router.

Also, remember to attach zones to the appropriate interface at the very last step. Do not assign interface to the zone before configuring policy as it will effectively drop a legitimate traffic because traffic will never go between two interfaces where one of them is not in the zone.

The same is true if two interfaces are in two different zone but there is no policy attached to that zone-pair. The traffic is blocked in this case as well.

ZFW Policy

A Policy building process uses 3 simple steps which are based on Modular QoS CLI framework (MQC in short). Here, it is called C3PL which basically uses "type inspect" components to build the policy. Nothing more!!!

First step is to configure a "class-map" to specify interesting traffic. This is not regular class map but "inspection type" class map. We configure it using a command of "class-map type inspect match-all (or match-any) plus the class-name.

Second step is to associate an action to the previously "classified" traffic. How to do that? Exactly in the same way as it was in MQC – using policy map, again "type inspect".

And finally, third step is to apply policy map to the zone-pair. How to do that? Again, nothing new – using „service-policy type inspect" command.

ZFW Class-maps

As you already know there are two different logical qualifiers available: match-all (which is a default) and match-any:

Match-all – introduces AND logic; traffic must match ALL filters; exit on first NON-match;

Match-any – introduces OR logic; traffic must match at least one filter; exit on first match

We can match traffic using three types of match statements:

- match protocol <protocol-name> - it determines which service match the class-map, and how the traffic will be inspected. This is so important because if the policy-map applies the inspect action; the traffic will be expected to behave as the specified service if the traffic matches the protocol filter in the class-map
- match access-group <number | name> - matches using an access-list.
- match class <class-map-name> - which nesting other class-map and allows defining of more flexible matching criteria.

Let's take a closer look at match protocol filter. What does it do and how it works? Basically speaking it matches the port/protocol in the packet headers against the specified protocol:

- For Layer 4 protocols - match protocol <tcp | udp | icmp>
- For Layer 7 protocols - match protocol <http | smtp | telnet|…>

In case of L7 protocols, the ports associated with the protocol are dictated by the existing Port-to-Application-Mapping (PAM) database entry.

For example, 'match protocol http' will match packets bound for port 8080 (in addition to port 80) if the router has 'ip port-map http port 8080' configured. There is no NBAR used for that matching!!!

ZFW Actions

We have matched our interesting traffic. Now it's time to perform some actions on that traffic. And again, we have 3 options under policy-map type inspect:

- Inspect - which basically speaking opens a hole for returning traffic. However it is stateful inspection, so that more information about packet are used like for example sequence numbers, ports, messages, methods, etc.
- Drop - which is self-explanatory
- Pass - this action does not have any stateful capability, so that it won't open any dynamic holes for returning traffic. Is it useful, someone could ask? Yes it is – for example in the policy for traffic destined or originated from the router.

If a stateful firewall is not enough for us we can still add additional control using ACLs. However it is worth noticing that inbound ACL is applied before

ZFW and outbound ACL is applied after ZFW. This needs to be considered during ACL design. For example, what is a value in the outbound ACL blocking FTP if ZFW policy does not allow that traffic?

L3/L4 vs. L7

There are two types of class-map and policy-map L3/L4 and L7. L3/L4 matches and applies actions to traffic up to Layer 4 level based on available information. L7 class/policy-maps are protocol specific; the options appearing under them depend on the protocol and the capabilities of the existing application inspection module. As the inspection engines of individual protocols are enhanced, more options will be added by Cisco to the corresponding L7 class/policy-maps to provision the new functionality.

As of now, L7 policies can be configured for the following protocols: HTTP, SMTP, POP3, IMAP, IM (AOL, ICQ, MSN, YAHOO), P2P (eDonkey, FastTrack, Gnutella, kazaa2), Voice traffic (SIP, H323), and Sun RPC.

The L7 policy-map is attached to the top-level (L3/L4) policy using the "service-policy <protocol-name <policy-name>" command. The class in the top-level policy for which an L7 policy-map is configured MUST have a "match protocol" filter. This protocol and the L7 policy-map protocol must be the same. If only 'match access-group' filters are present in the class-map, L7 policy cannot be configured for that class!

Two things must be remembered:

First: you can only apply L3/L4 policy map to the zone-pair, not L7. L7 policy-maps are applied under L3/L4 policy-maps only.

Second: L3/L4 class map must be configured with „match protocol" statement in order to apply L7 policy map to that traffic.

SELF Zone

There is also a special zone called SELF. This zone represents a router itself and every interface is a member of that zone by default. The zone is useful when we want to control traffic destined to the router or originated from the router. Then we just put a SELF zone in a zone-pair as a source (if we want to control traffic originated from the router) or as a destination (if we want to control traffic destined to the router).

Unfortunately there are some caveats in this solution. First, we can only inspect TCP, UDP, ICMP and H323 packets and second, we can't use ZFW policing when SELF zone is involved.

ZFW DoS Protection

The „parameter maps" are used to specify inspection behavior and prevent Denial-of-Service attacks. They are also used to define matching criteria in the class map in more flexible way – using regex. There are a couple of parameter map types but only three of them are really useful in ZFW. The „inspect" type where we configure some anti-DOS stuff and logging, the „regex" type for configuring regex expressions finally used in the class map and „urlfpolicy" which is useful in URL Filtering.

Verification

After successful implementation we should check if everything is OK and our configuration works the way we wanted. There are a couple of show commands available.

Most powerful command for checking almost all things is: "show policy-map type inspect zone-pair". We can specify a zone-pair name to narrow the command output. Anyway, this command displays the policy and counters for our inspected traffic.

If we configured Deep packet inspection, a useful command would be „show policy-map type inspect <protocol-name>" where L7 policy for specified protocol is displayed.

To see our zones and policies attached to the zone-pairs use: "show zone security" and „show zone-pair security" commands.

Task 1

Configure R2 using the following policy:

- Permit all TCP, UDP and ICMP traffic that is initiated on the inside network to access the DMZ and the outside network. Traffic that is not initiated from the inside should be denied
- Ensure that ONLY ICMP and HTTP traffic that is initiated from the outside is allowed to access the hosts on the DMZ.

Configuration

Complete these steps:

Step 1 R2 configuration.

First let's configure *class-map* for traffic from the inside and for traffic from the outside.

```
R2(config)#class-map type inspect match-any cmInside
R2(config-cmap)#match protocol tcp
R2(config-cmap)#match protocol udp
R2(config-cmap)#match protocol icmp

R2(config-cmap)#class-map type inspect match-any cmOutside
R2(config-cmap)#match protocol http
R2(config-cmap)#match protocol icmp
```

Next we need to configure *policy-map* for each flow direction

```
R2(config)#policy-map type inspect pmInside2Outside
R2(config-pmap)#class cmInside
R2(config-pmap-c)#inspect
R2(config-pmap-c)#policy-map type inspect pmInside2DMZ
R2(config-pmap)#class cmInside
R2(config-pmap-c)#inspect
R2(config-pmap-c)#policy-map type inspect pmOutside2DMZ
R2(config-pmap)#class cmOutside
R2(config-pmap-c)#inspect
```

Next we need to define security zones, assign the zones to the interfaces and set the policy between each zone pair.

```
R2(config)#zone security inside
R2(config-sec-zone)#zone security outside
R2(config-sec-zone)#zone security DMZ

R2(config)#int g0/0
R2(config-if)#zone-member security inside
R2(config-if)#int g0/1
R2(config-if)#zone-member security DMZ
R2(config-if)#int s0/1/0.24
R2(config-if)#zone-member security outside

R2(config)#zone-pair security zIO source inside destination outside
R2(config-sec-zone-pair)#service-policy type inspect pmInside2Outside
R2(config-sec-zone-pair)#zone-pair security zID source inside destination DMZ
R2(config-sec-zone-pair)#service-policy type inspect pmInside2DMZ
R2(config-sec-zone-pair)#zone-pair security zOS source outside destination
DMZ
R2(config-sec-zone-pair)#service-policy type inspect pmOutside2DMZ
```

```
R2(config-sec-zone-pair)#exi
```

Verification

Let's try to ping and telnet from R1 to R4 and R5.

```
R1#ping 10.1.25.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.25.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R1#ping 131.1.1.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 131.1.1.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms

R1#tel 131.1.1.4
Trying 131.1.1.4 ... Open


User Access Verification

Password:
R4>exi

[Connection to 131.1.1.4 closed by foreign host]

R1#tel 10.1.25.5
Trying 10.1.25.5 ... Open


User Access Verification

Password:
R5>exi

[Connection to 10.1.25.5 closed by foreign host]
R1#


R2#sh policy-map type inspect zone-pair zID

policy exists on zp zID
 Zone-pair: zID
```

```
  Service-policy inspect : pmInside2DMZ

    Class-map: cmInside (match-any)
      Match: protocol tcp
        1 packets, 24 bytes
        30 second rate 0 bps
      Match: protocol udp
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol icmp
        1 packets, 80 bytes
        30 second rate 0 bps

   Inspect
        Packet inspection statistics [process switch:fast switch]
        tcp packets: [0:41]
        icmp packets: [0:10]

        Session creations since subsystem startup or last reset 2
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [1:1:1]
        Last session created 00:00:27
        Last statistic reset never
        Last session creation rate 1
        Maxever session creation rate 1
        Last half-open session total 0

    Class-map: class-default (match-any)
      Match: any
      Drop
        0 packets, 0 bytes
```

Success! Now let's try to ping and telnet from R4 to R1 and R5.

```
R4#ping 10.1.12.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.12.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R4#ping 10.1.25.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.25.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms

R4#tel 10.1.12.1
Trying 10.1.12.1 ...
```

```
% Connection timed out; remote host not responding

R4#tel 10.1.25.5
Trying 10.1.25.5 ...
% Connection timed out; remote host not responding
```

As expected only ping between Outside and DMZ works. Let's try HTTP. To do that you need to enable HTTP server on R5 (and R1 for test).

On R1 and R5

```
R1(config)#ip http server
R5(config)#ip http server
```

Verification (cont'd)

```
R4#tel 10.1.12.1 80
Trying 10.1.12.1, 80 ...
% Connection timed out; remote host not responding

R4#tel 10.1.25.5 80
Trying 10.1.25.5, 80 ... Open
GET \
HTTP/1.1 400 Bad Request
Date: Fri, 03 Sep 2010 12:08:33 GMT
Server: cisco-IOS
Accept-Ranges: none

400 Bad Request

[Connection to 10.1.25.5 closed by foreign host]
```

Only HTTP between Outside and DMZ is allowed!

```
R2#sh zone-pair security
Zone-pair name zIO
    Source-Zone inside  Destination-Zone outside
    service-policy pmInside2Outside
Zone-pair name zID
    Source-Zone inside  Destination-Zone DMZ
    service-policy pmInside2DMZ
Zone-pair name zOS
    Source-Zone outside  Destination-Zone DMZ
    service-policy pmOutside2DMZ


R2#sh policy-map type inspect zone-pair zOS

policy exists on zp zOS
```

```
Zone-pair: zOS

 Service-policy inspect : pmOutside2DMZ

   Class-map: cmOutside (match-any)
     Match: protocol http
       1 packets, 24 bytes
       30 second rate 0 bps
     Match: protocol icmp
       1 packets, 80 bytes
       30 second rate 0 bps

  Inspect
       Packet inspection statistics [process switch:fast switch]
       tcp packets: [0:19]
       icmp packets: [0:10]

       Session creations since subsystem startup or last reset 2
       Current session counts (estab/half-open/terminating) [0:0:0]
       Maxever session counts (estab/half-open/terminating) [1:1:1]
       Last session created 00:03:29
       Last statistic reset never
       Last session creation rate 0
       Maxever session creation rate 1
       Last half-open session total 0

   Class-map: class-default (match-any)
     Match: any
     Drop
       4 packets, 96 bytes
```

Task 2

Configure R2 based on the following policy:

- R2 should wait 3 seconds for all the TCP connections to be established, if any of the connections are not established with 3 seconds, they should be dropped.
- R2 should wait 10 seconds before it removes an entry from its state table when either the source or the destination begins the tear down process of a TCP session.
- R2 should begin deleting half-open sessions if they reach 800, R2 should stop deleting these sessions once they fall below 500.

- The maximum number of half-sessions to a specific host should NOT exceed 50, if this policy is violated, the IOS should delete all half-opened sessions and block all new connection requests for 5 minutes.

Configuration

Complete these steps:

Step 1 R2 configuration.

The parameters in ZFW are very similar to those configured using CBAC. All parameters have been described in more details in the CBAC configuration task.

The only difference is the way of configuration. In ZFW we use "parameter-map type inspect" which is then applied as an argument to the "inspect" action under L3/L4 policy-map. This allows us to configure different parameters to each zone-pair.

```
R2(config)#parameter-map type inspect PARAM
R2(config-profile)#max-incomplete low  500
R2(config-profile)#max-incomplete high 800
R2(config-profile)#tcp idle-time 10
R2(config-profile)#tcp synwait-time 3
R2(config-profile)#tcp max-incomplete host 50 block-time 5
R2(config-profile)#exi

R2(config)#policy-map type inspect pmOutside2DMZ
R2(config-pmap)#class type inspect cmOutside
R2(config-pmap-c)#inspect PARAM
R2(config-pmap-c)#exi
R2(config-pmap)#exi

R2(config)#policy-map type inspect pmInside2DMZ
R2(config-pmap)#class type inspect cmInside
R2(config-pmap-c)#inspect PARAM
R2(config-pmap-c)#exi
R2(config-pmap)#exi

R2(config)#policy-map type inspect pmInside2Outside
R2(config-pmap)#class type inspect cmInside
R2(config-pmap-c)#inspect PARAM
R2(config-pmap-c)#exi
R2(config-pmap)#exi
```

Verification

```
R2#sh policy-map type inspect zone-pair
 Zone-pair: zIO

  Service-policy inspect : pmInside2Outside

    Class-map: cmInside (match-any)
      Match: protocol tcp
        1 packets, 24 bytes
        30 second rate 0 bps
      Match: protocol udp
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol icmp
        1 packets, 80 bytes
        30 second rate 0 bps
      Inspect
        Packet inspection statistics [process switch:fast switch]
        tcp packets: [0:41]
        icmp packets: [0:10]

        Session creations since subsystem startup or last reset 2
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [1:1:1]
        Last session created 00:18:41
        Last statistic reset never
        Last session creation rate 0
        Maxever session creation rate 2
        Last half-open session total 0

    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        114 packets, 0 bytes
 Zone-pair: zID

  Service-policy inspect : pmInside2DMZ

    Class-map: cmInside (match-any)
      Match: protocol tcp
        1 packets, 24 bytes
        30 second rate 0 bps
      Match: protocol udp
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol icmp
        1 packets, 80 bytes
        30 second rate 0 bps
      Inspect
        Packet inspection statistics [process switch:fast switch]
        tcp packets: [0:42]
        icmp packets: [2:7]

        Session creations since subsystem startup or last reset 2
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [1:1:1]
        Last session created 00:18:32
        Last statistic reset never
        Last session creation rate 0
        Maxever session creation rate 1
        Last half-open session total 0

    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        114 packets, 0 bytes
 Zone-pair: zOS

  Service-policy inspect : pmOutside2DMZ

    Class-map: cmOutside (match-any)
      Match: protocol http
        1 packets, 24 bytes
        30 second rate 0 bps
      Match: protocol icmp
        1 packets, 80 bytes
        30 second rate 0 bps
      Inspect
        Packet inspection statistics [process switch:fast switch]
        tcp packets: [0:18]
        icmp packets: [0:10]

        Session creations since subsystem startup or last reset 2
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [1:1:1]
        Last session created 00:14:01
        Last statistic reset never
        Last session creation rate 0
        Maxever session creation rate 1
        Last half-open session total 0

    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        118 packets, 96 bytes
R2#
```

Task 3

Configure R2 so that it will send TCP Reset packets to the inside hosts trying to connect to the following addresses on the outside network:

- mail.google.com
- mail.yahoo.com

This event should be logged to the local buffer on R2.

Configuration

Complete these steps:

Step 1 R2 configuration.

In order to match strings in the HTTP header we need L7 class map when we use regex matching for those strings. Then that L7 class map must be used under L7 policy map where action of “reset” and “log” is configured.

```
R2(config)#parameter-map type regex DeniedSites
R2(config-profile)#pattern .*mail.google.com
R2(config-profile)#pattern .*mail.yahoo.com
R2(config-profile)#exi

R2(config)#class-map type inspect cmL3Websites
R2(config-cmap)#match protocol http
R2(config-cmap)#exi

R2(config)#class-map type inspect http cmL7Websites
R2(config-cmap)#match req-resp header host regex DeniedSites
R2(config-cmap)#exi

R2(config)#policy-map type inspect http pmL7Websites
R2(config-pmap)#class cmL7Websites
R2(config-pmap-c)#reset
R2(config-pmap-c)#log
R2(config-pmap-c)#exi
R2(config-pmap)#exi
```

The L7 policy map must be nested under our L3/L4 policy map for Inside to Outside zone pair. However, we need to be careful here as there is already class map under that policy matching TCP traffic. Thus, our HTTP packets will be treated as TCP traffic and not like HTTP traffic. To configure it correctly we need to move our L7 policy at the beginning of the list so that it will be enforced first.

```
R2(config)#policy-map type inspect pmInside2Outside
```

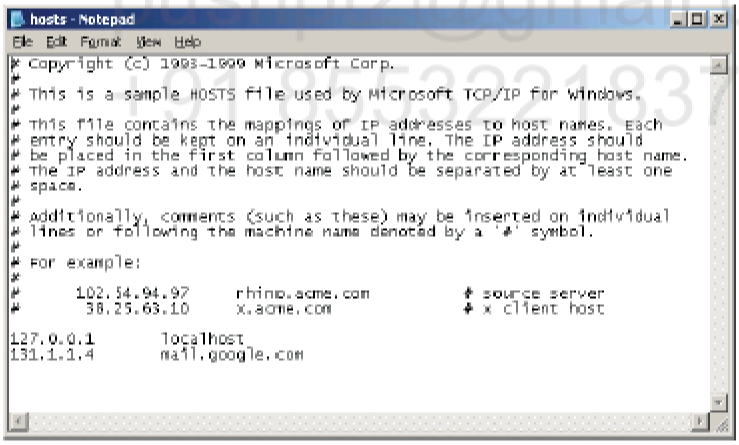
```
R2(config-pmap)#no class type inspect cmInside

R2(config-pmap)#class type inspect cmL3Websites
R2(config-pmap-c)#inspect
R2(config-pmap-c)#service-policy http pmL7Websites
R2(config-pmap-c)#exi

R2(config-pmap)#class type inspect cmInside
R2(config-pmap-c)#inspect PARAM
R2(config-pmap-c)#exi
R2(config-pmap)#exi

R2(config)#logg buffered 7
R2(config)#logg on
```

Verification

```
R2#sh policy-map type inspect zone-pair zIO
 Zone-pair: zIO

  Service-policy inspect : pmInside2Outside

    Class-map: cmL3Websites (match-all)
      Match: protocol http
      Inspect
        Packet inspection statistics [process switch:fast switch]
        tcp packets: [1:17]
        http packets: [0:7]

        Session creations since subsystem startup or last reset 1
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [1:1:1]
        Last session created 00:00:29
        Last statistic reset never
        Last session creation rate 1
        Maxever session creation rate 1
        Last half-open session total 0
      Deep packet inspection
        Policy: http pmL7Websites
        0 packets, 0 bytes

       No HTTP packets have been matched so far.

    Class-map: cmInside (match-any)
      Match: protocol tcp
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol udp
```

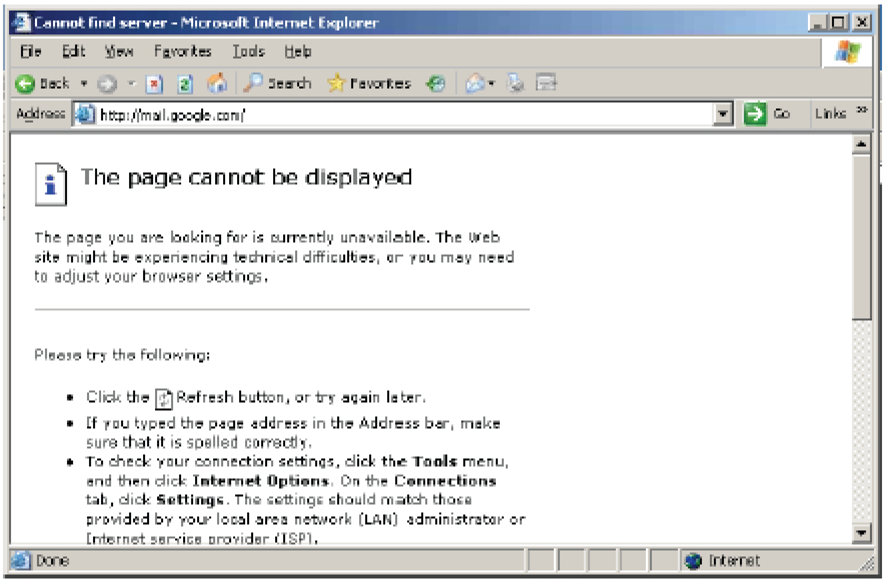
```
          0 packets, 0 bytes
          30 second rate 0 bps
        Match: protocol icmp
          0 packets, 0 bytes
          30 second rate 0 bps
        Inspect
          Session creations since subsystem startup or last reset 0
          Current session counts (estab/half-open/terminating) [0:0:0]
          Maxever session counts (estab/half-open/terminating) [0:0:0]
          Last session created never
          Last statistic reset never
          Last session creation rate 0
          Maxever session creation rate 0
          Last half-open session total 0

      Class-map: class-default (match-any)
        Match: any
        Drop (default action)
          1064 packets, 0 bytes
```

To verify put the ACS or PC in VLAN 12, change the IP address of this computer to 10.1.12.200/24 and default geteway to 10.1.12.2. Then make a change in the hosts file located in c:\windows\system32\drivers\etc and add the following line:



```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost
131.1.1.4       mail.google.com
```

Run web browser and enter the following URL in the address bar:


Cannot find server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://mail.google.com/
Go Links
Done
Internet

The page cannot be displayed

The page you are looking for is currently unavailable. The Web site might be experiencing technical difficulties, or you may need to adjust your browser settings.

Please try the following:

- Click the Refresh button, or try again later.
- If you typed the page address in the Address bar, make sure that it is spelled correctly.
- To check your connection settings, click the **Tools** menu, and then click **Internet Options**. On the **Connections** tab, click **Settings**. The settings should match those provided by your local area network (LAN) administrator or Internet service provider (ISP).

The web page shouldn't be reached.

```
R2#sh logg
Syslog logging: enabled (12 messages dropped, 2 messages rate-limited,
                0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.



No Inactive Message Discriminator.


    Console logging: disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 2 messages logged, xml disabled,
                     filtering disabled
    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.

ESM: 0 messages dropped

    Trap logging: level informational, 38098 message lines logged

Log Buffer (4096 bytes):

*Sep 24 14:25:19.488: %SYS-5-CONFIG_I: Configured from console by console
*Sep 24 14:25:28.128: %APPFW-4-HTTP_HDR_FIELD_REGEX_MATCHED: Header field
(^[Hh][Oo][Ss][Tt]:.*mail.google.com) matched - resetting session 10.1.12.200:2928
131.1.1.4:80 on zone-pair zIO class cmL3Websites appl-class cmL7Websites
```

A SYSLOG message has been generated on R2.

```
R2#sh policy-map type inspect zone-pair zIO
 Zone-pair: zIO

  Service-policy inspect : pmInside2Outside

    Class-map: cmL3Websites (match-all)
      Match: protocol http
      Inspect
        Packet inspection statistics [process switch:fast switch]
        tcp packets: [3:23]
        http packets: [0:9]

        Session creations since subsystem startup or last reset 3
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [1:1:1]
        Last session created 00:00:11
        Last statistic reset never
        Last session creation rate 2
        Maxever session creation rate 2
        Last half-open session total 0
      Deep packet inspection
        Policy: http pmL7Websites
        8 packets, 216 bytes
```

Now, HTTP packets has been matched and policy enforced.

```
    Class-map: cmInside (match-any)
      Match: protocol tcp
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol udp
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol icmp
        0 packets, 0 bytes
        30 second rate 0 bps
      Inspect
        Session creations since subsystem startup or last reset 0
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [0:0:0]
        Last session created never
        Last statistic reset never
        Last session creation rate 0
        Maxever session creation rate 0
        Last half-open session total 0

    Class-map: class-default (match-any)
      Match: any
```

```
        Drop (default action)
          1064 packets, 0 bytes
```

Task 4

Configure Zone-Based Policy Firewall on R2 so that there is only Telnet traffic possible to the router from every network. Ensure that RIP updates are not affected by this change.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
       Since there is RIP routing protocol enabled on R2 on every directly
       connected network enabling policy for traffic destined to the router
       may drop that traffic. Hence, we need to match and allow two types of
       traffic: RIP nad TELNET. Since, there is no “match protocol rip”
       command we can use an access list to do that.

R2(config)#access-list 120 permit udp any any eq 520

R2(config)#class-map type inspect match-any cmL3TelnetRIP
R2(config-cmap)#match protocol telnet
R2(config-cmap)#match access-group 120
R2(config-cmap)#exi

R2(config)#policy-map type inspect pmToSelf
R2(config-pmap)#class cmL3TelnetRIP
R2(config-pmap-c)#pass

       “pass” is enough here as we do not expect to open a dynamic hole for
returning packets.

R2(config-pmap-c)#exi
R2(config-pmap)#exi

R2(config)#zone-pair security zpInside2Self source inside destination self
R2(config-sec-zone-pair)#service-policy type inspect pmToSelf
R2(config-sec-zone-pair)#exi

R2(config)#zone-pair security zpOutside2Self source outside destination self
R2(config-sec-zone-pair)#service-policy type inspect pmToSelf
R2(config-sec-zone-pair)#exi
R2(config)#exi
```

```
R2(config)#zone-pair security zpDMZ2Self source DMZ destination self
R2(config-sec-zone-pair)#service-policy type inspect pmToSelf
R2(config-sec-zone-pair)#exi
R2(config)#exi
```

Verification

```
R2#ping 10.1.12.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.12.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R2#tel 10.1.12.1
Trying 10.1.12.1 ...
% Connection timed out; remote host not responding

R2#ping 131.1.1.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 131.1.1.4, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Note that enabling SELF zone and configuring unidirectional zone pairs will affect traffic originated from the R2.

```
R2#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     5.0.0.0/32 is subnetted, 1 subnets
R       5.5.5.5 [120/1] via 10.1.25.5, 00:00:03, GigabitEthernet0/1
     10.0.0.0/24 is subnetted, 2 subnets
C       10.1.12.0 is directly connected, GigabitEthernet0/0
C       10.1.25.0 is directly connected, GigabitEthernet0/1
     131.1.0.0/24 is subnetted, 1 subnets
C       131.1.1.0 is directly connected, Serial0/1/0.24
```

Seems that RIP is still working.

```
R2#sh policy-map type inspect zone-pair zpInside2Self
 Zone-pair: zpInside2Self

  Service-policy inspect : pmToSelf

    Class-map: cmL3TelnetRIP (match-any)
      Match: protocol telnet
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: access-group 120
        0 packets, 0 bytes
        30 second rate 0 bps
      Pass
        0 packets, 0 bytes

    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        102 packets, 556 bytes
```

```
R2#sh policy-map type inspect zone-pair zpOutside2Self
 Zone-pair: zpOutside2Self

  Service-policy inspect : pmToSelf

    Class-map: cmL3TelnetRIP (match-any)
      Match: protocol telnet
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: access-group 120
        0 packets, 0 bytes
        30 second rate 0 bps
      Pass
        0 packets, 0 bytes

    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        95 packets, 400 bytes
```

```
R2#sh policy-map type inspect zone-pair zpDMZ2Self
 Zone-pair: zpDMZ2Self

  Service-policy inspect : pmToSelf

    Class-map: cmL3TelnetRIP (match-any)
      Match: protocol telnet
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: access-group 120
        0 packets, 0 bytes
        30 second rate 0 bps
      Pass
        0 packets, 0 bytes

    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        90 packets, 0 bytes
```

```
R1#tel 10.1.12.2
Trying 10.1.12.2 ... Open


User Access Verification

Password:
R2>exit

[Connection to 10.1.12.2 closed by foreign host]
```

TELNET traffic destined to R2 works. ICMP does NOT!

```
R1#ping 10.1.12.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.12.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

```
R1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.1.12.2 to network 0.0.0.0

     5.0.0.0/32 is subnetted, 1 subnets
R       5.5.5.5 [120/2] via 10.1.12.2, 00:00:12, FastEthernet0/0
     10.0.0.0/24 is subnetted, 2 subnets
C       10.1.12.0 is directly connected, FastEthernet0/0
R       10.1.25.0 [120/1] via 10.1.12.2, 00:00:12, FastEthernet0/0
```

```
     131.1.0.0/24 is subnetted, 1 subnets
R       131.1.1.0 [120/1] via 10.1.12.2, 00:00:12, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 10.1.12.2
```

There are some RIP prefixes in the routing table on R1. To test if RIP still works we can clear those prefixes and update the table again.

```
R1#cle ip route *
```

```
R1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.1.12.2 to network 0.0.0.0

     5.0.0.0/32 is subnetted, 1 subnets
R       5.5.5.5 [120/2] via 10.1.12.2, 00:00:07, FastEthernet0/0
     10.0.0.0/24 is subnetted, 2 subnets
C       10.1.12.0 is directly connected, FastEthernet0/0
R       10.1.25.0 [120/1] via 10.1.12.2, 00:00:07, FastEthernet0/0
     131.1.0.0/24 is subnetted, 1 subnets
R       131.1.1.0 [120/1] via 10.1.12.2, 00:00:07, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 10.1.12.2
R1#
```

RIP works fine. R1 got all RIP prefixes from R2.

```
R2#sh policy-map type inspect zone-pair zpInside2Self
 Zone-pair: zpInside2Self

  Service-policy inspect : pmToSelf

    Class-map: cmL3TelnetRIP (match-any)
      Match: protocol telnet
        22 packets, 487 bytes
        30 second rate 0 bps
      Match: access-group 120
        0 packets, 0 bytes
        30 second rate 0 bps
      Pass
        22 packets, 487 bytes

    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        107 packets, 956 bytes
```

Why there are 0 packets for RIP? Tjis is because R2 sends out its routing table information to R1 using UDP which is connection-less. This means R1 gets the update. This counter would be incremented if R1 sends any RIP updates to R2.

Task 5

Enable URL filtering function on R2 so that when HTTP request originated form the inside network is going towards outside network the router first consults Websense server at IP address of 10.1.12.200 on port 2030 before allowing that connection. Set the maximum number of outstanding requests for Websense server that can exist at any given time to 500.

Configuration

Complete these steps:

Step 1 R2 configuration.

There is the same URL Filtering feature as it is for CBAC scenarios. We can use external Websense URL filtering server to consult before enabling the traffic go out.
In ZFW we use special type of parameter-map to do that.

```
R2(config)#parameter-map type urlfilter URL-Server
R2(config-profile)#server vendor websense 10.1.12.200 port 2030
R2(config-profile)#max-request 500
R2(config-profile)#exi

R2(config)#policy-map type inspect pmInside2Outside
R2(config-pmap)#class type inspect cmL3Websites
R2(config-pmap-c)#urlfilter URL-Server
R2(config-pmap-c)#exit
R2(config-pmap)#exit
```

Verification

```
R2#sh parameter-map type urlfilter
 parameter-map type urlfilter URL-Server
  server vendor websense 10.1.12.200 port 2030 retrans 2 timeout 6
  urlf-server-log off
  audit-trail off
  alert on
  max-request 500
  max-resp-pak 200
  source-interface default
  allow-mode off
  truncate script-parameters off
  truncate hostname off
  cache 5000

R2#sh policy-map type inspect zone-pair zIO
 Zone-pair: zIO

  Service-policy inspect : pmInside2Outside

    Class-map: cmL3Websites (match-all)
      Match: protocol http
      Inspect
        Packet inspection statistics [process switch:fast switch]
        tcp packets: [4:26]
        http packets: [0:10]

        Session creations since subsystem startup or last reset 4
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [1:1:1]
        Last session created 04:23:38
        Last statistic reset never
        Last session creation rate 0
        Maxever session creation rate 2
        Last half-open session total 0
      Deep packet inspection
        Policy: http pmL7Websites
        11 packets, 300 bytes
      Urlfilter
        Websense URL Filtering is DISABLED
```

This is because there is no Websense server enabled in the network

```
        Current requests count: 0
        Current packet buffer count(in use): 0
        Current cache entry count: 0

        Maxever request count: 0
        Maxever packet buffer count: 0
        Maxever cache entry count: 0

        Total requests sent to URL Filter Server :0
        Total responses received from URL Filter Server :0
        Total requests allowed: 0
        Total requests blocked: 0


    Class-map: cmInside (match-any)
```

```
        Match: protocol tcp
          0 packets, 0 bytes
          30 second rate 0 bps
        Match: protocol udp
          0 packets, 0 bytes
          30 second rate 0 bps
        Match: protocol icmp
          0 packets, 0 bytes
          30 second rate 0 bps
        Inspect
          Session creations since subsystem startup or last reset 0
          Current session counts (estab/half-open/terminating) [0:0:0]
          Maxever session counts (estab/half-open/terminating) [0:0:0]
          Last session created never
          Last statistic reset never
          Last session creation rate 0
          Maxever session creation rate 0
          Last half-open session total 0

      Class-map: class-default (match-any)
        Match: any
        Drop (default action)
          1109 packets, 0 bytes
R2#
```

Task 6

Configure R2 so that all JAVA applets are blocked from IP address of 10.1.25.5 for clients accessing this router from the inside network. Other hosts in DMZ network should not be affected.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
    We need to match two things:
        (1) HTTP traffic destined to IP 10.1.25.5 on port 80
        (2) HTTP traffic consisting of JAVA applets
    Note that first thing requires L3/L4 information and second thing
    requires L7 information. Hence, we need to use two methods of matching.

R2(config)#access-list 130 permit tcp any host 10.1.25.5 eq 80

R2(config)#class-map type inspect http match-all cmL7BlockJava
R2(config-cmap)#match response body java-applet
```

```
R2(config-cmap)#exi

R2(config)#class-map type inspect match-all cmL3BlockJava
R2(config-cmap)#match protocol http
R2(config-cmap)#match access-group 130
R2(config-cmap)#exi

R2(config)#policy-map type inspect http pmL7JavaPolicy
R2(config-pmap)#class type inspect http cmL7BlockJava
R2(config-pmap-c)#reset
R2(config-pmap-c)#log
R2(config-pmap-c)#exit
R2(config-pmap)#exi
```

Here we have conflict as there is already enabled inspection for TCP traffic. This would be enforced instead of our HTTP JAVA classification so that we need to move our specific requirement at the beginning of the list.

```
R2(config)#policy-map type inspect pmInside2DMZ
R2(config-pmap)#no class type inspect cmInside

R2(config-pmap)#class type inspect cmL3BlockJava
R2(config-pmap-c)#inspect
R2(config-pmap-c)#service-policy http pmL7JavaPolicy
R2(config-pmap-c)#exi

R2(config-pmap)#class type inspect cmInside
R2(config-pmap-c)#inspect PARAM
R2(config-pmap-c)#exi
R2(config-pmap)#exi
```

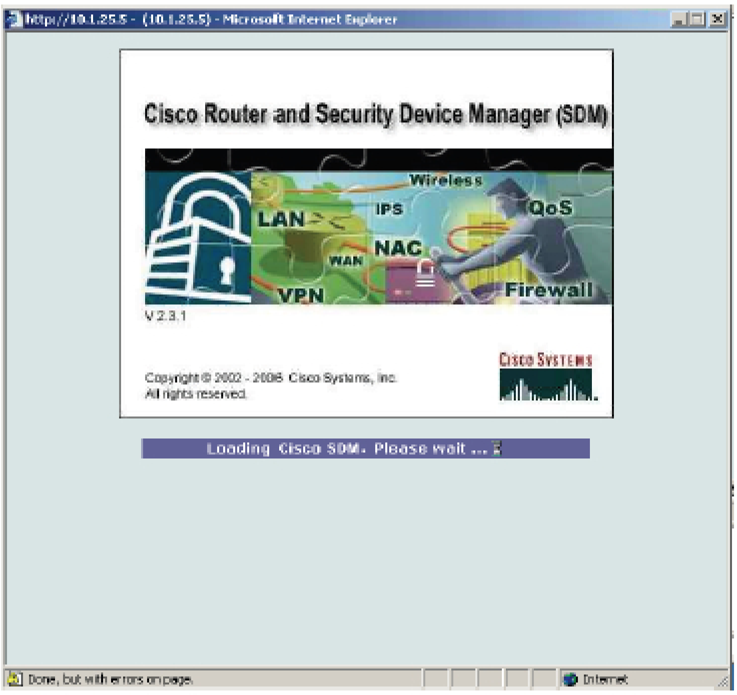
Verification

```
R2#sh policy-map type inspect zone-pair zID
 Zone-pair: zID

  Service-policy inspect : pmInside2DMZ

    Class-map: cmL3BlockJava (match-all)
      Match: protocol http
      Match: access-group 130
      Inspect
        Session creations since subsystem startup or last reset 0
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [0:0:0]
        Last session created never
        Last statistic reset never
        Last session creation rate 0
        Maxever session creation rate 0
        Last half-open session total 0
      Deep packet inspection
        Policy: http pmL7JavaPolicy
        0 packets, 0 bytes
```

No packets for JAVA blocking so far.

```
    Class-map: cmInside (match-any)
      Match: protocol tcp
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol udp
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol icmp
        0 packets, 0 bytes
        30 second rate 0 bps
      Inspect
        Session creations since subsystem startup or last reset 0
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [0:0:0]
        Last session created never
        Last statistic reset never
        Last session creation rate 0
        Maxever session creation rate 0
        Last half-open session total 0

    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        474 packets, 0 bytes
R2#
```

Let's test by connecting from ACS or PC located in VLAN 12 to the R5 via web browser – the SDM should be loaded on this router.



http://10.1.25.5 - (10.1.25.5) - Microsoft Internet Explorer

Cisco Router and Security Device Manager (SDM)

V 2.3.1

Copyright © 2002 - 2006 Cisco Systems, Inc.
All rights reserved.

Cisco Systems

Loading Cisco SDM. Please wait ...

Done, but with errors on page.

Internet

The page is not loaded correctly as there are JAVA applets bloacked by our policy.

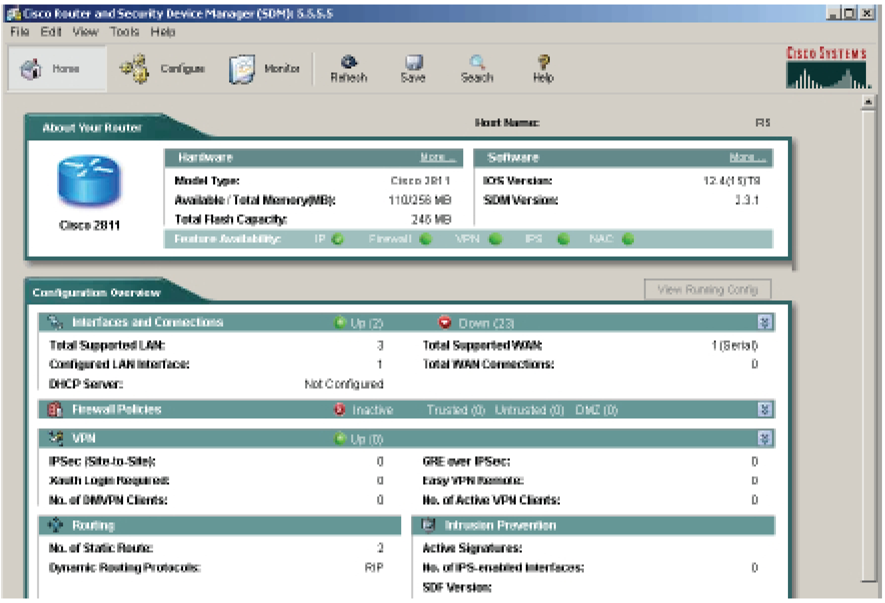
```
R2#sh policy-map type inspect zone-pair zID
 Zone-pair: zID

  Service-policy inspect : pmInside2DMZ

    Class-map: cmL3BlockJava (match-all)
      Match: protocol http
      Match: access-group 130
      Inspect
        Packet inspection statistics [process switch:fast switch]
        tcp packets: [30:717]
        http packets: [0:424]

        Session creations since subsystem startup or last reset 30
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [2:2:1]
        Last session created 00:02:13
        Last statistic reset never
        Last session creation rate 0
        Maxever session creation rate 30
        Last half-open session total 0
      Deep packet inspection
        Policy: http pmL7JavaPolicy
        89 packets, 2492 bytes
```

Packet counter indicates that some JAVA has been matched.

```
    Class-map: cmInside (match-any)
```

```
      Match: protocol tcp
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol udp
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol icmp
        0 packets, 0 bytes
        30 second rate 0 bps
      Inspect
        Session creations since subsystem startup or last reset 0
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [0:0:0]
        Last session created never
        Last statistic reset never
        Last session creation rate 0
        Maxever session creation rate 0
        Last half-open session total 0

    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        474 packets, 0 bytes
R2#

R2#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     5.0.0.0/32 is subnetted, 1 subnets
R       5.5.5.5 [120/1] via 10.1.25.5, 00:00:24, GigabitEthernet0/1
     10.0.0.0/24 is subnetted, 2 subnets
C       10.1.12.0 is directly connected, GigabitEthernet0/0
C       10.1.25.0 is directly connected, GigabitEthernet0/1
     131.1.0.0/24 is subnetted, 1 subnets
C       131.1.1.0 is directly connected, Serial0/1/0.24
```

There is also 5.5.5.5 address known in the network so that you can check and connect to that address via web browser. Since this address is not in the ACL for Java blocking it should be allowed.



Cisco Router and Security Device Manager (SDM): 5.5.5.5
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Cisco Systems
View Running Config

About Your Router — Host Name: R5

Cisco 2811

Hardware	
Model Type:	Cisco 2811
Available / Total Memory(MB):	110/256 MB
Total Flash Capacity:	246 MB

Software	
IOS Version:	12.4(15)T8
SDM Version:	2.3.1

Feature Availability: IP ● Firewall ● VPN ● IPS ● NAC ●

Configuration Overview

Interfaces and Connections — Up (2) Down (23)

Total Supported LAN:	3	Total Supported WAN:	1 (Serial)
Configured LAN Interface:	1	Total WAN Connections:	0
DHCP Server:	Not Configured		

Firewall Policies — Inactive Trusted (0) Untrusted (0) DMZ (0)

VPN — Up (0)

IPSec (Site-to-Site):	0	GRE over IPSec:	0
Xauth Login Required:	0	Easy VPN Remote:	0
No. of DMVPN Clients:	0	No. of Active VPN Clients:	0

Routing		Intrusion Prevention	
No. of Static Route:	2	Active Signatures:	
Dynamic Routing Protocols:	RIP	No. of IPS-enabled interfaces:	0
		SDF Version:	

```
SDM is accessible via 5.5.5.5 address. JAVA is not blocked for this address.
```

Task 7

You have been requested to configure ZFW on R2 so that it does not allow more than 1Mbps traffic destined to DMZ from the outside networks. You may use burst of 100KB.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#policy-map type inspect pmOutside2DMZ
R2(config-pmap)# class type inspect cmOutside
R2(config-pmap-c)#police rate 1000000 burst 100000
R2(config-pmap-c)#exi
R2(config-pmap)#exi
```

Verification

```
R2#sh policy-map type inspect zone-pair zOS
 Zone-pair: zOS
      Police
      rate 1000000 bps,100000 limit
      conformed 0 packets, 0 bytes; actions: transmit
      exceeded 0 packets, 0 bytes; actions: drop
      conformed 0 bps, exceed 0 bps
```

Rate limiting is enabled and no packets have been limited so far.

```
  Service-policy inspect : pmOutside2DMZ

    Class-map: cmOutside (match-any)
      Match: protocol http
        1 packets, 24 bytes
        30 second rate 0 bps
      Match: protocol icmp
        1 packets, 80 bytes
        30 second rate 0 bps
      Inspect
        Packet inspection statistics [process switch:fast switch]
        tcp packets: [0:18]
        icmp packets: [0:10]

        Session creations since subsystem startup or last reset 2
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [1:1:1]
        Last session created 16:50:08
        Last statistic reset never
        Last session creation rate 0
        Maxever session creation rate 1
        Last half-open session total 0

    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        587 packets, 96 bytes
R2#
```

Let's ping R5 from the outside network with no timeout configured so that the packet rate should be high.

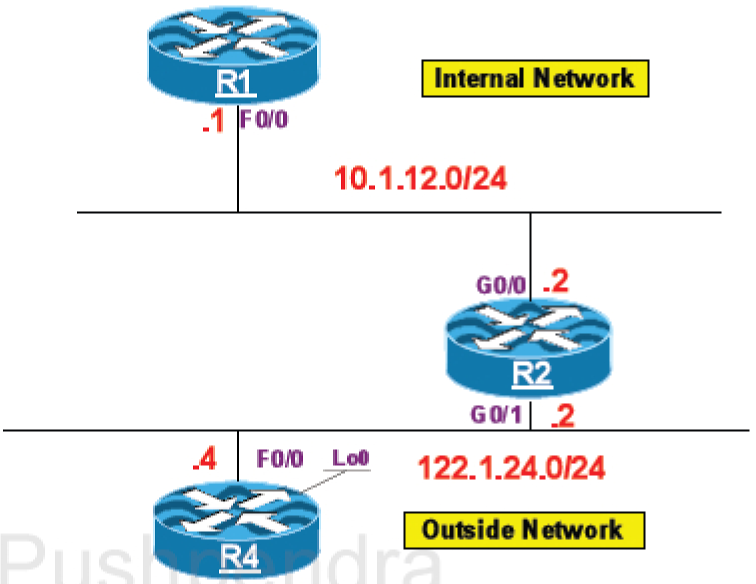
```
R4#ping 10.1.25.5 size 1000 rep 100 timeout 0

Type escape sequence to abort.
Sending 100, 1000-byte ICMP Echos to 10.1.25.5, timeout is 0 seconds:
......................................................................
..............................
Success rate is 0 percent (0/100)
R4#


R2#sh policy-map type inspect zone-pair zOS
 Zone-pair: zOS
      Police
```

```
          rate 1000000 bps,100000 limit
          conformed 136 packets, 137194 bytes; actions: transmit
          exceeded 13 packets, 13112 bytes; actions: drop
          conformed 0 bps, exceed 0 bps
```

There are some packets matched.
In a real world we often have QoS policies applied on the interface. The difference between interface service policy and inter-zone security policy is in the traffic aggregation: the interface service policy works on traffic classes entering or leaving a single interface and the inter-zone policy works on aggregate traffic between zones, including the return traffic if you've used the inspect command to configure stateful inspection of the traffic class.

```
  Service-policy inspect : pmOutside2DMZ

    Class-map: cmOutside (match-any)
      Match: protocol http
        1 packets, 24 bytes
        30 second rate 0 bps
      Match: protocol icmp
        2 packets, 1060 bytes
        30 second rate 0 bps
      Inspect
        Packet inspection statistics [process switch:fast switch]
        tcp packets: [0:18]
        icmp packets: [0:146]

        Session creations since subsystem startup or last reset 3
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [1:1:1]
        Last session created 00:00:23
        Last statistic reset never
        Last session creation rate 1
        Maxever session creation rate 1
        Last half-open session total 0

    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        587 packets, 96 bytes
R2#
```

LAB 3.34. Implementing security RFCs



Lab Setup

- Configure the routers with the following IP addressing:

Router	Interface	IP address
R1	F0/0	10.1.12.1/24
R2	G0/0 G0/1	10.1.12.2/24 122.1.24.2/24
R4	F0/0 Lo0	122.1.24.4/24 4.4.4.4/24

- Configure static default routing on R1 and R4 pointing to R2 and R2 pointing to R4

Task 1

Protect Internal Network by implementing access list blocking RFC 1918 and RFC 3330 IP addresses coming from the outside network. There is a requirement that in the near future your Internet Service Provider will deploy new outside connection

using BGP as a routing protocol (BGP peer will be at R4's F0/0 IP address). Ensure this requirement is addressed in your solution.
Use RFC 2827 as a guideline for configuring access list.

There are three RFCs useful when you want to configure anti-spoofing access list:

RFC 1918 – defines IPv4 reserved address space that is not a valid source address on the Internet - this traffic should never be seen as source at your Internet edge.

RFC 3330 – defines IPv4 special use addresses that might require filtering like:

- ***0.0.0.0/0 – "this" network***
- ***127.0.0.0/8 – Loopback***
- ***169.254.0.0/16 - Link Local***
- ***192.0.2.0/24 - Test-Net***
- ***224.0.0.0/4 - Multicast***

RFC 2827 - provides ingress filtering guidelines.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
       Block RFC 1918 addresses:

R2(config)#access-list 110 deny ip 10.0.0.0 0.255.255.255 any
R2(config)#access-list 110 deny ip 172.16.0.0 0.15.255.255 any
R2(config)#access-list 110 deny ip 192.168.0.0 0.0.255.255 any

       Block RFC 3330 addresses:

R2(config)#access-list 110 deny ip host 0.0.0.0 any
R2(config)#access-list 110 deny ip 127.0.0.0 0.255.255.255 any
R2(config)#access-list 110 deny ip 169.254.0.0 0.0.255.255 any
R2(config)#access-list 110 deny ip 192.0.2.0 0.0.0.255 any
R2(config)#access-list 110 deny ip 224.0.0.0 31.255.255.255 any

       Allow BGP connections from ISP peer in the future:

R2(config)#access-list 110 permit tcp host 122.1.24.4 host 122.1.24.2 eq bgp
R2(config)#access-list 110 permit tcp host 122.1.24.4 eq bgp host 122.1.24.2

       Block your public IP address scheme as a source (only BGP connection
```

is allowed) – this is per RFC 2827 guidelines which state you should filter out your internal IP address block at the network edge. As internal network is 10.1.12.0/24 it is already blocked by RFC 1918 filters, but your external IP address scheme should also be filtered

```
R2(config)#access-list 110 deny ip 122.1.24.0 0.0.0.255 any
```

Permit all other IP traffic.

```
R2(config)#access-list 110 permit ip any any
```

This newly constructed ACL must be applied inbound on all ingress interfaces.

```
R2(config)#int g0/1
R2(config-if)#ip access-group 110 in
```

Verification

R4#p 10.1.12.1

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.12.1, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
```

The ping is unsuccessful as it is blocked by ACL (sourced from 122.1.24.0/24 network).

R2#sh access-list

```
Extended IP access list 110
    10 deny ip 10.0.0.0 0.255.255.255 any
    20 deny ip 172.16.0.0 0.15.255.255 any
    30 deny ip 192.168.0.0 0.0.255.255 any
    40 deny ip host 0.0.0.0 any
    50 deny ip 127.0.0.0 0.255.255.255 any
    60 deny ip 169.254.0.0 0.0.255.255 any
    70 deny ip 192.0.2.0 0.0.0.255 any
    80 deny ip 224.0.0.0 31.255.255.255 any
    90 permit tcp host 122.1.24.4 host 122.1.24.2 eq bgp
    100 permit tcp host 122.1.24.4 eq bgp host 122.1.24.2
    110 deny ip 122.1.24.0 0.0.0.255 any (5 matches)
    120 permit ip any any
```

However, changing source result in success.

```
R4#p 10.1.12.1 so lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.12.1, timeout is 2 seconds:
Packet sent with a source address of 4.4.4.4
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/41/80 ms
```

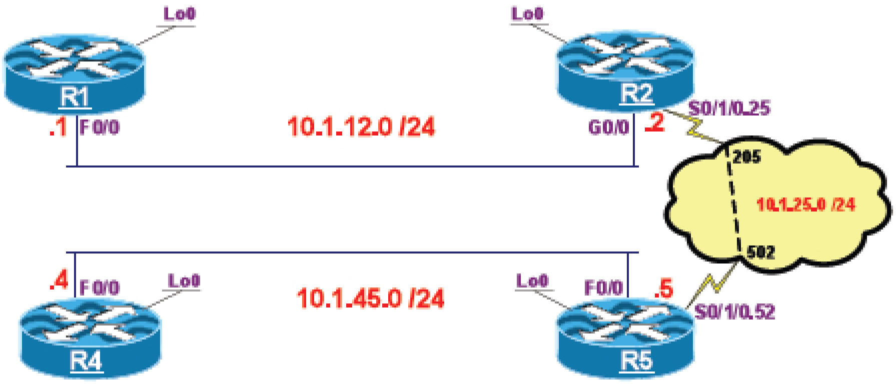
Potential pit fails:

- blocking Multicast you will block out dynamic routing protocols
- ICMP will be filtered out even for ping destined to the host on the outside network because ICMP echo-reply will be blocked
- Services accessible from the outside network will be blocked as whole "external" subnet is filtered

Task 2

Erase the startup config and reload the routers before proceeding to the next lab.

LAB 3.35. Using MQC as a filtering tool



Lab Setup

- R1 and R2's G0/0 interface should be configured in VLAN 12
- R2 and R5's S0/1/0 interface should be configured in a frame-relay point-to-point manner.
- R5 and R4's F0/0 interface should be configured in VLAN 45
- Configure telnet on all routers using password "cisco"
- Run RIPv2 on the routers and advertise their directly connected networks

IP Addressing

Router	Interface	IP address
R1	Lo0 F0/0	1.1.1.1/24 10.1.12.1/24
R2	Lo0 G0/0 S0/1/0.25	2.2.2.2/24 10.1.12.2/24 10.1.25.2/24
R4	Lo0 F0/0	4.4.4.4/24 10.1.45.4/24
R5	Lo0 F0/0 S0/1/0.52	5.5.5.5/24 10.1.45.5/24 10.1.25.5/24

Task 1

Configure R1 to perform classification and marking. This router should mark all egress telnet traffic with IP precedence of 1.

Configuration

Complete these steps:

Step 1 R1 configuration.

```
R1(config)#access-list 100 permit tcp any any eq 23

R1(config)#class-map TELNET
R1(config-cmap)#match access-group 100

R1(config)#policy-map TST
R1(config-pmap)#class TELNET
R1(config-pmap-c)#set ip precedence 1

R1(config-pmap-c)#int f0/0
R1(config-if)#service-policy output TST
```

Verification

```
R1#sh class-map TELNET

 Class Map match-all TELNET (id 1)
   Match access-group  100

R1#sh policy-map TST
  Policy Map TST
    Class TELNET
      set ip precedence 1
```

Test

```
      To generate telnet traffic:

R1#telnet 10.1.45.4
Trying 10.1.45.4 ... Open


User Access Verification
```

```
Password:
R4>exi

[Connection to 10.1.45.4 closed by foreign host]
```

To verify the marking of the traffic:

```
R1#sh policy-map interface f0/0
 FastEthernet0/0

  Service-policy output: TST

    Class-map: TELNET (match-all)
      23 packets, 1468 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group 100
      QoS Set
        precedence 1
          Packets marked 23

    Class-map: class-default (match-any)
      15 packets, 1804 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

Task 2

Configure R5 to block all IP Precedence 1 packets coming from S0/0/0.52 interface. You must use MQC to accomplish this task.

Configuration

Complete these steps:

Step 1 R5 configuration.

```
R5(config)#class-map IP-Prec
R5(config-cmap)#match ip precedence 1

R5(config)#policy-map TEST
R5(config-pmap)#class IP-Prec
R5(config-pmap-c)#drop

R5(config-pmap)#int S0/1/0.52
R5(config-subif)#service-policy input TEST
```

Verification

```
R1#telnet 10.1.45.4
Trying 10.1.45.4 ...
% Connection timed out; remote host not responding

       Note the telnet session failed.

R5#sh policy-map interface s0/1/0.52

 Serial0/1/0.52

  Service-policy input: TEST

    Class-map: IP-Prec (match-all)
      4 packets, 192 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 1
      drop

    Class-map: class-default (match-any)
      2 packets, 192 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

Task 3

Remove the configuration from the previous task (Task 2) and perform the same task using correct DSCP value instead of IP Precedence 1.

Configuration

Complete these steps:

Step 1 R5 configuration.

```
R5(config-pmap)#int S0/1/0.52
R5(config-subif)#no service-policy input TEST

R5(config)#class-map DSCP
R5(config-cmap)#match ip DSCP CS1

R5(config)#policy-map PM-DSCP
R5(config-pmap)#class DSCP
R5(config-pmap-c)#drop

R5(config-pmap)#int S0/1/0.52
```

```
R5(config-subif)#service-policy input PM-DSCP
```

Verification

```
R1#telnet 10.1.45.4
Trying 10.1.45.4 ...
% Connection timed out; remote host not responding

R5#sh policy-map interface s0/1/0.52

 Serial0/1/0.52

  Service-policy input: PM-DSCP

    Class-map: DSCP (match-all)
      4 packets, 192 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip dscp cs1 (8)
      drop

    Class-map: class-default (match-any)
      6 packets, 576 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

Task 4

Configure R2 so that it will limit packet rate to 8000 bps for all ICMP packets leaving serial interface. You must use MQC to accomplish this task.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#class-map ICMP
R2(config-cmap)#match protocol icmp

R2(config-cmap)#policy-map PM-ICMP
R2(config-pmap)#class ICMP
R2(config-pmap-c)#police 8000 1000 conform-action transmit exceed-
action drop

R2(config-pmap-c-police)#int s0/1/0.25
R2(config-subif)#service-policy output PM-ICMP
```

Verification

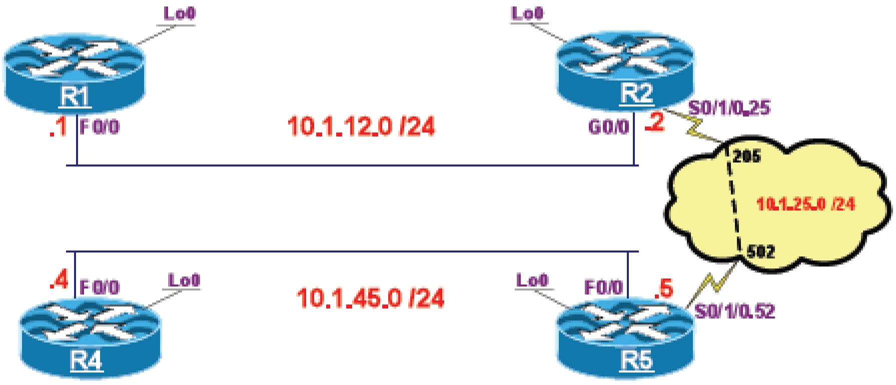
```
R2#sh policy-map interface s0/1/0.25

 Serial0/1/0.25

  Service-policy output: PM-ICMP

    Class-map: ICMP (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol icmp
      police:
          cir 8000 bps, bc 1000 bytes, be 1500 bytes
        conformed 0 packets, 0 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        violated 0 packets, 0 bytes; actions:
          drop
        conformed 0 bps, exceed 0 bps, violate 0 bps

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any

R2#ping 10.1.25.5 rep 20

Type escape sequence to abort.
Sending 20, 100-byte ICMP Echos to 10.1.25.5, timeout is 2 seconds:
!!!!!!!!!!!!.!!!!!!!
Success rate is 95 percent (19/20), round-trip min/avg/max = 1/24/100 ms

R2#sh policy-map interface s0/1/0.25

 Serial0/1/0.25

  Service-policy output: PM-ICMP

    Class-map: ICMP (match-all)
      20 packets, 2000 bytes
      5 minute offered rate 1000 bps, drop rate 0 bps
      Match: protocol icmp
      police:
          cir 8000 bps, bc 1000 bytes, be 1500 bytes
        conformed 19 packets, 1976 bytes; actions:
          transmit
        exceeded 1 packets, 104 bytes; actions:
          drop
        violated 0 packets, 0 bytes; actions:
          drop
        conformed 1000 bps, exceed 0 bps, violate 0 bps

    Class-map: class-default (match-any)
      2 packets, 672 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
R2#
```

Task 5

Erase the startup config and reload the routers before proceeding to the next lab.

LAB 3.36. Blackhole routing using PBR

Based on the previous Lab's IP addressing, topology and Lab setup



Task 1

R2 is seeing a lot of ICMP packets coming from frame-relay cloud. You have discovered that those packets are 250-320 bytes in size. Configure policy routing at R2 serial interface to block ICMP packets of size in range 250-320 destined to R1 and going through the router.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#access-list 120 permit icmp any any
R2(config)#
R2(config)#route-map BLACKHOLE permit 10
R2(config-route-map)# match ip address 120
R2(config-route-map)# match length 250 320
R2(config-route-map)# set interface Null0
%Warning:Use P2P interface for routemap set
                interface clause

R2(config-route-map)#
R2(config-route-map)#route-map BLACKHOLE permit 20
R2(config-route-map)#
R2(config-route-map)#int s0/1/0.25
```

```
R2(config-subif)# ip policy route-map BLACKHOLE
```

Verification

```
R2#sh route-map
route-map BLACKHOLE, permit, sequence 10
  Match clauses:
    ip address (access-lists): 120
    length 250 320
  Set clauses:
    interface Null0
  Policy routing matches: 0 packets, 0 bytes
route-map BLACKHOLE, permit, sequence 20
  Match clauses:
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
```

```
R5#p 10.1.25.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.25.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/25/84 ms
```

```
R5#p 10.1.12.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.12.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/42/100 ms
```

```
R5#p 10.1.12.1 size 300

Type escape sequence to abort.
Sending 5, 300-byte ICMP Echos to 10.1.12.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R5#
```

```
R2#sh route-map
route-map BLACKHOLE, permit, sequence 10
  Match clauses:
    ip address (access-lists): 120
    length 250 320
  Set clauses:
    interface Null0
  Policy routing matches: 5 packets, 1520 bytes
route-map BLACKHOLE, permit, sequence 20
  Match clauses:
  Set clauses:
  Policy routing matches: 5 packets, 520 bytes
```

Task 2

There is a Web server configured on R4's loopback0. On R4 drop all traffic destined to the Web server except the traffic coming from 1.1.1.1 using PBR.

Configuration

Complete these steps:

Step 1 R4 configuration.

```
R4(config)#ip http server

R4(config)#access-list 110 deny tcp host 4.4.4.4 eq www host
1.1.1.1
R4(config)#access-list 110 permit tcp host 4.4.4.4 eq www any

R4(config)#route-map WWW_ACCESS permit 10
R4(config-route-map)# match ip address 110
R4(config-route-map)# set interface Null0
%Warning:Use P2P interface for routemap set
                interface clause

R4(config-route-map)#route-map WWW_ACCESS permit 20
R4(config-route-map)#ip local policy route-map WWW_ACCESS
```

Verification

```
R1#tel 4.4.4.4 80 /source-interface lo0
Trying 4.4.4.4, 80 ...
% Connection timed out; remote host not responding

R1#tel 4.4.4.4 80 /source-interface lo0
Trying 4.4.4.4, 80 ... Open
GET /
HTTP/1.1 400 Bad Request
Date: Sun, 13 Sep 2009 22:44:58 GMT
Server: cisco-IOS
Connection: close
Accept-Ranges: none
```

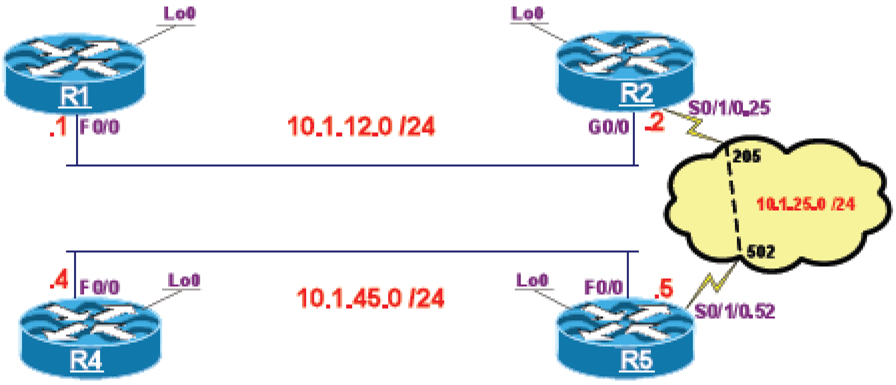
```
400 Bad Request

[Connection to 4.4.4.4 closed by foreign host]

R1#tel 4.4.4.4 80
Trying 4.4.4.4, 80 ...
% Connection timed out; remote host not responding


R4#sh ip local policy
Local policy routing is enabled, using route map WWW_ACCESS
route-map WWW_ACCESS, permit, sequence 10
  Match clauses:
    ip address (access-lists): 110
  Set clauses:
    interface Null0
  Policy routing matches: 7 packets, 408 bytes
route-map WWW_ACCESS, permit, sequence 20
  Match clauses:
  Set clauses:
  Policy routing matches: 35 packets, 2495 bytes
```

Task 3

Erase the startup config and reload the routers before proceeding to the next lab.

LAB 3.37. Configuring NAT

Based on the previous Lab's IP addressing, topology and Lab setup



Task 1

Configure NAT so that R1's loopback is always translated to 10.1.25.1 when connecting to R5 or R4.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#ip nat inside source static 1.1.1.1 10.1.25.1

R2(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface NVI0, changed state
to up
R2(config)#int g0/0
R2(config-if)#ip nat inside
R2(config-if)#int s0/1/0.25
R2(config-subif)#ip nat outside
```

Verification

```
R1#tel 4.4.4.4 /so lo0
Trying 4.4.4.4 ... Open


User Access Verification

Password:
R4>sh users
    Line       User       Host(s)              Idle       Location
   0 con 0                idle                 00:00:26
*  2 vty 0                idle                 00:00:00 10.1.25.1

  Interface    User               Mode         Idle     Peer Address

R2#sh ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 10.1.25.1:43346    1.1.1.1:43346      4.4.4.4:23         4.4.4.4:23
--- 10.1.25.1          1.1.1.1            ---                ---

R4#tel 10.1.25.1
Trying 10.1.25.1 ... Open


User Access Verification

Password:
R1>sh users
    Line       User       Host(s)              Idle       Location
   0 con 0                idle                 00:00:12
*  2 vty 0                idle                 00:00:00 10.1.45.4

  Interface    User               Mode         Idle     Peer Address
```

Task 2

On R2 configure NAT so that R5 and R4 can use IP address of 10.1.25.11 to connect to R1's f0/0 interface using TELNET port 2323 only.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#ip nat inside source static tcp 10.1.12.1 23 10.1.25.11 2323
```

Verification

```
R2#sh ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 10.1.25.1:23       1.1.1.1:23         10.1.45.4:39061    10.1.45.4:39061
tcp 10.1.25.1:43346    1.1.1.1:43346      4.4.4.4:23         4.4.4.4:23
--- 10.1.25.1          1.1.1.1            ---                ---
tcp 10.1.25.11:2323    10.1.12.1:23       ---                ---


R4#tel 10.1.25.11
Trying 10.1.25.11 ...
% Connection refused by remote host

R4#tel 10.1.25.11 2323
Trying 10.1.25.11, 2323 ... Open


User Access Verification

Password:
R1>sh users
    Line       User       Host(s)              Idle       Location
   0 con 0                idle                 00:05:24
*  2 vty 0                idle                 00:00:00 10.1.45.4

  Interface    User               Mode         Idle     Peer Address
```

Task 3

Add the following new interfaces on R1:

- loopback11 – 11.11.11.1/24
- loopback111 – 111.111.111.1/24

Configure R1 so that it translates both networks to the IP address range of 10.1.12.10-10.1.12.100.

Configuration

Complete these steps:

Step 1 R1 configuration.

```
R1(config)#int lo11
R1(config-if)#ip add 11.11.11.1 255.255.255.0
R1(config-if)#int lo111
R1(config-if)#ip add 111.111.111.1 255.255.255.0

R1(config-if)#access-list 1 permit 11.11.11.0 0.0.0.255
R1(config-if)#access-list 1 permit 111.111.111.0 0.0.0.255
R1(config)#ip  nat  pool  NAT_POOL  10.1.12.10  10.1.12.100  netmask
255.255.255.0
R1(config)#ip nat inside source list 1 pool NAT_POOL

R1(config)#int f0/0
R1(config-if)#ip nat outside
```

Verification

```
R1#tel 4.4.4.4 /source-interface lo11
Trying 4.4.4.4 ... Open


User Access Verification

Password:
R4>sh users
    Line       User       Host(s)              Idle       Location
   0 con 0                idle                 00:29:19
*  2 vty 0                idle                 00:00:00 10.1.12.10

  Interface    User               Mode         Idle     Peer Address
R4>exit
```

```
[Connection to 4.4.4.4 closed by foreign host]

R1#tel 4.4.4.4 /source-interface lo111
Trying 4.4.4.4 ... Open


User Access Verification

Password:
R4>sh users
    Line       User       Host(s)              Idle       Location
   0 con 0                idle                 00:30:01
*  2 vty 0                idle                 00:00:00 10.1.12.11

  Interface    User               Mode         Idle     Peer Address

R4>exit

[Connection to 4.4.4.4 closed by foreign host]

R1#sh ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 10.1.12.10:48787   11.11.11.1:48787   4.4.4.4:23         4.4.4.4:23
--- 10.1.12.10         11.11.11.1         ---                ---
tcp 10.1.12.11:63566   111.111.111.1:63566 4.4.4.4:23        4.4.4.4:23
--- 10.1.12.11         111.111.111.1      ---                ---
```

Task 4

On R2 perform dynamic address translation for all IP addresses in subnet 10.1.12.0/24 to use IP address of R2's s0/1/0.25 interface when going towards R5 and R4.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#access-list 1 permit 10.1.12.0 0.0.0.255
R2(config)#ip nat inside source list 1 interface s0/1/0.25 overload
```

Verification

```
R1#telnet 5.5.5.5
Trying 5.5.5.5 ... Open


User Access Verification

Password:
R5>sh users
    Line       User       Host(s)              Idle       Location
   0 con 0                idle                 00:00:07
*  2 vty 0                idle                 00:00:00 10.1.25.2

  Interface    User               Mode         Idle     Peer Address

R2#sh ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 10.1.25.1          1.1.1.1            ---                ---
tcp 10.1.25.11:2323    10.1.12.1:23       10.1.45.4:63341    10.1.45.4:63341
tcp 10.1.25.11:2323    10.1.12.1:23       ---                ---
tcp 10.1.25.2:54334    10.1.12.1:54334    5.5.5.5:23         5.5.5.5:23
```

Task 5

Configure network address translation on R2 so that it limits NAT translations to 2 for host 1.1.1.1 Set timeout for dynamic translations of TCP and ICMP to 10 and 5 respectively.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#ip nat translation max-entries host 1.1.1.1 2
R2(config)#ip nat translation tcp-timeout 10
R2(config)#ip nat translation icmp-timeout 5
```

Verification

```
R2#sh ip nat statistics
Total active translations: 4 (2 static, 2 dynamic; 3 extended)
Peak translations: 4, occurred 00:06:42 ago
Outside interfaces:
  Serial0/1/0.25
Inside interfaces:
  GigabitEthernet0/0
Hits: 232  Misses: 0
CEF Translated packets: 232, CEF Punted packets: 0
Expired translations: 2
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 interface Serial0/1/0.25 refcount 1
Appl doors: 0
Normal doors: 0
nat-limit statistics:
 host 1.1.1.1: max allowed 2, used 0, missed 0
Queued Packets: 0
```

```
R2#clear ip nat translation *


R1#tel 10.1.45.4 /so lo0
Trying 10.1.45.4 ... Open


User Access Verification

Password:
R4>
R4>exi

R1#tel 4.4.4.4 /so lo0
Trying 4.4.4.4 ... Open


User Access Verification

Password:
R4>exi

R1#tel 5.5.5.5 /so lo0
Trying 5.5.5.5 ...
% Connection timed out; remote host not responding

R1#
```

```
R2#sh ip nat statistics
Total active translations: 4 (2 static, 2 dynamic; 3 extended)
Peak translations: 4, occurred 00:10:36 ago
Outside interfaces:
  Serial0/1/0.25
Inside interfaces:
  GigabitEthernet0/0
Hits: 348  Misses: 0
CEF Translated packets: 348, CEF Punted packets: 3
Expired translations: 2
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 interface Serial0/1/0.25 refcount 0
Appl doors: 0
Normal doors: 0
nat-limit statistics:
 host 1.1.1.1: max allowed 2, used 2, missed 6
Queued Packets: 0


R2#sh ip nat translations ver
Pro Inside global      Inside local       Outside local      Outside global
tcp 10.1.25.1:24784    1.1.1.1:24784      4.4.4.4:23         4.4.4.4:23
    create 00:00:50, use 00:00:47 timeout:10000, left 00:00:12,
    flags:
extended, timing-out, limited, use_count: 0, entry-id: 10, lc_entries: 0
tcp 10.1.25.1:37445    1.1.1.1:37445      10.1.45.4:23       10.1.45.4:23
    create 00:01:03, use 00:00:52 timeout:10000, left 00:00:07,
    flags:
extended, timing-out, limited, use_count: 0, entry-id: 9, lc_entries: 0
--- 10.1.25.1          1.1.1.1            ---                ---
    create 00:13:23, use 00:00:13 timeout:0,
    flags:
static, use_count: 2, entry-id: 1, lc_entries: 0
tcp 10.1.25.11:2323    10.1.12.1:23       ---                ---
    create 00:10:52, use 00:01:22 timeout:0,
    flags:
static, extended, extendable, use_count: 0, entry-id: 4, lc_entries: 0
```

Task 5

Configure NAT on R5 so that when R4 connects to 10.1.25.1 (R1's loopback0 translated interface) using its loopback0 IP address it will be translated to 10.1.25.4. However if R4 uses its f0/0 interface as a source and connects to 10.1.25.11:2323 (R1's f0/0 translated interface), it will be translated to 10.1.25.44.

Configuration

Complete these steps:

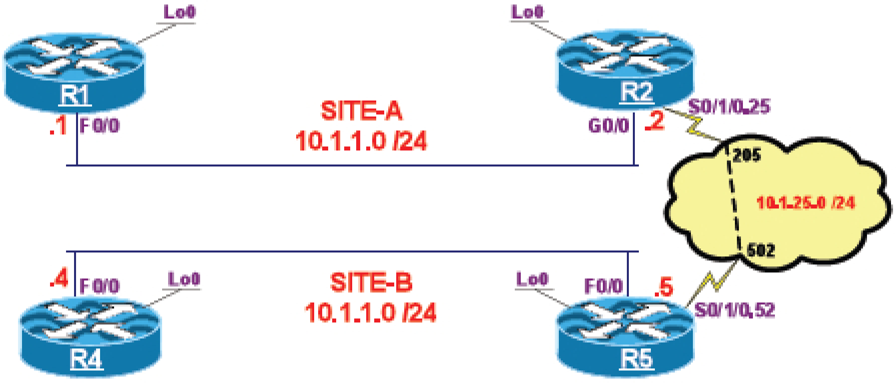
Step 1 R5 configuration.

```
R5(config)#ip access-list extended R4_lo0-to-R1_lo0
R5(config-ext-nacl)#permit ip host 4.4.4.4 host 10.1.25.1
R5(config-ext-nacl)#ip access-list extended R4_fa0-to-R1_fa0
R5(config-ext-nacl)#permit tcp host 10.1.45.4 host 10.1.25.11 eq 2323
R5(config-ext-nacl)#exi
R5(config)#route-map R4_lo0-to-R1_lo0
R5(config-route-map)#match ip address R4_lo0-to-R1_lo0
R5(config-route-map)#route-map R4_fa0-to-R1_fa0
R5(config-route-map)#match ip address R4_fa0-to-R1_fa0
R5(config-route-map)#exi

R5(config)#ip nat inside source static 4.4.4.4 10.1.25.4 route-map R4_lo0-
to-R1_lo0

R5(config)#ip  nat  inside  source  static  10.1.45.4  10.1.25.44  route-map
R4_fa0-to-R1_fa0

R5(config)#int f0/0
R5(config-if)#ip nat inside
R5(config-if)#int s0/1/0.52
R5(config-subif)#ip nat outside
```

Verification

```
R5#sh ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 10.1.25.4          4.4.4.4            ---                ---
--- 10.1.25.44         10.1.45.4          ---                ---

R5#sh ip nat translations ve
Pro Inside global      Inside local       Outside local      Outside global
--- 10.1.25.4          4.4.4.4            ---                ---
    create 00:00:34, use 00:00:34 timeout:0, Map-Id(In): 0,
    flags:
static, route-map-static, use_count: 0, entry-id: 1, lc_entries: 0
--- 10.1.25.44         10.1.45.4          ---                ---
    create 00:00:34, use 00:00:34 timeout:0, Map-Id(In): 0,
    flags:
static, route-map-static, use_count: 0, entry-id: 2, lc_entries: 0

R5#sh route-map
route-map R4_lo0-to-R1_lo0, permit, sequence 10
  Match clauses:
    ip address (access-lists): R4_lo0-to-R1_lo0
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
route-map R4_fa0-to-R1_fa0, permit, sequence 10
  Match clauses:
    ip address (access-lists): R4_fa0-to-R1_fa0
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes

R4#tel 10.1.25.1 /so lo0
Trying 10.1.25.1 ... Open


User Access Verification

Password:
R1>sh users
    Line       User       Host(s)              Idle       Location
   0 con 0                idle                 00:36:40
*  2 vty 0                idle                 00:00:00 10.1.25.4

  Interface    User               Mode         Idle     Peer Address

R5#sh ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 10.1.25.4:60841    4.4.4.4:60841      10.1.25.1:23       10.1.25.1:23
--- 10.1.25.4          4.4.4.4            ---                ---
--- 10.1.25.44         10.1.45.4          ---                ---

R4#tel 10.1.25.11 2323
Trying 10.1.25.11, 2323 ... Open


User Access Verification

Password:
R1>
R1>
R1>sh users
    Line       User       Host(s)              Idle       Location
   0 con 0                idle                 00:51:17
*  2 vty 0                idle                 00:00:00 10.1.25.44

  Interface    User               Mode         Idle     Peer Address

R5#sh ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 10.1.25.4:60841    4.4.4.4:60841      10.1.25.1:23       10.1.25.1:23
tcp 10.1.25.44:63024   10.1.45.4:63024    10.1.25.11:2323    10.1.25.11:2323
--- 10.1.25.4          4.4.4.4            ---                ---
--- 10.1.25.44         10.1.45.4          ---                ---
```

LAB 3.38. NAT with overlapping networks



Lab Setup

- R1 and R2's G0/0 interface should be configured in VLAN 12
- R2 and R5's S0/1/0 interface should be configured in a frame-relay point-to-point manner.
- R5 and R4's F0/0 interface should be configured in VLAN 45
- Configure telnet on all routers using password "cisco"

IP Addressing

Router	Interface	IP address
R1	Lo0 F0/0	1.1.1.1/24 10.1.1.1/24
R2	Lo0 G0/0 S0/1/0.25	2.2.2.2/24 10.1.1.2/24 10.1.25.2/24
R4	Lo0 F0/0	4.4.4.4/24 10.1.1.1/24
R5	Lo0 F0/0 S0/1/0.52	5.5.5.5/24 10.1.1.5/24 10.1.25.5/24

Task 1

R1 and R4 have the same IP address of 10.1.1.1/24. Configure R2 so that those routers can communicate using static translated addresses of 10.1.25.65 and 10.1.25.129 respectively.

You can configure static default routes on R1 and R4 to establish full connectivity.

Configuration

Complete these steps:

Step 1 R1 configuration.

```
R1(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.2
```

Step 2 R4 configuration.

```
R4(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.5
```

Step 3 R2 configuration.

```
R2(config)#ip nat inside source static 10.1.1.1 10.1.25.65
R2(config)#ip nat outside source static 10.1.1.1 10.1.25.129

R2(config)#int g0/0
R2(config-if)#ip nat inside
R2(config-if)#int s0/1/0.25
R2(config-subif)#ip nat outside
```

Verification

```
R2#sh ip nat tra
Pro Inside global      Inside local       Outside local      Outside global
--- ---                ---                10.1.25.129        10.1.1.1
--- 10.1.25.65         10.1.1.1           ---                ---

R1#tel 10.1.25.129
Trying 10.1.25.129 ... Open


User Access Verification

Password:

R2#deb ip nat detailed
```

```
IP NAT detailed debugging is on
R2#
Apr  5 13:57:53.767: NAT: i: tcp (10.1.1.1, 52217) -> (10.1.25.129, 23) [34536]
Apr  5 13:57:53.767: NAT: s=10.1.1.1->10.1.25.65, d=10.1.25.129 [34536]
Apr  5 13:57:53.767: NAT: s=10.1.25.65, d=10.1.25.129->10.1.1.1 [34536]
Apr  5 13:57:53.779: NAT*: o: tcp (10.1.1.1, 23) -> (10.1.25.65, 52217) [6962]
Apr  5 13:57:53.779: NAT*: s=10.1.1.1->10.1.25.129, d=10.1.25.65 [6962]
Apr  5 13:57:53.779: NAT*: s=10.1.25.129, d=10.1.25.65->10.1.1.1 [6962]

<snip>

R2#sh ip nat tra
Pro Inside global      Inside local       Outside local      Outside global
--- ---                ---                10.1.25.129        10.1.1.1
tcp 10.1.25.65:52217   10.1.1.1:52217     10.1.25.129:23     10.1.1.1:23
--- 10.1.25.65         10.1.1.1           ---                ---

R4#tel 10.1.25.65
Trying 10.1.25.65 ... Open


User Access Verification

Password:
R1>

R2#deb ip nat detailed
IP NAT detailed debugging is on
R2#
Apr  5 14:00:09.595: NAT*: o: tcp (10.1.1.1, 26584) -> (10.1.25.65, 23) [7007]
Apr  5 14:00:09.595: NAT*: o: tcp (10.1.1.1, 26584) -> (10.1.25.65, 23) [7007]
Apr  5 14:00:09.595: NAT*: s=10.1.1.1->10.1.25.129, d=10.1.25.65 [7007]
Apr  5 14:00:09.595: NAT*: s=10.1.25.129, d=10.1.25.65->10.1.1.1 [7007]
Apr  5 14:00:09.599: NAT: i: tcp (10.1.1.1, 23) -> (10.1.25.129, 26584) [37502]
Apr  5 14:00:09.599: NAT: s=10.1.1.1->10.1.25.65, d=10.1.25.129 [37502]
Apr  5 14:00:09.599: NAT: s=10.1.25.65, d=10.1.25.129->10.1.1.1 [37502]


R2#sh ip nat tra
Pro Inside global      Inside local       Outside local      Outside global
--- ---                ---                10.1.25.129        10.1.1.1
tcp 10.1.25.65:23      10.1.1.1:23        10.1.25.129:26584  10.1.1.1:26584
--- 10.1.25.65         10.1.1.1           ---                ---
```

Task 2

Reconfigure R2 so that it will translate dynamically SITE-A subnet between R1 and R2 and allow connections to R4. SITE-A subnet should use range of 10.1.25.64/26 for translation and R4 should be translated to the IP address of 10.1.25.129.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#no ip nat inside source static 10.1.1.1 10.1.25.65

R2(config)#ip nat pool SITE-A 10.1.25.65 10.1.25.126 prefix-length 26
R2(config)#access-list 1 permit 10.1.1.0 0.0.0.255
R2(config)#ip nat inside source list 1 pool SITE-A

R2(config)#ip nat outside source static 10.1.1.1 10.1.25.129
```

Verification

```
R2#sh ip nat tra
Pro Inside global      Inside local       Outside local      Outside global
--- ---                ---                10.1.25.129        10.1.1.1

R2#deb ip nat detail
IP NAT detailed debugging is on


R1#tel 10.1.25.129
Trying 10.1.25.129 ... Open


User Access Verification

Password:
R4>sh users
    Line       User       Host(s)              Idle       Location
   0 con 0                idle                 00:27:59
*  2 vty 0                idle                 00:00:00 10.1.25.65

R2#
Apr  5 14:03:40.522:  mapping pointer available mapping:0
Apr  5 14:03:40.522: NAT: setting up outside mapping 10.1.25.129->10.1.1.1, with
mapping-id 0
Apr  5 14:03:40.522: NAT: i: tcp (10.1.1.1, 53267) -> (10.1.25.129, 23) [62883]
Apr  5 14:03:40.522: NAT: s=10.1.1.1->10.1.25.65, d=10.1.25.129 [62883]
Apr  5 14:03:40.522: NAT: s=10.1.25.65, d=10.1.25.129->10.1.1.1 [62883]
Apr  5 14:03:40.522: NAT: installing alias for address 10.1.25.65
Apr  5 14:03:40.534: NAT*: o: tcp (10.1.1.1, 23) -> (10.1.25.65, 53267) [65278]
Apr  5 14:03:40.534: NAT*: s=10.1.1.1->10.1.25.129, d=10.1.25.65 [65278]
Apr  5 14:03:40.534: NAT*: s=10.1.25.129, d=10.1.25.65->10.1.1.1 [65278]
<snip>
```

```
R2#sh ip nat tra
Pro Inside global      Inside local       Outside local      Outside global
--- ---                ---                10.1.25.129        10.1.1.1
tcp 10.1.25.65:53267   10.1.1.1:53267     10.1.25.129:23     10.1.1.1:23
--- 10.1.25.65         10.1.1.1           ---                ---
```

Session initializing from R4 is not possible as there is no translation:

```
R2#cle ip nat tra *

R4#tel 10.1.25.65
Trying 10.1.23.65 ...
% Connection timed out; remote host not responding
```

However, if session is established from R1, it is possible to initialize new session from R4:

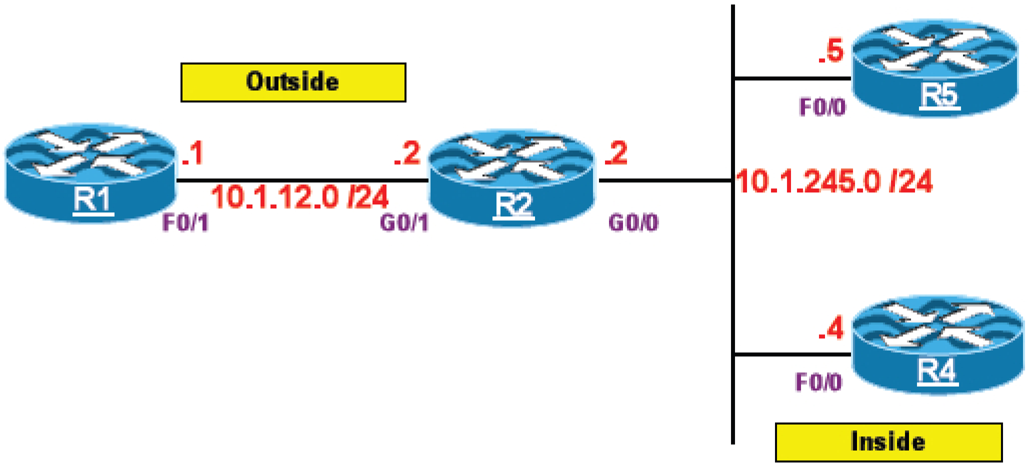
```
R1#tel 10.1.25.129
Trying 10.1.25.129 ... Open


User Access Verification

Password:


R2#sh ip nat tra
Pro Inside global      Inside local       Outside local      Outside global
--- ---                ---                10.1.25.129        10.1.1.1
tcp 10.1.25.66:12416   10.1.1.1:12416     10.1.25.129:23     10.1.1.1:23
--- 10.1.25.66         10.1.1.1           ---                ---

R4#tel 10.1.25.66
Trying 10.1.25.66 ... Open


User Access Verification

Password:
R1>



R2#
Apr  5 14:09:11.330: NAT*: o: tcp (10.1.1.1, 18348) -> (10.1.25.66, 23) [30580]
Apr  5 14:09:11.330: NAT*: o: tcp (10.1.1.1, 18348) -> (10.1.25.66, 23) [30580]
Apr  5 14:09:11.330: NAT*: s=10.1.1.1->10.1.25.129, d=10.1.25.66 [30580]
Apr  5 14:09:11.330: NAT*: s=10.1.25.129, d=10.1.25.66->10.1.1.1 [30580]
Apr  5 14:09:11.330: NAT: i: tcp (10.1.1.1, 23) -> (10.1.25.129, 18348) [26100]
Apr  5 14:09:11.330: NAT: s=10.1.1.1->10.1.25.66, d=10.1.25.129 [26100]
Apr  5 14:09:11.330: NAT: s=10.1.25.66, d=10.1.25.129->10.1.1.1 [26100]
```

```
<snip>

R2#sh ip nat tra
Pro Inside global      Inside local       Outside local      Outside global
--- ---                ---                10.1.25.129        10.1.1.1
tcp 10.1.25.66:23      10.1.1.1:23        10.1.25.129:18348  10.1.1.1:18348
tcp 10.1.25.66:12416   10.1.1.1:12416     10.1.25.129:23     10.1.1.1:23
--- 10.1.25.66         10.1.1.1           ---                ---
```

Task 3

Erase the startup config and reload the routers before proceeding to the next lab.

LAB 3.39. NAT TCP load balancing



Lab Setup

- R1's F0/1 and R2's G0/1 interface should be configured in VLAN 12.
- R2's G0/0, R4, and R5's F0/0 should be configured in VLAN 245.
- Configure telnet on all routers using password "cisco"

IP Addressing

Router	Interface	IP address
R1	F0/1	10.1.12.1/24
R2	G0/1 G0/0	10.1.12.2/24 10.1.245.2/24
R4	F0/0	10.1.245.4/24
R5	F0/0	10.1.245.5/24

Task 1

Configure R2 so that it translates connections from R1 to the IP address of 10.1.34.34 to two real IP addresses (R5 and R4 f0/0 interfaces' IP addresses) in round-robin fashion. Use static default routes on R1, R5 and R5 to achieve full network reachability.

Configuration

Complete these steps:

Step 1 R1 configuration.

```
R1(config)#ip route 0.0.0.0 0.0.0.0 10.1.12.2
```

Step 2 R4 and R5 configuration.

```
(config)#ip route 0.0.0.0 0.0.0.0 10.1.245.2
```

Step 3 R2 configuration.

```
R2(config)#ip nat pool REAL-HOSTS 10.1.245.4 10.1.245.5 prefix-length 24 type
rotary
R2(config)#access-list 2 permit 10.1.34.34
R2(config)#ip nat inside destination list 2 pool REAL-HOSTS

R2(config)#int g0/0
R2(config-if)#ip nat inside
R2(config-if)#int g0/1
R2(config-if)#ip nat outside
```

Verification

```
R1#tel 10.1.34.34
Trying 10.1.34.34 ... Open


User Access Verification

Password:
R5>sh users
    Line       User       Host(s)              Idle       Location
   0 con 0                idle                 00:00:29
*514 vty 0                idle                 00:00:00 10.1.12.1

  Interface    User               Mode         Idle     Peer Address

R5>exi

[Connection to 10.1.34.34 closed by foreign host]

R1#tel 10.1.34.34
Trying 10.1.34.34 ... Open
```

```
User Access Verification

Password:
R4>sh users
    Line       User       Host(s)              Idle       Location
   0 con 0                idle                 00:01:16
*514 vty 0                idle                 00:00:00 10.1.12.1

  Interface    User               Mode         Idle     Peer Address

R4>
```

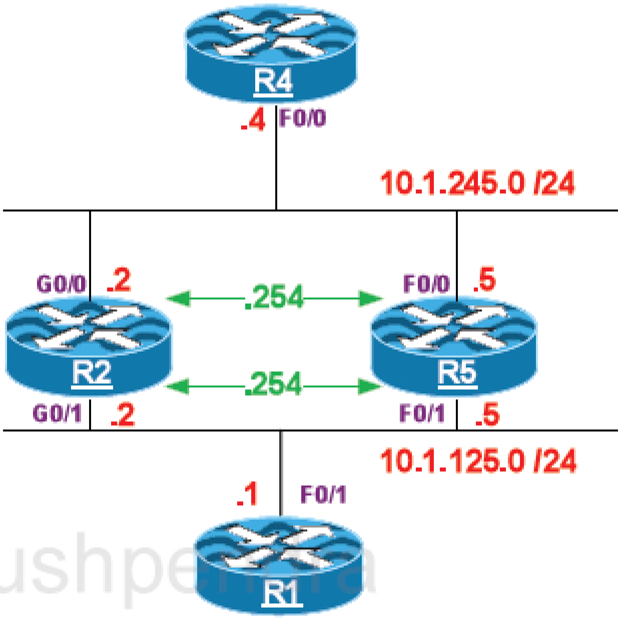
```
R2#deb ip nat det
IP NAT detailed debugging is on

*Sep  3 10:18:30.671: NAT*: o: tcp (10.1.12.1, 31110) -> (10.1.34.34, 23) [54420]
*Sep  3 10:18:30.671: NAT*: s=10.1.12.1, d=10.1.34.34->10.1.245.5 [54420]
*Sep  3 10:18:30.675: NAT*: i: tcp (10.1.245.5, 23) -> (10.1.12.1, 31110) [6122]
*Sep  3 10:18:30.675: NAT*: s=10.1.245.5->10.1.34.34, d=10.1.12.1 [6122]

<snip>

*Sep  3 10:19:08.123: NAT*: o: tcp (10.1.12.1, 61341) -> (10.1.34.34, 23) [5928]
*Sep  3 10:19:08.123: NAT*: s=10.1.12.1, d=10.1.34.34->10.1.245.4 [5928]
*Sep  3 10:19:08.127: NAT*: i: tcp (10.1.245.4, 23) -> (10.1.12.1, 61341) [42103]
*Sep  3 10:19:08.127: NAT*: s=10.1.245.4->10.1.34.34, d=10.1.12.1 [42103]

<snip>
```

```
R2#sh ip nat tra
Pro Inside global      Inside local       Outside local      Outside global
tcp 10.1.34.34:23      10.1.245.4:23      10.1.12.1:61341    10.1.12.1:61341
tcp 10.1.34.34:23      10.1.245.5:23      10.1.12.1:31110    10.1.12.1:31110
```

Task 2

Erase the startup config and reload the routers before proceeding to the next lab.

LAB 3.40. Stateful High Availability NAT



Lab Setup

- R1, R2 (G0/1) and R5's F0/1 interface should be configured in VLAN 125
- R2 (G0/0), R4 and R5's F0/0 interface should be configured in VLAN 245
- Configure telnet on all routers using password "cisco"
- Use only static routing.

IP Addressing

Device	Interface	IP address
R1	F0/1	10.1.125.1/24
R2	G0/0	10.1.245.2/24
	G0/1	10.1.125.2/24
R4	F0/0	10.1.245.4/24
R5	F0/0	10.1.245.5/24
	F0/1	10.1.125.5/24

Task 1

Configure R2 and R5 routers to be seen under one IP address of 10.1.125.254 from R1's perspective and IP address of 10.1.245.254 from R4 (configure correct default routes pointing to the VIP address). Both routers should statically translate IP address of R1's f0/1 interface to the IP address of 10.1.245.1. NAT should notice HSRP state change.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#int g0/1
R2(config-if)#standby 1 ip 10.1.125.254
R2(config-if)#standby 1 name HA_Inside
R2(config-if)#standby 1 preempt
R2(config-if)#standby 1 priority 105
R2(config-if)#standby 1 track g0/0

R2(config-if)#int g0/0
R2(config-if)#standby 2 ip 10.1.245.254
R2(config-if)#standby 2 name HA_Outside
R2(config-if)#standby 2 preempt
R2(config-if)#standby 2 priority 105
R2(config-if)#standby 2 track g0/1
```

Step 2 R5 configuration.

```
R5(config)#int f0/1
R5(config-if)#standby 1 ip 10.1.125.254
R5(config-if)#standby 1 name HA_Inside
R5(config-if)#standby 1 preempt
R5(config-if)#standby 1 track f0/0

R5(config-if)#int f0/0
R5(config-if)#standby 2 ip 10.1.245.254
R5(config-if)#standby 2 name HA_Outside
R5(config-if)#standby 2 preempt
R5(config-if)#standby 2 track f0/1
```

As dynamic routing is not allowed, configure static default routes on R1 and R4 pointing to appropriate VIP (Virtual IP) address.

Step 3 R1 configuration.

```
ip route 0.0.0.0 0.0.0.0 10.1.125.254
```

Step 4 R4 configuration.

```
ip route 0.0.0.0 0.0.0.0 10.1.245.254
```

Step 5 R2 configuration.

```
R2(config)#ip nat inside source static 10.1.125.1 10.1.245.1 redundancy
HA_Inside

R2(config)#int g0/1
R2(config-if)#ip nat inside
R2(config-if)#int g0/0
R2(config-if)#ip nat outside
```

Step 6 R5 configuration.

```
R5(config)#ip nat inside source static 10.1.125.1 10.1.245.1 redundancy
HA_Inside

R5(config)#int f0/1
R5(config-if)#ip nat inside
R5(config-if)#int f0/0
R5(config-if)#ip nat outside
```

Verification

```
R2#sh standby
GigabitEthernet0/0 - Group 2
  State is Active
    2 state changes, last state change 00:03:34
  Virtual IP address is 10.1.245.254
  Active virtual MAC address is 0000.0c07.ac02
    Local virtual MAC address is 0000.0c07.ac02 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.968 secs
  Preemption enabled
  Active router is local
  Standby router is 10.1.245.5, priority 100 (expires in 9.792 sec)
  Priority 105 (configured 105)
    Track interface GigabitEthernet0/1 state Up decrement 10
  Group name is "HA_Outside" (cfgd)
GigabitEthernet0/1 - Group 1
  State is Active
    2 state changes, last state change 00:03:34
  Virtual IP address is 10.1.125.254
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.128 secs
  Preemption enabled
  Active router is local
  Standby router is 10.1.125.5, priority 100 (expires in 11.296 sec)
  Priority 105 (configured 105)
    Track interface GigabitEthernet0/0 state Up decrement 10
  Group name is "HA_Inside" (cfgd)


R5#sh standby
FastEthernet0/0 - Group 2
  State is Standby
    1 state change, last state change 00:03:11
  Virtual IP address is 10.1.245.254
  Active virtual MAC address is 0000.0c07.ac02
    Local virtual MAC address is 0000.0c07.ac02 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.744 secs
  Preemption enabled
  Active router is 10.1.245.2, priority 105 (expires in 9.104 sec)
  Standby router is local
  Priority 100 (default 100)
    Track interface FastEthernet0/1 state Up decrement 10
  Group name is "HA_Outside" (cfgd)
FastEthernet0/1 - Group 1
  State is Standby
    1 state change, last state change 00:03:12
  Virtual IP address is 10.1.125.254
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.848 secs
  Preemption enabled
  Active router is 10.1.125.2, priority 105 (expires in 10.512 sec)
  Standby router is local
  Priority 100 (default 100)
    Track interface FastEthernet0/0 state Up decrement 10
  Group name is "HA_Inside" (cfgd)
```

Test

```
R1#tel 10.1.245.4
Trying 10.1.245.4 ... Open


User Access Verification

Password:
R4>sh users
    Line       User       Host(s)              Idle       Location
   0 con 0                idle                 00:05:31
*514 vty 0                idle                 00:00:00 10.1.245.1

  Interface    User               Mode         Idle     Peer Address

R4>

R2#sh ip nat tran
Pro Inside global      Inside local       Outside local      Outside global
tcp 10.1.245.1:36809   10.1.125.1:36809   10.1.245.4:23      10.1.245.4:23
--- 10.1.245.1         10.1.125.1         ---                ---

R5#sh ip nat tran
Pro Inside global      Inside local       Outside local      Outside global
--- 10.1.245.1         10.1.125.1         ---                ---
```

Now, shutdown the interface on R2 and check if translation still works.

```
R2#deb ip nat deta
IP NAT detailed debugging is on

R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int g0/1
R2(config-if)#shut
R2(config-if)#
%TRACKING-5-STATE: 2 interface Gi0/1 line-protocol Up->Down
%HSRP-5-STATECHANGE: GigabitEthernet0/1 Grp 1 state Active -> Init
NAT: redundancy_update: Active->Init grp:HA_Inside, Address:10.1.245.1
%HSRP-5-STATECHANGE: GigabitEthernet0/0 Grp 2 state Active -> Speak
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to
down
%HSRP-5-STATECHANGE: GigabitEthernet0/0 Grp 2 state Speak -> Standby


R5#sh ip nat tran
Pro Inside global      Inside local       Outside local      Outside global
tcp 10.1.245.1:36809   10.1.125.1:36809   10.1.245.4:23      10.1.245.4:23
```

```
--- 10.1.245.1         10.1.125.1         ---                ---
```

Task 2

Disable static NAT translation configured in the previous task.

Both routers should now dynamically translate IP addresses from 10.125.0/24 subnet to the pool of IP address of 10.1.245.10-100. Enable high availability for NAT so that state table is sent over to the backup router in case of link failure.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#no ip nat inside source static 10.1.125.1 10.1.245.1 redundancy
HA_Inside

R2(config)#ip nat Stateful id 1
R2(config-ipnat-snat)#primary 10.1.125.2
R2(config-ipnat-snat-pri)#peer 10.1.125.5
R2(config-ipnat-snat-pri)#mapping-id 10
R2(config-ipnat-snat-pri)#exit

R2(config)#ip nat Stateful id 1
R2(config-ipnat-snat)#redundancy HA_Inside
R2(config-ipnat-snat-red)#protocol tcp
TCP is deprecated, switching to UDP protocol by default
R2(config-ipnat-snat-red)#mapping-id 10
R2(config-ipnat-snat-red)#exit

R2(config)#ip nat pool NAT_POOL 10.1.245.10 10.1.245.100 prefix-length 24
R2(config)#access-list 1 permit 10.1.125.0 0.0.0.255
R2(config)#ip nat inside source list 1 pool NAT_POOL mapping-id 10
```

Step 2 R5 configuration.

```
R5(config)#no ip nat inside source static 10.1.125.1 10.1.245.1 redundancy
HA_Inside

R5(config)#ip nat Stateful id 1
R5(config-ipnat-snat)#backup 10.1.125.5
R5(config-ipnat-snat-bkp)#peer 10.1.125.2
R5(config-ipnat-snat-bkp)#mapping-id 10
R5(config-ipnat-snat-bkp)#
```

```
%SNAT-5-PROCESS: Id 1, System starts converging
SNAT-5-PROCESS: Id 1, System fully converged

R5(config-ipnat-snat-bkp)#exit

R5(config)#ip nat Stateful id 1
R5(config-ipnat-snat)#redundancy HA_Inside
R5(config-ipnat-snat-red)#protocol udp
R5(config-ipnat-snat-red)#mapping-id 10
R5(config-ipnat-snat-red)#exit

%SNAT-5-PROCESS: Id 1, System starts converging
%SNAT-5-PROCESS: Id 1, System fully converged

R5(config)#ip nat pool NAT_POOL 10.1.245.10 10.1.245.100 prefix-length 24
R2(config)#access-list 1 permit 10.1.125.0 0.0.0.255
R5(config)#ip nat inside source list 1 pool NAT_POOL mapping-id 10
```

Verification

```
R2#sh standby
GigabitEthernet0/0 - Group 2
  State is Active
    5 state changes, last state change 00:00:55
  Virtual IP address is 10.1.245.254
  Active virtual MAC address is 0000.0c07.ac02
    Local virtual MAC address is 0000.0c07.ac02 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.384 secs
  Preemption enabled
  Active router is local
  Standby router is 10.1.245.5, priority 100 (expires in 9.200 sec)
  Priority 105 (configured 105)
    Track interface GigabitEthernet0/1 state Up decrement 10
  Group name is "HA_Outside" (cfgd)
GigabitEthernet0/1 - Group 1
  State is Active
    5 state changes, last state change 00:00:27
  Virtual IP address is 10.1.125.254
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.864 secs
  Preemption enabled
  Active router is local
  Standby router is 10.1.125.5, priority 100 (expires in 8.832 sec)
  Priority 105 (configured 105)
    Track interface GigabitEthernet0/0 state Up decrement 10
  Group name is "HA_Inside" (cfgd)


R2#sh ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Peak translations: 2, occurred 01:18:06 ago
Outside interfaces:
  GigabitEthernet0/0
Inside interfaces:
  GigabitEthernet0/1
Hits: 192  Misses: 0
CEF Translated packets: 192, CEF Punted packets: 0
Expired translations: 2
Dynamic mappings:
-- Inside Source
[Id: 2] access-list 1 pool NAT_POOL refcount 0
 pool NAT_POOL: netmask 255.255.255.0
        start 10.1.245.10 end 10.1.245.100
        type generic, total addresses 91, allocated 0 (0%), misses 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0

R2#sh ip nat tra


R1#tel 10.1.245.4
Trying 10.1.245.4 ... Open


User Access Verification

Password:
R4>sh users
    Line       User       Host(s)              Idle       Location
   0 con 0                idle                 01:03:11
*514 vty 0                idle                 00:00:00 10.1.245.10

  Interface    User               Mode         Idle     Peer Address

R4>



R2#
R2#
*Sep  3 11:37:48.659:  mapping pointer available mapping:10
*Sep  3 11:37:48.659: SNAT (Add_node): Allocated database distributed-id 1
*Sep  3 11:37:48.663: SNAT (Add_node): Init RTree for distributed-id 1
*Sep  3 11:37:48.663: SNAT (Add_node): Allocate Node for nat-id 4, Router-id 1
*Sep  3 11:37:48.663: SNAT (Add_node): Allocate Node for nat-id 5, Router-id 1
*Sep  3 11:37:48.663: NAT: i: tcp (10.1.125.1, 11281) -> (10.1.245.4, 23) [38740]
```

```
*Sep  3 11:37:48.663: NAT: s=10.1.125.1->10.1.245.10, d=10.1.245.4 [38740]
*Sep  3 11:37:48.663: NAT: installing alias for address 10.1.245.10
*Sep  3 11:37:48.663: NAT: o: tcp (10.1.245.4, 23) -> (10.1.245.10, 11281) [42980]
R2#
*Sep  3 11:37:48.663: NAT: s=10.1.245.4, d=10.1.245.10->10.1.125.1 [42980]
```

```
R2#sh ip nat tra
Pro Inside global      Inside local       Outside local      Outside global
tcp 10.1.245.10:11281  10.1.125.1:11281   10.1.245.4:23      10.1.245.4:23
--- 10.1.245.10        10.1.125.1         ---                ---

R5#sh ip nat tra
Pro Inside global      Inside local       Outside local      Outside global
tcp 10.1.245.10:11281  10.1.125.1:11281   10.1.245.4:23      10.1.245.4:23
--- 10.1.245.10        10.1.125.1         ---                ---
```

Note that the same NAT information is on both routers. This is called Stateful NAT.

Test

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int g0/1
R2(config-if)#shut
SNAT: interface GigabitEthernet0/1 with address 10.1.125.2 is down
R2(config-if)#
*Sep  3 11:38:20.739: %TRACKING-5-STATE: 2 interface Gi0/1 line-protocol Up->Down
*Sep  3 11:38:20.743: %HSRP-5-STATECHANGE: GigabitEthernet0/1 Grp 1 state Active ->
Init
*Sep  3 11:38:20.743: %SNAT-5-PROCESS: Id 1, System starts converging
*Sep  3 11:38:20.743: %IP-4-DUPADDR: Duplicate address 10.1.245.10 on
GigabitEthernet0/0, sourced by 0012.8031.d118
*Sep  3 11:38:20.743: NAT: deleting alias from redundancy list for 10.1.245.10
*Sep  3 11:38:20.743: %SNAT-5-PROCESS: Id 1, System fully converged
*Sep  3 11:38:21.435: %SYS-5-CONFIG_I: Configured from console by console
*Sep  3 11:38:22.727: %LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to
administratively down
*Sep  3 11:38:23.031: %HSRP-5-STATECHANGE: GigabitEthernet0/0 Grp 2 state Active ->
Speak
*Sep  3 11:38:23.727: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to down
R2#
*Sep  3 11:38:33.119: %HSRP-5-STATECHANGE: GigabitEthernet0/0 Grp 2 state Speak ->
Standby
```

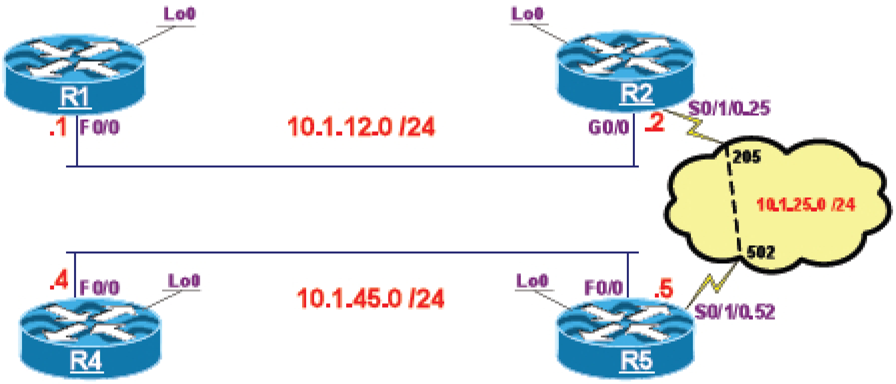
```
R2#sh ip nat tra
Pro Inside global      Inside local       Outside local      Outside global
```

```
tcp 10.1.245.10:11281  10.1.125.1:11281   10.1.245.4:23      10.1.245.4:23
--- 10.1.245.10        10.1.125.1         ---                ---
R2#



R5#
Sep  3 16:16:34.630: %HSRP-5-STATECHANGE: FastEthernet0/1 Grp 1 state Standby -> Active
Sep  3 16:16:34.630: %SNAT-5-PROCESS: Id 1, System starts converging
Sep  3 16:16:34.634: %SNAT-5-PROCESS: Id 1, System fully converged
R5#
Sep  3 16:16:34.642: %IP-4-DUPADDR: Duplicate address 10.1.245.10 on FastEthernet0/0,
sourced by 0011.9368.8270
R5#
Sep  3 16:16:36.930: %HSRP-5-STATECHANGE: FastEthernet0/0 Grp 2 state Standby -> Active


R5#sh ip nat tra
Pro Inside global      Inside local       Outside local      Outside global
tcp 10.1.245.10:11281  10.1.125.1:11281   10.1.245.4:23      10.1.245.4:23
--- 10.1.245.10        10.1.125.1         ---                ---
```

Task 3

Erase the startup config and reload the routers before proceeding to the next lab.

LAB 3.41. NAT Virtual Interface



Lab Setup

- R1 and R2's G0/0 interface should be configured in VLAN 12
- R2 and R5's S0/1/0 interface should be configured in a frame-relay point-to-point manner.
- R5 and R4's F0/0 interface should be configured in VLAN 45
- Configure telnet on all routers using password "cisco"
- Run RIPv2 on the routers and advertise their directly connected networks

IP Addressing

Router	Interface	IP address
R1	Lo0 F0/0	1.1.1.1/24 10.1.12.1/24
R2	Lo0 G0/0 S0/1/0.25	2.2.2.2/24 10.1.12.2/24 10.1.25.2/24
R4	Lo0 F0/0	4.4.4.4/24 10.1.45.4/24
R5	Lo0 F0/0 S0/1/0.52	5.5.5.5/24 10.1.45.5/24 10.1.25.5/24

Task 1

Configure R2 so that it will translate all IP addresses from 10.1.12.0/24 and 10.1.45.0/24 subnet to the IP range from 10.1.25.10 to 10.1.25.100. Do not specify direction for this translation.

The NAT Virtual Interface (NVI) feature removes the requirement to configure an interface as either Network Address Translation (NAT) inside or NAT outside.
An interface can be configured to use NAT or not use NAT.
A NAT table is maintained per interface for better performance and scalability.
However, route maps are not supported in NVI scenarios.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#ip nat pool NAT_POOL 10.1.25.10 10.1.25.100 netmask 255.255.255.0
R2(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface NVI0, changed state to up
R2(config)#ip nat source list 1 pool NAT_POOL

R2(config)#access-list 1 permit 10.1.12.0 0.0.0.255
R2(config)#access-list 1 permit 10.1.45.0 0.0.0.255

R2(config)#int g0/0
R2(config-if)#ip nat enable
R2(config-if)#int s0/1/0.25
R2(config-subif)#ip nat enable
```

Verification

```
R2#sh ip nat nvi statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
NAT Enabled interfaces:
  GigabitEthernet0/0, Serial0/1/0.25
Hits: 0  Misses: 0
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
```

```
-- Source [Id: 3] access-list 1 pool NAT_POOL refcount 0
 pool NAT_POOL: netmask 255.255.255.0
        start 10.1.25.10 end 10.1.25.100
        type generic, total addresses 91, allocated 0 (0%), misses 0
```

TEST 1: Telnet from R1 to R4

```
R1#tel 4.4.4.4
Trying 4.4.4.4 ... Open


User Access Verification

Password:
R4>sh users
    Line       User       Host(s)              Idle       Location
   0 con 0                idle                 00:07:33
*514 vty 0                idle                 00:00:00 10.1.25.10

  Interface    User               Mode         Idle     Peer Address

R4>


R2#
*Sep  3 11:54:52.067: NAT*: i: tcp (10.1.12.1, 56140) -> (4.4.4.4, 23) [15933]
*Sep  3 11:54:52.067: NAT*: s=10.1.12.1->10.1.25.10, d=4.4.4.4 [15933]
*Sep  3 11:54:52.067: NAT: installing alias for address 10.1.25.10
*Sep  3 11:54:52.079: NAT: i: tcp (4.4.4.4, 23) -> (10.1.25.10, 56140) [39209]
*Sep  3 11:54:52.079: NAT: s=4.4.4.4, d=10.1.25.10->10.1.12.1 [39209]


R2#sh ip nat nvi translations
Pro Source global      Source local       Destin  local      Destin  global
tcp 10.1.25.10:56140   10.1.12.1:56140    4.4.4.4:23         4.4.4.4:23
--- 10.1.25.10         10.1.12.1          ---                ---
```

TEST 2: Telnet from R4 to R1

```
R4#tel 1.1.1.1
Trying 1.1.1.1 ... Open


User Access Verification

Password:
R1>sh users
    Line       User       Host(s)              Idle       Location
   0 con 0                4.4.4.4              00:00:31
*514 vty 0                idle                 00:00:00 10.1.25.11
```

```
  Interface    User               Mode         Idle     Peer Address

R1>


*Sep  3 11:55:23.671: NAT*: i: tcp (10.1.45.4, 39512) -> (1.1.1.1, 23) [55125]
*Sep  3 11:55:23.671: NAT*: s=10.1.45.4->10.1.25.11, d=1.1.1.1 [55125]
*Sep  3 11:55:23.671: NAT: installing alias for address 10.1.25.11
*Sep  3 11:55:23.675: NAT: i: tcp (1.1.1.1, 23) -> (10.1.25.11, 39512) [51323]
*Sep  3 11:55:23.675: NAT: s=1.1.1.1, d=10.1.25.11->10.1.45.4 [51323]
```

```
R2#sh ip nat nvi translations
Pro Source global      Source local      Destin  local      Destin  global
tcp 10.1.25.10:56140   10.1.12.1:56140   4.4.4.4:23         4.4.4.4:23
--- 10.1.25.10         10.1.12.1         ---                ---
tcp 10.1.25.11:39512   10.1.45.4:39512   1.1.1.1:23         1.1.1.1:23
--- 10.1.25.11         10.1.45.4         ---                ---
```

Task 2

R5's loopback0 IP address should be translated to R2's g0/0 interface IP address when R5 connects to R1. Do not specify direction for this translation.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#ip nat source static 5.5.5.5 interface g0/0
```

Verification

```
R2#clear ip nat nvi tran *

R2#sh ip nat nvi translations
Pro Source global      Source local      Destin  local      Destin  global
--- 10.1.12.2          5.5.5.5           ---                ---
```

TEST 1: Telnet from R5 to R1

```
R5#tel 1.1.1.1 /so lo0
Trying 1.1.1.1 ... Open


User Access Verification

Password:
R1>sh users
    Line       User       Host(s)              Idle       Location
   0 con 0                idle                 00:00:34
*514 vty 0                idle                 00:00:00 10.1.12.2

  Interface    User               Mode         Idle     Peer Address

R1>

R2#
*Sep  3 12:08:18.111: NAT*: i: tcp (5.5.5.5, 56459) -> (1.1.1.1, 23) [21824]
*Sep  3 12:08:18.111: NAT*: s=5.5.5.5->10.1.12.2, d=1.1.1.1 [21824]
*Sep  3 12:08:18.115: NAT: i: tcp (1.1.1.1, 23) -> (10.1.12.2, 56459) [10318]
*Sep  3 12:08:18.115: NAT: s=1.1.1.1, d=10.1.12.2->5.5.5.5 [10318]

R2#sh ip nat nvi translations
Pro Source global      Source local       Destin  local      Destin  global
tcp 10.1.12.2:56459    5.5.5.5:56459      1.1.1.1:23         1.1.1.1:23
--- 10.1.12.2          5.5.5.5            ---                ---
```

TEST 2: Telnet from R1 to R5

```
R1#tel 5.5.5.5 /so lo0
Trying 5.5.5.5 ...
% Connection timed out; remote host not responding

R2#
*Sep  3 12:12:31.375: NAT*: Can't create new inside entry - forced_punt_flags: 0
*Sep  3 12:12:31.387: NAT*: i: tcp (5.5.5.5, 23) -> (1.1.1.1, 51490) [34459]
*Sep  3 12:12:31.387: NAT*: s=5.5.5.5->10.1.12.2, d=1.1.1.1 [34459]
*Sep  3 12:12:31.391: NAT: i: tcp (1.1.1.1, 51490) -> (10.1.12.2, 23) [51546]
*Sep  3 12:12:31.391: NAT: s=1.1.1.1, d=10.1.12.2->5.5.5.5 [51546]
```

Note that telnet from R1 to R5 does not work. This is because static entry automatically translates "Source local" to "Source global" for returning traffic from R5. Hence, the flow is as follows:

- R1 sends telnet from 1.1.1.1 to 5.5.5.5
- R2 does not perform translation since it has no static or dynamic translation defined for that flow
- R5 replies to R1 from 5.5.5.5 to 1.1.1.1
- R2 translates 5.5.5.5 to its f0/0 interface IP address (10.1.12.2)

- R1 silently drops returning packets as they are coming from "unknown" source

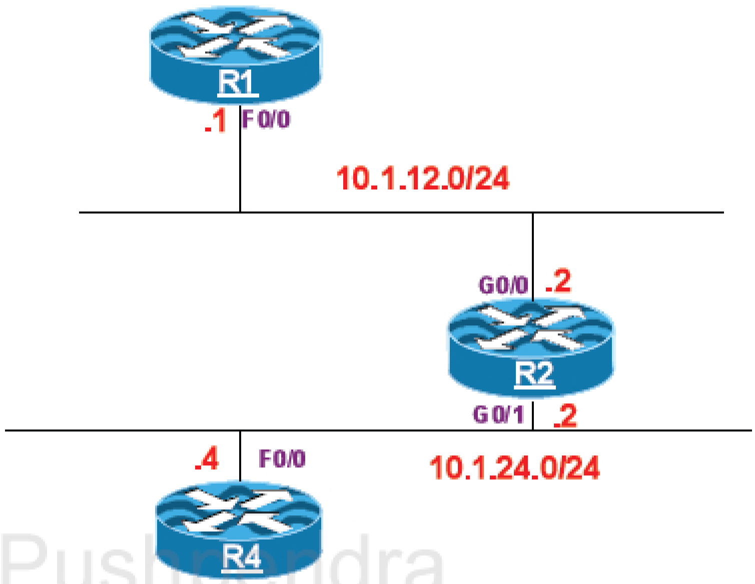
Here's the "deb ip packet detail" output from R1. It sends out SYN packet to 5.5.5.5 and receives SYN/ACK from 10.1.12.2.

```
IP: s=1.1.1.1 (local), d=5.5.5.5 (FastEthernet0/0), len 44, sending full packet
TCP src=38831, dst=23, seq=3487002752, ack=0, win=4128 SYN
IP: s=10.1.12.2 (FastEthernet0/0), d=1.1.1.1, len 44, input feature
TCP src=23, dst=38831, seq=1593419983, ack=3487002753, win=4128 ACK SYN, MCI Check(64),
rtype 0, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
FIBipv4-packet-proc: route packet from FastEthernet0/0 src 10.1.12.2 dst 1.1.1.1
FIBfwd-proc: Default:1.1.1.1/32 receive entry
FIBipv4-packet-proc: packet routing failed
```

Task 3

Erase the startup config and reload the routers before proceeding to the next lab.

LAB 3.42. TCP Intercept



Lab Setup:

- Configure the routers with the following IP addressing:

Router	Interface	IP address
R1	F0/0	10.1.12.1/24
R2	G0/0 G0/1	10.1.12.2/24 10.1.24.2/24
R4	F0/0	10.1.24.4/24

- Configure static default routing on R1 and R4 pointing to R2 and R2 pointing to R4

Task 1

R4's F0/0 interface is getting overwhelmed by SYN packets coming to the TELNET port. R2 should watch the traffic and if it does not complete the TCP handshake in 20 seconds, it should drop the packets.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#access-list 100 permit tcp any host 10.1.24.4 eq 23

R2(config)#ip tcp intercept list 100
R2(config)#ip tcp intercept mode watch
R2(config)#ip tcp intercept watch-timeout 20
```

Verification

```
R1#tel 10.1.24.4
Trying 10.1.24.4 ... Open



User Access Verification


Password:
R4>exit

[Connection to 10.1.24.4 closed by foreign host]

R2#deb ip tcp intercept
TCP intercept debugging is on
R2#
INTERCEPT: new connection (10.1.12.1:57467 SYN -> 10.1.24.4:23)
INTERCEPT: (10.1.12.1:57467 <- ACK+SYN 10.1.24.4:23)
INTERCEPT: (10.1.12.1:57467 ACK -> 10.1.24.4:23)

R2#sh tcp intercept statistics
Watching new connections using access-list 100
0 incomplete, 0 established connections (total 0)
1 connection requests per minute
```

TEST 1: Telnet from R1 to R4 when R4 has ACL on the VTY.

```
R4(config)#access-list 1 permit 1.1.1.1
R4(config)#line vty 0 4
R4(config-line)#access-class 1 in
R4(config-line)#exi

R1#tel 10.1.24.4
Trying 10.1.24.4 ...
% Connection refused by remote host
```

```
R2#
INTERCEPT: new connection (10.1.12.1:17456 SYN -> 10.1.24.4:23)
INTERCEPT: in synsent_watch (10.1.12.1:17456 <- RST 10.1.24.4:23)

       Note that when there is ACL on the VTY the router sends RST back.
```

TEST 2: Telnet from R1 to R4 when R4 is not responding (ACL on the f0/0 interface)

```
R4(config)#access-list 140 deny tcp any any
R4(config)#int f0/0
R4(config-if)#ip access-group 140 in
R4(config-if)#exi

R1#deb ip icmp
ICMP packet debugging is on

R1#tel 10.1.24.4
Trying 10.1.24.4 ...
% Destination unreachable; gateway or host down
ICMP: dst (10.1.12.1) administratively prohibited unreachable rcv from 10.1.24.4

       Note that R1 suddenly drops the connection. This is due to ICMP
       Administratively Prohibited message sent back by R4. There is no TCP RST as it
       was in previous test.

R2#
*Sep  3 12:40:15.575: INTERCEPT: new connection (10.1.12.1:59833 SYN -> 10.1.24.4:23)

*Sep  3 12:40:35.575: INTERCEPT: SYNSENT timing out (10.1.12.1:59833 <-> 10.1.24.4:23)
*Sep  3 12:40:35.575: INTERCEPT(*): (10.1.12.1:59833 RST -> 10.1.24.4:23)

       Note that after 20 seconds R2 sends RST back to R1!
```

Task 2

R2 should start deleting half open connection to R4 if the number reaches 1500. It should stop deleting half open connection if they fall to 1200. Set the one-minute high to 1000 and the one-minute low to 800. Additionally, configure R2 so that it randomly drops partial connection.

Configuration

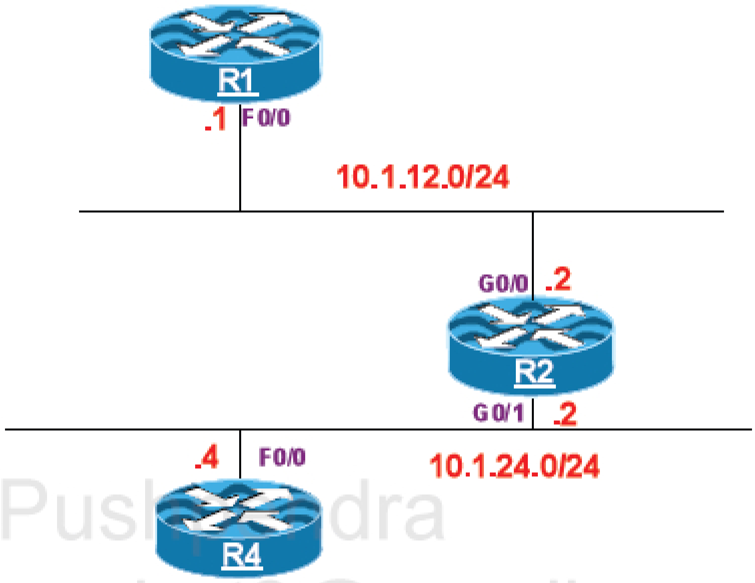
Complete these steps:

Step 1 R2 configuration.

```
R2(config)#ip tcp intercept max-incomplete low 1200 high 1500
R2(config)#ip tcp intercept one-minute low 800 high 1000

R2(config)#ip tcp intercept drop-mode random
```

LAB 3.43. Configuring NBAR

Based on the previous Lab's IP addressing, topology and Lab setup



Task 1

R4 is experiencing a DoS attack against a web server located on interface F0/0. You have discovered that there are lots of URLs in web server's logs with the following strings:

- cmd.exe
- root.exe

Configure R2 to secure that web server by dropping HTTP packets containing the above strings in HTTP header.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#ip cef

R2(config)#class-map match-any URL
R2(config-cmap)#match protocol http url "*cmd.exe*"
R2(config-cmap)#match protocol http url "*root.exe*"
```

```
R2(config-cmap)#policy-map ATTACK
R2(config-pmap)#class URL
R2(config-pmap-c)#drop

R2(config-pmap-c)#int g0/0
R2(config-if)#service-policy input ATTACK
```

Verification

```
R2#sh policy-map interface g0/0
 GigabitEthernet0/0

  Service-policy input: ATTACK

    Class-map: URL (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol http url "*cmd.exe*"
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol http url "*root.exe*"
        0 packets, 0 bytes
        5 minute rate 0 bps
      drop

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

Task 2

You are wondering on what application protocols are operating on the network between R1 and R2. That information will be used in the future so that appropriate quality of service (QoS) features can be applied. Display top 3 protocol used.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#int g0/0
R2(config-if)#ip nbar protocol-discovery
```

Verification

```
R1#tel 10.1.24.4
Trying 10.1.24.4 ... Open


User Access Verification

Password:
R4>exit

[Connection to 10.1.24.4 closed by foreign host]

R2#sh ip nbar protocol-discovery top-n 3

 GigabitEthernet0/0

 Last clearing of "show ip nbar protocol-discovery" counters 00:00:39


                         Input                    Output
                         -----                    ------
   Protocol              Packet Count             Packet Count
                         Byte Count               Byte Count
                         5min Bit Rate (bps)      5min Bit Rate (bps)
                         5min Max Bit Rate (bps)  5min Max Bit Rate (bps)
   ------------------------ ------------------------ ------------------------
   telnet                24                       20
                         1449                     1170
                         0                        0
                         0                        0
   bgp                   0                        0
                         0                        0
                         0                        0
                         0                        0
   bittorrent            0                        0
                         0                        0
                         0                        0
                         0                        0
   unknown               0                        0
                         0                        0
                         0                        0
                         0                        0
   Total                 24                       20
                         1449                     1170
                         0                        0
                         0                        0
```

Task 3

There is a business application running on R4 which listens on TCP ports 8888 and 9999. Configure R4 so that it will NOT allow connections to that application from R2's f0/0 interface IP address using NBAR. NBAR should recognize that application. To avoid memory issues when using NBAR, change the system link age to 20 seconds, the initial memory to 100 kilobytes, and the expanded memory to 50 kilobytes. Also, set the link age for your custom protocol to 180 seconds.

Configuration

Complete these steps:

Step 1 R4 configuration.

```
R4(config)#ip cef

R4(config)#ip nbar custom MY_APP destination tcp 8888 9999

R4(config)#ip access-list extended ACL_MY_APP
R4(config-ext-nacl)#permit tcp host 10.1.12.2 host 10.1.24.4

R4(config)#class-map CM-MY-APP
R4(config-cmap)#match protocol MY_APP
R4(config-cmap)#match access-group name ACL_MY_APP

R4(config-cmap)#policy-map NBAR
R4(config-pmap)#class CM-MY-APP
R4(config-pmap-c)#drop

R4(config)#int f0/0
R4(config-if)#service-policy input NBAR

R4(config)#ip nbar resources system 20 100 50
R4(config)#ip nbar resources protocol 180 MY_APP

R4(config-if)#ip http server
R4(config)#ip http port 8888
```

Verification

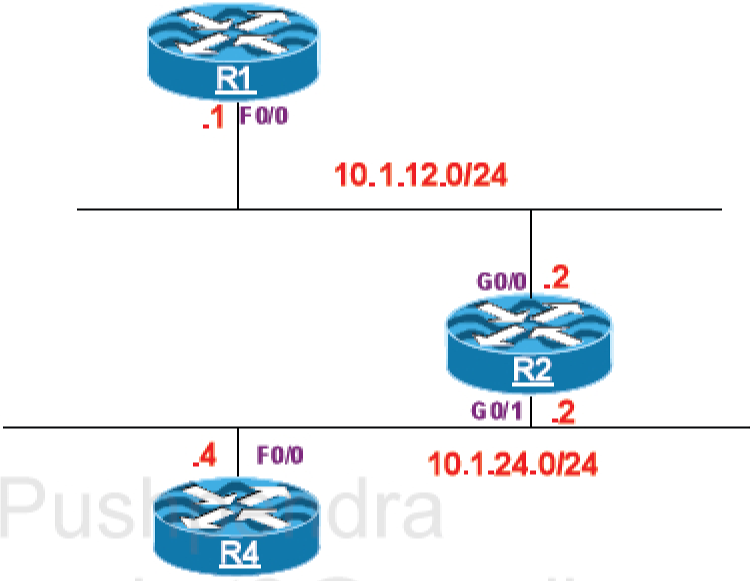
```
R1#tel 10.1.24.4 8888
Trying 10.1.24.4, 8888 ... Open
GET /
HTTP/1.1 400 Bad Request
```

```
Date: Sat, 04 Sep 2010 05:59:02 GMT
Server: cisco-IOS
Connection: close
Accept-Ranges: none

400 Bad Request

[Connection to 10.1.24.4 closed by foreign host]

R2#tel 10.1.24.4 8888
Trying 10.1.24.4, 8888 ... Open
GET /
HTTP/1.1 400 Bad Request
Date: Sat, 04 Sep 2010 05:59:13 GMT
Server: cisco-IOS
Connection: close
Accept-Ranges: none

400 Bad Request

[Connection to 10.1.24.4 closed by foreign host]

R2#tel 10.1.24.4 8888 /so g0/0
Trying 10.1.24.4, 8888 ...
% Connection timed out; remote host not responding


R4#sh policy-map interface f0/0
 FastEthernet0/0

  Service-policy input: NBAR

    Class-map: CM-MY-APP (match-all)
      4 packets, 240 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol MY_APP
      Match: access-group name ACL_MY_APP
      drop

    Class-map: class-default (match-any)
      22 packets, 1320 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any


R4#sh ip nbar port-map MY_APP
port-map MY_APP                  tcp 8888 9999


R4#sh ip nbar resources
NBAR memory usage for tracking Stateful sessions
```

```
System link age       : 20 secs
Initial memory        : 100 KBytes
Max initial memory    : 8896 KBytes
Memory expansion      : 50 KBytes
Max memory expansion  : 112 KBytes
Memory in use         : 99 KBytes
Max memory allowed    : 17792 KBytes
Active links          : 0
Total links           : 892
```

LAB 3.44. Configuring NetFlow

Based on the previous Lab's IP addressing, topology and Lab setup



Task 1

Configure NetFlow version 5 on R2 so that it gathers traffic flows between R1 and R4 and sends them to the management station on IP address 10.1.12.100 on UDP port 9991.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#ip flow-export version 5
R2(config)#ip flow-export destination 10.1.12.100 9991 udp

R2(config)#int g0/0
R2(config-if)#ip flow ingress
R2(config-if)#int g0/1
R2(config-if)#ip flow egress
```

Verification

```
R1#tel 10.1.24.4
Trying 10.1.24.4 ... Open


User Access Verification

Password:
R4>exit

[Connection to 10.1.24.4 closed by foreign host]


R2#show ip flow export
Flow export v5 is enabled for main cache
  Export source and destination details :
  VRF ID : Default
    Destination(1)  10.1.12.100 (9991)
  Version 5 flow records
  2 flows exported in 1 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
```

Task 2

Use the NetFlow Layer 2 and Security Monitoring Exports feature to find out that your network is being attacked by ICMP traffic. The following L2 and L3 values should be captured:

- Time-to-live (TTL) field
- Packet length field
- ICMP type and code fields
- Fragment offset
- Source and Destination MAC address

The Layer 2 and Layer 3 fields supported by the NetFlow Layer 2 and Security Monitoring Exports feature increase the amount of information that can be obtained by NetFlow.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#ip flow-capture fragment-offset
R2(config)#ip flow-capture packet-length
R2(config)#ip flow-capture ttl
R2(config)#ip flow-capture icmp
R2(config)#ip flow-capture mac-addresses
```

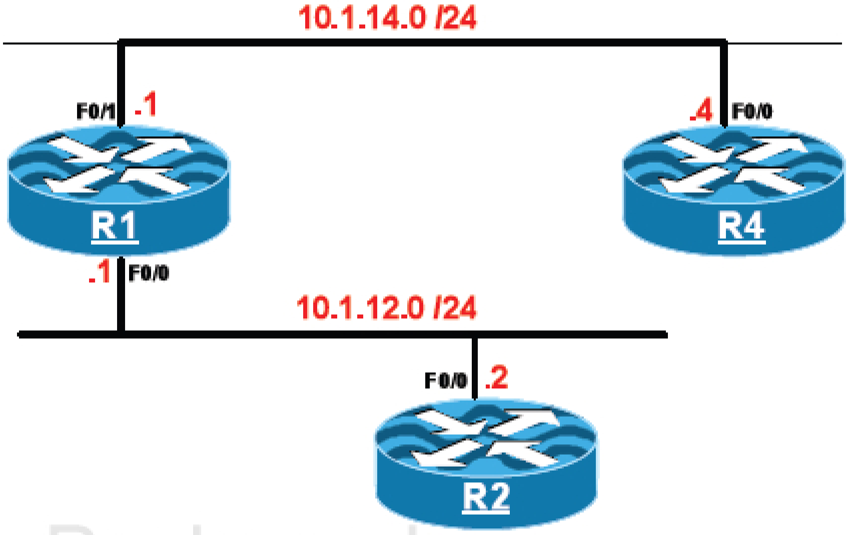
Verification

```
R1#ping 10.1.24.4 rep 10

Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 10.1.24.4, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/2/4 ms


R1#ping 10.1.24.4 rep 10 size 1000

Type escape sequence to abort.
Sending 10, 1000-byte ICMP Echos to 10.1.24.4, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/2/4 ms


R1#ping 10.1.24.4 rep 10 size 2000

Type escape sequence to abort.
Sending 10, 2000-byte ICMP Echos to 10.1.24.4, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 4/4/8 ms


R2#sh ip cache verbose flow
```

```
IP packet size distribution (124 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .354 .000 .161 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .161 .000 .161 .161 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  4 active, 4092 inactive, 6 added
  68 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 34056 bytes
  12 active, 1012 inactive, 14 added, 6 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total     Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows      /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet           2       0.0        22    42      0.0       3.5       1.6
Total:               2       0.0        22    42      0.0       3.5       1.6

SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active
Gi0/0          10.1.12.1       Gi0/1*         10.1.24.4       01 00  00      10
0000 /24 0                     0000 /24 0     10.1.24.4             520     0.0
FFlags: 01
MAC:           001b.d518.3c90                 001b.d504.52e8
Min plen:      520                            Max plen:       520
Min TTL:       255                            Max TTL:        255
ICMP type:       0                            ICMP code:        0
FO:         185

Gi0/0          10.1.12.1       Gi0/1          10.1.24.4       01 00  00      10
0000 /24 0                     0000 /24 0     10.1.24.4             520     0.0
MAC:           001b.d518.3c90                 001b.d504.52e8
Min plen:      520                            Max plen:       520
Min TTL:       255                            Max TTL:        255
ICMP type:       0                            ICMP code:        0
FO:         185

Gi0/0          10.1.12.1       Gi0/1*         10.1.24.4       01 00  10      30
0000 /24 0                     0800 /24 0     10.1.24.4             866     8.0
FFlags: 01
MAC:           001b.d518.3c90                 001b.d504.52e8
Min plen:      100                            Max plen:       1500

SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active
Min TTL:       255                            Max TTL:        255
ICMP type:       8                            ICMP code:        0
```

```
Gi0/0          10.1.12.1      Gi0/1          10.1.24.4      01 00  10      30
0000 /24 0                    0800 /24 0     10.1.24.4            866     8.0
MAC:           001b.d518.3c90                001b.d504.52e8
Min plen:      100                           Max plen:      1500
Min TTL:       255                           Max TTL:       255
ICMP type:       8                           ICMP code:       0
```

LAB 3.45. Configuring IOS IPS



Lab Setup

- The F0/1 interface of R1 and R4's F0/0 should be configured in VLAN 14
- The F0/0 interface of R1 and R2's G0/0 should be configured in VLAN 12
- Configure RIPv2 on all routers and advertise their directly connected interfaces in this routing protocol.

IP Addressing

Router	Interface	IP address
R1	F0/0 F0/1	10.1.12.1/24 10.1.14.1/24
R2	G0/0	10.1.12.2/24
R4	F0/0	10.1.14.4/24

Task 1

Configure IOS Intrusion Prevention System (IPS) to monitor inbound traffic on R1's F0/0 interface. IPS event should be logged to the syslog server located at 10.1.12.100. Store all IPS configuration in the folder MYIPS on the flash. You can use signature pack file (PKG) and crypto key file (realm-cisco.pub.key.txt) located on the flash to accomplish this task.

IPS on a router must load signatures from the PKG file first as there are no default signatures in the IOS. The file is loaded into memory when you assign IPS instance to the interface.

By default most of the signatures are disabled or their action is set to Alarm.

Configuration

Complete these steps:

Step 1 R1 configuration.

```
R1#mkdir flash:MYIPS
Create directory filename [MYIPS]?
Created dir flash:MYIPS

R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip ips name MYIPS
R1(config)#ip ips notify log
R1(config)#loggin 10.1.12.100
R1(config)#loggin on

R1(config)#ip ips config location flash:MYIPS

R1(config)#int f0/0
R1(config-if)#ip ips MYIPS in
```

Note that you have assigned MYIPS to the interface but it is not working since there are no signatures.

Step 2 Import crypto keys.

The appropriate crypto key needs to be imported first. The crypto key is used to verify the digital signature for the master signature file (sigdef-default.xml) whose contents are signed by a Cisco private key to guarantee its authenticity and integrity at every release. The key is stored on the flash in the file realm-cisco.pub.key.txt. You can display the content of the file, copy it and paste as a regular IOS command. The signature pack and crypto key can be found on http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup.

Display files on the flash:

```
R1#sh flash
System flash directory:
File  Length   Name/status
  1   6503441  IOS-S359-CLI.pkg
  2   704      MYIPS/R1-sigdef-default.xml
  3   255      MYIPS/R1-sigdef-delta.xml
  4   6632     MYIPS/R1-sigdef-typedef.xml
  5   27118    MYIPS/R1-sigdef-category.xml
  6   257      MYIPS/R1-seap-delta.xml
  7   491      MYIPS/R1-seap-typedef.xml
  8   805      realm-cisco.pub.key.txt
[6539356 bytes used, 9713568 available, 16252924 total]
16384K bytes of processor board System flash (Read/Write)
```

Display contents of realm-cisco.pub.key.txt file where crypto key is stored

```
R1#more flash:realm-cisco.pub.key.txt
crypto key pubkey-chain rsa
 named-key realm-cisco.pub signature
  key-string
   30820122
(… output omitted…)
```

Copy and paste the output from the previous command to create crypto key:

```
R1(config)#crypto key pubkey-chain rsa
R1(config-pubkey-chain)#named-key realm-cisco.pub signature
R1(config-pubkey-key)#key-string
Enter a public key as a hexidecimal number ....
R1(config-pubkey)# 30820122 (...output omitted)
R1(config-pubkey)# quit
R1(config-pubkey-key)# exit
R1(config-pubkey-chain)# exit
```

Step 3 Enable signatures.

IOS IPS with Cisco 5.x format signatures operates with signature categories, just like Cisco IPS appliances do. All signatures are pre-grouped into categories and the categories are hierarchical. This is so to help classifying signatures for easy grouping and tuning. The "all" signature category contains ALL the signatures in a signature release. Since IOS IPS cannot compile and use all the signatures contained in a signature release at one time, DO NOT UNRETIRE the "all" category, otherwise the router will run out of

memory.
When configuring IOS IPS, it is required to FIRST RETIRE all the signatures in the "all" category, and then UNRETIRE selected signature categories.

```
R1(config)#ip ips signature-category
R1(config-ips-category)#category all
R1(config-ips-category-action)#retired true
R1(config-ips-category-action)#exit
R1(config-ips-category)#category ios_ips basic
R1(config-ips-category-action)#retired false
R1(config-ips-category-action)#exit
R1(config-ips-category)#exit
Do you want to accept these changes? [confirm]
```

Verification

The IPS signatures for IOS software release 12.4(15)T3 and later are fully compatible with appliance IPS 5.x signatures. This means, the format is exactly the same and the signature package should be in *.PKG file.
If you are unsure if you need to use SDF or PKG file enter the following command:

```
R1#show subsys name ips
Name                Class      Version
ips                 Protocol    3.001.002
```

Note: the version 3.x means there is new signature format needed (PKG), version 2.x means it is old format (SDF).

The appropriate signature package file is located on the flash (note the number inside the file name can be different for latest signature releases), so you can easily load it into router's memory:

```
R1#copy flash:IOS-S359-CLI.pkg idconf

%IPS-6-ENGINE_BUILDS_STARTED:  02:12:01 UTC Mar 1 2002
%IPS-6-ENGINE_BUILDING: multi-string - 11 signatures - 1 of 13 engines
%IPS-6-ENGINE_READY: multi-string - build time 36 ms - packets for this engine will be
scanned
%IPS-6-ENGINE_BUILDING: service-http - 649 signatures - 2 of 13 engines
%IPS-6-ENGINE_READY: service-http - build time 8141 ms - packets for this engine will
be scanned
%IPS-6-ENGINE_BUILDING: string-tcp - 1127 signatures - 3 of 13 engines
%IPS-6-ENGINE_READY: string-tcp - build time 26419 ms - packets for this engine will be
scanned
```

```
%IPS-6-ENGINE_BUILDING: string-udp - 75 signatures - 4 of 13 engines
%IPS-6-ENGINE_READY: string-udp - build time 737 ms - packets for this engine will be
scanned
%IPS-6-ENGINE_BUILDING: state - 31 signatures - 5 of 13 engines
%IPS-6-ENGINE_READY: state - build time 76 ms - packets for this engine will be scanned
%IPS-6-ENGINE_BUILDING: atomic-ip - 304 signatures - 6 of 13 engines
%IPS-6-ENGINE_READY: atomic-ip - build time 1166 ms - packets for this engine will be
scanned
%IPS-6-ENGINE_BUILDING: string-icmp - 3 signatures - 7 of 13 engines
%IPS-6-ENGINE_READY: string-icmp - build time 44 ms - packets for this engine will be
scanned
%IPS-6-ENGINE_BUILDING: service-ftp - 3 signatures - 8 of 13 engines
%IPS-6-ENGINE_READY: service-ftp - build time 4 ms - packets for this engine will be
scanned
%IPS-6-ENGINE_BUILDING: service-rpc - 75 signatures - 9 of 13 engines
%IPS-6-ENGINE_READY: service-rpc - build time 333 ms - packets for this engine will be
scanned
%IPS-6-ENGINE_BUILDING: service-dns - 38 signatures - 10 of 13 engines
%IPS-6-ENGINE_READY: service-dns - build time 60 ms - packets for this engine will be
scanned
%IPS-6-ENGINE_BUILDING: normalizer - 9 signatures - 11 of 13 engines
```

To verify, start HTTP server on R4 and try to trigger well know signature no. 5081 which checks URI field of HTTP packet to ensure there is no /system32/cmd.exe string. This attack was performed against Microsoft IIS a couple years ago.

```
R4(config)#ip http server
```

```
R2#telnet 4.4.4.4 80
Trying 4.4.4.4, 80 ... Open
GET /system32/cmd.exe
```

Note that the following message is generated on R1:

```
R1#
%IPS-4-SIGNATURE: Sig:5081 Subsig:0 Sev:100 WWW WinNT cmd.exe Access [10.1.12.2:11002 -
> 4.4.4.4:80] RiskRating:100
```

Check the IPS configuration to see if all required features are configured

```
R1#sh ip ips conf
IPS Signature File Configuration Status
    Configured Config Locations: flash:MYIPS/
    Last signature default load time: 02:12:39 UTC Mar 1 2002
    Last signature delta load time: 02:09:41 UTC Mar 1 2002
    Last event action (SEAP) load time: -none-
    General SEAP Config:
    Global Deny Timeout: 3600 seconds
    Global Overrides Status: Enabled
    Global Filters Status: Enabled

IPS Auto Update is not currently configured

IPS Syslog and SDEE Notification Status
    Event notification through syslog is enabled
    Event notification through SDEE is disabled

IPS Signature Status
    Total Active Signatures: 338
    Total Inactive Signatures: 2057

IPS Packet Scanning and Interface Status
    IPS Rule Configuration
      IPS name MYIPS
    IPS fail closed is disabled
    IPS deny-action ips-interface is false
    Interface Configuration
      Interface FastEthernet0/0
        Inbound IPS rule is MYIPS
        Outgoing IPS rule is not set

IPS Category CLI Configuration:
    Category all:
        Retire: True
    Category ios_ips basic:
        Retire: False
```

Task 2

Reconfigure the signature triggered in the previous task to Reset Connection and generate an Alarm.

By default most of signatures are just generate an Alarm. The IOS software 12.4(15)T3 and later allows signature tuning in the meaning of changing severity level, action taken or enabling/disabling.

Configuration

Complete these steps:

Step 1 Check signature 5081 configuration on R1.

```
R1# sh ip ips sign | inc 5081|SigID
SigID:SubID En  Cmp   Action Sev    Trait   EC   AI    GST   SI   SM SW SFR Rel
  5081:0     Y   Y      A     HIGH     0     1    0      0     0  FA  N 100 S109
```

Note that the default action for signature 5081 is Alarm.

Step 2 Reconfigure signature.

```
R1(config)#ip ips signature-definition
R1(config-sigdef)#signature 5081
R1(config-sigdef-sig)#engine
R1(config-sigdef-sig-engine)#event-action reset-tcp-connection produce-alert
R1(config-sigdef-sig-engine)#exit
R1(config-sigdef-sig)#exit
R1(config-sigdef)#exit
Do you want to accept these changes? [confirm]
%IPS-6-ENGINE_BUILDS_STARTED:  02:32:15 UTC Mar 1 2002
%IPS-6-ENGINE_BUILDING: service-http - 649 signatures - 1 of 13 engines
%IPS-6-ENGINE_READY: service-http - build time 854 ms - packets for this
engine will be scanned
%IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 2298 ms
R1(config)#
```

You need to confirm changes before exit. Note that signature is re-compiled to apply the changes.

Verification

To verify perform the same attack type as it was in the previous task.

```
R1#sh ip ips sign | inc 5081
  5081:0     Y   Y      A R   HIGH     0     1    0      0     0  FA  N 100 S109
R1#
```

Note that signature 5081 is now generating an Alarm (A) and sends TCP Reset (R).

```
R2#telnet 4.4.4.4 80
Trying 4.4.4.4, 80 ... Open
GET /system32/cmd.exe
[Connection to 4.4.4.4 closed by foreign host]
```

```
R2#

        Note that the connection is suddenly closed and Alarm has been generated on the
        console.

R1#
%IPS-4-SIGNATURE: Sig:5081 Subsig:0 Sev:100 WWW WinNT cmd.exe Access [10.1.12.2:11005 -
> 4.4.4.4:80] RiskRating:100
```

Task 3

Reconfigure R1 to perform transparent bridging between R2 and R4. This new network segment should have IP address of 10.1.24.0/24. Configure IOS IPS to transparently monitor this segment on the R1's f0/0 interface.

☑ *IOS software 12.4 and above allows using Transparent IPS which can be useful when customers want to protect their network via a typical Cisco IOS IPS device and can NOT readdress each of the statically defined devices on the trusted network.*

This feature works in conjunction with Integrated Routed Bridging (IRB), which allows a device to bridge on some interfaces while a Layer 3 Bridged Virtual Interface (BVI) is presented for routing

Configuration

Complete these steps:

Step 1 R1 bridging configuration.

```
R1(config)#bridge 1 protocol ieee
R1(config)#int f0/0
R1(config-if)#bridge-group 1
R1(config-if)#int f0/1
R1(config-if)#bridge-group 1
R1(config-if)#exit
R1(config)#bridge irb
IRB: generating 'bridge 1 route ip' configuration command
R1(config)#int bvi1
R1(config-if)#ip add 10.1.24.1 255.255.255.0
R1(config-if)#no sh
```

Step 2 R2 reconfiguration.

```
R2(config)#int g0/0
R2(config-if)#ip add 10.1.24.2 255.255.255.0
```

Step 3 R4 reconfiguration.

```
R4(config)#int f0/1
R4(config-if)#ip add 10.1.24.4 255.255.255.0
```

Step 4 Connectivity check.

A quick verification if we still have connectivity.

```
R2#ping 10.1.24.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.24.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/133/272 ms
R2#

R2#ping 10.1.24.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.24.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 92/401/1260 ms
R2#
```

Step 5 IPS configuration.

Since the IPS configuration remained from the previous tasks, the only thing to do is to assign IPS with R1's f0/0 interface and load the signature package into routers memory (as it flushes when IPS is disabled).

```
R1(config)#int f0/0
R1(config-if)#ip ips MYIPS in
R1(config-if)#
%IPS-6-ENGINE_BUILDS_STARTED:  03:01:10 UTC Mar 1 2002
%IPS-6-ENGINE_BUILDING: atomic-ip - 3 signatures - 1 of 13 engines
%IPS-6-ENGINE_READY: atomic-ip - build time 20 ms - packets for this engine
will be scanned
%IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 20 ms
```

verification

```
R1#copy flash:IOS-S359-CLI.pkg idconf
%IPS-3-IPS_FILE_OPEN_ERROR: flash:MYIPS/R1-sigdef-typedef.xml - Device in exclusive use
%IPS-3-IPS_FILE_OPEN_ERROR: flash:MYIPS/R1-sigdef-category.xml - Device in exclusive
use
%IPS-6-ENGINE_BUILDS_STARTED:  03:06:45 UTC Mar 1 2002
%IPS-6-ENGINE_BUILDING: multi-string - 11 signatures - 1 of 13 engines
%IPS-6-ENGINE_READY: multi-string - build time 56 ms - packets for this engine will be
scanned
%IPS-6-ENGINE_BUILDING: service-http - 649 signatures - 2 of 13 engines
%IPS-6-ENGINE_READY: service-http - build time 13919 ms - packets for this engine will
be scanned
%IPS-6-ENGINE_BUILDING: string-tcp - 1127 signatures - 3 of 13 engines
%IPS-6-ENGINE_READY: string-tcp - build time 46352 ms - packets for this engine will be
scanned
%IPS-6-ENGINE_BUILDING: string-udp - 75 signatures - 4 of 13 engines
%IPS-6-ENGINE_READY: string-udp - build time 1238 ms - packets for this engine will be
scanned
%IPS-6-ENGINE_BUILDING: state - 31 signatures - 5 of 13 engines
%IPS-6-ENGINE_READY: state - build time 128 ms - packets for this engine will be
scanned
%IPS-6-ENGINE_BUILDING: atomic-ip - 304 signatures - 6 of 13 engines
%IPS-6-ENGINE_READY: atomic-ip - build time 1839 ms - packets for this engine will be
scanned
%IPS-6-ENGINE_BUILDING: string-icmp - 3 signatures - 7 of 13 engines
%IPS-6-ENGINE_READY: string-icmp - build time 81 ms - packets for this engine will be
scanned
%IPS-6-ENGINE_BUILDING: service-ftp - 3 signatures - 8 of 13 engines
%IPS-6-ENGINE_READY: service-ftp - build time 28 ms - packets for this engine will be
scanned
%IPS-6-ENGINE_BUILDING: service-rpc - 75 signatures - 9 of 13 engines
%IPS-6-ENGINE_READY: service-rpc - build time 793 ms - packets for this engine will be
scanned
%IPS-6-ENGINE_BUILDING: service-dns - 38 signatures - 10 of 13 engines
%IPS-6-ENGINE_READY: service-dns - build time 188 ms - packets for this engine will be
scanned
%IPS-6-ENGINE_BUILDING: normalizer - 9 signatures - 11 of 13 engines
%IPS-6-ENGINE_READY: normalizer - build time 0 ms - packets for this engine will be
scanned
%IPS-6-ENGINE_BUILDING: service-smb-advanced - 43 signatures - 12 of 13 engines
%IPS-6-ENGINE_READY: service-smb-advanced - build time 108 ms - packets for this engine
will be scanned
%IPS-6-ENGINE_BUILDING: service-msrpc - 27 signatures - 13 of 13 engines
%IPS-6-ENGINE_READY: service-msrpc - build time 81 ms - packets for this engine will be
scanned
%IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 65123 ms
```

To verify perform the same attack type as it was in the previous task.

```
R2#tel 4.4.4.4 80
```

```
Trying 4.4.4.4, 80 ... Open
GET /system32/cmd.exe
```

The signature has been triggered as expected.

```
R1#
%IPS-4-SIGNATURE: Sig:5081 Subsig:0 Sev:100 WWW WinNT cmd.exe Access [10.1.24.2:11010 -> 4.4.4.4:80] RiskRating:100
```

This page is intentionally left blank.

Advanced

CCIE SECURTY v4

LAB WORKBOOK

Implementing Control Plane and Management Plane Security

Narbik Kocharians

CCIE #12410 (R&S, Security, SP)

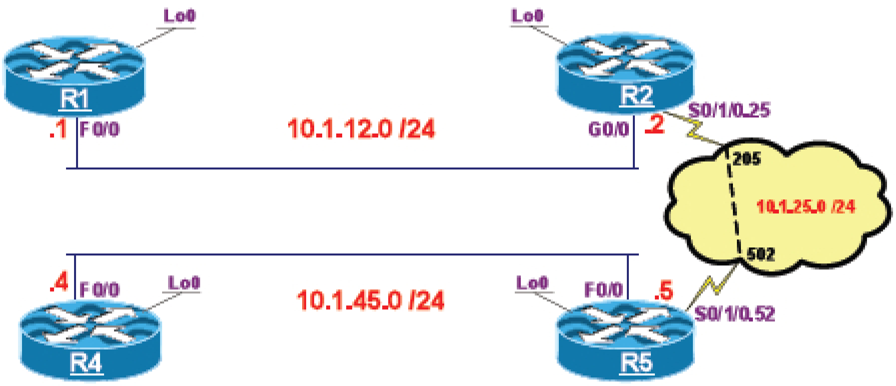
CCSI #30832

Piotr Matusiak

CCIE #19860 (R&S, Security)

C|EH, CCSI #33705

LAB 3.46. CPU protection mechanisms



Lab Setup

- R1 and R2's G0/0 interface should be configured in VLAN 12
- R2 and R5's S0/1/0 interface should be configured in a frame-relay point-to-point manner.
- R5 and R4's F0/0 interface should be configured in VLAN 45
- Configure telnet on all routers using password "cisco"
- Run RIPv2 on the routers and advertise their directly connected networks

IP Addressing

Router	Interface	IP address
R1	Lo0 F0/0	1.1.1.1/24 10.1.12.1/24
R2	Lo0 G0/0 S0/1/0.25	2.2.2.2/24 10.1.12.2/24 10.1.25.2/24
R4	Lo0 F0/0	4.4.4.4/24 10.1.45.4/24
R5	Lo0 F0/0 S0/1/0.52	5.5.5.5/24 10.1.45.5/24 10.1.25.5/24

Task 1

Configure R2 so that it will drop traffic from R1's loopback0 interface coming towards R4's loopback0 interface. Enable logging of dropped traffic. Ensure that only 5 packets per second will be process-switched and no more than 10 syslog messages per second can be generated except level 4 messages and lower.

No ICMP unreachable messages should be sent back to the source.

☑ *ACL logging can be CPU intensive and can negatively affect other functions of the network device. There are two primary factors that contribute to the CPU load increase from ACL logging:*

- *process switching of packets that match log-enabled access control entries*
- *generation and transmission of log messages*

To mitigate that issue you can increase logging interval and rate limit generation of messages.

In real life there are quite common issues related to high CPU on routers and switches which are usually caused by the following:

- *Packet with TTL=1 came to the router/switch*
- *Fragmented packets*
- *ARP (when router/switch must resolve ARP for the traffic going through it)*
- *ACL with logging*

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#ip access-list extended R1-to-R4
R2(config-ext-nacl)#deny ip host 1.1.1.1 host 4.4.4.4 log
R2(config-ext-nacl)#permit ip any any

R2(config-ext-nacl)#int g0/0
R2(config-if)#ip access-group R1-to-R4 in
R2(config-if)#no ip unreachables
```

Logging interval limits log-inducted process switching to one packet per specified time. So, if you specify 200 it means there will be 1

```
               packet per 200ms process switched, resulting 5 packets per 1 second.

        R2(config)#ip access-list logging interval 200

               Logging rate limiter limits log generation to specified number of logs
               per second. Exception means that specified log levels will NOT be
               limited. Note that when you specify level 4 it contains levels 0,1,2,3
               as well.

        R2(config)#logging rate-limit 10 except warnings
```

verification

```
R1#ping 4.4.4.4 so lo0 rep 50
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
..................................................
Success rate is 0 percent (0/50)

%SEC-6-IPACCESSLOGDP: list R1-to-R4 denied icmp 1.1.1.1 -> 4.4.4.4 (0/0), 5 packets
```

Task 2

On R5 enable IP packets debugging with details for only ICMP and TCP packets between R2 and R5 loopback0 interfaces. Logging should be disabled on the console and all debug messages should be directed to the memory buffer without timestamp information.

☑ *Debugging is a high priority and high CPU utilization process that can render your device unusable. Use debug commands only to troubleshoot specific problems. The best times to run debugging are during periods of low network traffic and using specified ACL to "filter" debug messages. Debugs should be also destined to the memory buffer, not the console.*

Configuration

Complete these steps:

Step 1 R5 configuration.

```
R5(config)#no logging console
R5(config)#logging buffered 7
R5(config)#no service timestamps

R5(config)#access-list 199 permit icmp host 2.2.2.2 host 5.5.5.5
R5(config)#access-list 199 permit tcp host 2.2.2.2 host 5.5.5.5

R5#debug ip packet detail 199
IP packet debugging is on (detailed) for access list 199
```

Verification

```
R5#clear logging
Clear logging buffer [confirm]


R2#p 5.5.5.5 so lo0 rep 1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 5.5.5.5, timeout is 2 seconds:
Packet sent with a source address of 2.2.2.2
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 56/56/56 ms


R5#sh logging
Syslog logging: enabled (0 messages dropped, 3 messages rate-limited,
                0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.



No Inactive Message Discriminator.


    Console logging: disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 15 messages logged, xml disabled,
                     filtering disabled
    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled
```

```
No active filter modules.

ESM: 0 messages dropped

    Trap logging: level informational, 46 message lines logged

Log Buffer (4096 bytes):

IP: s=2.2.2.2 (Serial0/1/0.52), d=5.5.5.5, len 100, input feature
    ICMP type=8, code=0, MCI Check(64), rtype 0, forus FALSE, sendself FALSE, mt
u 0, fwdchk FALSE
FIBipv4-packet-proc: route packet from Serial0/1/0.52 src 2.2.2.2 dst 5.5.5.5
FIBfwd-proc: Default:5.5.5.5/32 receive entry
FIBipv4-packet-proc: packet routing failed
IP: tableid=0, s=2.2.2.2 (Serial0/1/0.52), d=5.5.5.5 (Loopback0), routed via RIB
IP: s=2.2.2.2 (Serial0/1/0.52), d=5.5.5.5, len 100, rcvd 4
    ICMP type=8, code=0
IP: s=2.2.2.2 (Serial0/1/0.52), d=5.5.5.5, len 100, stop process pak for forus p
acket
    ICMP type=8, code=0
```

Task 3

You will terminate IPSec VPN on the R4 in a near future using onboard hardware accelerator. To ensure this will not affect router's performance disable hardware failover to the software crypto engine.

☑ *For those situations in which the amount of IPSec traffic is more than can be handled by hardware accelerator, the failover to the software can affect CPU performance.*

Configuration

Complete these steps:

Step 1 R4 configuration.

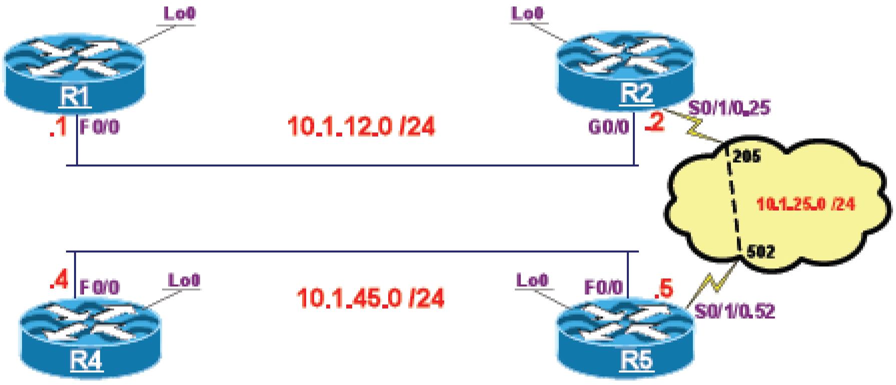
```
R4(config)#no crypto engine software ipsec
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
%CRYPTO-6-GDOI_ON_OFF: GDOI is OFF
```

Verification

```
R4#sh cry eli
Hardware Encryption : ACTIVE
 Number of hardware crypto engines = 1

 CryptoEngine NETGX details: state = Active
 Capability      : IPPCP, DES, 3DES, AES, IPv6, GDOI, FAILCLOSE

 IPSec-Session :     0 active,  2400 max, 0 failed


R4#sh crypto engine accelerator statistic

Device:   NETGX
Location: Onboard: 0
        :Statistics for encryption device since the last clear
         of counters 3179 seconds ago
                      0 packets in                           0 packets out
                      0 bytes in                             0 bytes out
                      0 paks/sec in                          0 paks/sec out
                      0 Kbits/sec in                         0 Kbits/sec out
                      0 packets decrypted                    0 packets encrypted
                      0 bytes before decrypt                 0 bytes encrypted
                      0 bytes decrypted                      0 bytes after encrypt
                      0 packets decompressed                 0 packets compressed
                      0 bytes before decomp                  0 bytes before comp
                      0 bytes after decomp                   0 bytes after comp
                      0 packets bypass decompr               0 packets bypass compres
                      0 bytes bypass decompres               0 bytes bypass compressi
                      0 packets not decompress               0 packets not compressed
                      0 bytes not decompressed               0 bytes not compressed
                  1.0:1 compression ratio                1.0:1 overall
                Last 5 minutes:
                      0 packets in                           0 packets out
                      0 paks/sec in                          0 paks/sec out
                      0 bits/sec in                          0 bits/sec out
                      0 bytes decrypted                      0 bytes encrypted
                      0 Kbits/sec decrypted                  0 Kbits/sec encrypted
                  1.0:1 compression ratio                1.0:1 overall

        pkts dropped:      0
        fw_failure:        0   invalid_flow:    0     netgx sessions:    0
        ownership_err:     0   null_data:       0     reqId mismatch:    0
        fw_qs_filled:      0   fw_resource_lock:0
        tx_hi_drops:       0   pak_too_big:     0
        pak_mp_length_spec_fault: 0
        Interrupts: Notify = 0, Reflected = 0, Spurious = 0
        ring limit:64  current desc used: 0  current ring index: 0
        wait session queue: 0 msg   session buf queue: 1024
```

LAB 3.47. Disabling unnecessary services

Based on the previous Lab's IP addressing, topology and Lab setup



Task 1

On R2 disable the following unnecessary services in the global configuration mode:

- CDP
- TCP and UDP Small Servers
- Finger
- Web Server and Secure Web Server
- BootP Server
- DHCP Server

It is highly recommended to manually or automatically (with AutoSecure) disable all services that you are not using. This is because a service could be disabled by default in the previous IOS release and it might be enabled by default in the new release. Hence, disabling all services protect you from this kind of issues.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#no cdp run
R2(config)#no service tcp-small-servers
R2(config)#no service udp-small-servers
R2(config)#no ip http server
R2(config)#no ip http secure-server
R2(config)#no ip bootp server
R2(config)#no service dhcp
```

Task 2

On R5 use automatic script to secure and lock the router's management plane.

The auto secure command allows a user to disable common IP services that can be exploited during network attacks by using a single CLI command. This command eliminates the complexity of securing a router both by automating the configuration of security features and by disabling certain features that are enabled by default and that could be exploited for security holes.

Configuration

Complete these steps:

Step 1 R5 configuration.

```
R5#auto secure management
                --- AutoSecure Configuration ---

*** AutoSecure configuration enhances the security of
the router, but it will not make it absolutely resistant
to all security attacks ***

AutoSecure will modify the configuration of your device.
All configuration changes will be shown. For a detailed
explanation of how the configuration changes enhance security
and any possible side effects, please refer to Cisco.com for
Autosecure documentation.
At any prompt you may enter '?' for help.
```

```
Use ctrl-c to abort this session at any prompt.

Gathering information about the router for AutoSecure

Is this router connected to internet? [no]:

Securing Management plane services...

Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol

Disabling the bootp server
Disabling the http server
Disabling the finger service
Disabling source routing
Disabling gratuitous arp

Here is a sample Security Banner to be shown
at every access to device. Modify it to suit your
enterprise requirements.

Authorized Access only
  This system is the property of So-&-So-Enterprise.
  UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.
  You must have explicit permission to access this
  device. All activities performed on this device
  are logged. Any violations of access policy will result
  in disciplinary action.

Enter the security banner {Put the banner between
k and k, where k is any character}:
k
Authorized Access only
  This system is the property of So-&-So-Enterprise.
  UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.
  You must have explicit permission to access this
  device. All activities performed on this device
  are logged. Any violations of access policy will result
  in disciplinary action.
k
Enable secret is either not configured or
 is the same as enable password
Enter the new enable secret:
Confirm the enable secret :
Enter the new enable password:
Confirm the enable password:
```

```
Configuration of local user database
Enter the username: piotr
Enter the password:
Confirm the password:
Configuring AAA local authentication
Configuring Console, Aux and VTY lines for
local authentication, exec-timeout, and transport
Securing device against Login Attacks
Configure the following parameters

Blocking Period when Login Attack detected: 10

Maximum Login failures with the device: 3

Maximum time period for crossing the failed login attempts: 1

Configure SSH server? [yes]:
Enter the domain-name: MicronicsTraining.com

Configuring interface specific AutoSecure services
Disabling the following ip services on all interfaces:

 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
Disabling mop on Ethernet interfaces

This is the configuration generated:

no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
service password-encryption
service tcp-keepalives-in
service tcp-keepalives-out
no cdp run
no ip bootp server
no ip http server
no ip finger
no ip source-route
no ip gratuitous-arps
no ip identd
banner motd ^C^C
security passwords min-length 6
security authentication failure rate 10 log
enable secret 5 $1$Bu/M$Zb6ZlcYK1i4hvJ.wOLRHJ.
enable password 7 045802150C2E021F5B4A
```

```
username piotr password 7 03145204121D701E1D
aaa new-model
aaa authentication login local_auth local
line con 0
 login authentication local_auth
 exec-timeout 5 0
 transport output telnet
line aux 0
 login authentication local_auth
 exec-timeout 10 0
 transport output telnet
line vty 0 4
 login authentication local_auth
 transport input telnet
line tty 1
 login authentication local_auth
 exec-timeout 15 0
login block-for 10 attempts 3 within 1
ip domain-name MicronicsTraining.com
crypto key generate rsa general-keys modulus 1024
ip ssh time-out 60
ip ssh authentication-retries 2
line vty 0 4
 transport input ssh telnet
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
logging facility local2
logging trap debugging
service sequence-numbers
logging console critical
logging buffered
interface FastEthernet0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
interface FastEthernet0/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
interface Serial0/0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
```

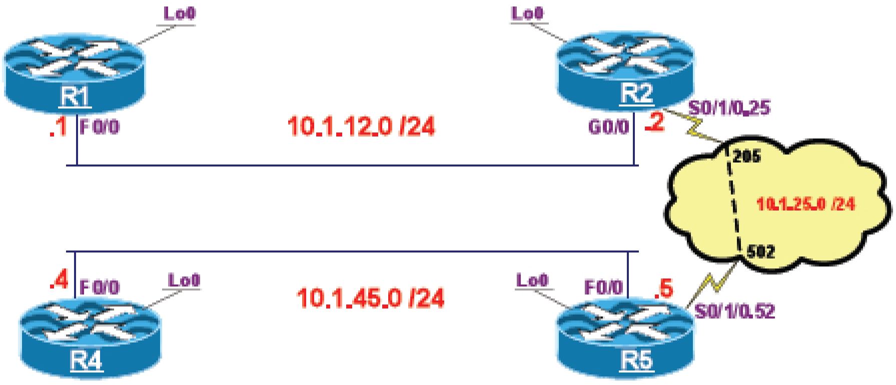
```
interface Serial0/0/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
interface Serial0/1/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
interface Serial0/1/0.52
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
interface Serial0/2/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
!
end


Apply this configuration to running-config? [yes]:

Applying the config generated to running-config

The name for the keys will be: R5.MicronicsTraining.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R5#


%AUTOSEC-1-MODIFIED: AutoSecure configuration has been Modified on this device
```

Task 3

Erase the startup config and reload the routers before proceeding to the next lab.

LAB 3.48. Configuring SNMP

Based on the previous Lab's IP addressing, topology and Lab setup



Task 1

On R1 configure SNMP version 2 so that it can be managed remotely only from the NMS (Network Management System) at IP address of 172.16.1.254.

Use the following configuration:

Read-Only Community name:	SNMP-RO
Read-Write Community name:	SNMP-RW
SNMP Location:	Los Angeles, CA
SNMP Contact:	Micronics Training Inc.
SNMP Chassis ID:	6786239AC

In addition to that, configure R1 to send out SNMP Traps to the same NMS station using version 2c and community string of SNMP-TRAPS. Those traps must be sourced from R1's loopback0 interface.

Configuration

Complete these steps:

Step 1 R1 configuration.

```
R1(config)#access-list 99 permit 172.16.1.254
R1(config)#snmp-server community SNMP-RO ro 99
R1(config)#snmp-server community SNMP-RW rw 99
R1(config)#snmp-server location Los Angeles, CA
R1(config)#snmp-server contact Micronics Training Inc.
R1(config)#snmp-server chassis-id 6786239AC
R1(config)#snmp-server enable traps snmp authentication linkdown linkup
R1(config)#snmp-server host 172.16.1.254 version 2c SNMP-TRAPS
R1(config)#snmp-server source-interface traps lo0
```

Verification

```
R1#sh snmp host
Notification host: 172.16.1.254 udp-port: 162   type: trap
user: SNMP-TRAPS        security model: v2c


R1#sh snmp community

Community name: ILMI
Community Index: cisco0
Community SecurityName: ILMI
storage-type: read-only  active
```

```
Community name: SNMP-RO
Community Index: cisco1
Community SecurityName: SNMP-RO
storage-type: nonvolatile        active access-list: 99


Community name: SNMP-RW
Community Index: cisco2
Community SecurityName: SNMP-RW
storage-type: nonvolatile        active access-list: 99


Community name: SNMP-TRAPS
Community Index: cisco3
Community SecurityName: SNMP-TRAPS
storage-type: nonvolatile        active


R1#sh snmp chassis
6786239AC


R1#sh snmp contact
```

```
Micronics Training Inc.


R1#sh snmp location
Los Angeles, CA
```

Task 2

On R2 configure SNMP version 3 with a group of GR_SNMPv3 and a user named SNMPuser with a secure password of “cisco123”. Allow the NMS station from IP address of 172.16.1.254 to access the router and authenticate using SNMPuser’s credentials.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#snmp-server group GR_SNMPv3 v3 auth
R2(config)#snmp-server user SNMPuser GR_SNMPv3 v3 auth md5 cisco123

Configuring snmpv3 USM user, persisting snmpEngineBoots. Please Wait...

R2(config)#snmp-server host 172.16.1.254 version 3 auth SNMPuser
```

Verification

```
R2#sh snmp host
Notification host: 172.16.1.254 udp-port: 162   type: trap
user: SNMPuser  security model: v3 auth


R2#sh snmp user

User name: SNMPuser
Engine ID: 800000090300001819F33D50
storage-type: nonvolatile        active
Authentication Protocol: MD5
Privacy Protocol: None
Group-name: GR_SNMPv3
```

```
R2#sh snmp group
groupname: ILMI                             security model:v1
readview : *ilmi                            writeview: *ilmi
notifyview: <no notifyview specified>
row status: active

groupname: ILMI                             security model:v2c
readview : *ilmi                            writeview: *ilmi
notifyview: <no notifyview specified>
row status: active

groupname: GR_SNMPv3                        security model:v3 auth
readview : v1default                        writeview: <no writeview specified>
notifyview: *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.F
row status: active


R2#sh snmp view
*ilmi system - included permanent active
*ilmi atmForumUni - included permanent active
v1default iso - included permanent active
v1default internet.6.3.15 - excluded permanent active
v1default internet.6.3.16 - excluded permanent active
v1default internet.6.3.18 - excluded permanent active
v1default ciscoMgmt.394 - excluded permanent active
v1default ciscoMgmt.395 - excluded permanent active
v1default ciscoMgmt.399 - excluded permanent active
v1default ciscoMgmt.400 - excluded permanent active
*tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F ieee802dot11 - included volatile active
*tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F internet - included volatile active
```

Task 3

Your company's helpdesk support needs an access to R2 router via SNMP to perform basic troubleshooting. You are asked to configure the router with the following options:

SNMP version: 3
SNMP user name: U_HELP1 (no password)
SNMP user permissions: read all system and interfaces MIBs, no write permissions

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#snmp-server group GR_HELP1 v3 noauth read V_HELP1
R2(config)#snmp-server user U_HELP1 GR_HELP1 v3
R2(config)#snmp-server view V_HELP1 system included
R2(config)#snmp-server view V_HELP1 interfaces included
```

Verification

```
R2#sh snmp user

User name: U_HELP1
Engine ID: 800000090300001819F33D50
storage-type: nonvolatile        active
Authentication Protocol: None
Privacy Protocol: None
Group-name: GR_HELP1

User name: SNMPuser
Engine ID: 800000090300001819F33D50
storage-type: nonvolatile        active
Authentication Protocol: MD5
Privacy Protocol: None
Group-name: GR_SNMPv3


R2#sh snmp group
groupname: ILMI                              security model:v1
readview : *ilmi                             writeview: *ilmi
notifyview: <no notifyview specified>
row status: active

groupname: ILMI                              security model:v2c
readview : *ilmi                             writeview: *ilmi
notifyview: <no notifyview specified>
row status: active

groupname: GR_HELP1                          security model:v3 noauth
readview : V_HELP1                           writeview: <no writeview specified>
notifyview: <no notifyview specified>
row status: active

groupname: GR_SNMPv3                         security model:v3 auth
readview : v1default                         writeview: <no writeview specified>
```

```
notifyview: *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.F
row status: active


R2#sh snmp view
*ilmi system - included permanent active
*ilmi atmForumUni - included permanent active
V_HELP1 system - included nonvolatile active
V_HELP1 interfaces - included nonvolatile active
v1default iso - included permanent active
v1default internet.6.3.15 - excluded permanent active
v1default internet.6.3.16 - excluded permanent active
v1default internet.6.3.18 - excluded permanent active
v1default ciscoMgmt.394 - excluded permanent active
v1default ciscoMgmt.395 - excluded permanent active
v1default ciscoMgmt.399 - excluded permanent active
v1default ciscoMgmt.400 - excluded permanent active
*tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F ieee802dot11 - included volatile active
*tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F internet - included volatile active
```

Task 2

You company's 3rd line network support needs access to R5 router to perform troubleshooting and secure management via SNMP version 3.

Configure R5 so that it allows secure SNMPv3 connections using username of "U_PRIVATE" with a password of "cisco123". The connection must be secured using AES 256 encryption algorithm with a key of "cisco456".

The user must have read-write access to all system, interfaces and ip MIBs. The NMS station is at 172.16.1.254.

Configuration

Complete these steps:

Step 1 R5 configuration.

```
R5(config)#snmp-server group GR_PRIVATE v3 priv write V_PRIVATE
R5(config)#snmp-server user U_PRIVATE GR_PRIVATE v3 auth md5 cisco123 priv
aes 256 cisco456
R5(config)#
Configuring snmpv3 USM user, persisting snmpEngineBoots. Please Wait...

R5(config)#snmp-server view V_PRIVATE system included
R5(config)#snmp-server view V_PRIVATE interfaces included
R5(config)#snmp-server view V_PRIVATE ip  included
```

```
R5(config)#snmp-server host 172.16.1.254 version 3 priv U_PRIVATE
```

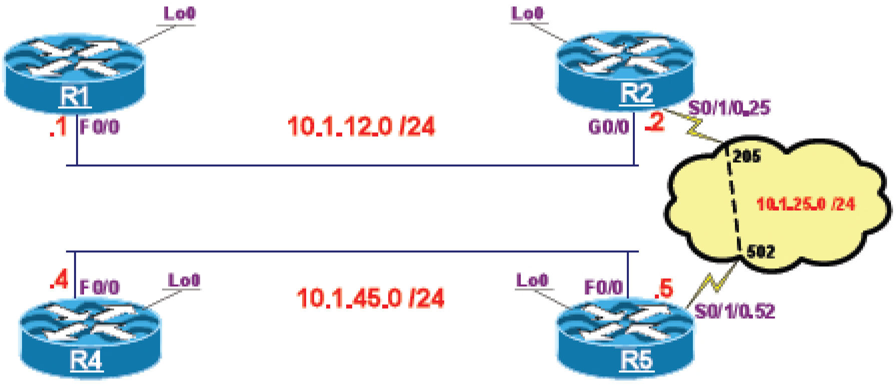
Verification

```
R5#sh snmp host
Notification host: 172.16.1.254 udp-port: 162   type: trap
user: U_PRIVATE security model: v3 priv


R5#sh snmp user

User name: U_PRIVATE
Engine ID: 800000090300001BD515A160
storage-type: nonvolatile        active
Authentication Protocol: MD5
Privacy Protocol: AES256
Group-name: GR_PRIVATE


R5#sh snmp group
groupname: ILMI                             security model:v1
readview : *ilmi                            writeview: *ilmi
notifyview: <no notifyview specified>
row status: active

groupname: ILMI                             security model:v2c
readview : *ilmi                            writeview: *ilmi
notifyview: <no notifyview specified>
row status: active

groupname: GR_PRIVATE                       security model:v3 priv
readview : v1default                        writeview: V_PRIVATE
notifyview: *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.F
row status: active


R5#sh snmp view
*ilmi system - included permanent active
*ilmi atmForumUni - included permanent active
V_PRIVATE system - included nonvolatile active
V_PRIVATE interfaces - included nonvolatile active
V_PRIVATE ip - included nonvolatile active
v1default iso - included permanent active
v1default internet.6.3.15 - excluded permanent active
v1default internet.6.3.16 - excluded permanent active
v1default internet.6.3.18 - excluded permanent active
v1default ciscoMgmt.394 - excluded permanent active
v1default ciscoMgmt.395 - excluded permanent active
v1default ciscoMgmt.399 - excluded permanent active
```

```
v1default ciscoMgmt.400 - excluded permanent active
*tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F ieee802dot11 - included volatile active
*tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F internet - included volatile active
```

LAB 3.49. Configuring SYSLOG

Based on the previous Lab's IP addressing, topology and Lab setup



Task 1

On R1 configure system logging so that the router sends SYSLOG messages to the server at 172.16.1.254 using its loopback0 interface as a source.
All system messages must have time and date attached to the message. The console should be configured to display system messages up to Critical severity level.

Configuration

Complete these steps:

Step 1 R1 configuration.

```
R1(config)#logging host 172.16.1.254
R1(config)#service timestamps log datetime
R1(config)#logging console critical
R1(config)#logging source-interface lo0
```

Verification

```
R1#sh logging
Syslog logging: enabled (0 messages dropped, 3 messages rate-limited,
                0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.



No Inactive Message Discriminator.


    Console logging: level critical, 27 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  disabled, xml disabled,
                     filtering disabled
    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.

ESM: 0 messages dropped

    Trap logging: level informational, 31 message lines logged
        Logging to 172.16.1.254  (udp port 514,  audit disabled,
              authentication disabled, encryption disabled, link up),
              2 message lines logged,
              0 message lines rate-limited,
              0 message lines dropped-by-MD,
              xml disabled, sequence number disabled
              filtering disabled
```

Task 2

SYSLOG server administrator noticed you that you must send all SYSLOG messages to the server using facility name of “local7” to be correctly processed by the server.

In addition to that enable logging of user info on privileged mode enabling and rate limit SYSLOG messages sent to the console to 2 messages per second. Do not rate limit messages with a severity level of Critical or higher.

Configuration

Complete these steps:

Step 1 R1 configuration.

```
R1(config)#logging facility local7
R1(config)#logging rate-limit console 2 except 2
R1(config)#logging userinfo
```

Task 3

On R2 enable configuration change archiving so that the router sends its configuration on TFTP server at 172.16.1.254 in the “backups” directory. The archiving process should notice SYSLOG server at 172.16.1.254. Ensure that no passwords are visible in the archived copy and the router writes its configuration every time before archiving.

Configuration

Complete these steps:

Step 1 R2 configuration.

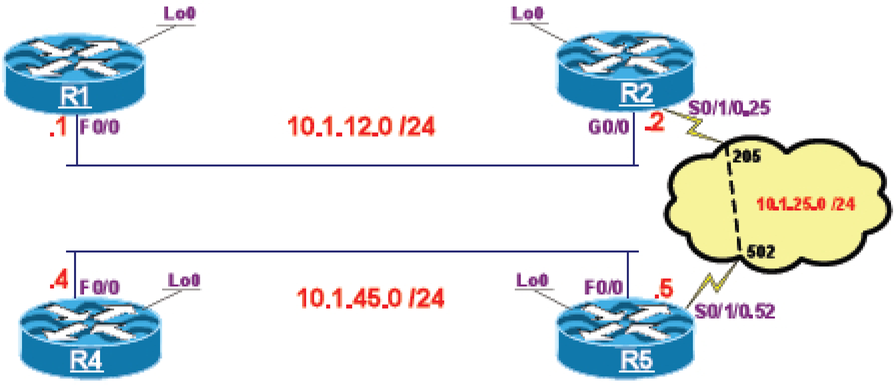
```
R2(config)#archive
R2(config-archive)#path tftp://172.16.1.254/backups/
R2(config-archive)#write-memory

R2(config-archive)#log config
R2(config-archive-log-cfg)#logging enable
R2(config-archive-log-cfg)#hidekeys
R2(config-archive-log-cfg)#notify syslog


R2(config)#logging host 172.16.1.254
```

Verification

```
R2#sh logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,
                0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.



No Inactive Message Discriminator.


    Console logging: level debugging, 36 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 36 messages logged, xml disabled,
                     filtering disabled
    Logging Exception size (8192 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.

ESM: 0 messages dropped

    Trap logging: level informational, 40 message lines logged
        Logging to 172.16.1.254  (udp port 514,  audit disabled,
              authentication disabled, encryption disabled, link up),
              13 message lines logged,
              0 message lines rate-limited,
              0 message lines dropped-by-MD,
              xml disabled, sequence number disabled
              filtering disabled

Log Buffer (8192 bytes):


R2#sh archive
The maximum archive configurations allowed is 14.
The next archive file will be named tftp://172.16.1.254/backups/-0
 Archive #  Name
   1
   2
   3
   4
   5
   6
   7
   8
   9
   10
R2#wr
Building configuration...
[OK]!!


R2#sh archive
The maximum archive configurations allowed is 14.
The next archive file will be named tftp://172.16.1.254/backups/-1
 Archive #  Name
   1        tftp://172.16.1.254/backups/-0 <- Most Recent
   2
   3
   4
   5
   6
   7
   8
   9
   10
R2#
```

LAB 3.50. Configuring NTP

Based on the previous Lab's IP addressing, topology and Lab setup



Task 1

On R1 and R4 configure NTP server with Stratum 5 and server authentication using MD5 key of "cisco123". The R1 can be synced with an IP address of 4.4.4.4 and give out time to R2 only.

Allow only R2's loopback0 interface to get time from this server and configure R2 as a client to that server.

☑ *This lab illustrates structured NTP configuration with verification. Hence, the final configuration is divided to a few parts.*

First, configure basic NTP server without any authentication or filtering.

Configure R2 as a client to that server and see if it gets the time.

Configuration

Complete these steps:

Step 1 R1 configuration – NTP Server.

```
R1(config)#ntp master 5
R1(config)#ntp access-group serve-only 5
R1(config)#access-list 5 permit 2.2.2.2
R1(config)#ntp access-group peer 1
R1(config)#access-list 1 permit 4.4.4.4
R1(config)#ntp peer 4.4.4.4
```

Step 2 R2 configuration – NTP client.

```
R2(config)#ntp source lo0
R2(config)#ntp server 1.1.1.1
```

Step 3 R4 configuration – NTP Server.

```
R4(config)#ntp master 5
R4(config)#ntp source lo0
```

Quick verification

```
R1#sh ntp associations

  address         ref clock       st   when   poll reach  delay  offset   disp
*~127.127.1.1     .LOCL.           4     15     16   377  0.000   0.000  0.237
 ~4.4.4.4         127.127.1.1      5     40     64   357  0.000 -216379  5.681
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
```

```
R1#sh ntp status
Clock is synchronized, stratum 5, reference is 127.127.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**24
reference time is D02DCE53.322C5EA5 (08:07:47.195 UTC Sun Sep 5 2010)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 0.00 msec, peer dispersion is 0.00 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000000 s/s
system poll interval is 16, last update was 3 sec ago.
```

```
R1#sh ntp associations detail
127.127.1.1 configured, our_master, sane, valid, stratum 4
ref ID .LOCL., time D02DCE43.322BD3D9 (08:07:31.195 UTC Sun Sep 5 2010)
our mode active, peer mode passive, our poll intvl 16, peer poll intvl 16
root delay 0.00 msec, root disp 0.00, reach 377, sync dist 0.00
delay 0.00 msec, offset 0.0000 msec, dispersion 0.23
precision 2**24, version 4
org time D02DCE43.322BD3D9 (08:07:31.195 UTC Sun Sep 5 2010)
rec time D02DCE43.322C7E78 (08:07:31.195 UTC Sun Sep 5 2010)
xmt time D02DCE43.322B5862 (08:07:31.195 UTC Sun Sep 5 2010)
filtdelay =     0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
```

```
filtoffset =    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filterror =     0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
minpoll = 4, maxpoll = 4

4.4.4.4 configured, insane, invalid, stratum 5
ref ID 127.127.1.1   , time D02DCE16.BF84656C (08:06:46.748 UTC Sun Sep 5 2010)
our mode active, peer mode passive, our poll intvl 64, peer poll intvl 64
root delay 0.00 msec, root disp 0.38, reach 357, sync dist 156.57
delay 0.00 msec, offset -216379.3748 msec, dispersion 5.68
precision 2**24, version 4
org time D02DCE21.BF83EC63 (08:06:57.748 UTC Sun Sep 5 2010)
rec time D02DCE2B.055B3A63 (08:07:07.020 UTC Sun Sep 5 2010)
xmt time D02DCE22.322C1D2F (08:06:58.195 UTC Sun Sep 5 2010)
filtdelay =     0.01    0.01    0.01    0.01    0.01    0.01    0.01    0.01
filtoffset =   -9.26   -9.26   -9.26   -9.26 -216.38 -216.38 -216.37 -216.37
filterror =     0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
minpoll = 6, maxpoll = 10
```

```
R4#sh ntp status
Clock is synchronized, stratum 5, reference is 127.127.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**24
reference time is D02DCE59.BF84377D (08:07:53.748 UTC Sun Sep 5 2010)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 0.00 msec, peer dispersion is 0.00 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000000 s/s
system poll interval is 16, last update was 15 sec ago.
```

```
R4#sh ntp associations detail
10.1.12.1 dynamic, insane, invalid, stratum 5
ref ID 127.127.1.1   , time D02DCE53.322C5EA5 (08:07:47.195 UTC Sun Sep 5 2010)
our mode passive, peer mode active, our poll intvl 64, peer poll intvl 64
root delay 0.00 msec, root disp 0.44, reach 376, sync dist 189.08
delay 0.00 msec, offset 216380.7571 msec, dispersion 5.68
precision 2**24, version 4
org time D02DCE61.322C2A3A (08:08:01.195 UTC Sun Sep 5 2010)
rec time D02DCE57.F024178D (08:07:51.938 UTC Sun Sep 5 2010)
xmt time D02DCE61.BF839FFD (08:08:01.748 UTC Sun Sep 5 2010)
filtdelay =     0.01    0.01    0.01    0.01    0.01  207.13    0.01    0.01
filtoffset =    9.26    9.26    9.26    9.26    9.26  112.82  216.38  216.37
filterror =     0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
minpoll = 6, maxpoll = 17

127.127.1.1 configured, our_master, sane, valid, stratum 4
ref ID .LOCL., time D02DCE69.BF83B0D0 (08:08:09.748 UTC Sun Sep 5 2010)
our mode active, peer mode passive, our poll intvl 16, peer poll intvl 16
root delay 0.00 msec, root disp 0.00, reach 377, sync dist 0.00
delay 0.00 msec, offset 0.0000 msec, dispersion 0.23
precision 2**24, version 4
org time D02DCE69.BF83B0D0 (08:08:09.748 UTC Sun Sep 5 2010)
```

```
rec time D02DCE69.BF8464BC (08:08:09.748 UTC Sun Sep 5 2010)
xmt time D02DCE69.BF831DDD (08:08:09.748 UTC Sun Sep 5 2010)
filtdelay =     0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filtoffset =    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filterror =     0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
minpoll = 4, maxpoll = 4


R2#sh ntp associations detail
1.1.1.1 configured, our_master, sane, valid, stratum 5
ref ID 127.127.1.1   , time D02DCE65.322C1ADD (08:08:05.195 UTC Sun Sep 5 2010)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
root delay 0.00 msec, root disp 0.42, reach 377, sync dist 0.00
delay 0.00 msec, offset 12.4633 msec, dispersion 3.27
precision 2**24, version 4
org time D02DCE71.481565AF (08:08:17.281 UTC Sun Sep 5 2010)
rec time D02DCE71.44BDF376 (08:08:17.268 UTC Sun Sep 5 2010)
xmt time D02DCE71.445A8560 (08:08:17.267 UTC Sun Sep 5 2010)
filtdelay =     0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filtoffset =    0.01    0.01    0.01    0.01    0.01    0.01    0.01    0.01
filterror =     0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
minpoll = 6, maxpoll = 10


R2#sh ntp status
Clock is synchronized, stratum 6, reference is 1.1.1.1
nominal freq is 250.0000 Hz, actual freq is 249.9999 Hz, precision is 2**24
reference time is D02DCD2F.43E2EE63 (08:02:55.265 UTC Sun Sep 5 2010)
clock offset is 0.0124 msec, root delay is 0.00 msec
root dispersion is 0.02 msec, peer dispersion is 0.00 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000091 s/s
system poll interval is 64, last update was 358 sec ago.
```

Configure authentication on R1 and R2.

Configuration

Complete these steps:

Step 4 R1 NTP authentication.

```
R1(config)#ntp authentication-key 1 md5 cisco123
R1(config)#ntp authenticate
R1(config)#ntp trusted-key 1
```

Step 5 R2 NTP authentication.

```
R2(config)#ntp authentication-key 1 md5 cisco123
R2(config)#ntp authenticate
R2(config)#ntp trusted-key 1
```

Verification

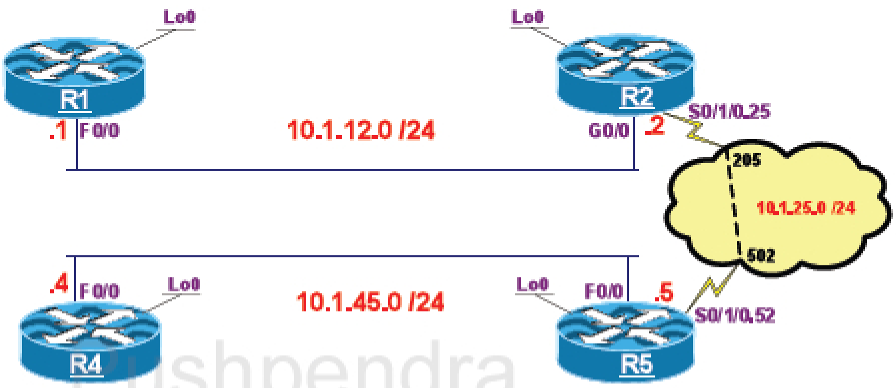
```
R2#sh ntp associations

  address         ref clock       st   when   poll reach  delay  offset   disp
*~1.1.1.1         127.127.1.1      5     53     64    17  0.000  19.670 938.40
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
```

```
R2#sh ntp associations detail
1.1.1.1 configured, our_master, sane, valid, stratum 5
ref ID 127.127.1.1   , time D02DD16D.322887E1 (08:21:01.195 UTC Sun Sep 5 2010)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
root delay 0.00 msec, root disp 0.45, reach 17, sync dist 0.94
delay 0.00 msec, offset 19.6706 msec, dispersion 938.40
precision 2**24, version 4
org time D02DD17C.4B1B66A8 (08:21:16.293 UTC Sun Sep 5 2010)
rec time D02DD17C.464A2AD2 (08:21:16.274 UTC Sun Sep 5 2010)
xmt time D02DD17C.45C3D437 (08:21:16.272 UTC Sun Sep 5 2010)
filtdelay =     0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filtoffset =    0.01    0.01    0.01    0.01    0.00    0.00    0.00    0.00
filterror =     0.00    0.00    0.00    0.00   16.00   16.00   16.00   16.00
minpoll = 6, maxpoll = 10
```

```
R2#sh ntp status
Clock is synchronized, stratum 6, reference is 1.1.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**24
reference time is D02DD17C.464A2AD2 (08:21:16.274 UTC Sun Sep 5 2010)
clock offset is 0.0196 msec, root delay is 0.00 msec
root dispersion is 0.96 msec, peer dispersion is 0.93 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000000 s/s
system poll interval is 64, last update was 30 sec ago.
```

LAB 3.51. Protocol authentication and route filtering

Based on the previous Lab's IP addressing, topology and Lab setup



Task 0 - Preconfiguration:

- Initially, do NOT run any routing dynamic protocol.

Task 1

Run RIPv2 between R1 and R2 on the following directly connected networks:

- R1 – f0/0, lo0
- R2 – G0/0

Configure MD5 authentication for RIPv2 updates with a key string of "cisco123".

Configuration

Complete these steps:

Step 1 R1 configuration.

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#no auto-summary
R1(config-router)#network 10.0.0.0
```

```
R1(config-router)#network 1.0.0.0

R1(config)#key chain RIP
R1(config-keychain)#key 1
R1(config-keychain-key)#key-string cisco123

R1(config)#int f0/0
R1(config-if)#ip rip authentication mode md5
R1(config-if)#ip rip authentication key-chain RIP
```

Step 2 R2 configuration.

```
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#no auto-summary
R2(config-router)#network 10.0.0.0
R2(config-router)#passive-interface default
R2(config-router)#no passive-interface g0/0

R2(config)#key chain RIP
R2(config-keychain)#key 1
R2(config-keychain-key)#key-string cisco123

R2(config-keychain-key)#int g0/0
R2(config-if)#ip rip authentication mode md5
R2(config-if)#ip rip authentication key-chain RIP
```

Verification

```
R1#sh ip protocols
Routing Protocol is "rip"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Sending updates every 30 seconds, next due in 20 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Redistributing: rip
  Default version control: send version 2, receive version 2
    Interface             Send  Recv  Triggered RIP  Key-chain
    FastEthernet0/0       2     2                    RIP
    Loopback0             2     2
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    1.0.0.0
    10.0.0.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.1.12.2            120      00:00:11
  Distance: (default is 120)

R1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/24 is subnetted, 1 subnets
C       1.1.1.0 is directly connected, Loopback0
     10.0.0.0/24 is subnetted, 2 subnets
C       10.1.12.0 is directly connected, FastEthernet0/0
R       10.1.25.0 [120/1] via 10.1.12.2, 00:00:00, FastEthernet0/0


R2#sh ip protocols
Routing Protocol is "rip"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Sending updates every 30 seconds, next due in 15 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Redistributing: rip
  Default version control: send version 2, receive version 2
    Interface             Send  Recv  Triggered RIP  Key-chain
    GigabitEthernet0/0    2     2                    RIP
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    10.0.0.0
  Passive Interface(s):
    GigabitEthernet0/1
    Serial0/1/0
    Serial0/1/0.25
    Serial0/2/0
    FastEthernet1/0
    FastEthernet1/1
    FastEthernet1/2
    FastEthernet1/3
    FastEthernet1/4
  Passive Interface(s):
    FastEthernet1/5
    FastEthernet1/6
    FastEthernet1/7
    FastEthernet1/8
    FastEthernet1/9
    FastEthernet1/10
    FastEthernet1/11
    FastEthernet1/12
    FastEthernet1/13
    FastEthernet1/14
    FastEthernet1/15
    Vlan1
    Loopback0
    VoIP-Null0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.1.12.1            120      00:00:20
  Distance: (default is 120)
```

R2#sh ip route

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/24 is subnetted, 1 subnets
R       1.1.1.0 [120/1] via 10.1.12.1, 00:00:22, GigabitEthernet0/0
     2.0.0.0/24 is subnetted, 1 subnets
C       2.2.2.0 is directly connected, Loopback0
     10.0.0.0/24 is subnetted, 2 subnets
C       10.1.12.0 is directly connected, GigabitEthernet0/0
C       10.1.25.0 is directly connected, Serial0/1/0.25
```

R2#deb ip rip

```
RIP protocol debugging is on
R2#
RIP: sending v2 update to 224.0.0.9 via GigabitEthernet0/0 (10.1.12.2)
RIP: build update entries
   10.1.25.0/24 via 0.0.0.0, metric 1, tag 0
R2#
RIP: received packet with MD5 authentication
RIP: received v2 update from 10.1.12.1 on GigabitEthernet0/0
      1.1.1.0/24 via 0.0.0.0 in 1 hops
```

Task 2

R1 receives prefix for 10.1.25.0/24 subnet. Configure route filtering on R2 so that it will NOT send this network prefix to R1. You are not allowed to use ACL to accomplish this task.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#ip prefix-list TO_R1 deny 10.1.25.0/24
R2(config)#ip prefix-list TO_R1 permit 0.0.0.0/0 le 32

R2(config)#router rip
R2(config-router)#distribute-list prefix TO_R1 out
```

Verification

```
R2#deb ip rip
RIP protocol debugging is on
R2#
RIP: received packet with MD5 authentication
RIP: received v2 update from 10.1.12.1 on GigabitEthernet0/0
      1.1.1.0/24 via 0.0.0.0 in 1 hops

RIP: sending v2 update to 224.0.0.9 via GigabitEthernet0/0 (10.1.12.2)
RIP: build update entries - suppressing null update
```

```
R1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/24 is subnetted, 1 subnets
C       1.1.1.0 is directly connected, Loopback0
     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.12.0 is directly connected, FastEthernet0/0
```

Task 3

Configure EIGRP AS 45 between R4 and R5. The following directly connected networks should participate in EIGRP process:

- R4 – f0/0, lo0
- R5 – f0/0

Configure MD5 authentication for EIGRP updates with a key string of "cisco456".

Configuration

Complete these steps:

Step 1 R5 configuration.

```
R5(config)#router eigrp 45
R5(config-router)#no auto-summary
R5(config-router)#network 10.1.45.5 0.0.0.0

R5(config)#key chain EIGRP
R5(config-keychain)#key 1
R5(config-keychain-key)#key-string cisco456

R5(config-keychain-key)#int f0/0
R5(config-if)#ip authentication mode eigrp 45 md5
R5(config-if)#ip authentication key-chain eigrp 45 EIGRP
```

Step 2 R4 configuration.

```
R4(config)#router eigrp 45
R4(config-router)#no auto-summary
R4(config-router)#network 10.1.45.4 0.0.0.0
R4(config-router)#network 4.4.4.4 0.0.0.0

R4(config)#key chain EIGRP
R4(config-keychain)#key 1
R4(config-keychain-key)#key-string cisco456

R4(config-keychain-key)#int f0/0
R4(config-if)#ip authentication mode eigrp 45 md5
R4(config-if)#ip authentication key-chain eigrp 45 EIGRP

%DUAL-5-NBRCHANGE: IP-EIGRP(0) 45: Neighbor 10.1.45.5
(FastEthernet0/0) is up: new adjacency
```

Verification

```
R4#sh ip protocols
Routing Protocol is "eigrp 45"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 45
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    4.4.4.4/32
    10.1.45.4/32
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: internal 90 external 170
```

```
R4#sh ip eigrp interfaces detail
IP-EIGRP interfaces for process 45

                    Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface    Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Fa0/0          1        0/0         8       0/1           50           0
  Hello interval is 5 sec
  Next xmit serial <none>
  Un/reliable mcasts: 0/1  Un/reliable ucasts: 4/3
  Mcast exceptions: 1  CR packets: 1  ACKs suppressed: 0
  Retransmissions sent: 0  Out-of-sequence rcvd: 0
  Authentication mode is md5,  key-chain is "EIGRP"
  Use multicast
Lo0            0        0/0         0       0/1            0           0
  Hello interval is 5 sec
  Next xmit serial <none>
  Un/reliable mcasts: 0/0  Un/reliable ucasts: 0/0
  Mcast exceptions: 0  CR packets: 0  ACKs suppressed: 0
  Retransmissions sent: 0  Out-of-sequence rcvd: 0
  Authentication mode is not set
  Use multicast
```

```
R4#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     4.0.0.0/24 is subnetted, 1 subnets
C       4.4.4.0 is directly connected, Loopback0
     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.45.0 is directly connected, FastEthernet0/0
```

```
R5#sh ip protocols
Routing Protocol is "eigrp 45"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 45
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    10.1.45.5/32
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.1.45.4             90      00:01:22
  Distance: internal 90 external 170
```

```
R5#sh ip eigrp interfaces detail
IP-EIGRP interfaces for process 45

                        Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface        Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Fa0/0              1        0/0         5       0/1           50           0
  Hello interval is 5 sec
  Next xmit serial <none>
  Un/reliable mcasts: 0/2  Un/reliable ucasts: 1/3
  Mcast exceptions: 1  CR packets: 1  ACKs suppressed: 0
  Retransmissions sent: 0  Out-of-sequence rcvd: 0
  Authentication mode is md5,  key-chain is "EIGRP"
  Use multicast
```

```
R5#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     4.0.0.0/24 is subnetted, 1 subnets
D       4.4.4.0 [90/156160] via 10.1.45.4, 00:01:34, FastEthernet0/0
     5.0.0.0/24 is subnetted, 1 subnets
C       5.5.5.0 is directly connected, Loopback0
     10.0.0.0/24 is subnetted, 2 subnets
C       10.1.25.0 is directly connected, Serial0/1/0.52
C       10.1.45.0 is directly connected, FastEthernet0/0
```

Task 4

Configure OSPF Area 0 between R2 and R5 with interface authentication using MD5 and a key of “cisco789”. The following interfaces should in Area 0:

R2 – s0/0.25, lo0

R5 – s0/0.52, lo0

Configure mutual redistribution to achieve full connectivity in the network.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#router ospf 1
R2(config-router)#network 10.1.25.2 0.0.0.0 area 0
R2(config-router)#network 2.2.2.2 0.0.0.0 area 0
R2(config-router)#redistribute rip subnets

R2(config-router)#router rip
R2(config-router)#redistribute ospf 1 metric 2

R2(config)#int s0/1/0.25
R2(config-subif)#ip ospf authentication message-digest
R2(config-subif)#ip ospf message-digest-key 1 md5 cisco789
```

Step 2 R5 configuration.

```
R5(config)#router ospf 1
R5(config-router)#network 10.1.25.5 0.0.0.0 area 0
R5(config-router)#network 5.5.5.5 0.0.0.0 area 0
R5(config-router)#redistribute eigrp 45 subnets

R5(config-router)#router eigrp 45
R5(config-router)#redistribute ospf 1 metric 100000 0 255 1 1500

R5(config)#int s0/1/0.52
R5(config-subif)#ip ospf authentication message-digest
R5(config-subif)#ip ospf message-digest-key 1 md5 cisco789
```

Verification

```
R2#sh ip ospf interface s0/1/0.25
Serial0/1/0.25 is up, line protocol is up
  Internet Address 10.1.25.2/24, Area 0
  Process ID 1, Router ID 2.2.2.2, Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:09
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 5.5.5.5
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1


R2#sh ip protocols | begin "ospf 1"
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 2.2.2.2
  It is an autonomous system boundary router
  Redistributing External Routes from,
    rip, includes subnets in redistribution
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    2.2.2.2 0.0.0.0 area 0
    10.1.25.2 0.0.0.0 area 0
 Reference bandwidth unit is 100 mbps
  Routing Information Sources:
    Gateway         Distance      Last Update
    5.5.5.5              110      00:02:55
  Distance: (default is 110)
```

R2#sh ip route

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/24 is subnetted, 1 subnets
R       1.1.1.0 [120/1] via 10.1.12.1, 00:00:26, GigabitEthernet0/0
     2.0.0.0/24 is subnetted, 1 subnets
C       2.2.2.0 is directly connected, Loopback0
     4.0.0.0/24 is subnetted, 1 subnets
O E2    4.4.4.0 [110/20] via 10.1.25.5, 00:03:01, Serial0/1/0.25
     5.0.0.0/32 is subnetted, 1 subnets
O       5.5.5.5 [110/65] via 10.1.25.5, 00:03:01, Serial0/1/0.25
     10.0.0.0/24 is subnetted, 3 subnets
C       10.1.12.0 is directly connected, GigabitEthernet0/0
C       10.1.25.0 is directly connected, Serial0/1/0.25
O E2    10.1.45.0 [110/20] via 10.1.25.5, 00:03:02, Serial0/1/0.25
```

R5#sh ip ospf interface s0/1/0.52

```
Serial0/1/0.52 is up, line protocol is up
  Internet Address 10.1.25.5/24, Area 0
  Process ID 1, Router ID 5.5.5.5, Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:05
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1


R5#sh ip protocols | begin "ospf 1"
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 5.5.5.5
  It is an autonomous system boundary router
  Redistributing External Routes from,
    eigrp 45, includes subnets in redistribution
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    5.5.5.5 0.0.0.0 area 0
    10.1.25.5 0.0.0.0 area 0
 Reference bandwidth unit is 100 mbps
  Routing Information Sources:
    Gateway         Distance      Last Update
    2.2.2.2              110      00:03:25
  Distance: (default is 110)


R5#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/24 is subnetted, 1 subnets
O E2    1.1.1.0 [110/20] via 10.1.25.2, 00:03:30, Serial0/1/0.52
     2.0.0.0/32 is subnetted, 1 subnets
O       2.2.2.2 [110/65] via 10.1.25.2, 00:03:30, Serial0/1/0.52
     4.0.0.0/24 is subnetted, 1 subnets
D       4.4.4.0 [90/156160] via 10.1.45.4, 00:10:09, FastEthernet0/0
     5.0.0.0/24 is subnetted, 1 subnets
C       5.5.5.0 is directly connected, Loopback0
     10.0.0.0/24 is subnetted, 3 subnets
O E2    10.1.12.0 [110/20] via 10.1.25.2, 00:03:30, Serial0/1/0.52
C       10.1.25.0 is directly connected, Serial0/1/0.52
C       10.1.45.0 is directly connected, FastEthernet0/0
```

```
R1#ping 4.4.4.4 so lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/17/20 ms
```

Task 5

R4 should NOT install route prefixes for 2.2.2.0/24 and 5.5.5.0/24. Use ACL to accomplish this task.

Configuration

Complete these steps:

Step 1 R4 configuration.

```
R4(config)#ip access-list standard TO_R4
R4(config-ext-nacl)#deny 2.2.2.0 0.0.0.255
R4(config-ext-nacl)#deny 5.5.5.0 0.0.0.255
R4(config-ext-nacl)#permit any

R4(config)#router eigrp 45
R4(config-router)#distribute-list TO_R4 in

%DUAL-5-NBRCHANGE: IP-EIGRP(0) 45: Neighbor 10.1.45.5
(FastEthernet0/0) is resync: route configuration changed
```

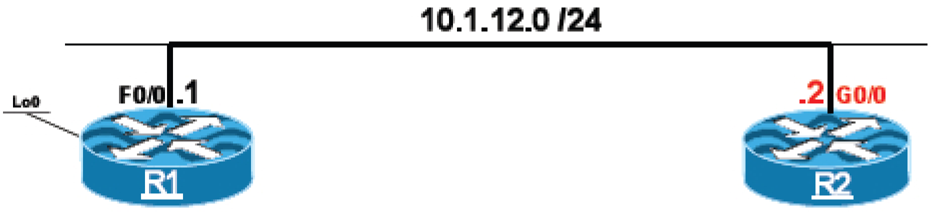
Verification

```
R4#sh ip protocols
Routing Protocol is "eigrp 45"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is TO_R4
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 45
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    4.4.4.4/32
    10.1.45.4/32
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.1.45.5             90      00:00:38
  Distance: internal 90 external 170


R4#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/24 is subnetted, 1 subnets
D EX    1.1.1.0 [170/28160] via 10.1.45.5, 00:00:44, FastEthernet0/0
     4.0.0.0/24 is subnetted, 1 subnets
C       4.4.4.0 is directly connected, Loopback0
     10.0.0.0/24 is subnetted, 3 subnets
D EX    10.1.12.0 [170/28160] via 10.1.45.5, 00:00:44, FastEthernet0/0
D EX    10.1.25.0 [170/28160] via 10.1.45.5, 00:00:44, FastEthernet0/0
C       10.1.45.0 is directly connected, FastEthernet0/0


R4#sh access-list
Standard IP access list TO_R4
    10 deny   2.2.2.0, wildcard bits 0.0.0.255 (3 matches)
    20 deny   5.5.5.0, wildcard bits 0.0.0.255 (3 matches)
    30 permit any (3 matches)


R4#ping 1.1.1.1 so lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 4.4.4.4
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/17/20 ms
```

Task 6

Erase the startup config and reload the routers before proceeding to the next lab.

LAB 3.52. Control Plane Policy (CoPP)



Lab Setup

- The F0/0 interface of R1 and R2 should be configured in VLAN 12
- Configure RIPv2 on all routers and advertise their directly connected interfaces in this routing protocol
- Enable VTY logging on both devices

IP Addressing

Router	Interface	IP address
R1	F0/0 Lo0	10.1.12.1/24 1.1.1.1/8
R2	G0/0	10.1.12.2/24

Task 1

On R2 configure policing for ICMP echo request messages to rate limit it up to 50kbps using Control Plane Policy.

☑ *The Control Plane Policing feature allows to configure a quality of service (QoS) filter that manages the traffic flow of control plane packets to protect the control plane of Cisco IOS routers and switches against reconnaissance and denial-of-service (DoS) attacks. Control Plane is responsible for handling traffic like routing protocols, management protocols, event sending, authentication requests, etc. destined to or originated from the router.*

Configuration

Complete these steps:

Step 1 R2 configuration.

Create ACL that will match the traffic

```
R2(config)#access-list 120 permit icmp any any echo
```

Match interesting traffic using class map

```
R2(config)#class-map ICMP
R2(config-cmap)#match access-group 120
R2(config-cmap)#exit
```

Create policy map and assign previously created class map. Police (rate limit) will drop the traffic which exceeded 50k.

```
R2(config)#policy-map CPP-IN
R2(config-pmap)#class ICMP
R2(config-pmap-c)#police 50000 conform transmit exceed drop
R2(config-pmap-c-police)#exit
R2(config-pmap-c)#exit
R2(config-pmap)#exit
```

Assign policy to the Control Plane in the inbound direction.

```
R2(config)#control-plane
R2(config-cp)#service-policy input CPP-IN
%CP-5-FEATURE: Control-plane Policing feature enabled on Control plane
aggregate path
R2(config-cp)#exi
```

Verification

You can verify this feature by issuing large ping from R1 towards R2 and see if the traffic is limited.

```
R2#show policy-map control-plane
 Control Plane

  Service-policy input: CPP-IN

    Class-map: ICMP (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group 120
      police:
          cir 50000 bps, bc 1562 bytes
        conformed 0 packets, 0 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        conformed 0 bps, exceed 0 bps

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any

R1#ping 10.1.12.2 size 1500

Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 10.1.12.2, timeout is 2 seconds:
.!.!.
Success rate is 40 percent (2/5), round-trip min/avg/max = 1/1/1 ms
```

Note that only 2 pings are successful. The below command clearly shows that that traffic has been rate limited.

```
R2#show policy-map control-plane
 Control Plane

  Service-policy input: CPP-IN

    Class-map: ICMP (match-all)
      4 packets, 6056 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group 120
      police:
          cir 50000 bps, bc 1562 bytes
        conformed 2 packets, 3028 bytes; actions:
          transmit
        exceeded 2 packets, 3028 bytes; actions:
          drop
        conformed 0 bps, exceed 0 bps

    Class-map: class-default (match-any)
      2 packets, 451 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

Note that the first ICMP packet has missed because the router tried to resolve ARP first.

Task 2

Configure R2 so that it allows telnet connections only to the IP address of 1.1.1.1. Do not use ACL on any of router's interfaces or VTY lines configuration.

☑ *This can be done using Control Plane Policing. Note that wording of this task does not mention Control Plane.*

Configuration

Complete these steps:

Step 1 R2 configuration.

```
          Create ACL that will match TELNET traffic from any routers interface
          to any host but 1.1.1.1.

R2(config)#access-list 130 deny tcp any host 1.1.1.1 eq telnet
R2(config)#access-list 130 permit tcp any any eq telnet

          Match interesting traffic using class map

R2(config)#class-map TELNET
R2(config-cmap)#match access-group 130
R2(config-cmap)#exit

          Create policy map and assign previously created class map. This policy
          map should be applied on the OUTBOUND direction.

R2(config)#policy-map CPP-OUT
R2(config-pmap)#class TELNET
R2(config-pmap-c)#drop
R2(config-pmap-c)#exit
R2(config-pmap)#exit

          Apply the policy map

R2(config)#control-plane
R2(config-cp)#service-policy output CPP-OUT
```

Verification

To verify initiate telnet connection from R2 towards R1's IP addresses and check the counters for the policy map.

```
R2#show policy-map control-plane out
 Control Plane

  Service-policy output: CPP-OUT

    Class-map: TELNET (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group 130
      drop

    Class-map: class-default (match-any)
      10 packets, 894 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any


R2#tel 1.1.1.1
Trying 1.1.1.1 ... Open


User Access Verification

Password:
R1>exit

[Connection to 1.1.1.1 closed by foreign host]


R2#show policy-map control-plane out
 Control Plane

  Service-policy output: CPP-OUT

    Class-map: TELNET (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group 130
      drop

    Class-map: class-default (match-any)
      36 packets, 2463 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

```
R2#tel 10.1.12.1
Trying 10.1.12.1 ...
% Connection timed out; remote host not responding


R2#show policy-map control-plane out
 Control Plane

  Service-policy output: CPP-OUT

    Class-map: TELNET (match-all)
      4 packets, 240 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group 130
      drop

    Class-map: class-default (match-any)
      41 packets, 3057 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

Task 3

On R2 enable Control Plane logging feature for all dropped packets.

By default Control Plane Policing silently performs all configured operations. However a good security administrator should be aware what is going on in his network, so logging is always recommended.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
        Create a special class map type and match all dropped packets.

R2(config)#class-map type logging match-any TEST
R2(config-cmap)#match packets dropped
R2(config-cmap)#exit

        Create a special policy map type and assign previously created class
        map. Enable logging of all packets matched that policy.
```

```
R2(config)#policy-map type logging CPP-LOG
R2(config-pmap)#class TEST
R2(config-pmap-c)#log
R2(config-pmap-c)#exit
R2(config-pmap)#exit
```

Assign the policy map to the Control Plane.

```
R2(config)#control-plane
R2(config-cp)#service-policy type logging input CPP-LOG
%CP-5-FEATURE: Control-plane Logging feature enabled on Control plane
aggregate path
```

Verification

To verify perform the test from Task 1 and see if it generates the log message.

```
R1#ping 10.1.12.2 size 1500

Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 10.1.12.2, timeout is 2 seconds:
!.!.!
Success rate is 60 percent (3/5), round-trip min/avg/max = 1/1/1 ms

R2#
%CP-6-IP: DROP Control-plane Policing  10.1.12.1 -> 10.1.12.2 icmp
R2#
%CP-6-IP: DROP Control-plane Policing  10.1.12.1 -> 10.1.12.2 icmp
```

Note: Two drops have been logged as two ICMP echo messages have been dropped. To see what features on the Control Plane are configured, use the following command:

```
R2#show control-plane features
Total 2 features configured
Control plane aggregate path features :
--------------------------------------------------------
Control-plane Logging activated Mar 01 2002 00:4
Control-plane Policing activated Mar 01 2002 00:2
```

Task 4

Erase the startup config and reload the routers before proceeding to the next lab.

This page is intentionally left blank.

Advanced
CCIE SECURTY v4
LAB WORKBOOK

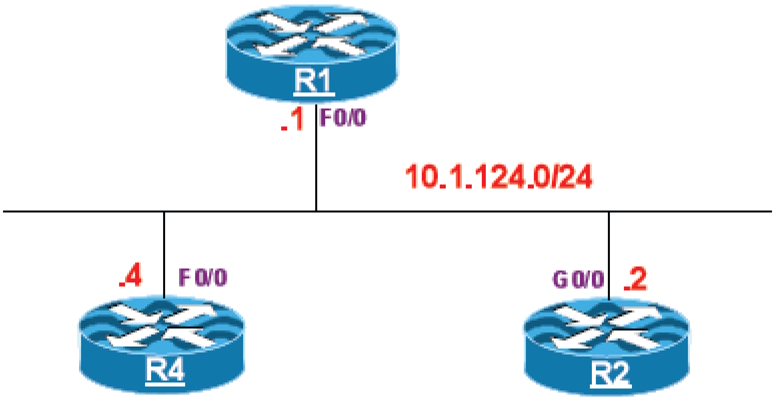
Network Attacks

Narbik Kocharians
CCIE #12410 (R&S, Security, SP)
CCSI #30832

Piotr Matusiak
CCIE #19860 (R&S, Security)
C|EH, CCSI #33705

www.MicronicsTraining.com

LAB 3.53. Protecting against fragmentation attacks



Lab Setup

- Configure the routers with the following IP addressing:

Router	Interface	IP address
R1	F0/0	10.1.124.1/24
R2	G0/0	10.1.124.2/24
R4	F0/0	10.1.124.4/24

- All routers' 0/0 interfaces are in VLAN 124

Task 1

R1 is sending a lot of fragmented IP packets towards R2. Configure it to drop all ICMP fragmented packets when they come to R2's G0/0.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#ip access-list extended NON_FRAGMENTS
R2(config-ext-nacl)# deny icmp any host 10.1.124.2 fragments log
```

```
R2(config-ext-nacl)# permit ip any any
R2(config-ext-nacl)#exi
```

The "NON_FRAGMENTS" access-list is intended to drop fragmented ICMP packets directed towards 10.1.124.2 (R2's G0/0). The ACL permits any remaining IP packets.

```
R2(config)#int g0/0
R2(config-if)#ip access-group NON_FRAGMENTS in
R2(config-if)#exi
```

Verification

```
R1#ping 10.1.124.2 size 1500

Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 10.1.124.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

Packets of size less or equal 1500 (a default IP MTU for Ethernet interfaces) bytes have not been fragmented. Note that loss of first packet has been caused by ARP address resolution (not by "NON_FRAGMENTS" ACL).

```
R1#ping 10.1.124.2 size 1501

Type escape sequence to abort.
Sending 5, 1501-byte ICMP Echos to 10.1.124.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

On R2:

```
%SEC-6-IPACCESSLOGDP: list NON_FRAGMENTS denied icmp 10.1.124.1 -> 10.1.124.2 (0/0), 1
packet
```

Packets of size greater than 1500 bytes have been fragmented by the IOS. ACL "NON_FRAGMENT" placed on R2's G0/0 interface has drop fragmented pieces of IP packets. Note that "log" keyword in the ACE generates log message for first hit.

Task 2

Configure R4 so that it tracks all fragmented packets coming into F0/0 interface. The router should use maximum of 2 fragments per reassembly with a timeout of 2 seconds.

☑ *Virtual Fragmentation Reassembly (VFR) feature was designed work with any features that requires IP fragment reassembly to work properly. VFR assembles fragmented IP packet to enable further processing of whole IP packet. (to match the packet with firewall access control rules or to extract information relevant to network protocols from layers higher than third ISO/OSI layer). The IOS features such as NAT or Cisco IOS Firewall (CBAC or IPS) use VFR. Configuring of the feature that requires VFR enables "ip virtual-reassembly" on the interface automatically. When more than one features enabled on the interface requires VFR than IOS maintains the counter which references number of features that use VFR. If this counter is equal to 0 then VFR is automatically disabled. VFR might be enabled at any time when required even if there is no features that requires this feature to run. This command might be used for control the flow of fragmented packets through the router to protect the network from detected fragmented attacks such as: tiny fragment attack, overlapping fragment attack, buffer overflow attack (when security flaw exists in IP stack code).*

Configuration

Complete these steps:

Step 1 R4 configuration.

```
R4(config)#int f0/0
R4(config-if)#ip virtual-reassembly max-fragments 2 timeout 2
```

This command enables VFR on the Fa0/0 and allows for processing of fragmented IP packets that consist of two or less fragments (default 32). VFR requires that all fragments must be received and assembled in specified amount of time (default 3 seconds). If not, all the fragments and IP datagram will be dropped. This command also allows specifying the maximum number of fragments that can be assembled at any given time.

Verification

```
R1#ping 10.1.124.4 size 1501

Type escape sequence to abort.
Sending 5, 1501-byte ICMP Echos to 10.1.124.4, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 4/4/4 ms
```

The packet of 1501 bytes has been fragmented to two chunks (original IP datagram and the one fragment that is the remaining part of IP packet). VFR configured on R4's F0/0 permits this flow through the router.

```
R1#ping 10.1.124.4 size 5000

Type escape sequence to abort.
Sending 5, 5000-byte ICMP Echos to 10.1.124.4, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

On R4:

```
%IP_VFR-4-TOO_MANY_FRAGMENTS: FastEthernet0/0: Too many fragments per datagram (more
than 2) - sent by 10.1.124.1, destined to 10.1.124.4
```

The packet of size 5000 bytes has been fragmented into more than two fragments. Thus, VFR configured on R4's Fa0/0 has blocked the ICMP fragmented packets. Note that log messages have appeared. This has been caused by defined max-fragments option (if max-fragment value is exceeded then IP_VFR-4-TOO_MANY_FRAGMENTS log message is generated)

```
R4#sh ip virtual-reassembly
FastEthernet0/0:
   Virtual Fragment Reassembly (VFR) is ENABLED...
   Concurrent reassemblies (max-reassemblies): 16
   Fragments per reassembly (max-fragments): 2
   Reassembly timeout (timeout): 2 seconds
   Drop fragments: OFF

   Current reassembly count:0
   Current fragment count:0
   Total reassembly count:4
   Total reassembly timeout count:5
```

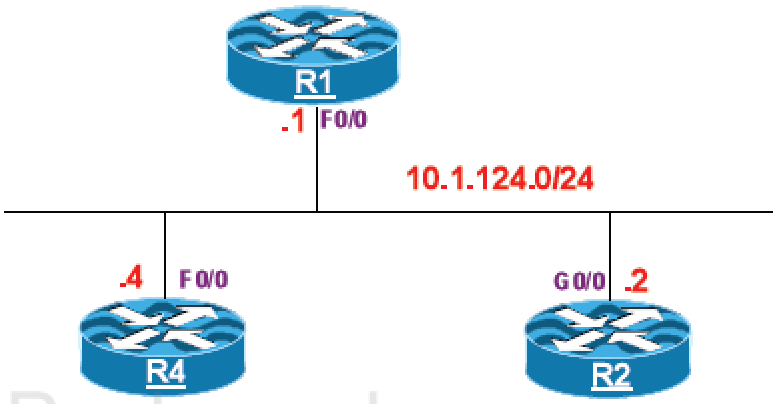
This show command displays VFR configuration along with statistics. Note that concurrent reassemblies (max-reassemblies) is set to the default value of 16. This parameter defines the number of IP packets that can be reassembled at any given time. "Drop fragments" indicates that VFR option "drop-fragments" is disabled (it is a default setting). "drop-fragments" enables the VFR to drop all fragments that arrive on the configured interface

Task 3

Erase the startup config and reload the routers before proceeding to the next lab.

LAB 3.54. Protecting against malicious IP option usage

Based on the previous Lab's IP addressing, topology and Lab setup



Task 1

Configure R1 so that it will drop and log packets containing the following IP Options:

- Loose Source Route,
- Strict Source Routing,
- Base Security.

In real scenario source routing may be used for conducting various network attacks, therefore it is blocked by many routers across the Internet. Source routing enables the sender of a packet to partially (LSR) or completely (SSR) specify the route the packet takes through the network. Base Security IP option enables the sender of the packet to send security, compartmentation, handling restrictions, and TCC (closed user group) parameters. The flow of IP packet with IP options enabled may be controlled selectively by using access-list along with "option" parameter or by enabling global IOS configuration option: `ip options` *which enables the router to drop all packets with ip options (*`ip options drop`*) or processing them as though IP options are not enabled in the packet (*`ip option ignore`*).*

Configuration

Complete these steps:

Step 1 R1 configuration.

```
R1(config)#ip access-list extended IP_OPTIONS
R1(config-ext-nacl)#deny ip any any option lsr log
R1(config-ext-nacl)#deny ip any any option ssr log
R1(config-ext-nacl)#deny ip any any option security log
R1(config-ext-nacl)#permit ip any any

R1(config-ext-nacl)#int f0/0
R1(config-if)#ip access-group IP_OPTIONS in
```

The ACL that denies LSR, SSR and security option has been created and enabled on the R1's Fa0/0. When packet matches ACE pattern then log message is generated for first hit and subsequent hits in accordance with IOS options which define logging intervals, thresholds or rate limiting settings for access list logging.

Verification

```
R2#ping
Protocol [ip]:
Target IP address: 10.1.124.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: gigabitethernet0/0
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]: L
Source route: 10.1.124.4
Loose, Strict, Record, Timestamp, Verbose[LV]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.124.1, timeout is 2 seconds:
Packet sent with a source address of 10.1.124.2
Packet has IP options:  Total option bytes= 7, padded length=8
 Loose source route: <*>
   (10.1.124.4)

Request 0 timed out
```

```
Unreachable from 10.1.124.1.  Received packet has options
 Total option bytes= 7, padded length=8
 Loose source route: <*>
   (10.1.124.4)

Unreachable from 10.1.124.1.  Received packet has options
 Total option bytes= 7, padded length=8
 Loose source route: <*>
   (10.1.124.4)

Unreachable from 10.1.124.1.  Received packet has options
 Total option bytes= 7, padded length=8
 Loose source route: <*>
   (10.1.124.4)

Unreachable from 10.1.124.1.  Received packet has options
 Total option bytes= 7, padded length=8
 Loose source route: <*>
   (10.1.124.4)

Success rate is 0 percent (0/5)
```

R2 (source: 10.1.124.2) has pinged R1 (destination: 10.1.124.1) but ICMP packets have been directed through R4 (forwarder: 10.1.124.4) due to Loose Source Routing enabled. Note that R1 has replied with ICMP destination unreachable (ICMP type 3 - Destination Unreachable, ICMP code 13 - Communication Administratively Prohibited) because of "ip unreachables" enabled by default on the router interface. This configuration setting is responsible for sending ICMP 3/13 packets when inbound packet has been denied by the ACE.

```
R1#
%SEC-6-IPACCESSLOGDP: list IP_OPTIONS denied icmp 10.1.124.2 -> 10.1.124.1 (0/0), 1
packet
```

R1: The packet sent from R2 has been denied and log message has been generated due to log parameter enabled in ACE.

Task 2

On R2 configure an access list allows TCP packets only if the TCP flags ACK and SYN are set and the FIN flag is not set. Additionally, permit only IP packets with TTL between 254 and 255 and drop the rest with logging Layer 2 information.

Apart from well-known features the extended access control list enables to create an ACE which may define the following parameters:

- *IP options*
- *TCP flags*
- *Noncontiguous ports*
- *TTL value*

for permitting or denying the packets flowing through the router.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#ip access-list extended TCP_FLAGS
R2(config-ext-nacl)#permit tcp any any match-all +ack +syn -fin
R2(config-ext-nacl)#permit ip any any ttl range 254 255
R2(config-ext-nacl)#deny ip any any log-input

R2(config-ext-nacl)#int g0/0
R2(config-if)#ip access-group TCP_FLAGS in
```

The ACL that permits TCP packets with SYN/ACK flags enabled and FIN flag disabled and permits any ip packet with TTL value in the range from 254 to 255. "log-input" in deny ip any any ACE will add the name and the MAC address of the router interface.

Verification

```
R2#sh ip access-lists
Extended IP access list TCP_FLAGS
    10 permit tcp any any match-all +ack -fin +syn
    20 permit ip any any ttl range 254 255
    30 deny ip any any log-input


R2#tel 10.1.124.1
Trying 10.1.124.1 ... Open


User Access Verification

Password:
R1>exi
```

```
[Connection to 10.1.124.1 closed by foreign host]


R2#sh ip access-lists
Extended IP access list TCP_FLAGS
    10 permit tcp any any match-all +ack -fin +syn (1 match)
    20 permit ip any any ttl range 254 255 (40 matches)
    30 deny ip any any log-input
```

The TCP session from R2 to R1 has been established successfully. It has been possible by second ACE. Note that first ACE matches the second packet which has been exchanged during TCP handshake.

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip route 10.1.124.2 255.255.255.255 10.1.124.4
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

Adding the routing from R1 towards R2 through R4 will cause of decrease of TTL value below the value defined in second ACE of the access-list.

```
R1#
R1#ping 10.1.124.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.124.2, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)


R2#
%SEC-6-IPACCESSLOGDP: list TCP_FLAGS denied icmp 10.1.124.1 (GigabitEthernet0/0
0018.737a.a3e8) -> 10.1.124.2 (8/0), 1 packet
```

The ICMP packets have been blocked by the ACL. Note that "log-input" in last deny ip any any statement has added name and MAC address of the interface.

```
R2#sh ip access-lists
Extended IP access list TCP_FLAGS
    10 permit tcp any any match-all +ack -fin +syn (1 match)
    20 permit ip any any ttl range 254 255 (45 matches)
    30 deny ip any any log-input (5 matches)
```

Note that five ICMP packets have been blocked by the access-list

Task 3

Configure R4 so that it will drop all packets with any IP Option set. You are allowed to use only one command to accomplish this task.

Configuration

Complete these steps:

Step 1 R4 configuration.

```
R4(config)#ip options drop

% Warning: RSVP and other protocols that use IP Options packets may not
function as expected.
```

This command will result of dropping all the IP packets with IP options enabled. Remember that several protocols such as RSVP, MPLS TE will not work if this option is enabled on the router.

Verification

```
R2#ping 10.1.124.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.124.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Pinging the R4 Fa0/0 interface without IP options set is successful.

```
R2#ping
Protocol [ip]:
Target IP address: 10.1.124.4
Repeat count [5]: 1
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: gigabitethernet0/0
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]: ST
Source route: 10.1.124.4
Loose, Strict, Record, Timestamp, Verbose[SV]:
Sweep range of sizes [n]:
```

```
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 10.1.124.4, timeout is 2 seconds:
Packet sent with a source address of 10.1.124.2
Packet has IP options:  Total option bytes= 7, padded length=8
 Strict source route: <*>
   (10.1.124.4)

Request 0 timed out
Success rate is 0 percent (0/1)
```

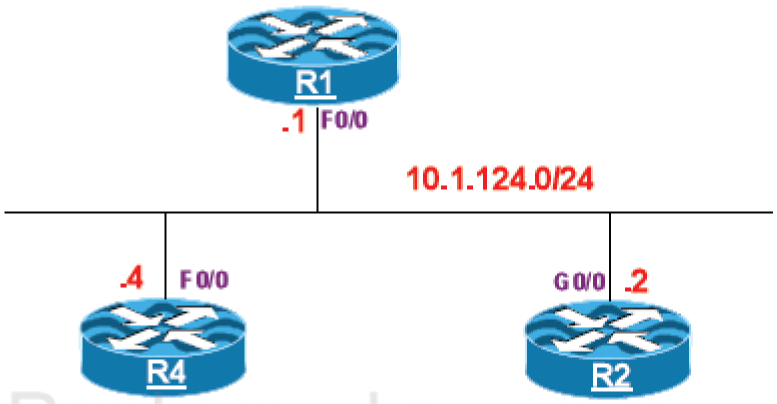
Pinging the R4 Fa0/0 interface with LSR is unsuccessful. "ip options drop" has blocked all ICMP packets with Strict Source Route option enabled.

Task 4

Erase the startup config and reload the routers before proceeding to the next lab.

LAB 3.55. Protecting against network mapping

Based on the previous Lab's IP addressing, topology and Lab setup



Task 1

Configure R4 not to leak any useful information via ICMP.

Configuration

Complete these steps:

Step 1 R4 configuration.

```
R4(config)#int f0/0
R4(config-if)# no ip unreachables
```

This option prevents the router from sending the ICMP Destination Unreachable packets in case of network error occurrence or when packet is blocked by the ACL. This command changes default router behavior (ip unreachables is enabled on all the interfaces by default).

Verification

```
R4#sh ip int f0/0
FastEthernet0/0 is up, line protocol is up
  Internet address is 10.1.124.4/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are never sent   Sending ICMP packets of code 3 is disabled on
Fa0/0
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP CEF switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is disabled
  Network address translation is disabled
  BGP Policy Mapping is disabled
  Input features: Virtual Fragment Reassembly, Virtual Fragment Reassembly After IPSec
Decryption, MCI Check
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled


R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip route 4.4.4.4 255.255.255.255 10.1.124.4

        The route to non-existing network through R4 has been set.

R1(config)#do ping 4.4.4.4
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

The ping is unsuccessful that is obvious but note that there is no "U" indicating that ICMP unreachable packet has been obtained as the reply.

Task 2

Configure R2 to enable ICMP rate limit so that the router can send 1 ICMP unreachable (code=1) packet per 5 seconds and only 1 ICMP unreachable (code=4) packet per 3 seconds.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#ip icmp rate-limit unreachable 5000
R2(config)#ip icmp rate-limit unreachable DF 3000
```

The icmp rate-limit has been changed. By default the router sends one ICMP unreachable packet per 500 milliseconds. Remember that the value set by this configuration command is expressed in milliseconds.

Verification

```
R1(config)#ip route 2.2.2.2 255.255.255.255 10.1.124.2
```

The route to non-existing network through R4 has been set.

```
R1#ping 2.2.2.2 rep 10

Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
.U...U...U
Success rate is 0 percent (0/10)
```

Note that unreachables appear but some of them have been suppressed.

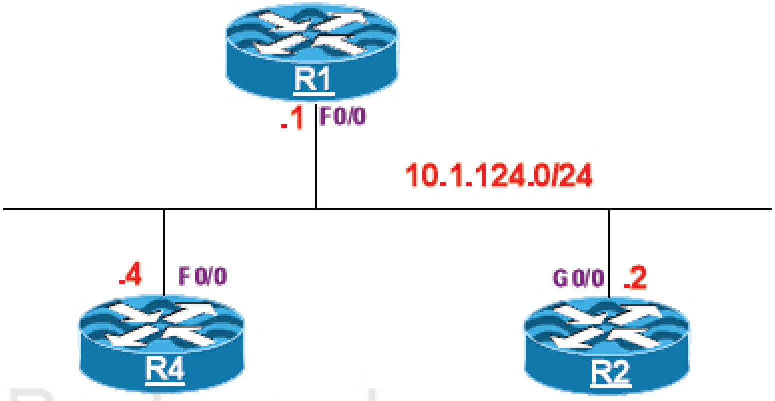
```
R2#sh ip icmp rate-limit g0/0
```

```
                           DF bit unreachables      All other unreachables
Interval (millisecond)     3000                     5000

Interface                  # DF bit unreachables    # All other unreachables
---------                  ---------------------    ------------------------
GigabitEthernet0/0         0                        2
```

This command shows setting and statistics relevant to ICMP unreachables rate limiting.

LAB 3.56. Protecting Against DoS Attacks using CAR

Based on the previous Lab's IP addressing, topology and Lab setup



Task 1

You have discovered that R1 is sending a lot of ICMP packets towards R4. That traffic causes performance degradation and high bandwidth utilization on the router. Use Committed Access Rate (CAR) feature to limit the traffic to 8 kbps coming into the f0/0 interface. Use 2 KB and 4 KB for normal and excess burst values.

Configuration

Complete these steps:

Step 1 R4 configuration.

```
R4(config)#access-list 130 permit icmp any any
R4(config)#int f0/0
R4(config-if)#rate-limit input access-group 130 8000 2000 4000 conform-action
transmit exceed-action drop
```

Verification

```
R1#p 10.1.124.4 rep 100 time 1

Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 10.1.124.4, timeout is 1 seconds:
.!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!.!!!!!!!!.!!!!!!!!!.!!!!!!!!!.!!!!!
!!!!.!!!!!!!!!.!!!!!!!!!.!!!!!
Success rate is 91 percent (91/100), round-trip min/avg/max = 1/1/4 ms
```

Note that some of the packets that have been sent toward R4, are blocked (drop action has been set for the traffic that has exceeded the normal limit) by CAR feature enabled on R4's Fa0/0.

```
R4#sh int f0/0 rate-limit
FastEthernet0/0
  Input
    matches: access-group 130
      params:  8000 bps, 2000 limit, 4000 extended limit
      conformed 91 packets, 10374 bytes; action: transmit
      exceeded 8 packets, 912 bytes; action: drop
      last packet: 14632ms ago, current burst: 2140 bytes
      last cleared 00:00:41 ago, conformed 2000 bps, exceeded 0 bps
```

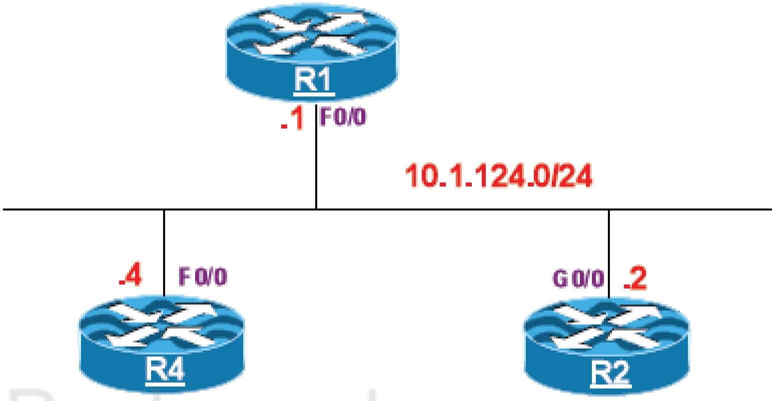
Note that 91 packets over limit of 8 kbps have been transmitted due to conform-action defined and 8 packets have been dropped due to exceed-action.

Task 2

Erase the startup config and reload the routers before proceeding to the next lab.

LAB 3.57. Preventing port redirection attacks

Based on the previous Lab's IP addressing, topology and Lab setup



Task 1

On R4's f0/0 interface disable the service that instructs an end node to use another and more efficient path to a particular destination.

Configuration

Complete these steps:

Step 1 R4 configuration.

```
R4(config)#int f0/0
R4(config)#no ip redirects
```

Verification

```
R1(config)#ip route 10.1.124.2 255.255.255.255 10.1.124.4

Before disabling ICMP Redirect:

R1#deb ip icmp
ICMP packet debugging is on
```

```
R1#ping 10.1.124.2 rep 2

Type escape sequence to abort.
Sending 2, 100-byte ICMP Echos to 10.1.124.2, timeout is 2 seconds:
.!
Success rate is 50 percent (1/2), round-trip min/avg/max = 1/1/1 ms
R1#
ICMP: redirect rcvd from 10.1.124.4- for 10.1.124.2 use gw 10.1.124.2
ICMP: echo reply rcvd, src 10.1.124.2, dst 10.1.124.1
```

Note that R4 has pointed R1 to R2 which is the best router for 10.1.124.2/32.

After disabling ICMP redirects:

```
R1#deb arp
ARP packet debugging is on

R1#cle ip redirect


R1#ping 10.1.124.2 rep 2

Type escape sequence to abort.
Sending 2, 100-byte ICMP Echos to 10.1.124.2, timeout is 2 seconds:

IP ARP: sent req src 10.1.124.1 000a.b819.c8a8,
                 dst 10.1.124.4 0000.0000.0000 FastEthernet0/0
IP ARP: rcvd rep src 10.1.124.4 0018.737a.a3e8, dst 10.1.124.1 FastEthernet0/0
.!
Success rate is 50 percent (1/2), round-trip min/avg/max = 1/1/1 ms
R1#
ICMP: echo reply rcvd, src 10.1.124.2, dst 10.1.124.1
```

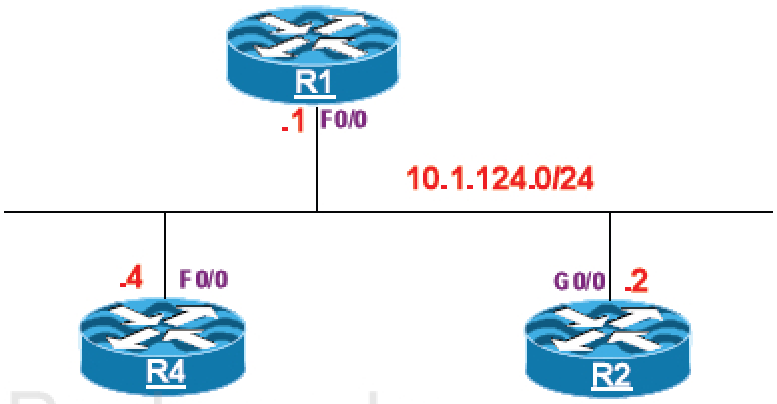
Note that R1 has requested the MAC address of 10.1.124.4 that has been required for sending the ICMP echo request to the next hop (R4). The ARP reply has been received thus R1 has sent ICMP packet towards R2 trough R4 as the next hop. The ICMP echo reply has been received.

Task 2

Erase the startup config and reload the routers before proceeding to the next lab.

LAB 3.58. Protecting against Smurf attacks

Based on the previous Lab's IP addressing, topology and Lab setup



Task 1

You are worried about Smurf attacks coming from the network. Configure R4 to block DoS Smurf attacks coming from Ethernet segment to its loopback0 interface (create a new Loopback interface with IP address of 4.4.4.4/24). You should use an access-list to accomplish this task.

☑ *Smurf attack occurs when a large number of ICMP packets are sent to a router's subnet broadcast address with a spoofed source IP address of a host within that subnet. Post IOS 12.0 the routers are default with the "no ip directed-broadcast" command which prevents this kind of attacks. But if the "ip directed-broadcast" is enabled for whatever reason, then, the access-list will block these types of attacks.*

Configuration

Complete these steps:

Step 1 R4 configuration.

```
R4(config)#int lo0
```

```
R4(config-if)#ip add 4.4.4.4 255.255.255.0

R4(config)#access-list 100 deny icmp any host 4.4.4.255 log
R4(config)#access-list 100 permit ip any any

R4(config)#int f0/0
R4(config-if)#ip directed-broadcast
R4(config-if)#ip access-group 100 in
```

Verification

```
R1(config)#ip route 4.4.4.0 255.255.255.0 10.1.124.4

R1#ping 4.4.4.255

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.255, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)

R4#
%SEC-6-IPACCESSLOGDP: list 100 denied icmp 10.1.124.1 -> 4.4.4.255 (0/0), 1 packet
```

The traffic sent towards broadcast of 4.4.4.0/24 has been blocked by the access-list.

```
R4#sh ip access-lists
Extended IP access list 100
    10 deny icmp any host 4.4.4.255 log (5 matches)
    20 permit ip any any
```

The ACE has matched the ICMP packets sent to broadcast address.

```
R4#sh ip int f0/0
FastEthernet0/0 is up, line protocol is up
  Internet address is 10.1.124.4/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is enabled
```

Directed broadcast has been enabled (the default setting has been changed)

```
  Outgoing access list is not set
  Inbound  access list is 100
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
```

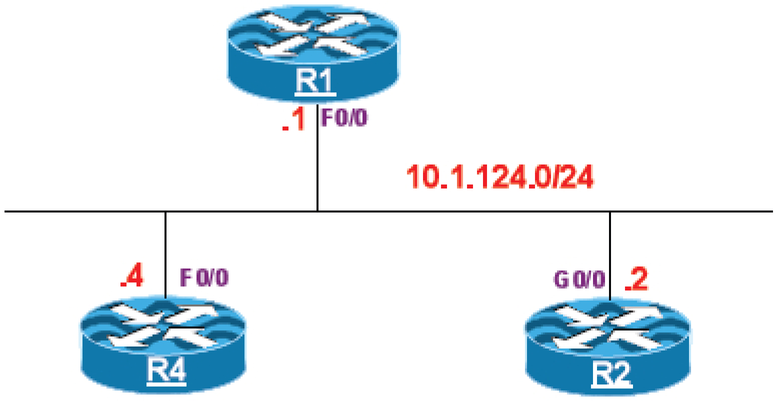
```
ICMP redirects are never sent
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP CEF switching is enabled
IP CEF switching turbo vector
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast, CEF
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Policy routing is disabled
Network address translation is disabled
BGP Policy Mapping is disabled
Input features: Access List, CAR, MCI Check
Post encapsulation features: CAR
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
```

Task 2

Erase the startup config and reload the routers before proceeding to the next lab.

LAB 3.59. Port Security

Based on the previous Lab's IP addressing, topology and Lab setup



Task 1

Configure SW1 ports so that only R2 and R4 can connect to ports F0/2 (or G0/2 depending on your rack topology) and F0/4 respectively. Configure their MAC addresses on those ports and ensure that ports will shut down and send SNMP Trap if some other device tries to communicate on that ports. You can configure static MAC addresses on R2 and R4.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#int g0/0
R2(config-if)# mac-address 0022.0022.0022
```

Step 2 R4 configuration.

```
R4(config)#int f0/0
R4(config-if)# mac-address 0044.0044.0044
```

The MAC addresses have been set on the R2's and R's interfaces.

Step 3 Switchport where R2 and R4 are connected to.

```
SW1(config)#interface GigabitEthernet0/2
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 124
SW1(config-if)#switchport port-security violation shutdown
SW1(config-if)#switchport port-security mac 0022.0022.0022
SW1(config-if)#switchport port-security

SW1(config-if)#interface FastEthernet0/4
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 124
SW1(config-if)#switchport port-security violation shutdown
SW1(config-if)#switchport port-security mac 0044.0044.0044
SW1(config-if)#switchport port-security
SW1(config-if)#exi
```

Port security has been enabled on switch ports. Remember that apart from shutdown action which result of sending the SNMP trap (if SNMP server is defined) and shut the switch port down, there are two remaining violation actions: protect (packets with unknown source MAC address will be dropped until a sufficient number of secure MAC addresses are removed to drop below the maximum value and the port will not be shut down. SNMP trap will not be sent and Security Violation Counter will not be incremented) and restrict (the same as protect violation action but in addition Security Violation Counter is incremented and SNMP Trap will be sent. The port will not be shut down). Remember that "shutdown" violation action will put switch port in err-disable state immediately when violation of port security rules occurs.

Verification

```
R2#ping 10.1.124.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.124.4, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

R2 is able to send the traffic and port security has not blocked R2.

```
R2#sh arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.124.2               -  0022.0022.0022  ARPA   GigabitEthernet0/0
Internet  10.1.124.4               0  0044.0044.0044  ARPA   GigabitEthernet0/0
```

```
SW1#sh mac address-table interface g0/2
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 124    0022.0022.0022    DYNAMIC     Gi0/2
Total Mac Addresses for this criterion: 1


SW1#sh mac address-table interface f0/4
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 124    0044.0044.0044    DYNAMIC     Fa0/4
Total Mac Addresses for this criterion: 1
```

ARP cache and MAC address table entries displayed. Note that R2's and R4's configured MAC addresses are visible.

```
SW1#sh port-security interface g0/2
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0022.0022.0022:124
Security Violation Count   : 0


SW1#sh port-security interface f0/4
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0044.0044.0044:124
```

```
Security Violation Count   : 0
```

Port security settings displayed. Note that Maximum MAC Addresses has value of 1 which is a default.

Task 2

Configure F0/1 and F0/4 as an access ports in VLAN 124 on SW1. Enable Port security for these ports such that only 1 MAC address can be connected to them. The switch should learn MAC addresses dynamically and store it as secure address in memory.

Configuration

Complete these steps:

Step 1 SW1 configuration.

```
SW1(config)#interface range f0/1 , f0/4
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switchport access vlan 124
SW1(config-if-range)#switchport port-security mac sticky
SW1(config-if-range)#switchport port-security
SW1(config-if-range)#exi
```

"switchport port-security mac sticky" enables the switch to learn secure MAC addresses until Maximum MAC addresses parameter is not exceeded. Learnt MAC addresses will be put into the running-config.

Verification

```
R1#pi 10.1.124.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.124.4, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/4 ms
```

Ping is successful – the traffic has not been blocked by the port-security feature.

```
R1#sh arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.124.1              -   000a.b819.c8a8  ARPA   FastEthernet0/0
Internet  10.1.124.4              0   0044.0044.0044  ARPA   FastEthernet0/0
```

MAC address of R1 has been dynamically learnt by the switch

```
SW1#sh port-security interface f0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 000a.b819.c8a8:124
Security Violation Count   : 0
```

Note that "Sticky MAC Addresses" counter has been incremented.

```
SW1#sh port-security interface f0/4
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0044.0044.0044:124
Security Violation Count   : 0
```

Test: Change MAC address on R4

```
R4(config)#int f0/0
R4(config-if)#no mac-address 0044.0044.0044
R4(config-if)#exi
```

```
R1#pi 10.1.124.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.124.4, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

```
SW1#
%PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/4, putting Fa0/4 in err-disable state
```

```
%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address
0018.737a.a3e8 on port FastEthernet0/4.
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to down
%LINK-3-UPDOWN: Interface FastEthernet0/4, changed state to down

       Note that SW1's Fa0/4 has been put into err-disable state due to configured
       shutdown violation action

SW1#sh port-security interface f0/4
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0018.737a.a3e8:124
Security Violation Count   : 1

       Note that "Port Status" is Secure-shutdown due to violation occurrence.
       Security Violation Count has been incremented.
```

Task 3

You use two computers in your office: desktop (MAC: 0055.0055.0055) and laptop (MAC: 0066.0066.0066). Both of them are connected to port F0/3 on SW1. Configure VLAN 20 on that port and enable Port Security so that only 2 MAC address can be connected on that port. Configure restriction so that if someone else tries to connect to the port SNMP Trap will be sent and port doesn't shut down.

Configuration

Complete these steps:

Step 1 SW1 configuration.

```
SW1(config)#interface FastEthernet0/3
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 20
% Access VLAN does not exist. Creating vlan 20
SW1(config-if)#switchport port-security maximum 2
SW1(config-if)#switchport port-security mac-address 0055.0055.0055
SW1(config-if)#switchport port-security mac-address 0066.0066.0066
SW1(config-if)#switchport port-security violation restrict
SW1(config-if)#switchport port-security
```

```
SW1(config-if)#exi
```

"port-security maximum" enables to add more than one secure MAC address.

Verification

```
SW1#sh port-security interface f0/3
Port Security              : Enabled
Port Status                : Secure-down
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 2
Configured MAC Addresses   : 2
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

```
SW1#sh port-security interface f0/3 address
          Secure Mac Address Table
-------------------------------------------------------------------------
Vlan    Mac Address       Type                       Ports   Remaining Age
                                                                (mins)
----    -----------       ----                       -----   -------------
  20    0055.0055.0055    SecureConfigured           Fa0/3         -
  20    0066.0066.0066    SecureConfigured           Fa0/3         -
-------------------------------------------------------------------------
Total Addresses: 2
```

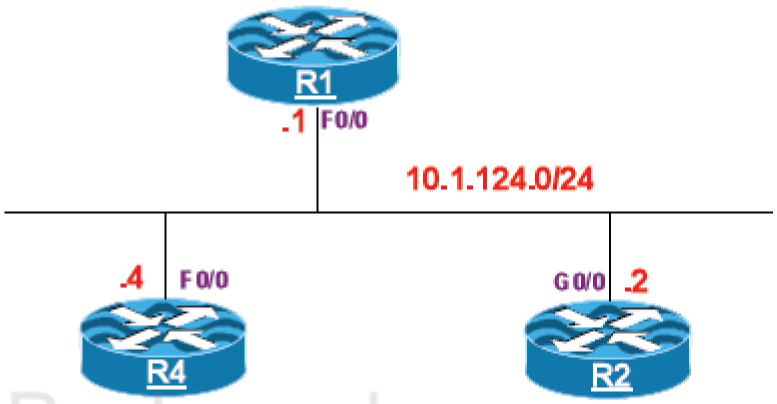
Both MAC addresses have been added.

Task 4

Erase the startup config and reload the routers before proceeding to the next lab.

LAB 3.60. Preventing VLAN Hoping Attacks

Based on the previous Lab's IP addressing, topology and Lab setup



Task 1

Configure F0/7 on SW1 in VLAN 40. Make sure devices connected to this port are prevented from conducting the VLAN Hoping attack.

Configuration

Complete these steps:

Step 1 SW1 configuration.

```
SW1(config)#vlan 40

SW1(config-vlan)#interface FastEthernet0/7
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 40
SW1(config-if)#switchport nonegotiate
SW1(config-if)#exi
```

"switchport nonegotiate" specifies that Dynamic Trunking Protocol (DTP) negotiation packets are not sent from switch interface. "switchport mode access" disables trunking on the interface and causes that only non-tagged frames will be sent and received. Static access port may be assigned only to one VLAN.

Verification

```
SW1#sh interf f0/7 switchport
Name: Fa0/7
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: Off
Access Mode VLAN: 40 (VLAN0040)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

Task 2

You plan to connect Cisco IP Phone to port f0/8 on SW1. Reconfigure it using the following information:

- Data VLAN 40
- Voice VLAN 44
- Encapsulation 802.1Q

Ensure that you prevent VLAN hoping attack on this port.

Configuration

Complete these steps:

Step 1 SW1 configuration.

```
SW1(config)#vlan 44

SW1(config-vlan)#interface FastEthernet0/8
SW1(config-if)#switchport trunk encapsulation dot1q
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport trunk native vlan 40
SW1(config-if)#switchport trunk allowed vlan 40,44
SW1(config-if)#switchport access vlan 40
SW1(config-if)#switchport voice vlan 44
SW1(config-if)#switchport nonegotiate
SW1(config-if)#exi
```

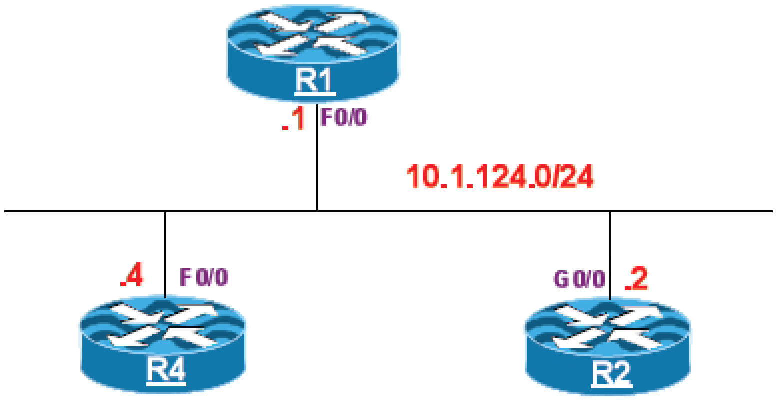
VLAN hopping on this interface is ensured by: disabled DTP negotiation, definition of allowed VLANs, definition of VLAN for the data and for the Voice traffic, definition of native VLAN for untagged frames, defining trunk encapsulation protocol.

Verification

```
SW1#sh interf f0/8 switchport
Name: Fa0/8
Switchport: Enabled
Administrative Mode: trunk                  (switchport mode trunk)
Operational Mode: down
Administrative Trunking Encapsulation: dot1q(switchport trunk encapsulation dot1q)
Negotiation of Trunking: Off                (switchport nonegotiate)
Access Mode VLAN: 40 (VLAN0040)             (switchport access vlan 40)
Trunking Native Mode VLAN: 40 (VLAN0040)    (switchport trunk native vlan 40)
Administrative Native VLAN tagging: enabled (switchport trunk native vlan 40)
Voice VLAN: 44 (VLAN0044)                   (switchport voice vlan 44)
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: 40,44               (switchport trunk allowed vlan 40,44)
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

LAB 3.61. VLAN access list

Based on the previous Lab's IP addressing, topology and Lab setup



Task 1

Configure the following policy for VLAN 124 on the switch:

- Hosts in VLAN 124 should not have access to a web server located at R4,
- There is a TELNET server running on R1. Only R4 should be able to access it,
- R2 is trying to attack VLAN 124. It uses MAC address of 0022.0022.0022 (configure it statically). Block this MAC address from accessing any device on VLAN 124,
- Block PPPoE packets (EtherType 0x8863 and 0x8864) coming into VLAN 124.

Do not apply any access lists on any of the routers' interfaces.

Configuration

Complete these steps:

Step 1 SW1 configuration.

```
SW1(config)#access-list 110 permit tcp any host 10.1.124.4 eq 80

SW1(config)#access-list 120 permit tcp host 10.1.124.2 host 10.1.124.1 eq 23

SW1(config)#mac access-list extended Block_R2_MAC
SW1(config-ext-macl)# permit host 0022.0022.0022 any
```

```
SW1(config-ext-macl)#mac access-list extended Block_PPPoE
SW1(config-ext-macl)# permit any any 0x8863 0
SW1(config-ext-macl)# permit any any 0x8864 0

SW1(config-ext-macl)#vlan access-map BLOCK 10
SW1(config-access-map)# action drop
SW1(config-access-map)# match ip address 110

SW1(config-access-map)#vlan access-map BLOCK 20
SW1(config-access-map)# action drop
SW1(config-access-map)# match ip address 120

SW1(config-access-map)#vlan access-map BLOCK 30
SW1(config-access-map)# action drop
SW1(config-access-map)# match mac address Block_R2_MAC

SW1(config-access-map)#vlan access-map BLOCK 40
SW1(config-access-map)# action drop
SW1(config-access-map)# match mac address Block_PPPoE

SW1(config-access-map)#vlan access-map BLOCK 100
SW1(config-access-map)# action forward
       The last sequence of VLAN access-map has action "forward" to permit
       other traffic that is not chosen by patterns configured in prior VLAN
       access-map sequences.


SW1(config-access-map)#vlan filter BLOCK vlan-list 124
```

Verification

```
SW1#sh vlan access-map
Vlan access-map "BLOCK"  10
  Match clauses:
    ip  address: 110
  Action:
    drop
Vlan access-map "BLOCK"  20
  Match clauses:
    ip  address: 120
  Action:
    drop
Vlan access-map "BLOCK"  30
  Match clauses:
    mac address: Block_R2_MAC
  Action:
    drop
```

```
Vlan access-map "BLOCK"  40
  Match clauses:
    mac address: Block_PPPoE
  Action:
    drop
Vlan access-map "BLOCK"  100
  Match clauses:
  Action:
    forward

R2(config)#int g0/0
R2(config-if)#mac-address 0022.0022.0022
R2(config-if)#exi

R4(config)#ip http server
```

Checklist:

1. Hosts in VLAN 124 should not have access to a web server located at R4,

```
R1#tel 10.1.124.4 80
Trying 10.1.124.4, 80 ...
% Connection timed out; remote host not responding

R2#tel 10.1.124.4 80
Trying 10.1.124.4, 80 ...
% Connection timed out; remote host not responding

R4#tel 10.1.124.4 80
Trying 10.1.124.4, 80 ... Open
GET \
HTTP/1.1 400 Bad Request
Date: Sun, 05 Sep 2010 11:50:08 GMT
Server: cisco-IOS
Accept-Ranges: none

400 Bad Request

[Connection to 10.1.124.4 closed by foreign host]
```

2. There is a TELNET server running on R1. Only R4 should be able to access it,

```
R2#tel 10.1.124.1
Trying 10.1.124.1 ...
% Connection timed out; remote host not responding

R4#tel 10.1.124.1
Trying 10.1.124.1 ... Open


User Access Verification
```

```
Password:
R1>exit

[Connection to 10.1.124.1 closed by foreign host]
```

3. R2 is trying to attack VLAN 124. It uses MAC address of 0022.0022.0022 (configure it statically). Block this MAC address from accessing any device on VLAN 124,

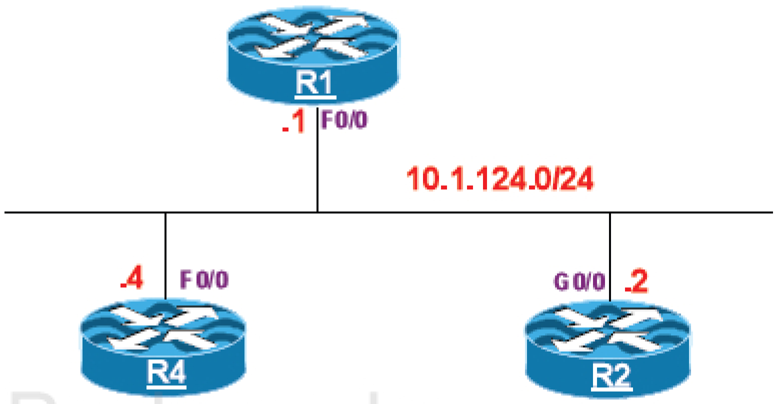
```
R2#ping 10.1.124.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.124.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)


R2#tel 10.1.124.4 80
Trying 10.1.124.4, 80 ...
% Connection timed out; remote host not responding


R2#ping 10.1.124.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.124.4, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Task 2

Erase the startup config and reload the routers before proceeding to the next lab.

LAB 3.62. DHCP Snooping and Dynamic ARP Inspection

Based on the previous Lab's IP addressing, topology and Lab setup



Task 1

Configure DHCP Snooping on SW1 to build MAC<->IP mapping database for ports in VLAN 124.

Configuration

Complete these steps:

Step 1 SW1 configuration.

```
SW1(config)#ip dhcp snooping
SW1(config)#ip dhcp snooping vlan 124
```

Remember that to enable the dhcp snooping in the given VLAN, the "ip dhcp snooping" global command must be issued before. Enabling the IP DHCP Snooping only in the VLAN will cause that DHCP snooping will not work.

Task 2

Reconfigure all routers (R1, R2, R4) to be DHCP clients in VLAN 124. Enable DHCP server on R5 with IP address of 10.1.124.5/24 and give out a pool of 10.1.124.0/24. Make sure switch does not insert Option 82 into DHCP requests. Configure VLAN 124 on port F0/5 and enable DHCP trusting. Control the number of DHCP packets on this port to 10 requests per second.

Configuration

Complete these steps:

Step 1 R5 configuration.

```
Router(config)#hostname R5
R5(config)#int f0/0
R5(config-if)#ip add 10.1.124.5 255.255.255.0
R5(config-if)#no shut
R5(config-if)#exit

R5(config)#ip dhcp pool VLAN-124
R5(dhcp-config)#network 10.1.124.0 /24
R5(dhcp-config)#exi
```

Step 2 R1 configuration.

```
R1(config)#int f0/0
R1(config-if)#ip address dhcp
R1(config-if)#exi
```

Step 3 R2 configuration.

```
R2(config)#int g0/0
R2(config-if)#ip address dhcp
R2(config-if)#exi
```

Step 4 R4 configuration.

```
R4(config)#int f0/0
R4(config-if)#ip address dhcp
R4(config-if)#exi
```

Step 5 SW1 configuration.

```
SW1(config)#no ip dhcp snooping information option
```

This command disables inserting Option 82 into DHCP requests.

```
SW1(config)#int f0/5
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 124
SW1(config-if)#ip dhcp snooping trust
SW1(config-if)#ip dhcp snooping limit rate 10
SW1(config-if)#exi
```

"ip dhcp snooping trust" causes that DHCP Server is able to work. DHCP offer will not be blocked by switch. Remember that this command must be enabled on trunk port if DHCP client and DHCP server are connected to different switches and ip dhcp snooping is enabled. "ip dhcp snooping limit rate 10" limits the number of DHCP messages that can be received per second.

Verification

```
R1#sh int f0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is MV96340 Ethernet, address is 000a.b86b.a3f0 (bia 000a.b86b.a3f0)
  Internet address is 10.1.124.2/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:21, output 00:00:02, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     241 packets input, 60000 bytes
     Received 107 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     639 packets output, 109725 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     14 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
```

```
      0 lost carrier, 0 no carrier
      0 output buffer failures, 0 output buffers swapped out
```

R2#sh int g0/0

```
GigabitEthernet0/0 is up, line protocol is up
  Hardware is BCM1125 Internal MAC, address is 0022.0022.0022 (bia 0017.9527.ba00)
  Internet address is 10.1.124.1/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s, link type is autonegotiation, media type is SX
  output flow-control is XON, input flow-control is XON
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:33, output 00:00:08, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     81 packets input, 38413 bytes, 0 no buffer
     Received 68 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 1390 multicast, 0 pause input
     0 input packets with dribble condition detected
     503 packets output, 88720 bytes, 0 underruns
     2 output errors, 0 collisions, 1 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     2 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

R4#sh int f0/0

```
FastEthernet0/0 is up, line protocol is up
  Hardware is MV96340 Ethernet, address is 000a.b819.c920 (bia 000a.b819.c920)
  Internet address is 10.1.124.3/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:39, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     168 packets input, 43948 bytes
     Received 69 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     596 packets output, 94886 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

```
R5#sh ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
10.1.124.1          0063.6973.636f.2d30.    Sep 09 2009 04:32 AM    Automatic
                    3032.322e.3030.3232.
                    2e30.3032.322d.4769.
                    302f.30
10.1.124.2          0063.6973.636f.2d30.    Sep 09 2009 04:33 AM    Automatic
                    3030.612e.6238.3662.
                    2e61.3366.302d.4661.
                    302f.30
10.1.124.3          0063.6973.636f.2d30.    Sep 09 2009 04:33 AM    Automatic
                    3030.612e.6238.3139.
                    2e63.3932.302d.4661.
                    302f.30
```

R1, R2 and R4 have got their IP addresses by DHCP from R5.

```
R5#sh ip dhcp server statistics
Memory usage         23706
Address pools        1
Database agents      0
Automatic bindings   3
Manual bindings      0
Expired bindings     0
Malformed messages   0
Secure arp entries   0

Message              Received
BOOTREQUEST          0
DHCPDISCOVER         3
DHCPREQUEST          3
DHCPDECLINE          0
```

```
DHCPRELEASE          0
DHCPINFORM           0

Message              Sent
BOOTREPLY            0
DHCPOFFER            3
DHCPACK              3
DHCPNAK              0

SW1#sh ip dhc snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
124
DHCP snooping is operational on following VLANs:
124
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is disabled                 (no ip dhcp snooping information
option)
   circuit-id format: vlan-mod-port
    remote-id format: MAC
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                    Trusted     Rate limit (pps)
------------------------     -------     ----------------
FastEthernet0/5              yes         10         (ip dhcp snooping limit rate 10)

SW1#sh ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  -----------------
---
00:22:00:22:00:22   10.1.124.1       85710       dhcp-snooping   124
GigabitEthernet0/2
00:0A:B8:6B:A3:F0   10.1.124.2       85716       dhcp-snooping   124   FastEthernet0/1
00:0A:B8:19:C9:20   10.1.124.3       85728       dhcp-snooping   124   FastEthernet0/4
Total number of bindings: 3

       DHCP snooping database has been displayed.
```

Task 3

Configure SW1 to dynamically verify MAC<->IP mappings against the DHCP Snooping database for VLAN 124. Unmatched packets should be dropped. Validate an IP address inside each ARP packet.

Configuration

Complete these steps:

Step 1 SW1 configuration.

```
SW1(config)#ip arp inspection vlan 124
SW1(config)#ip arp inspection validate ip
```

Remember that in DHCP-environment Dynamic ARP Inspection feature uses DHCP Snooping binding database for the list of the valid IP-to-MAC mapping, therefore ip dhcp snooping must be enabled prior DAI is enabled. In non-DHCP environment ARP ACL must be configured to provide DAI with valid IP-to-MAC mapping.

```
SW1(config)#int f0/5
SW1(config-if)#ip arp inspection trust
SW1(config-if)#exi
```

By default all the interfaces are untrusted so DAI is inspecting ARP packets on all interfaces. Making the interface trusted causes that DAI will not perform ARP inspection on that interface. Remember that configuring interfaces as untrusted when they should be trusted can result in a loss of connectivity. You should consider configuring interfaces as trusted especially on inter-switch links but remember that DAI is ingress feature only.

Verification

```
SW1#sh ip arp inspection interfaces

 Interface        Trust State     Rate (pps)    Burst Interval
 ---------------  -----------     ----------    --------------
 Fa0/1            Untrusted               15                 1
 Fa0/2            Untrusted               15                 1
 Fa0/3            Untrusted               15                 1
 Fa0/4            Untrusted               15                 1
 Fa0/5            Trusted               None               N/A
 Fa0/6            Untrusted               15                 1
 Fa0/7            Untrusted               15                 1
 Fa0/8            Untrusted               15                 1
 Fa0/9            Untrusted               15                 1
 Fa0/10           Untrusted               15                 1
 Fa0/11           Untrusted               15                 1
 Fa0/12           Untrusted               15                 1
 Fa0/13           Untrusted               15                 1
 Fa0/14           Untrusted               15                 1
 Fa0/15          Untrusted              15                 1
 Fa0/16          Untrusted              15                 1
 Fa0/17          Untrusted              15                 1
 Fa0/18          Untrusted              15                 1
 Fa0/19          Untrusted              15                 1
 Fa0/20          Untrusted              15                 1

 Interface        Trust State     Rate (pps)    Burst Interval
 ---------------  -----------     ----------    --------------
 Fa0/21          Untrusted              15                 1
 Fa0/22          Untrusted              15                 1
 Fa0/23          Untrusted              15                 1
 Fa0/24          Untrusted              15                 1
 Gi0/1           Untrusted              15                 1
 Gi0/2           Untrusted              15                 1
```

Note that default value of rate limit set on untrusted interfaces as 15 incoming ARP packet per second is visible

```
SW1#sh ip arp inspection vlan 124

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Enabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
  124     Enabled          Active

 Vlan     ACL Logging      DHCP Logging      Probe Logging
 ----     -----------      ------------      -------------
  124     Deny             Deny              Off
```

```
SW1#sh ip arp inspection stat

 Vlan      Forwarded        Dropped     DHCP Drops      ACL Drops
 ----      ---------        -------     ----------      ---------
  124              0              0              0              0

 Vlan   DHCP Permits    ACL Permits  Probe Permits   Source MAC Failures
 ----   ------------    -----------  -------------   -------------------
  124              0              0              0                     0

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------
  124                   0                        0                       0
```

Dynamic ARP Inspection settings and statistics displayed.

Test:

Note that R2 has MAC address of 0022.0022.0022. Change it to something else and try to ping R2 from any other router.

```
F t
R2(config)#int g0/0
R2(config-if)#no mac-address

R4#ping 10.1.124.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.124.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW1#
*Mar  1 04:57:37.735: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Gi0/2, vlan
124.([0017.9527.ba00/10.1.124.1/000a.b819.c920/10.1.124.3/04:57:37 UTC Mon Mar 1 1993])
*Mar  1 04:57:39.748: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Gi0/2, vlan
124.([0017.9527.ba00/10.1.124.1/000a.b819.c920/10.1.124.3/04:57:39 UTC Mon Mar 1 1993])
*Mar  1 04:57:41.761: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Gi0/2, vlan
124.([0017.9527.ba00/10.1.124.1/000a.b819.c920/10.1.124.3/04:57:41 UTC Mon Mar 1 1993])
*Mar  1 04:57:43.775: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Gi0/2, vlan
124.([0017.9527.ba00/10.1.124.1/000a.b819.c920/10.1.124.3/04:57:43 UTC Mon Mar 1 1993])
*Mar  1 04:57:45.788: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Gi0/2, vlan
124.([0017.9527.ba00/10.1.124.1/000a.b819.c920/10.1.124.3/04:57:45 UTC Mon Mar 1 1993])
```

Ping has been unsuccessful and log message has been generated informing that invalid ARP request (IP address resolution) has been denied.

Task 4

Configure static MAC address on R4 to 0044.0044.0044 and IP address of 10.1.124.44/24. Configure static ARP access list for this host's IP/MAC address pair. This ARP ACL should be applied to VLAN 124. Log any matches for the ACL within VLAN 124 and validate an IP address inside ARP packets.

Configuration

Complete these steps:

Step 1 R4 configuration.

```
R4(config)#int f0/0
R4(config-if)#mac-address 0044.0044.0044
R4(config-if)#ip add 10.1.124.44 255.255.255.0
R4(config-if)#exi
```

Step 2 SW1 configuration.

```
SW1(config)#ip arp inspection vlan 124 logging acl-match matchlog
SW1(config)#ip arp inspection validate ip


SW1(config)#arp access-list ARP124
SW1(config-arp-nacl)# permit ip host 10.1.124.44 mac host 0044.0044.0044 log

SW1(config-arp-nacl)#ip arp inspection filter ARP124 vlan 124
```

ARP access-list creates static IP-to-MAC mapping for DAI.

Verification

```
SW1#sh ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  -----------------
---
00:22:00:22:00:22      10.1.124.1             83883            dhcp-snooping      124
GigabitEthernet0/2
00:0A:B8:6B:A3:F0   10.1.124.2       83888       dhcp-snooping   124   FastEthernet0/1
00:0A:B8:19:C9:20   10.1.124.3       83900       dhcp-snooping   124   FastEthernet0/4
Total number of bindings: 3
```

```
SW1#cle ip dhcp snooping binding interface f0/4
```

All entries of Fa0/4 interface, that have been learnt dynamically, have been cleared.

```
SW1#sh ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  -----------------
---
00:22:00:22:00:22      10.1.124.1             83858            dhcp-snooping      124
GigabitEthernet0/2
00:0A:B8:6B:A3:F0   10.1.124.2       83863       dhcp-snooping   124   FastEthernet0/1
Total number of bindings: 2
```

Note that there is no DHCP Snooping binding for R4.

```
SW1#ip dhcp snooping binding 0044.0044.0044 vlan 124 10.1.124.44 interface f0/4 expiry
86400
```

Static binding has been created

```
SW1#sh ip dhcp snooping binding
```

```
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  -----------------
---
00:22:00:22:00:22      10.1.124.1           83534           dhcp-snooping      124
GigabitEthernet0/2
00:44:00:44:00:44   10.1.124.44      86372       dhcp-snooping   124   FastEthernet0/4
00:0A:B8:6B:A3:F0   10.1.124.2       83539       dhcp-snooping   124   FastEthernet0/1
Total number of bindings: 3


R1#pi 10.1.124.44

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.124.44, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/4 ms

SW1#
*Mar    1   05:23:37.605:   %SW_DAI-6-ACL_PERMIT:   1   ARPs   (Res)   on   Fa0/4,   vlan
124.([0044.0044.0044/10.1.124.44/000a.b86b.a3f0/10.1.124.2/05:23:36   UTC   Mon   Mar   1
1993])
```

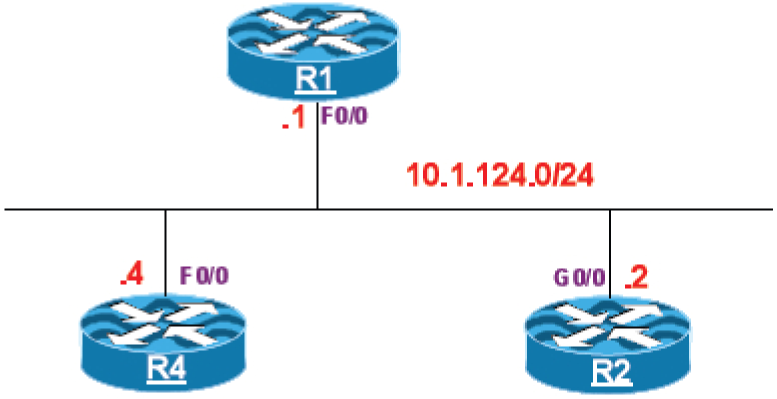
Note that ping is successful. DAI has permitted the ARP request (address resolution) and this activity has been logged due to enabling the logging of every ARP ACL match.

Task 5

Erase the startup config and reload the routers before proceeding to the next lab.

LAB 3.63. IP Source Guard

Based on the previous Lab's IP addressing, topology and Lab setup



Task 1

Configure static IP <-> MAC <-> Port <-> VLAN binding for R2's IP (10.1.124.2/24) and MAC (0022.0022.0022) addresses on SW1. Enable IP source guard on port F0/2. Configure protection against MAC address spoofing along with IP source guard.

☑ *IP Source Guard is a feature which enables to prevent IP spoofing attacks in LAN. IP Source Guard feature relies on DHCP Snooping binding database or static IP-to-MAC-to-Port-and-to-VLAN mapping. When IP Source Guard is enabled on switch port then all traffic except DHPC requests is blocked until valid mapping is entered dynamically into DHCP Snooping binding database or ip source binding is configured statically. Afterwards per-port and VLAN Access Control List (PVACL) is put on the port which permits legitimate traffic only (with valid IP source). Remember that if IP source guard is enabled in IP and MAC filtering mode, the DHCP snooping option 82 must be enabled to ensure that the DHCP protocol works properly.*

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#int g0/0
R2(config-if)#mac-address 0022.0022.0022
R2(config-if)#exi
```

Step 2 SW1 configuration.

```
SW1(config)#ip dhcp snooping
SW1(config)#ip dhcp snooping vlan 124
SW1(config)#ip source binding 0022.0022.0022 vlan 124 10.1.124.2 interface
g0/2
```

Static binding has been created because R2 IP address is static.

```
SW1(config)#int f0/2
SW1(config-if)#ip verify source port-security
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 124
SW1(config-if)#switchport port-security
SW1(config-if)#exi
```

Verification

```
SW1#sh ip source binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  -----------------
---
00:22:00:22:00:22   10.1.124.2       infinite    static          124
GigabitEthernet0/2
Total number of bindings: 1
```

Note that the entry is type of "static".

```
SW1#sh ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
124
DHCP snooping is operational on following VLANs:
124
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
   circuit-id format: vlan-mod-port
```

```
    remote-id format: MAC
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                    Trusted     Rate limit (pps)
------------------------     -------     ----------------
```

DHCP Snooping settings has been displayed. DHCP Snooping has been enabled for vlan 124.

```
SW1# show ip verify source interface g0/2
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----------
Gi0/2      ip-mac       active       10.1.124.2       00:22:00:22:00:22  124
```

IP Source Guard is securing R2 IP address on port Gi0/2

```
R1#pi 10.1.124.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.124.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/4 ms
```

Note that ping is successful because PVACL conditions are met basing on mapping that created.

```
R2(config)#int g0/0
R2(config-if)#no mac-address


R1#pi 10.1.124.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.124.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

When MAC address has been reverted to real value the traffic has been blocked by IP Source Guard feature.

```
R2(config)#int g0/0
R2(config-if)#mac-address 0022.0022.0022


R1#pi 10.1.124.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.124.2, timeout is 2 seconds:
```

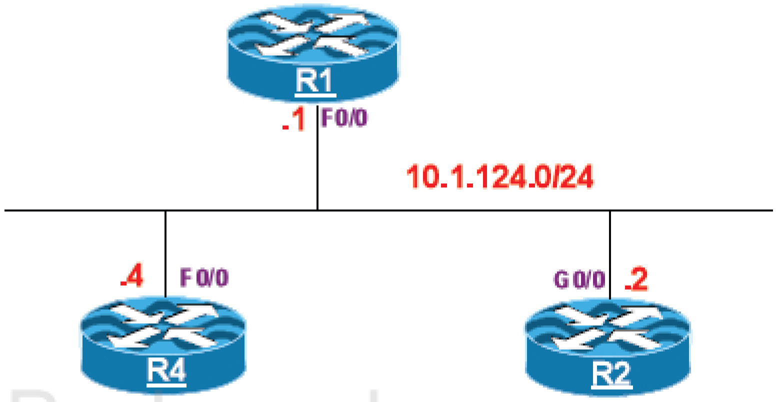
```
...!!
Success rate is 40 percent (2/5), round-trip min/avg/max = 1/1/1 ms

       Ping is successful when MAC address has been reverted to the value configured
       in static mapping

R2(config)#int g0/0
R2(config-if)#ip add 10.1.124.22 255.255.255.0


R1#pi 10.1.124.22

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.124.22, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

       Changing IP address causes that PVACL has blocked the traffic (conditions are
       not met)
```

Task 2

Erase the startup config and reload the routers before proceeding to the next lab.

LAB 3.64. Protecting Against Broadcast Storms

Based on the previous Lab's IP addressing, topology and Lab setup



Task 1

Ensure SW1 so that no more than 10% of broadcast traffic could be accepted from the R1 and R2 no more than 1Mbps of broadcast could be accepted from R2. Also, limit unicast packets to no more that 1M packets per second on the switch port where R4 is connected to.

Storm control prevents traffic on a LAN from being disrupted by a broadcast, a multicast, or a unicast storm on the interface. Storm control feature measures the traffic in one-second intervals and blocks the traffic if one of the following parameters is exceeded:

- *configured percentage of bandwidth available on the interface that can be utilized before storm-control will suppress excessive broadcast, multicast or unicast traffic,*
- *configured rate of packets per seconds that can be transmitted through the interface before storm-control will suppress excessive broadcast, multicast or unicast traffic.*

Configuration

Complete these steps:

Step 1 SW1 configuration.

```
SW1(config)#int f0/1
SW1(config-if)#storm-control broadcast level 10.00
SW1(config-if)#exi

SW1(config)#int g0/2
SW1(config-if)#storm-control broadcast level bps 1m
SW1(config-if)#exi

SW1(config)#int f0/4
SW1(config-if)#storm-control unicast level pps 1m
SW1(config-if)#exi
```

Verification

```
SW1#sh storm-control broadcast
Interface  Filter State   Upper        Lower        Current
---------  -------------  -----------  -----------  ----------
Fa0/1      Forwarding       10.00%       10.00%        0.00%
Gi0/2      Forwarding          1m bps       1m bps        0 bps
```

```
SW1#sh storm-control unicast
Interface  Filter State   Upper        Lower        Current
---------  -------------  -----------  -----------  ----------
Fa0/4      Forwarding          1m pps       1m pps        0 pps
```

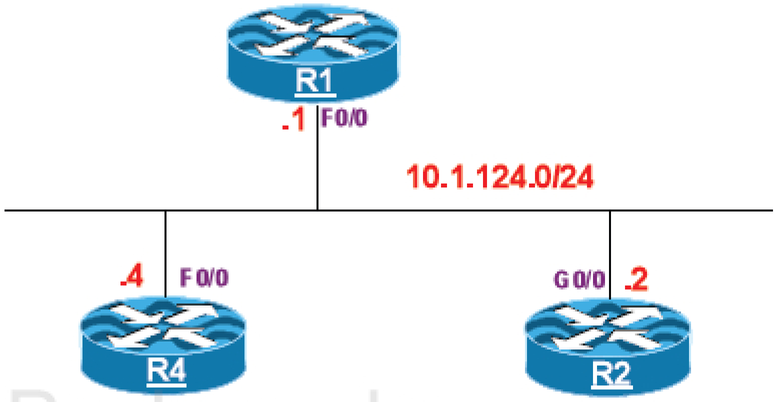
Storm control settings have been displayed for broadcast and unicast separately.

Task 2

Erase the startup config and reload the routers before proceeding to the next lab.

LAB 3.65. Protecting Spanning-Tree Protocol

Based on the previous Lab's IP addressing, topology and Lab setup



Task 1

Configure SW1 to be the STP Root for VLAN 124 and make sure that nobody else can claim itself as root.

Also, ensure that SW1 does not send or receive any BPDUs to/from R1 and put interface in err-disable state when receive BPDU from R4. Configure SW1 to automatically clear error-disabled ports (triggered by the BPDU Guard) after 2 minutes.

Configuration

Complete these steps:

Step 1 SW1 configuration.

```
SW1(config)#int ran f0/19 - 24
SW1(config-if-range)#sw trunk encap dot1
SW1(config-if-range)#sw mo trunk
SW1(config-if-range)#exi

SW1(config)#spanning-tree vlan 124 root primary

SW1(config)#int range f0/19 - 24
```

```
SW1(config-if-range)# spanning-tree guard root
%SPANTREE-2-ROOTGUARD_CONFIG_CHANGE: Root guard enabled on port
FastEthernet0/19.
%SPANTREE-2-ROOTGUARD_CONFIG_CHANGE: Root guard enabled on port
FastEthernet0/20.
%SPANTREE-2-ROOTGUARD_CONFIG_CHANGE: Root guard enabled on port
FastEthernet0/21.
%SPANTREE-2-ROOTGUARD_CONFIG_CHANGE: Root guard enabled on port
FastEthernet0/22.
%SPANTREE-2-ROOTGUARD_CONFIG_CHANGE: Root guard enabled on port
FastEthernet0/23.
%SPANTREE-2-ROOTGUARD_CONFIG_CHANGE: Root guard enabled on port
FastEthernet0/24.
%SPANTREE-2-ROOTGUARD_BLOCK: Root guard blocking port FastEthernet0/21 on
VLAN0001.
%SPANTREE-2-ROOTGUARD_BLOCK: Root guard blocking port FastEthernet0/19 on
VLAN0001.

SW1(config-if-range)#int f0/1
% Command exited out of interface range and its sub-modes.
  Not executing the command for second and later interfaces
SW1(config-if)#spanning-tree bpdufilter enable

SW1(config-if)#int f0/4
SW1(config-if)#spanning-tree bpduguard enable
SW1(config-if)#exi

SW1(config)#errdisable recovery cause bpduguard
SW1(config)#errdisable recovery interval 120
```

Verification

```
SW1#sh interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/19      on               802.1q         trunking      1
Fa0/20      on               802.1q         trunking      1
Fa0/21      on               802.1q         trunking      1
Fa0/22      on               802.1q         trunking      1
Fa0/23      on               802.1q         trunking      1
Fa0/24      on               802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/19      1-4094
Fa0/20      1-4094
Fa0/21      1-4094
Fa0/22      1-4094
```

```
Fa0/23      1-4094
Fa0/24      1-4094

Port        Vlans allowed and active in management domain
Fa0/19      1,124
Fa0/20      1,124
Fa0/21      1,124
Fa0/22      1,124
Fa0/23      1,124

Port        Vlans allowed and active in management domain
Fa0/24      1,124

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/19      none
Fa0/20      none
Fa0/21      none
Fa0/22      none
Fa0/23      none
Fa0/24      none

SW1#sh spanning-tree vlan 124

VLAN0124
  Spanning tree enabled protocol ieee
  Root ID    Priority    24700
             Address     0019.060c.7600
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24700  (priority 24576 sys-id-ext 124)
             Address     0019.060c.7600
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 15

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/2               Desg FWD 4         128.2    P2p
Fa0/1               Desg FWD 100       128.3    P2p
Fa0/4               Desg FWD 19        128.6    P2p
Fa0/19              Desg FWD 19        128.21   P2p
Fa0/20              Desg FWD 19        128.22   P2p
Fa0/21              Desg FWD 19        128.23   P2p
Fa0/22              Desg FWD 19        128.24   P2p
Fa0/23              Desg FWD 19        128.25   P2p
Fa0/24              Desg FWD 19        128.26   P2p
```

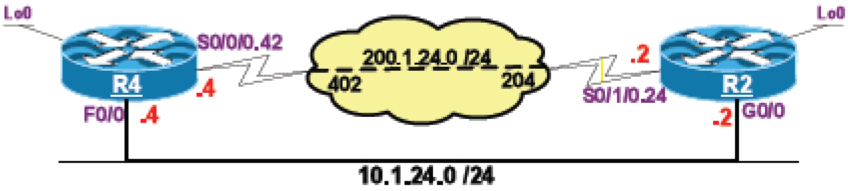
Note both Root MAC address and Bridge MAC address are the same. This means this switch is a root bridge for VLAN 124.

Also note that all trunks are in forwarding state. This is because all paths to the route bridge must be enabled.

Task 2

Erase the startup config and reload the routers before proceeding to the next lab.

LAB 3.66. Preventing IP spoofing



Lab Setup

- Configure the F0/0 interface of R4 and G0/0 interface of R2 in VLAN 24
- The Frame-relay interface of these routers should be configured in a point-to-point manner.

Task 1

Configure the routers such that R2 uses its G0/0 interface to reaches network 1.0.0.0 /8, whereas, R4 uses the frame-relay cloud to reach network 2.0.0.0 /8, .

Configuration

Complete these steps:

Step 1 R4 configuration.

```
R4(config)#ip route 2.0.0.0 255.0.0.0 s0/0/0.42
```

Step 2 R2 configuration.

```
R2(config)#ip route 4.0.0.0 255.0.0.0 g0/0
```

Verification

```
R4#show ip route static
S    2.0.0.0/8 is directly connected, Serial0/0/0.42

R2#show ip route static
S    4.0.0.0/8 is directly connected, GigabitEthernet0/0
```

Task 2

Configure uRPF on R2's Frame-relay interface

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#int S0/1/0.24
R2(config-subif)# ip verify unicast source reachable-via rx
```

Note that there is also an old format command which basically do the same "ip verify unicast reverse-path". However, Cisco recommends using a new command when configuring uRPF.

Verification

```
R2#show ip inter s0/1/0.24 | b IP verify
  IP verify source reachable-via RX
   0 verification drops
   0 suppressed verification drops
   0 verification drop-rate
```

Note with URPF enabled, the local router (R2) will compare the source IP address of all packets received to its routing table. This is done to ensure that they arrive on the best path interface, meaning that the closest interface back to the source. If the check fails, the packets are dropped, if the check passes, the packets are processed.

```
R4#ping 2.2.2.2 source lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 4.4.4.4
.....
Success rate is 0 percent (0/5)
```

```
R2#show ip inter s0/1/0.24 | b IP verify
  IP verify source reachable-via RX
   5 verification drops
   0 suppressed verification drops
   0 verification drop-rate
```

Note the ping failed because the source IP address of the ICMP Echo message is 4.4.4.4 and from R2's perspective these packets should have arrived through its G0/0 interface and NOT the Frame-relay interface.

To test the configuration further:

```
R2(config)#access-list 100 permit ip any any log-input

R2(config)#int g0/0
R2(config-if)#ip access-group 100 in

R2(config-if)#int s0/1/0.24
R2(config-subif)#ip access-group 100 in
```

In order to show the source/destination IP addresses and the interfaces, the above access-list is configured with "log-input" and applied to both S0/1/0.24 and G0/0.

```
R4#ping 2.2.2.2 source lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 4.4.4.4
.....
Success rate is 0 percent (0/5)
```

You should see the following message on R2's console:

```
%SEC-6-IPACCESSLOGDP: list 100 permitted icmp 4.4.4.4 (Serial0/1/0.24 ) -> 2.2.2.2
(0/0), 1 packet
```

Note the output of the following command shows that R2 expects the traffic from 4.4.4.4 to come through its G0/0 and NOT S0/1/0.24 interface; therefore, it drops the packets.

```
R2#sho ip route static
S    1.0.0.0/8 is directly connected, GigabitEthernet0/0
```

Task 3

Configure R2 such that it allows ingress traffic from network 1.0.0.0 /8 through any interface. DO NOT modify the routing table or remove the "ip verify unicast source reachable-via rx" command to accomplish this task.

Configuration

Complete these steps:

Step 1 R2 configuration.

Note to accomplish this task, an access-list is configured to permit all traffic from network 1.0.0.0 /8 and tied to the "ip verify unicast source reachable-via rx" command. The condition of the access-list is checked ONLY when the condition of URPF fails, IF THE CONDITION OF URPF IS SUCCESSFUL, THE ACCESS-LIST IS NOT CHECKED.

```
R2(config)#int s0/1/0.24
R2(config-subif)# ip verify unicast source reachable-via rx 104

R2(config)#access-list 104 permit ip 4.0.0.0 0.255.255.255 any
```

Verification

```
R2#sh ip int s0/1/0.24 | be IP verify
  IP verify source reachable-via RX, ACL 104
   10 verification drops
   0 suppressed verification drops
   0 verification drop-rate

R4#ping 2.2.2.2 source lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 4.4.4.4
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Note you should see the following message on R2's console:

```
%SEC-6-IPACCESSLOGDP: list 100 permitted icmp 4.4.4.4 (Serial0/1/0.24 ) -> 2.2.2.2
(0/0), 5 packets

R2#sh ip int s0/1/0.24 | be IP verify
  IP verify source reachable-via RX, ACL 104
   10 verification drops
   5 suppressed verification drops
   0 verification drop-rate
```

Task 4

Re-configure R2 based on the previous conditions such that ONLY ICMP packets are allowed through any interface, all other traffic from this network MUST come through G0/0 interface, if they don't, they should be dropped.

Configuration

Complete these steps:

Step 1 R2 configuration.

```
R2(config)#NO access-list 104

R2(config)#access-list 104 permit icmp 4.0.0.0 0.255.255.255 any
```

Verification

```
R4#ping 2.2.2.2 source lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 4.4.4.4
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

       Note the ICMP traffic works fine, whereas, the following TCP traffic failed.

R4#tel 2.2.2.2 /so lo0
Trying 2.2.2.2 ...
% Connection timed out; remote host not responding

R2#
%SEC-6-IPACCESSLOGP: list 100 permitted tcp 4.4.4.4(0) (Serial0/1/0.24 ) -> 2.2.2.2(0),
1 packet

R2#sh ip int S0/1/0.24 | be IP verify
  IP verify source reachable-via RX, ACL 104
   19 verification drops
   10 suppressed verification drops
   0 verification drop-rate
```