



Networkforyou

Subscribe to our
You Tube Channel



Networkforyou



**Welcome
To
Network for you
AAA**





Authentication
Who are you?

Authorization
How much can you spend?

Accounting
What did you spend it on?

Reference Number	Sold	Posted	Activity Since Last Statement	Amount
43210987	01-03	01-13	Payment, Thank You	-\$74.25
01234567	01-12	01-13	Wings 'N' Things Anytown, USA	\$25.25
78901234	01-14	01-17	Record Release Anytown, USA	\$40.00
45678901	01-14	01-17	Sports Stadium Anytown, USA	\$75.25
3210987	01-22	01-23	Tie Tack Anytown, USA	\$20.75
76543210	01-29	01-30	Electronic World Anytown, USA	\$89.25
2345678		01-30	Transaction Fees	\$3.00
34567890		01-01	Annual Fee	\$25.00

AAA (Authentication, Authorization and Accounting):

- Authentication: Verify the identity of the user, who are you.
- Authorization: What is the user allowed to do? Example what resource he can access etc? (How much you can spend)
- Accounting: It is like all record what is done by that user it will keep all record. Example used for billing and auditing (What did you spend it on record)

Email us:
networkforyou4@gmail.com

WhatsApp Us : **+918143809578**



AAA Stand for Authentication, Authorization and Accounting:

- It is a Centralized Management of users to access the network devices
- AAA Server allow setting up access control on Cisco Routers and Switches
- Like if we have 300 Switches and 10 Router in our organization then it will be very difficult to create all user in that all devices and delete when they leave organization etc. And it will take lot of memory of devise also to overcome with this type of issues we use AAA Server.
- AAA Server also control connections passing through router or switch for access network.
- When every user tries to connect to router or switch these network devices verifies by AAA Server (AAA Database)
- User Management is done with AAA Server without need to reconfigure to individual router or switch
- Like any new user came we need to configure only in AAA Server no need to add that user in Router or switch.
- AAA Server use two Main type of Protocol to configure this
- Radius Protocol (Remote Authentication Dial-in User Service)
- TACACS+ (Terminal Access Controller Access-Control System Plus)

Radius Protocol:

- It is open standard where as TACACS is Cisco Proprietary protocol.
- It uses UDP and users ports numbers 1812/1645 and 1813/1646.
- It Encrypts passwords only.
- It is light weight protocol (Consume less resources).

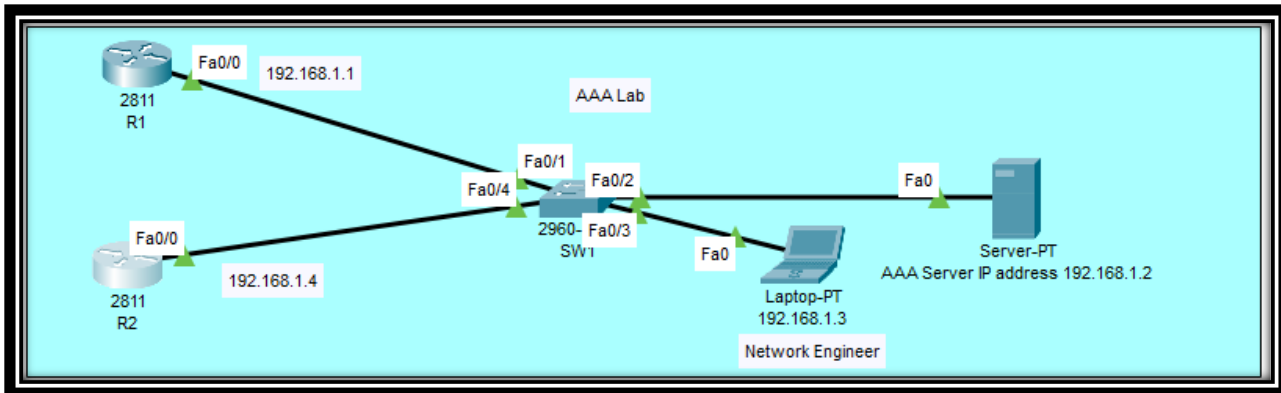
TACACS+:

- It is CISCO Proprietary protocol.
- It use TCP and port number user 49.
- It encrypts entire communication.
- It is heavy weight protocol consuming more resources.

Email us:
networkforyou4@gmail.com

3 of 7

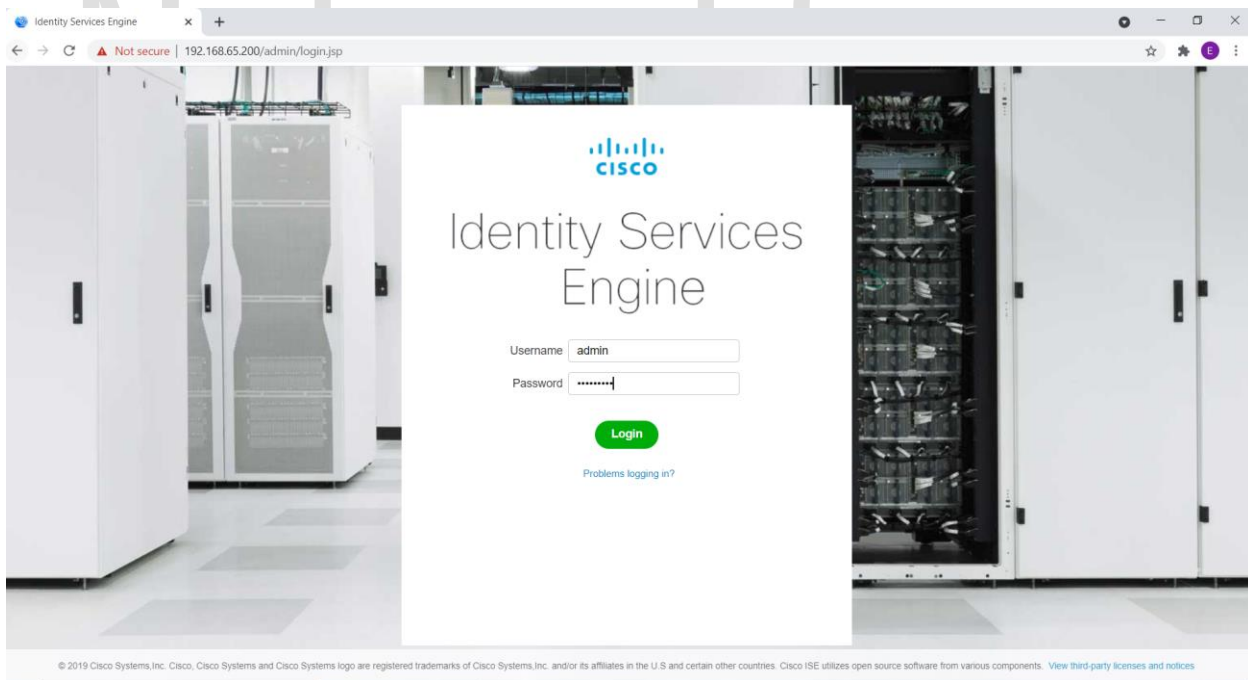
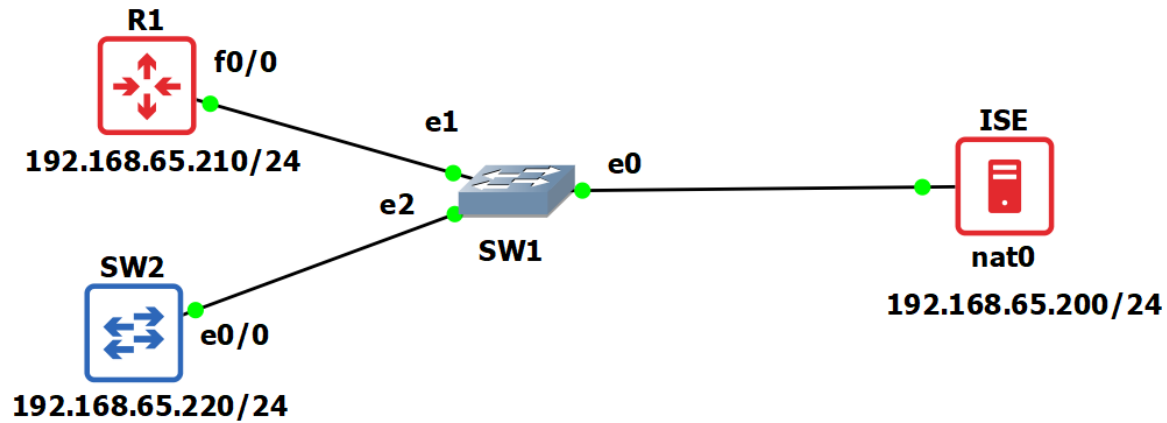
WhatsApp Us : +918143809578



R1 Configuration	R2 Configuration
<pre>en config t hostname R1 int f0/0 ip add 192.168.1.1 255.255.255.0 no sh aaa new-model Tacacs-server host 192.168.1.2 key abc123 aaa authentication login AAA group tacacs+ Line vty 0 1 login authentication AAA</pre>	<pre>en config t hostname R2 int f0/0 ip add 192.168.1.4 255.255.255.0 no sh aaa new-model radius-server host 192.168.1.2 key abc123 aaa authentication login AAA group radius Line vty 0 1 login authentication AAA</pre>

AAA with ISE Lab:

<p>Email us: networkforyou4@gmail.com</p>	<p>4 of 7</p>	<p>WhatsApp Us : +918143809578</p>
---	---------------	---



Email us:
networkforYou4@gmail.com

5 of 7

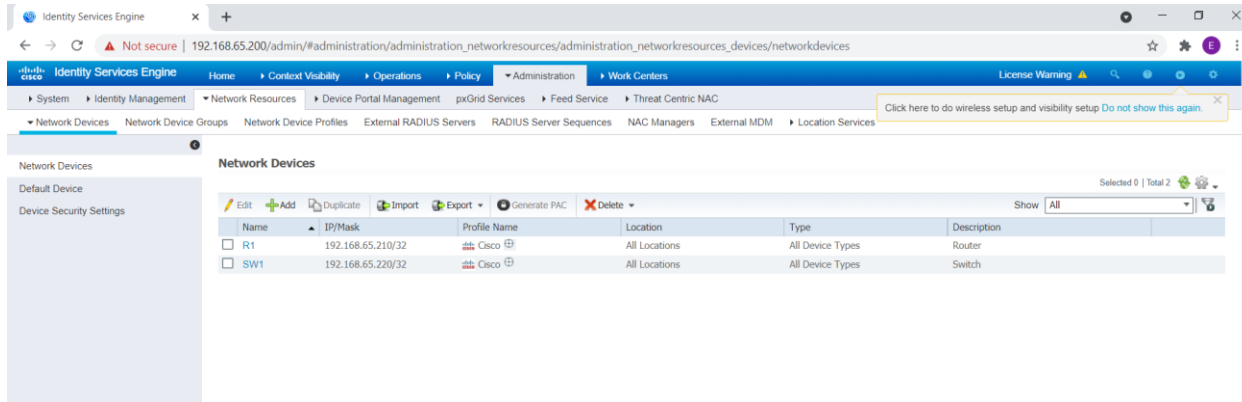
WhatsApp Us : **+918143809578**



NetworkforYou

Subscribe to our
YouTube Channel

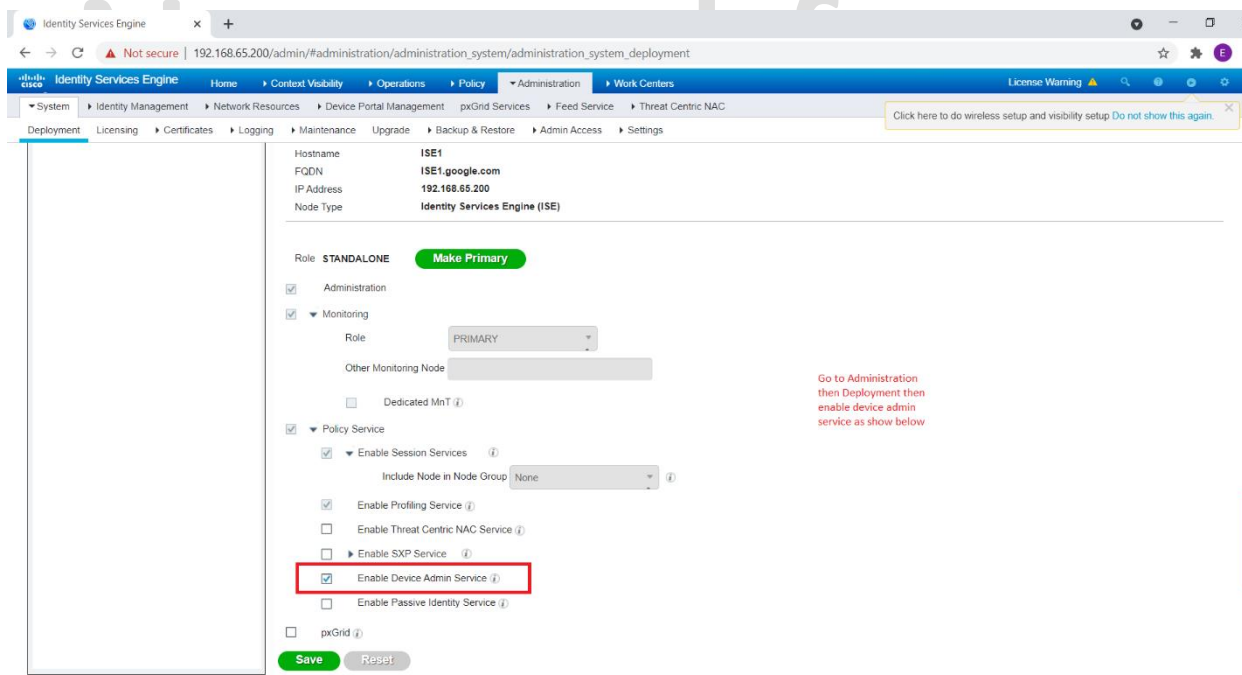
Login to Cisco ISE and Register devices



The screenshot shows the Cisco Identity Services Engine (ISE) interface. The browser address bar indicates the URL: 192.168.65.200/admin/#administration/administration_networkresources/administration_networkresources_devices/networkdevices. The page title is "Network Devices". On the left, there is a sidebar with "Default Device" and "Device Security Settings". The main content area shows a table of network devices:

Name	IP/Mask	Profile Name	Location	Type	Description
<input type="checkbox"/> R1	192.168.65.210/32	Cisco	All Locations	All Device Types	Router
<input type="checkbox"/> SW1	192.168.65.220/32	Cisco	All Locations	All Device Types	Switch

Go to Administrator then Deployment then enable device admin service



The screenshot shows the Cisco Identity Services Engine (ISE) Deployment page. The browser address bar indicates the URL: 192.168.65.200/admin/#administration/administration_system/administration_system_deployment. The page title is "Deployment". The main content area shows the deployment configuration for the ISE node:

Hostname: ISE1
FQDN: ISE1.google.com
IP Address: 192.168.65.200
Node Type: Identity Services Engine (ISE)

Role: STANDALONE **Make Primary**

- Administration
- Monitoring
 - Role: PRIMARY
 - Other Monitoring Node: [Empty]
 - Dedicated Mnt [?]
- Policy Service
 - Enable Session Services [?]
 - Include Node in Node Group: None [?]
 - Enable Profiling Service [?]
 - Enable Threat Centric NAC Service [?]
 - Enable SXP Service [?]
 - Enable Device Admin Service [?]**
 - Enable Passive Identity Service [?]
- pxGrid [?]

Save **Reset**

Go to Administration then Deployment then enable device admin service as show below

Email us:
networkforYou4@gmail.com

6 of 7

WhatsApp Us : +918143809578



Networkforyou

Subscribe to our
You Tube Channel

Networkforyou

Email us:
networkforyou4@gmail.com

7 of 7

WhatsApp Us : +918143809578