802.1X AUTHENTICATION AND CERTIFICATION IN A NETWORK SYSTEM

BY

MD. Salauddin Khan
ID: 191-15-12270
AND

MD. Rifat Ali
ID: 191-15-12131

This Report Presented in Partial Fulfillment of the Requirements for the Degree of Bachelor of Science in Computer Science and Engineering

Supervised By

Gazi Zahirul Islam

Assistant Professor

Department of Computer Science and Engineering

Daffodil International University

Co-Supervised By

Mr. Md. Mahade Hasan
Lecturer
Department of CSE
Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

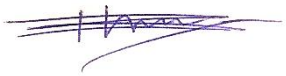
DECEMBER 2021

APPROVAL

This Project titled "**802.1X AUTHENTICATION AND CERTIFICATION IN A NETWORK SYSTEM**", submitted by **MD. Salauddin Khan,** ID No: **191-15-12270** and **MD. Rifat Ali** ID No: **191-15-12131** to the Department of Computer Science and Engineering, Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering and approved as to its style and contents.

BOARD OF EXAMINERS

Chairman



Dr. Sheak Rashed Haider Noori

Associate Professor and Associate Head

Department of Computer Science and Engineering

Faculty of Science & Information Technology

Daffodil International University

Internal Examiner

Subhenur Latif (SL)

Assistant Professor

Department of Computer Science and Engineering

Faculty of Science & Information Technology

Daffodil International University

Internal Examiner

Md. Azizul Hakim (MAH)

Senior Lecturer

Department of Computer Science and Engineering

Faculty of Science & Information Technology

Daffodil International University

External Examiner

Dr. Shamim H Ripon

Professor

Department of Computer Science and Engineering

East West University

DECLARATION

We hereby declare that, this project has been done by us under the supervision of Mr. Gazi Zahirul Islam, Assistant Professor of Department of Computer Science and Engineering, Daffodil International University, in partial fulfillment of the requirements for the degree of Bachelor of Science in Computer Science and Engineering. We also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

Supervised by:

Gazi Zahirul Islam
Assistant Professor
Department of Computer Science and Engineering
Daffodil International University

Co-Supervised by:

Mr. Md. Mahade Hasan
Lecturer
Department of Computer Science and Engineering
Daffodil International University

Submitted by:

MD, Salauddin Khan
ID: 191-15-12270
Department of CSE
Daffodil International University

MD. Rifat Ali
ID: 191-15-12131
Department of CSE
Daffodil International University

ACKNOWLEDGEMENT

First, we express our heartiest thanks and gratefulness to almighty God for His divine blessing makes us possible to complete the final year project/internship successfully.

We really grateful and wish our profound our indebtedness to Gazi Zahirul Islam, Assistant professor, Department of CSE Daffodil International University, Dhaka. Deep Knowledge & keen interest of our supervisor in the field of "Network Security" to carry out this project. His endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior drafts and correcting them at all stage have made it possible to complete this project.

We would like to express our heartiest gratitude to Professor Dr. Touhid Bhuiyan professor and Head**,** Department of CSE, for his kind help to finish our project and also to other faculty member and the staff of CSE department of Daffodil International University.

We would like to thank our entire course mate in Daffodil International University, who took part in this discuss while completing the course work.

Finally, we must acknowledge with due respect the constant support and patients of our parents.

ABSTRACT

We looked into some of the mechanisms for securing corporate wired Ethernet, which are usually ignored. After a detailed analysis of all options, we decided on an IEEE 802.1X port-based authenticator technique. The authentication server is a radius server, and the authenticator is a Cisco switch. The major goal of implementing IEEE 802.1X is to limit guest access to the LAN/wired network and ensure that only genuine users are authenticated. The network is only accessible to authenticated users. The suggested approach uses Microsoft Active Directory Services in Microsoft server to monitor active users using centralized user access management. Individual configurations of all entities engaged in the mechanism are addressed in detail in order to properly offer a pilot version of the protocol that could be used to debug all faults before being deployed on a live network. We will be able to keep track of all users/employee action on the organization's network by configuring the accounting tab on the Server Manager.

TABLE OF CONTENTS

LIST OF FIGURES [Font-14, Bold]

Chapter-1
INTRODUCTION

1.1 Introduction:

Words like ‘threat’, ’vulnerability’, and ‘risk’ in the context of computer security refer to anyone or anything that creates a herm to the information, software, or hardware, or even the users themselves. Threats, vulnerabilities could come from insiders or outsiders who are not part of the network. More and more organizations are adopting newer technologies in this era of technological growth for a number of reasons, running from improved customer service for better working conditions for their own employees. Every day, new vulnerabilities are identified, making it even more important for business to admit, map, and understand their infrastructure in an increasingly secure and connected world. Organizations must be aware that cybercriminal gangs are always developing new ways to get access to an organization’s resources, most commonly through their networks. Today’s businesses require knowledge of their network architecture, including hosts, VLANs, VPNs, Nat, routing protocols, network access rules, network components, OS update etcetera. After that, security administrators can utilize the network map to identify existing vulnerabilities and device better security policies to counter them.

1.2 Motivation:

We cannot think an organization’s server or network system without any security policies. It is must to ensure the security of the network. IEEE slandered policy 802.1x authentication is a small part of ensuring security. RADIUS server is used to configure that.

Chapter-2

Authentication Technology

2.1 Why Authentication:

The process of verifying that someone or something is what they claim to be is called authentication. Authentication technology checks a user's credentials. Match them in the database if the credentials are legit or not then he can get the access control to the network. Authentication ensures secure system and organizational information security in this way.

Organizations can keep their networks safe by allowing only authenticated users to their protected resources.

2.2 Authentication type:

2.2.1 Authentication protocols PPP Point-to-Point:

Before getting access to the server resources one remote client must have to be validated his identity by the point-to-point protocol. The majority of them rely on a password for authentication. In most circumstances, the password must be shared in advance between the communication parties. One of the oldest authentication systems is the password Authentication Protocol. The clients initiate authentication by sending a packet containing credentials (username and password) at the start of the connection, and then reporting the request until and acknowledgement is received. Because credentials are transferred "in the clear" and repeatedly, it is very unsafe, leaving it subject to even the most basic assaults like eavesdropping and man-in-the-middle attacks. Despite its widespread acceptance, it is required that if an implementation provides a stronger authentication technique, that method must be provided before PAP. Mixed authentication (e.g., the same clients using both PAP and CHAP) is also not intended, as PAP delivering the password in plain-text-might compromise CHAP authentication.

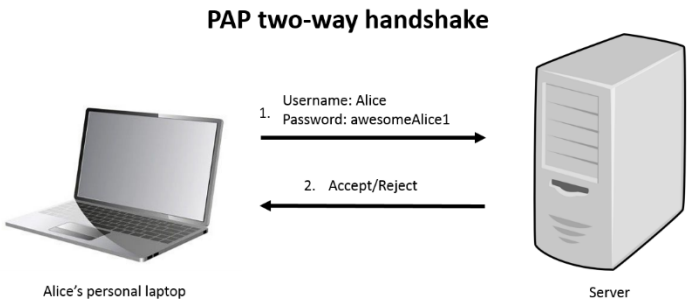


Figure 2.2.1: PAP 2-way handshake

2.2.2 AAA Architecture protocols:

AAA architecture protocols stands for Authentication, Authorization and Accounting. This protocol used in a very complex and large network to verifying the users, regulate access to server resource, and monitor network information for service billing.

2.2.2.1 TACACS, TACACS+, and XTACACS

This is the oldest IP based authentication which does not use any kind of encryption. Authorization and accounting were added on later version XTACACS. TACACS+ eventually replaced both of these protocols. TACACS+ isolates the AAA components, allowing them to be handled separately on separate servers. IT transports date via TCP and encrypts the entire packet. TACACS+ is a cisco only system.

2.2.2.2 RADIUS

RADIUS stands for remote authentication Dial-In user service, which is a full AAA protocol. It employs NAS and UDP protocol for transport. And credentials are based on username-password combination.

2.2.2.3 DIAMETER

Diameter developed from RADIUS. It has a number of upgrades, in diameter more reliable TCP or SCTP transport protocols and TLS based security is used.

2.2.3 KERBEROS

Kerberos is a core network authentication system developed at MIT that is available as a free MIT implementation as well as various commercial solutions. In windows 2000 and upper, it is the standard authentication technique, Kerberos uses symmetric key cryptography. It requires a trusted third party, and can use public key cryptography during some step of authentication if necessary. It made the authentication process far more involved than earlier protocols.

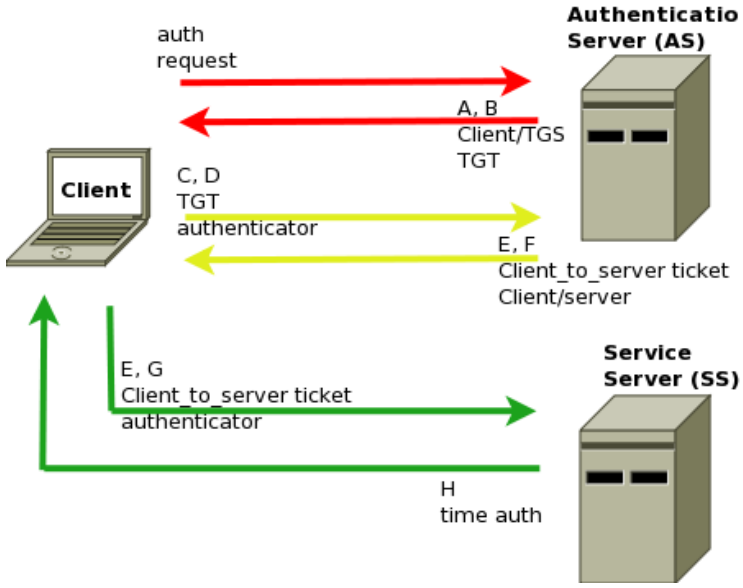


Figure 2.2.3: Kerberos authentication scheme

2.2.4 Authentication Protocols

- Basic Access Authentication
- CAVE based authentication
- CRAM-MD5
- OpenID Protocol
- Security Assertion markup language (SAML)
- Password authenticated key agreement protocols
- RFID- authentication Protocols
- Protocol for Carrying authentication for Network Access (PANA)

- Secured Remote Password Protocol (SRP)
- RFID- authentication Protocols
- Woo Lam 92 Protocol
- AKA

And many more.

Chapter-3

RADIUS

The Remote Authentication Dial-In-User (RADIUS) is a networking protocol that allows users to connect to and use a network service with authentication, authorization, and accounting (AAA) administration. Livingstone Enterprise created RADIUS in 1991 as an authentication and accounting protocol for access servers. Later on, it was included into IEEE 802 and IETF standards.

RADIUS is a TCP or UDP based client/server protocol that runs in the application layer. The RADIUS client component of network access server, which manage network access, normally connects with the RADIUS server. For 802.1X authentication, RADIUS is frequently used as the back end. A RADIUS server is generally a background process on UNIX or Microsoft windows that rubs in the background.

RADIUS is basically a dial-in access server which authenticate a user by checking his user name and password before connecting a network if the server already configured an 802.1x authentication service. When connecting in a network the device generates a message using the RADIUS shared secret in the message. The message is called Access Request message.

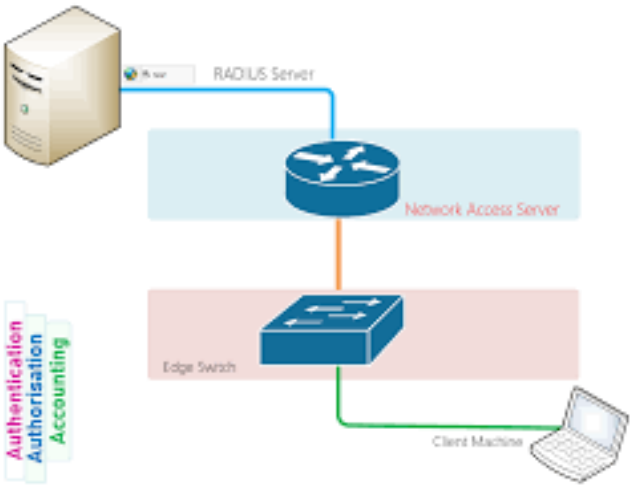


Figure 3: RADIUS

Chapter-4

IEEE 802.1X Technology

There are three elements of 802.1X authentication.

Supplicant Port Access Entity (PAE): The client side of the authentication process is handled by this program on the client device.

Authenticator: This device handles the port access to the network. Communications between the authenticator PAE and the supplicant PAE are tunneled through the authenticator PAE.

Server: A client is authenticated by this server with the supplicant PAE through EAP authentication conversations.

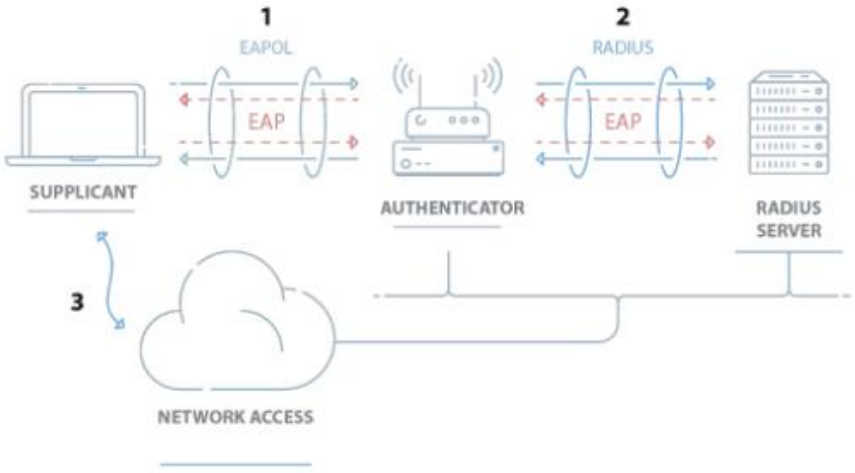


Figure 4: Elements of 802.1x authentication

4.1 Certificate Authentication

The main goal to install or configure certificate authentication is to verify that the device is connecting with the right RADIUS server. We need an active directory installed into the main server. After that we need to configure the Active Directory Certificate Service.

Chapter-5

Installation and Configuration

Before the installation first thing we need is an Active Directory Domain server. For that we will be using Windows Server 2016. RADIUS is basically a build-in service which we have to install and configure.

Here we will see the installation process step by step. It's a very sensitive process which can be failed if the pre-tasks aren't do properly. The IP address of the domain controller must be static. The IP address and the preferred DNS server have to be same on the ADDS (e.g., IP Address: 192.168.1.24; Preferred DNS Server: 192.168.1.24)

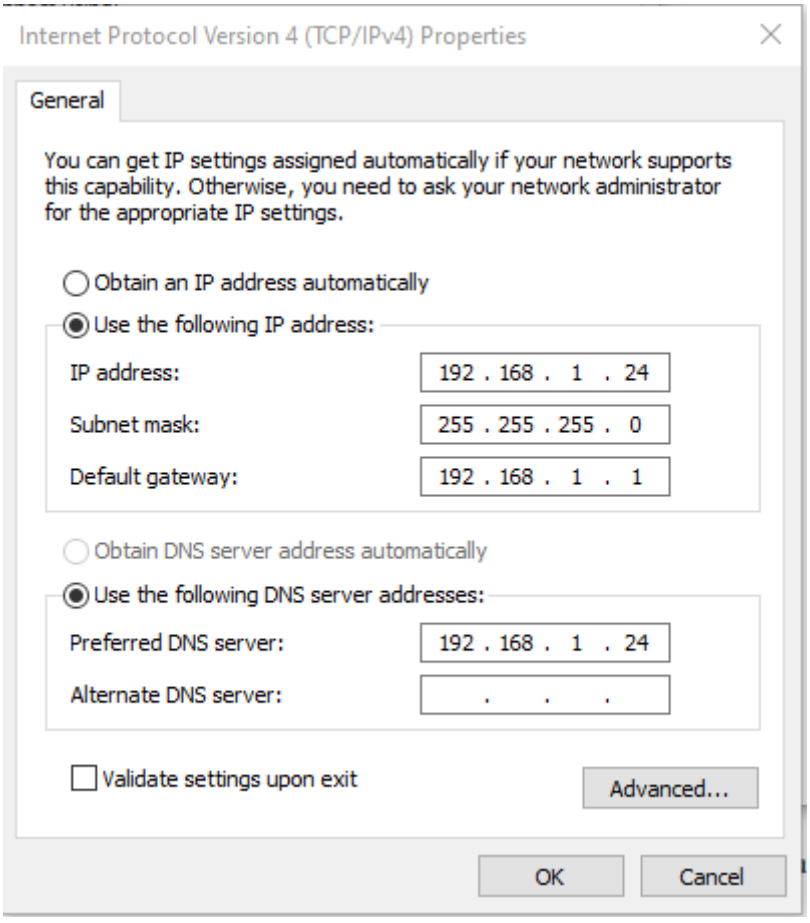


Figure 5: IP Configuration

And if there is not any ADDS on the sever 2016 then we have to install domain controller feature from Add roles and features.

1. Search “Server Manager”
2. Right click on “Manage” then “Add Roles and Features”
3. Then click next from “Before You Begin” to “Server Roles” and √ mark on “Active Directory Domain Services”. Then “Add Features” then popup window will come. Then next till install button arise. Then hit “Install” button.
4. Next “Promote This Server to a Domain Controller”.
5. “Add a new forest” Root domain name: “any name followed by .com or .local” then next.
6. Select a strong password. Then next.
7. Next. A window will show the domain name. Then next.
8. Next>...>Install…>Complete.
9. Now Log in > User Id: Administrator. Password:” Step 6”.

Now This ADDS will be the main server controller. And the main user will be the Administrator.

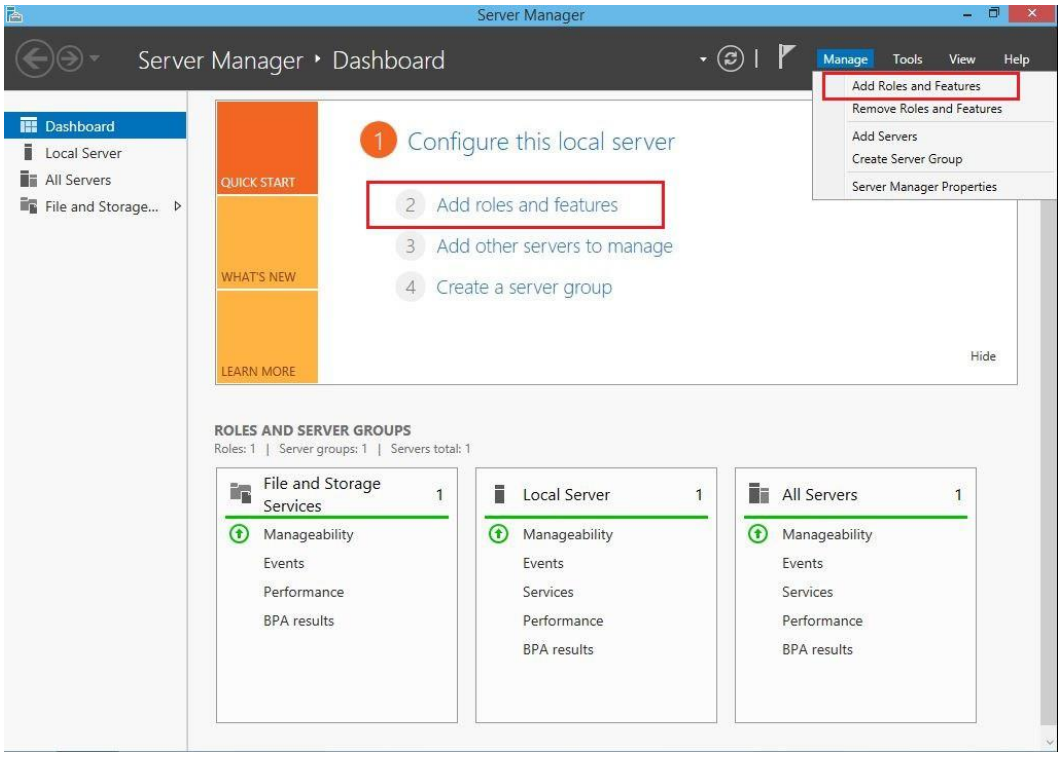


Figure 5: Server manager Dashboard.

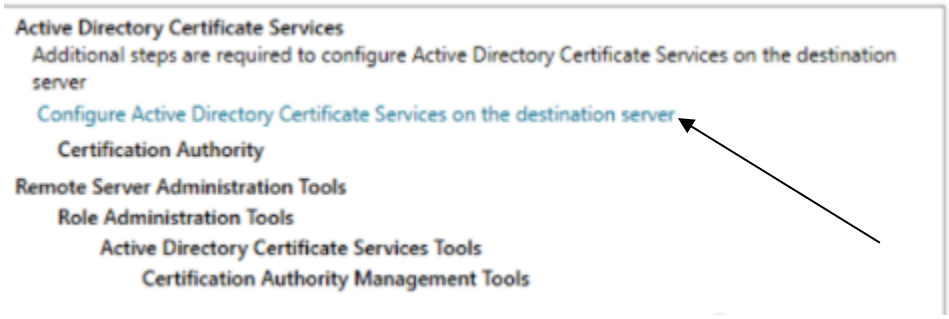
5.1 Active Directory Certificate Services installation

After finishing the installation of Active Directory Domain Services, we have to install Active Directory Certificate Services. For a organization ADCS build a public key infrastructure (PKI) for digital certificate and signature. ADCS is that service role that allows to do it.

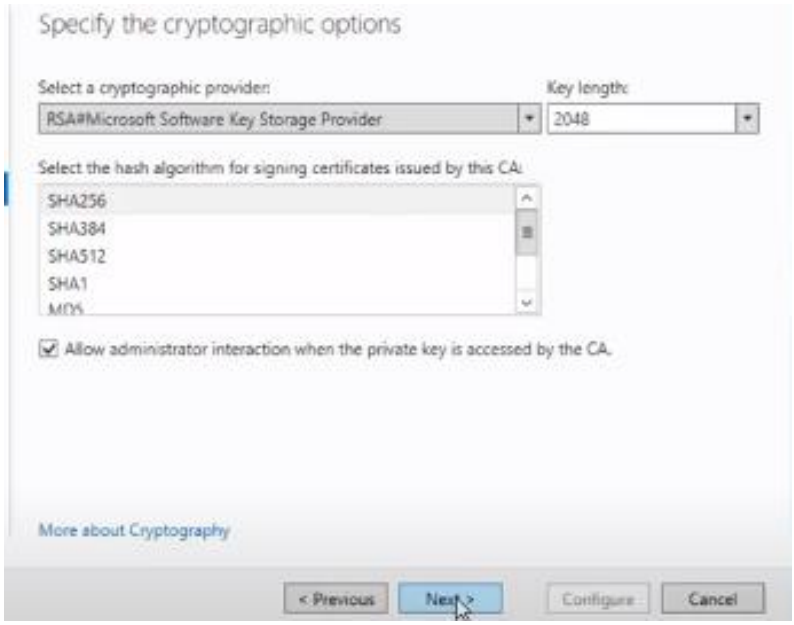
Steps:

1. From server manager click on “Manage” then “Add roles and Features”
2. Click “Next” till “Server Roles”
3. √ mark on “Active Directory Certificate Services”. Then click on “Add Features”.
4. √ mark on “Certificate Authority”. Then “Next” and “Install”. (It will take few minutes). Then close.

5. Now “Configure Active Directory Certificate Services on this destination server”



6. Then “next” then √ mark on “Certificate Authority”. And “next”
7. “Next” till “Cryptography” page.
8. Select the options as shown.



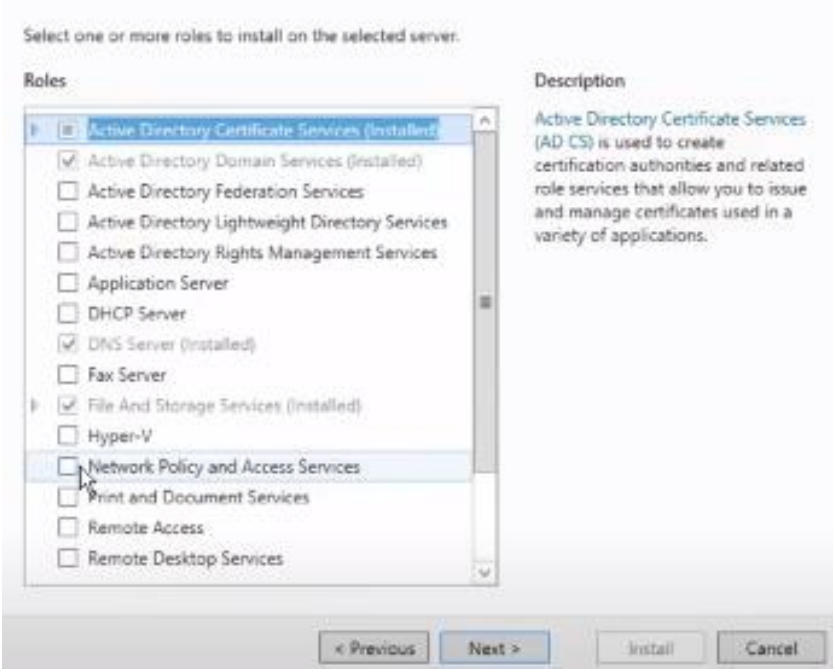
“Next”.

9. Then “Next” till “Configure” button arise. Click on “Configure” button.
10. And we are done installing “Active Directory Certificate Services (ADCS)”.

5.2 Network Policy and Access Services installation

Now we have to install “Network Policy and Access Services”.

1. From server manager click on “Manage” then “Add roles and Features”
2. Click “Next” till “Server Roles”

3. √ mark on “Network Policy and Access Services”.
4. 

5. Click on “Add Features”. And then click “Next” button until the “Install” button arise and hit “Install”.
6. “Close”.

Now the dashboard will look like this.

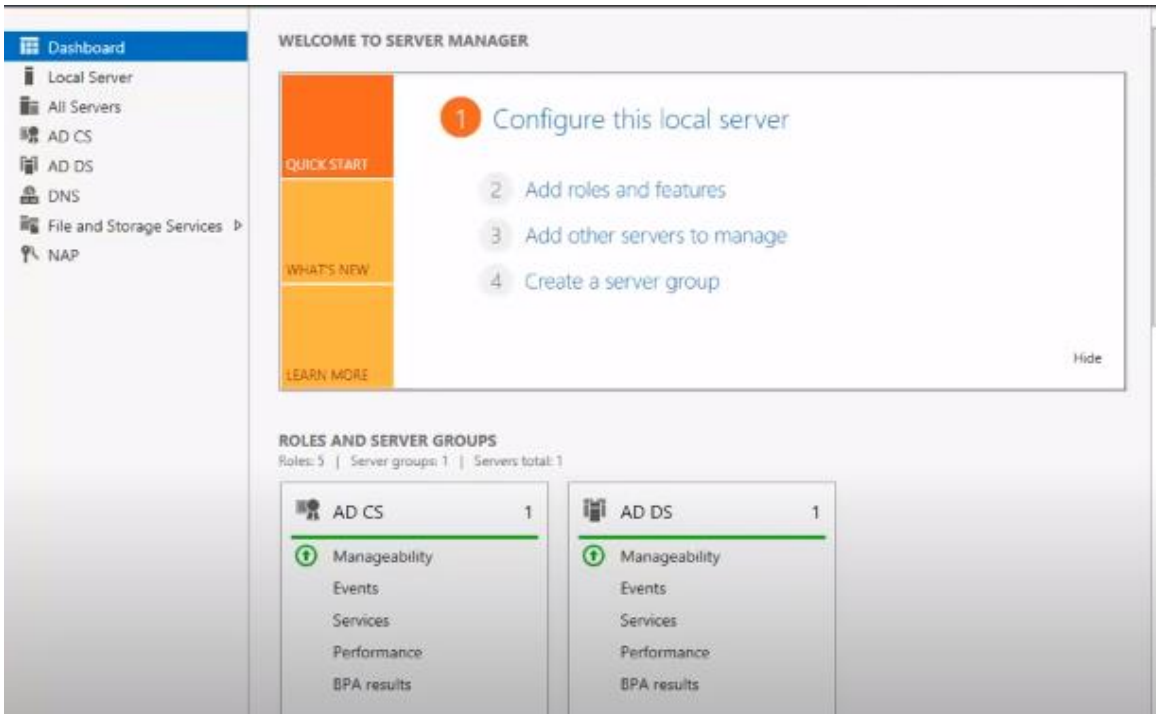
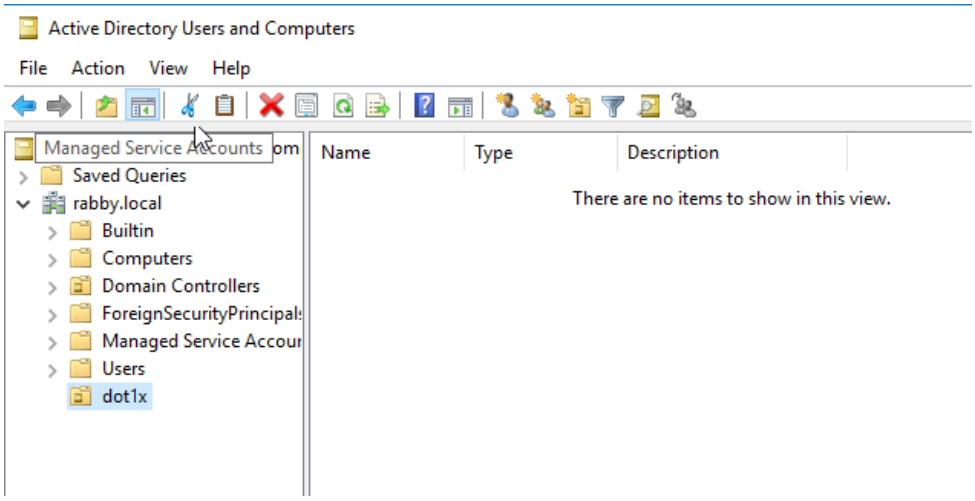


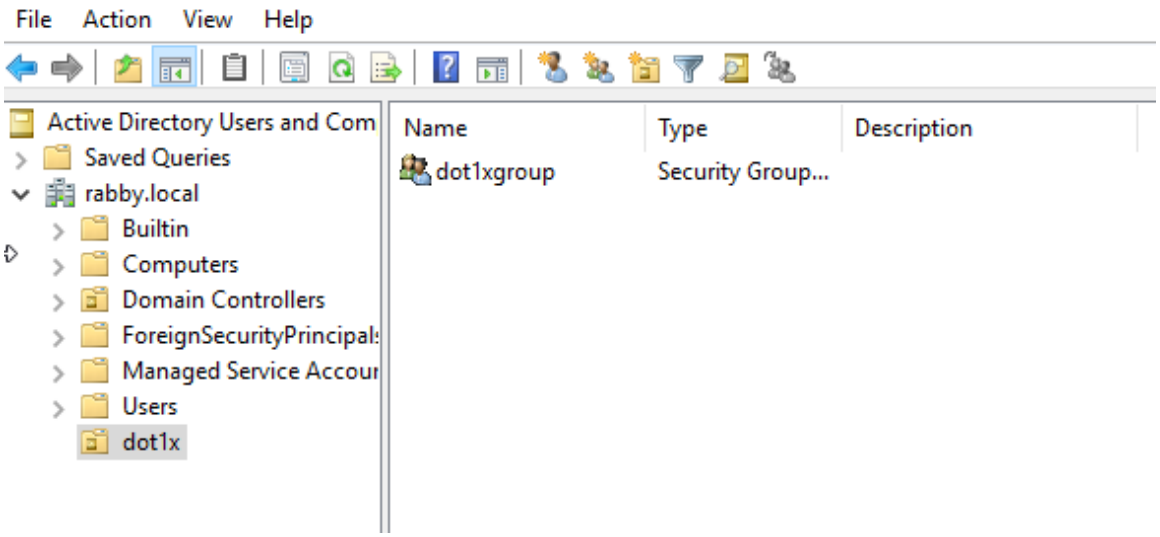
Figure 5.2: Server Manager

5.3 User and Group create

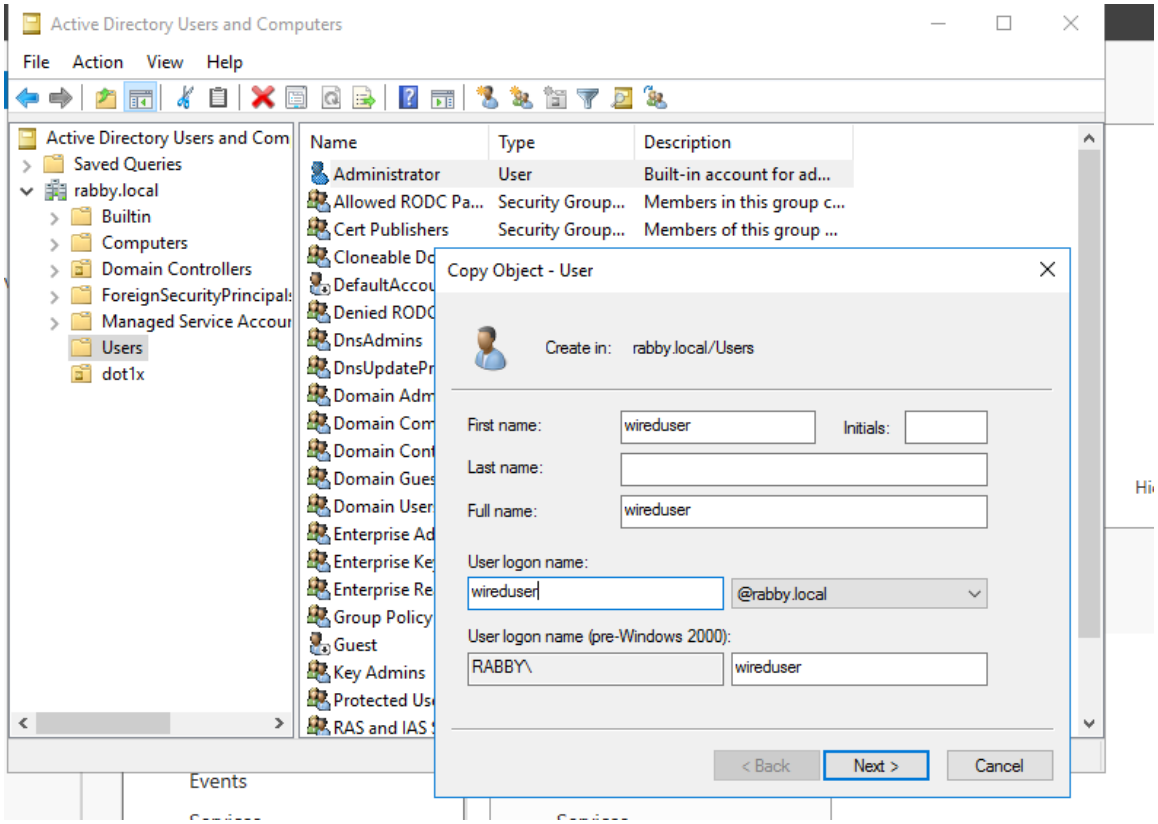
Now we have to create an organizational Unit “dot1x”

1. 

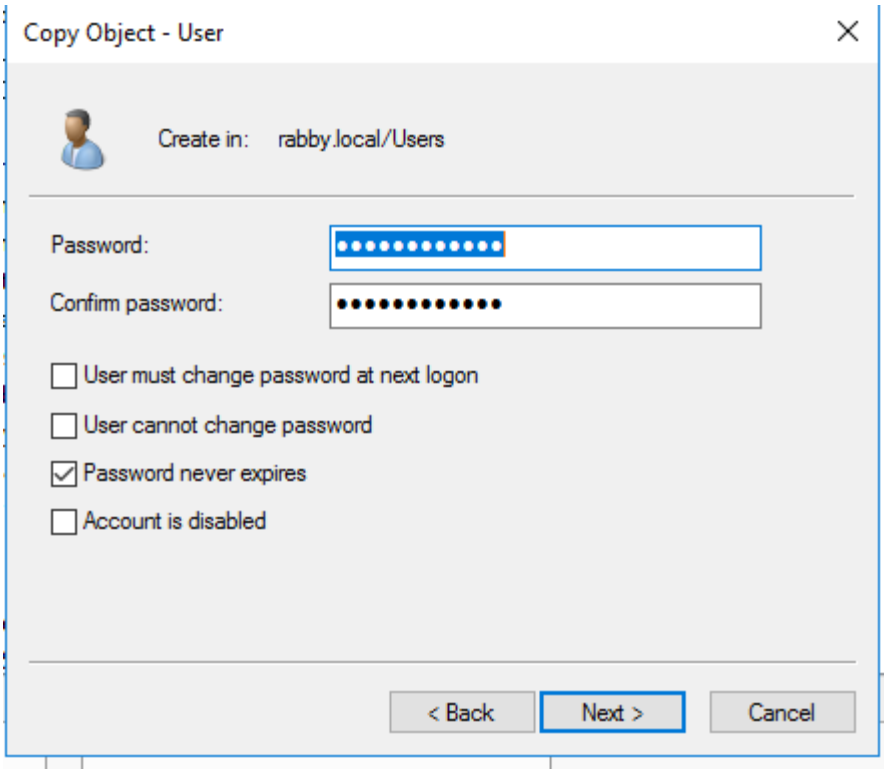
2. Make a group inside the unit



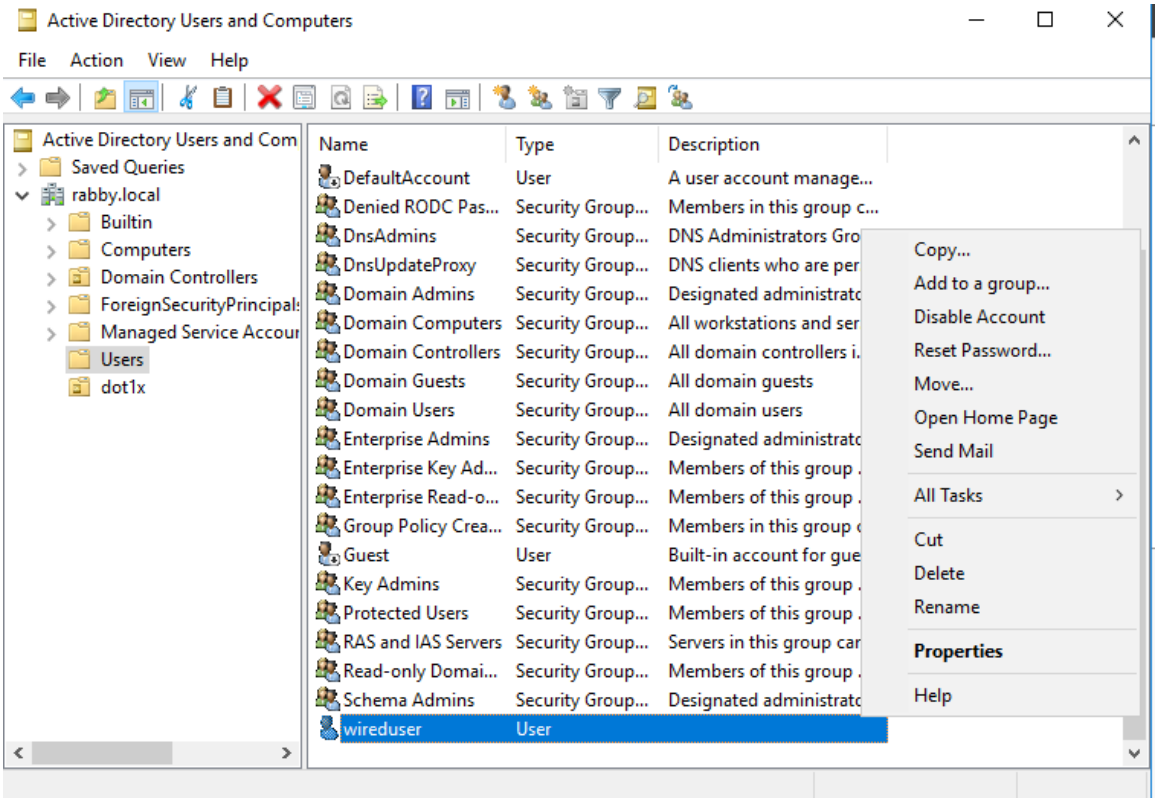
3. Copy the Administrator user and name it

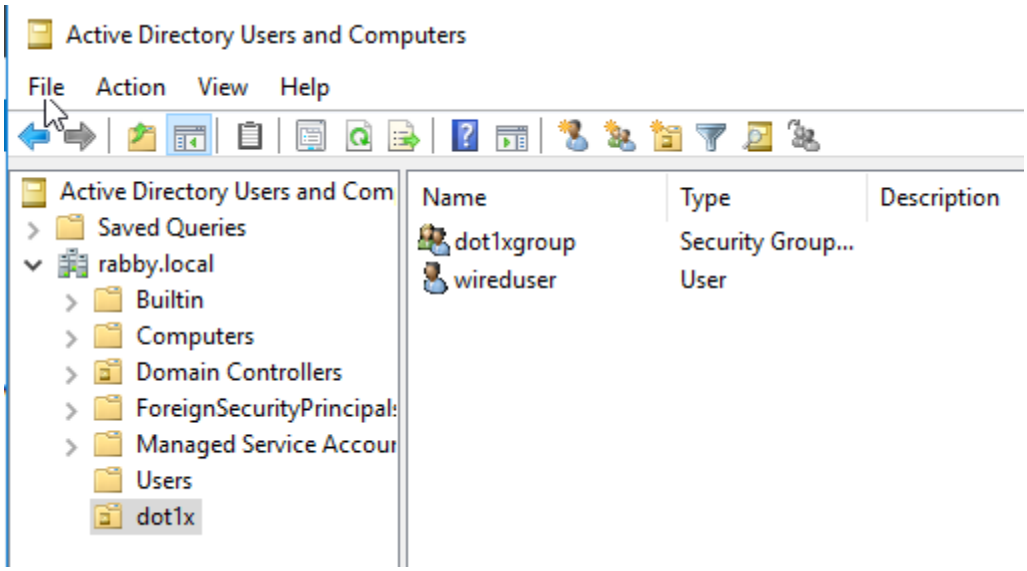


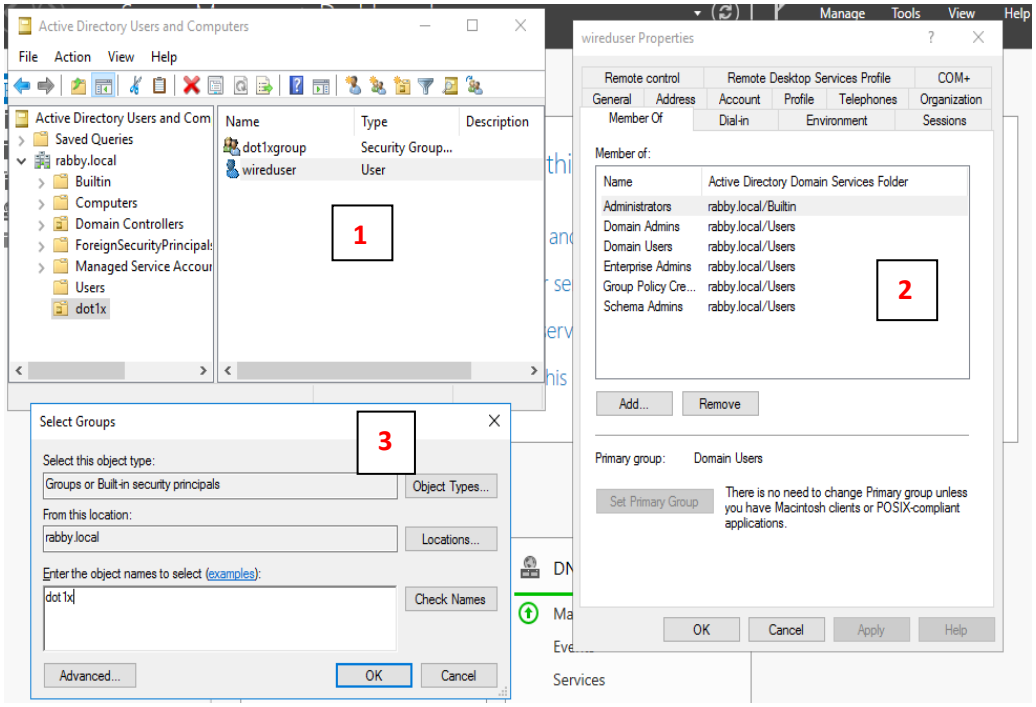
4. Create password

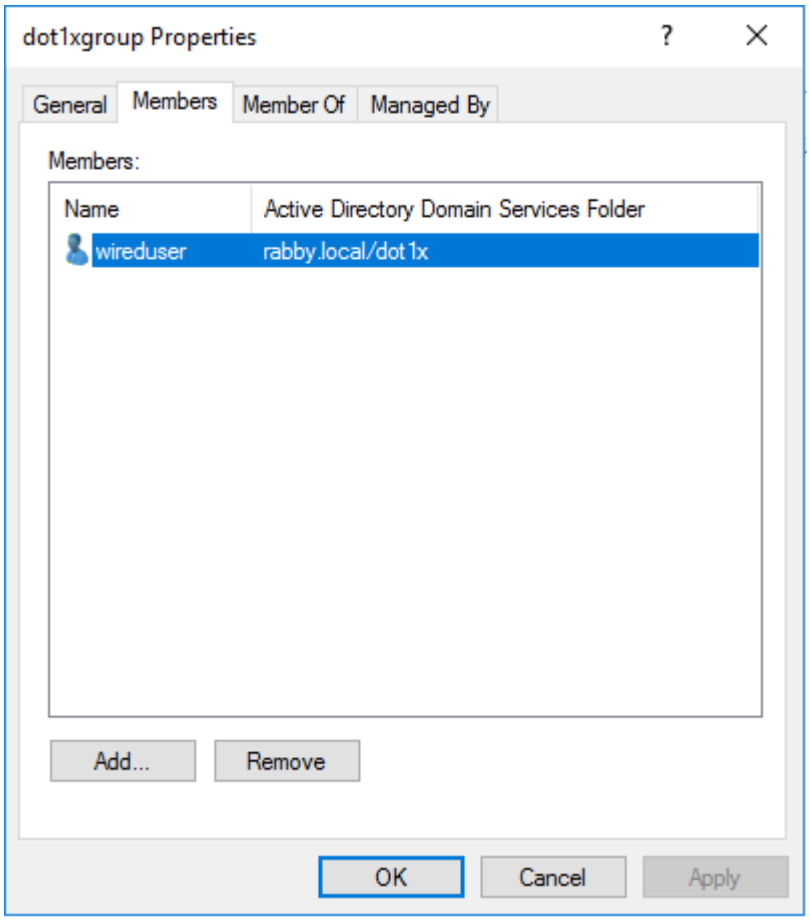


5. Move the user to the organizational unit



6. 
Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
rabby.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal:
Managed Service Accour
Users
dot1x
Name
Type
Description
dot1xgroup
Security Group...
wireduser
User

7. 
Active Directory Users and Computers
File Action View Help
1
wireduser Properties
Member Of
Member of:
Name
Active Directory Domain Services Folder
Administrators rabby.local/Builtin
Domain Admins rabby.local/Users
Domain Users rabby.local/Users
Enterprise Admins rabby.local/Users
Group Policy Cre... rabby.local/Users
Schema Admins rabby.local/Users
2
Add...
Remove
Primary group: Domain Users
Set Primary Group
There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.
OK
Cancel
Apply
Help
Select Groups
3
Select this object type:
Groups or Built-in security principals
Object Types...
From this location:
rabby.local
Locations...
Enter the object names to select (examples):
dot1x
Check Names
Advanced...
OK
Cancel
Services

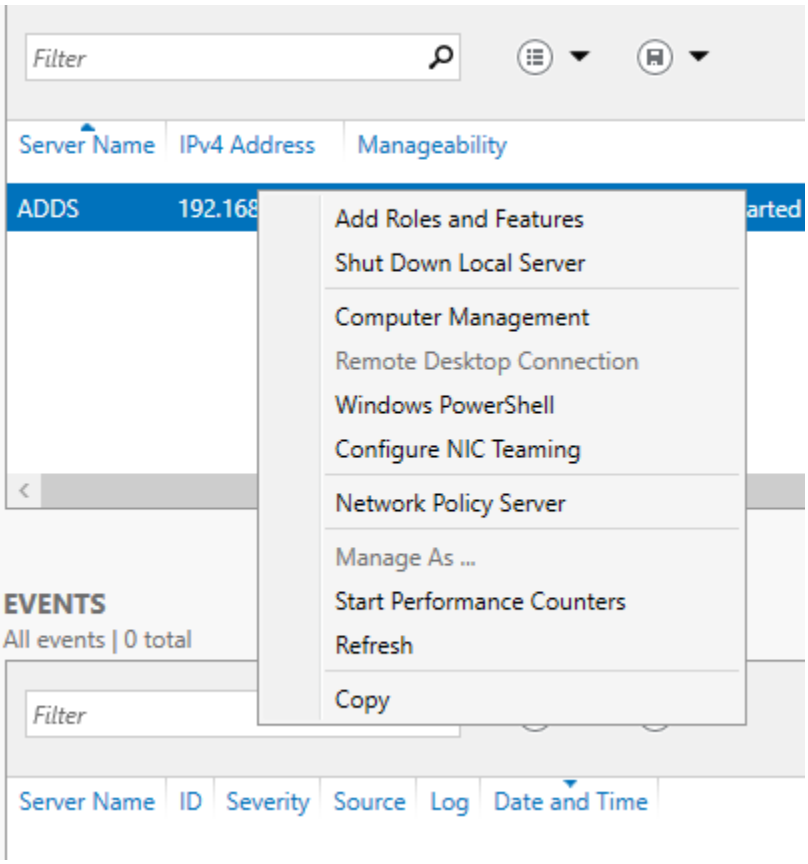
8. 

9. Done.

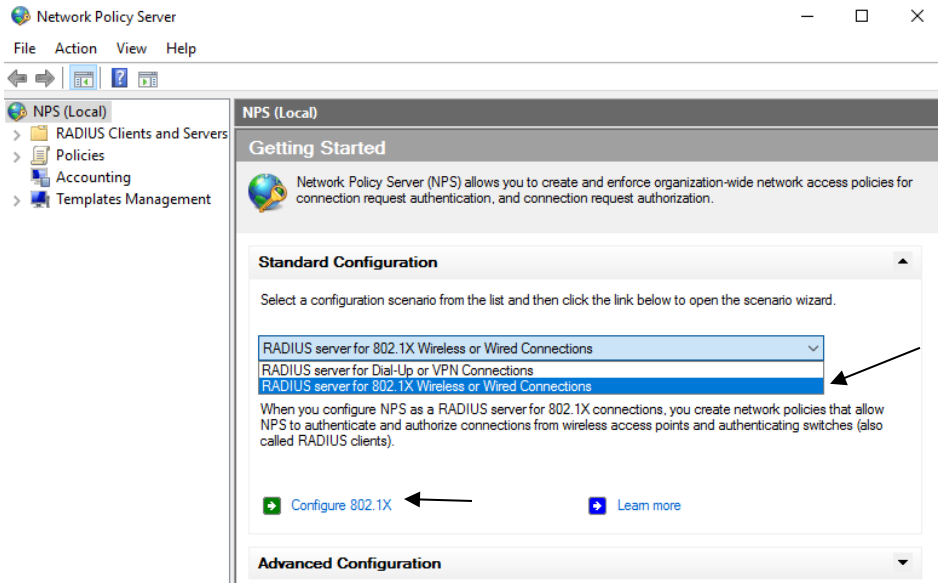
5.4 RADIUS Installation

Installation of RADIUS is as simple as the previous installation process. The steps and the process are shown below.

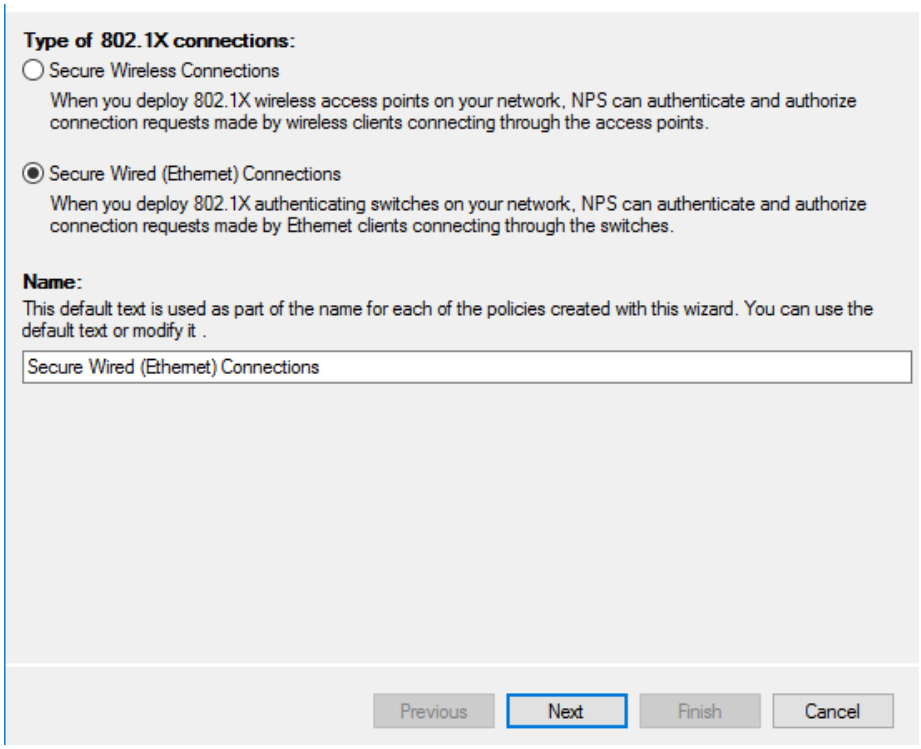
1. First go to “Network Policy Server”



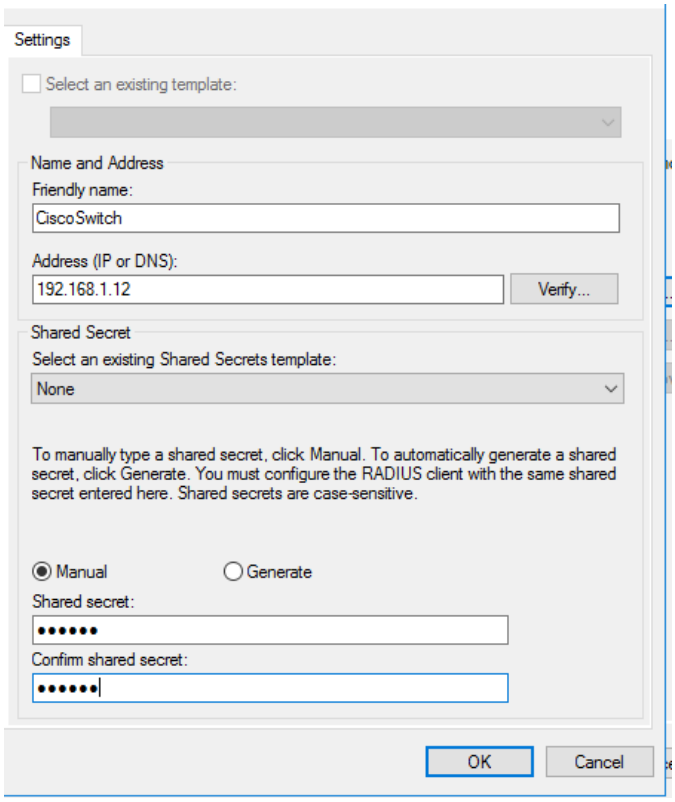
2. In “NSP” select “RADIUS server for 802.1X wireless or wired Connections” then click “Configure” 802.1X.

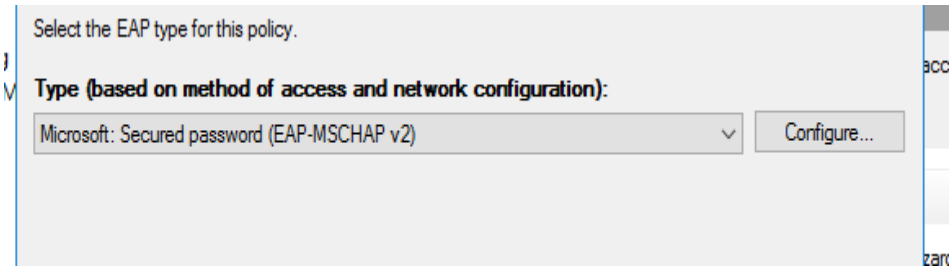


3. In This page select “Secured Wired (Ethernet) Connections” and then “Next”.

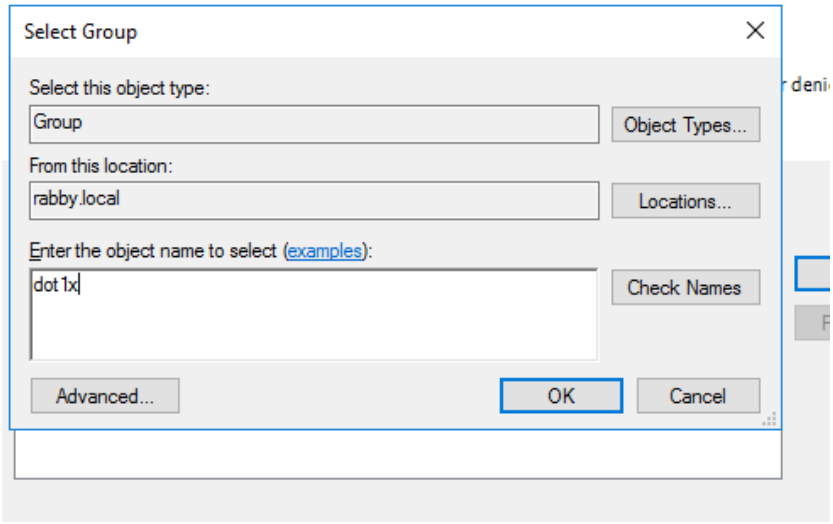


4. Here Give a Friendly name and the IP of the switch. Then a suitable key (Shared Secret) here mine is “secret”. Then ok.

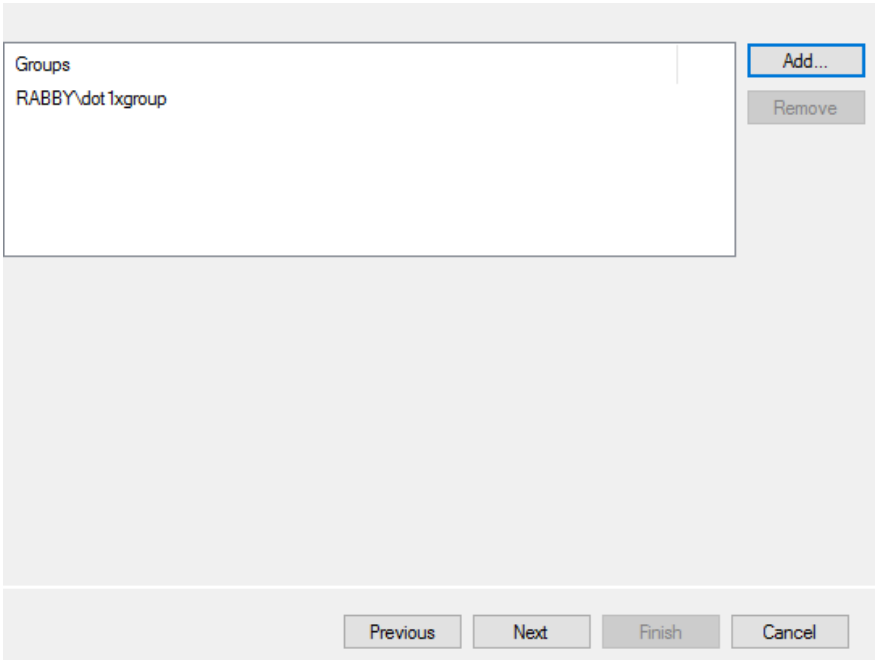


5. 

6. “Next” then click “Add”. And select the group we crated “dot1x”.

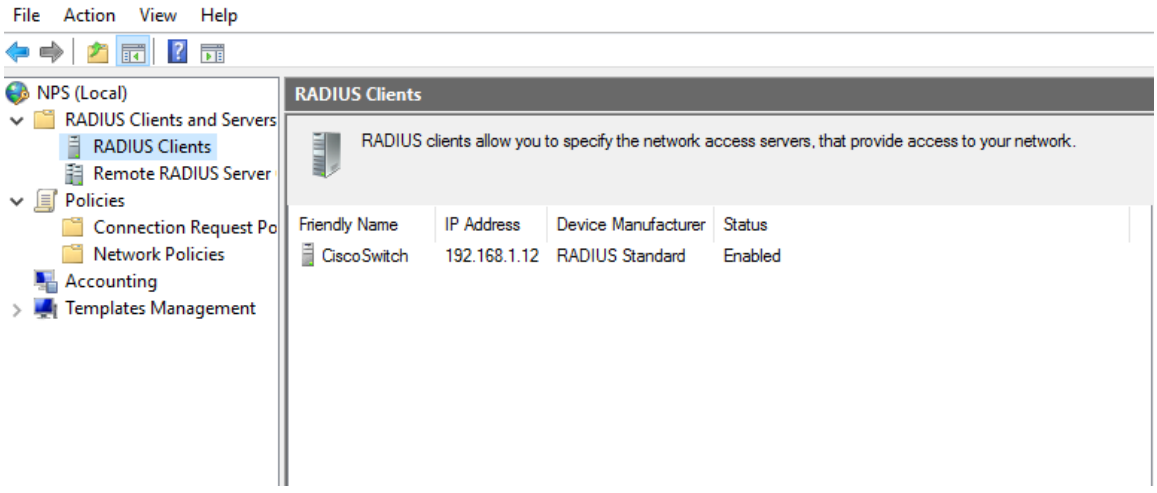


7. Then click “next”.

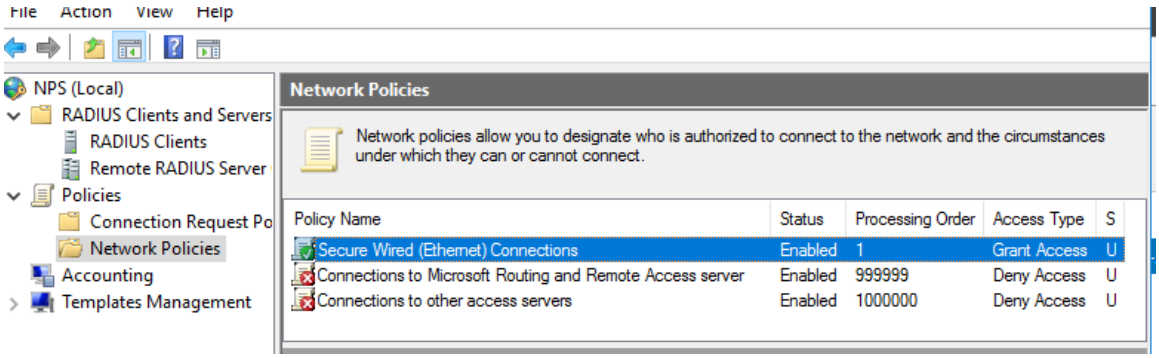


8. Now click “Finish”.

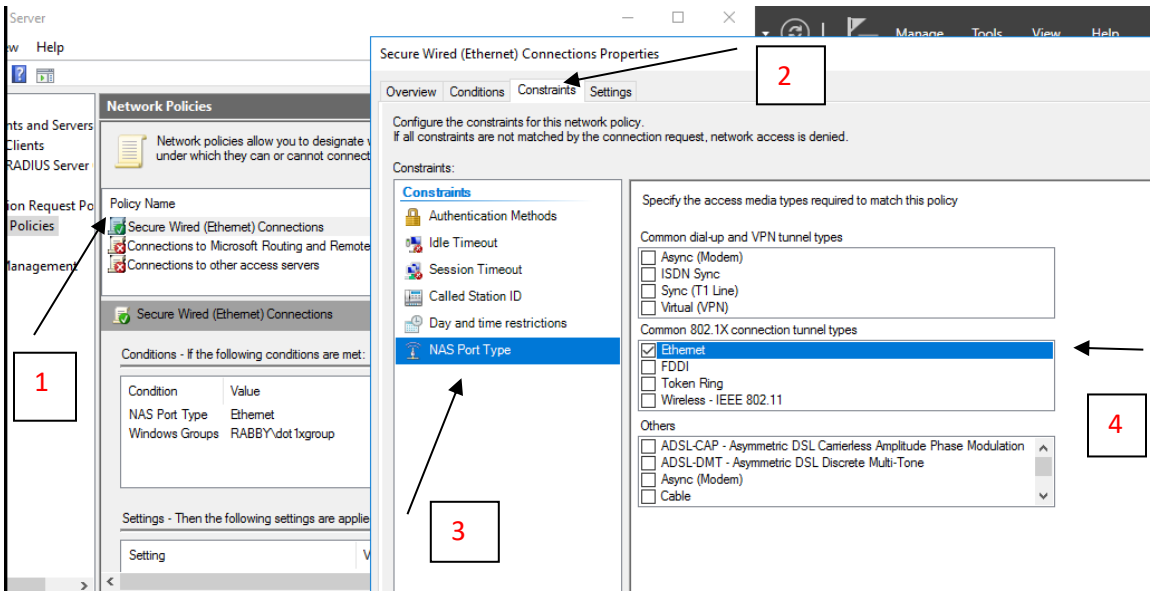
9. Here is the switch (Client).



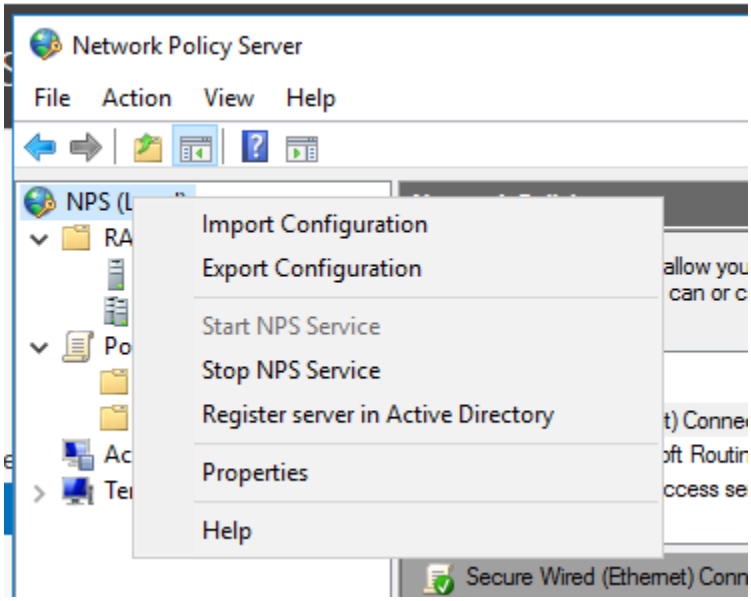
10. And here is the policy.

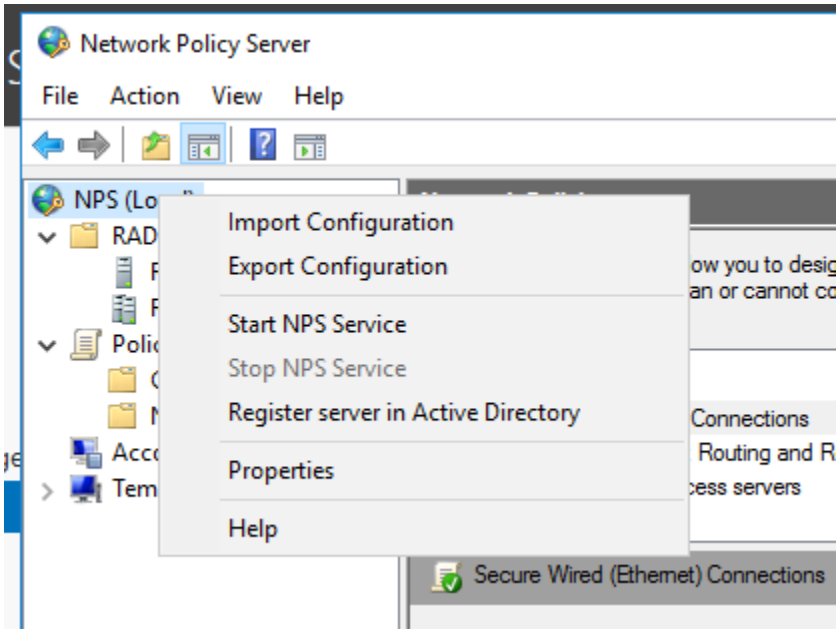


11. Double click on “Secure Wired (Ethernet) Connections”. (Tik Mark on “Ethernet” step 4) then next.



12. Now right click on “NPS”. Stop the service and then start it again.





13.

14. Done.

5.5 Switch configuration

Here we used a Cisco switch as a client. To configure we have to follow this command:

config t

aaa new-model

aaa authentication dot1x default group radius

dot1x system-auth-control

radius-server host 192.168.1.24 auth-port 1812 acct-port 1813 key secret

!radius-server host 192.168.1.24 key secret

int fa 0/1

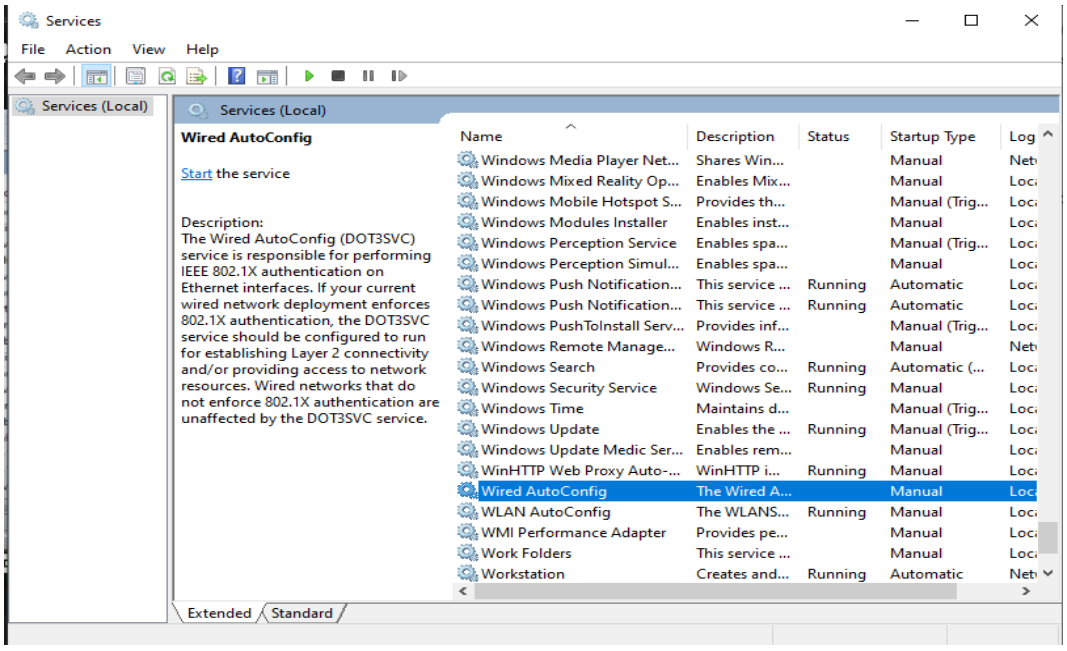
switchport mode access

dot1x port-control auto

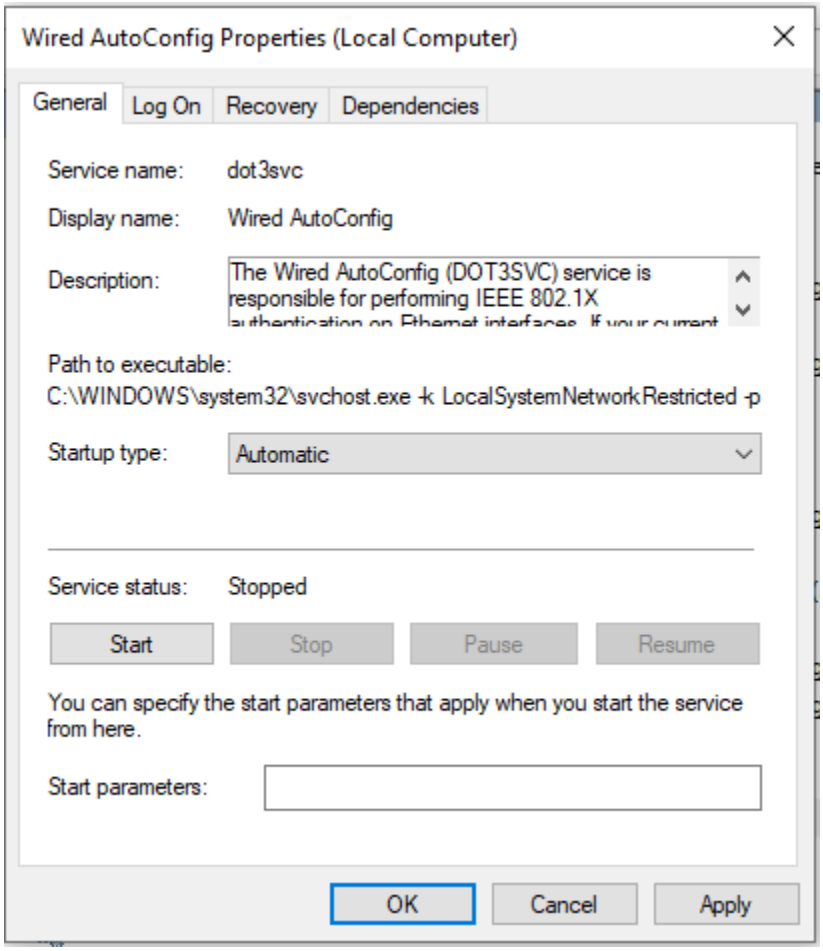
end

5.6 Client device connect

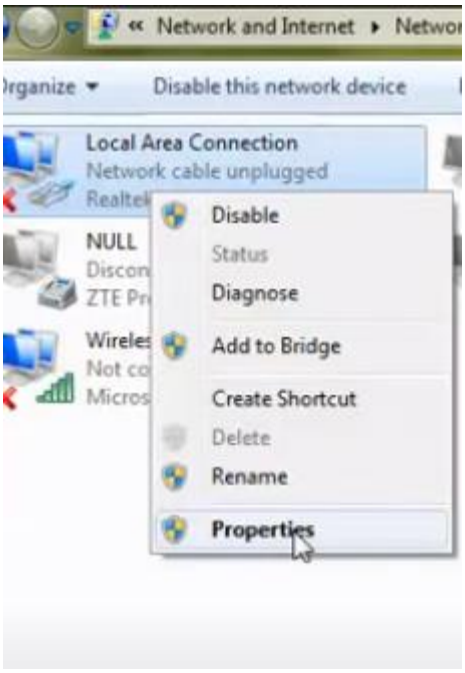
Here we used a windows computer as a client device. But first we have to check if the Wired AutoConfig service is installed or not. For that press the windows key along with "R" key to open "run". Now type "services.msc".



double click on Wired AutoConfig and set “startup type” to “Automatic”. Then “OK”.



Now we have to setup some setting. Go to network setting and then wired connection. Then the go to the actual physical connection and then properties.



Go to authentication and √ mark on “Enable IEEE 802.1X authentication. And we are done.

When we plugged in the LAN cable popup window will come. Here the user name will be “RABBY\wireduser”. And password is “Password128#”. Hit ok and we can successfully connect to the network.

5.7 Conclusion

Through the report paper we have made it clear that every physical device need security. And 8021x authentication is just only a simple part. We showed what is authentication, what is radius server, how the process work. RADIUS is a default security policy in windows server operating system. We showed how to enable it step by step, and how it works.

References

[1] Authentication protocol, online available <https://en.wikipedia.org/wiki/Authentication_protocol> last accessed on 01 Oct 2022 at 10.00 PM.

[2] RADIUS Server, online available <https://en.wikipedia.org/wiki/RADIUS>, last accessed on 01 Oct 2022 at 10.00 PM.

[3] What you need to know about this LAN-authentication standard by Josh Fruhlinger and Joel Snyder, online available <https://www.networkworld.com/article/2216499/wireless-what-is-802-1x.html> last accessed on 01 Oct 2022 at 10.00 PM.

[4] 802.1x-overview, online available <https://community.jisc.ac.uk/library/advisory-services/8021x-overview> last accessed on 01 Oct 2022 at 10.00 PM.

[5] Implementation of IEEE 802.1X in wired networks by Øystein Gyland, Tom Myren, Rune Sydskjør, Gunnar Bøe, online available <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjIqPr58rj0AhX_TGwGHSO7Av8QFnoECAIQAQ&url=https%3A%2F%2Fgeant3plus.archive.geant.net%2FDocuments%2Fgn3-na3-ufs_133.pdf&usg=AOvVaw2JyVjpePjPD38LhpO0Nw9B> last accessed on 01 Oct 2022 at 10.00 PM.

[6] What is 802.1x. how does it work, online available <https://www.securew2.com/solutions/802-1x> last accessed on 01 Oct 2022 at 10.00 PM.

802.1X AUTHENTICATION AND CERTIFICATION IN A NETWORK SYSTEM

ORIGINALITY REPORT

25%	18%	8%	15%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	en.wikipedia.org Internet Source	7%
2	Submitted to National School of Business Management NSBM, Sri Lanka Student Paper	2%
3	Submitted to ACIT Student Paper	2%
4	Submitted to University College London Student Paper	2%
5	Submitted to CTI Education Group Student Paper	1%
6	Submitted to University of Ghana Student Paper	1%
7	www.cesnet.asia Internet Source	1%
8	dokumen.pub Internet Source	1%