2021-2022

جامعة البعث

الكلية التطبيقية – السنة الرابعة – تقنيات الحاسوب

الفصل الثاني 2021-2022

Networks Security

Lecture 3

:SUPERVISED BY

ENG. ALI MUSTAFA

Academic Year 2021-2022

التوثّق عن طريق AAA Server

AAA Servers (Authentication, Authorization and Accounting Server)

➢ مقدمة

توفّر مخدمات إدارة التوثّق والوصول والحسابات AAA Servers حلًا مركزيّاً لإدارة الوصول للأجهزة الشبكية كالمُبدّلات والموجهات وبشكل خاص تؤمّن شركة Cisco هذه الميّزة من خلال استخدم أحد البروتوكولين Terminal Access Controller Access-Control System الذي يُعرف باسم TACACS+ الخاص بشركة Cisco أو باستخدام البروتوكول RADIUS (Remote Authentication Dial-in User Server) حيث يصبح تعريف طرق التوثّق على كل جهاز من الأجهزة الشبكية صعباً خاصةً إذا كان عدد الحسابات أو الأجهزة كبيراً جداً.

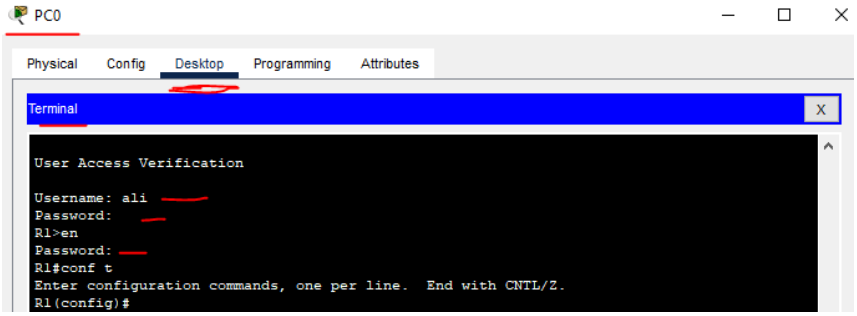
➢ طُرق التوثّق المحليّة

عندما نريد القيام بإعداد أي جهاز شبكي عن بعد فإننا نستخدم اما Telnet أو SSH ويمكن أن يتم التوثق من خلال استخدام اسم مستخدم وكلمة مرور يتم تعريفها بشكل محليّ على الجهاز الشبكي (موجّه في مثالنا) من خلال الأمر التالي:

(كل ما سيتم تطبيقه تالياً هو ضمن المُحاكي Packet Tracer)

```
username [username] password [password]
line console 0
Login local
```

ونلاحظ أنه سيتم طلب كلمة المرور عند الدخول لصفحة إعداد الجهاز الشبكيّ (المُوجّه في مثالنا) من الجهاز PC0 (الذي سنراه ضمن الطوبولوجيا لاحقاً):



إنّ البيانات التي يتم تبادلها عند استخدام بروتوكول telnet تكون غير مُشفّرة (plaintext) وبالتالي يمكن لأي مُهاجم أن يتنصّت على الشبكة ويعرف هذه البينات ويستخدمها لذلك دائماً ما يتم استخدام بروتوكول SSH (Secure Shell) لحماية البينات المُتبادلة بين جهاز المدير والجهاز الشبكيّ المُراد الوصول إليه عن بُعد.

لا يقتصر عمل بروتوكول Telnet على عملية التوثّق من هوية المستخدمين المتصلين عن بعد فقط (Remote Access) حيث انه يتم استخدامه من أجل الوصول للجهاز الشبكي عن طريق **Console/AUX cable**.

لتفعيل التوثق من اسم المستخدم وكلمة المرور عند الاتصال باستخدام Telnet نُطبّق الإعدادات التالية:

```
enable password [password] //set password for enable
username [username] password [password]
line vty 0 4 //means that the device can allow 5 con, accept <0-15>
login local //check credential from local DB
```

ملاحظة هامة:

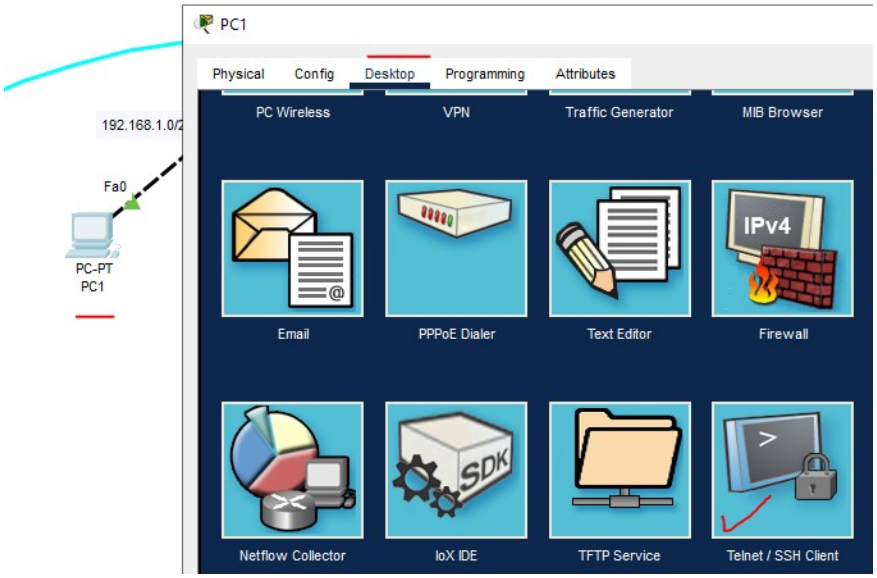
في حال عدم وجود كلمة مرور لوضع التفعيل (enable) لن نتمكّن من الدخول لوضع privileged EXEC وإعداد الجهاز الشبكي عن بُعد.

لذلك قمنا بتعيين كلمة مرور للوضع enable كما هو مُوضّح في التعليمات السابقة.

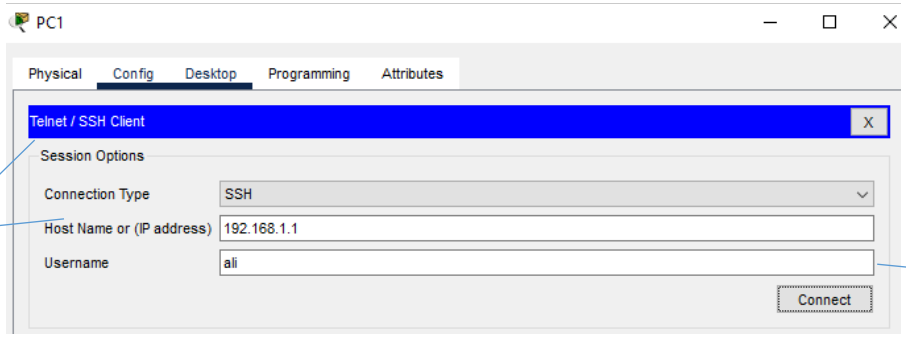
كما ذكرنا سابقا فإن بروتوكول Telnet يتبادل البيانات بطريقة غير مُشفّرة لذلك دائما ما يتم استخدام بروتوكول SSH للجلسات البعيدة Remote Access، ويتم تفعيل SSH عن طريق التعليمات التالية:

```
hostname R1
enable password [password] //set password for enable
Ip domain-name [domain.ex]
Ip ssh version 2
crypto key generate rsa //generate RSA key and use 1024 as modulus
username [username] password [password] // We did it recently
line vty 0 4
transport input ssh
```

ندخل إلى جهاز الحاسب الخاص بالمدير ونختار Telnet/SSH Client ضمن التبويب Desktop:



نُحدد نوع الاتصال

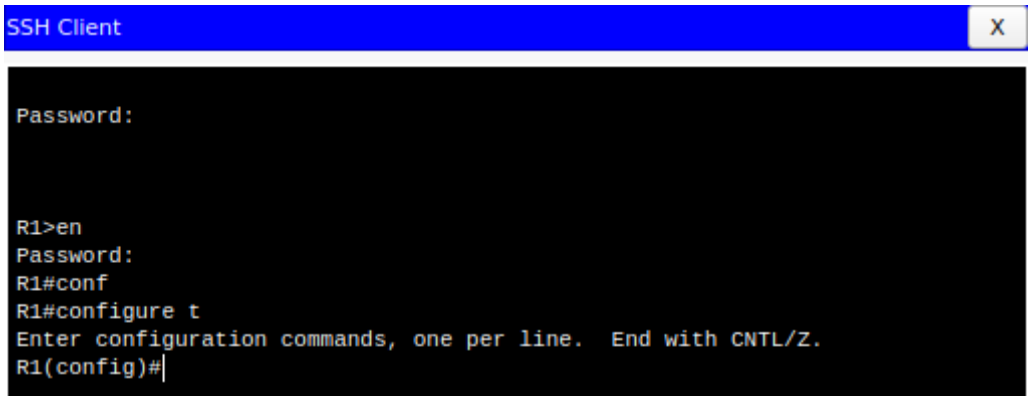


نُحدد نوع الاتصال

عنوان المُوجّه المُراد الوصول إليه عن بُعد

اسم المستخدم الذي تم إعداده ضمن قاعدة البيانات المحليّة ضمن المُوجّه

بعدها نضغط **Connect** وتتم المُطالبة بإدخال كلمة المرور للمُستخدم المُحدّد مُسبقاً وبعدها كلمة المرور الخاصة بوضع **enable** أولاً، وبعدها لا يمكن الدخول إلى الوضع **privileged EXEC** بدون إدخال اسم المستخدم وكلمة المرور اللذين تم إعدادهما لجلسة ال **SSH** في الخطوة السابقة:

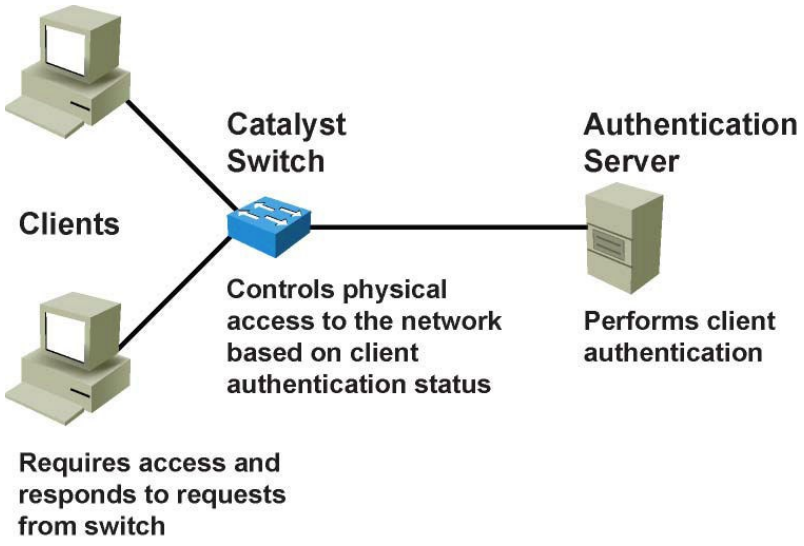


➢ التوثّق عن طريق AAA Server

قُلنا في محاضرة سابقة أن تقنية Port-security تُعاني من عدة مشاكل لذلك تم التوسّع واستخدام تقنية التحقّق من هوية المُستخدم من خلال المنفذ (**Port-Based Authentication**).

تعتمد تقنية التحقّق من هوية المُستخدم من خلال المنفذ على المعيار **IEEE 802.1 X**. (معيار IEEE للتحكّم في الوصول إلى الشبكة المُعتمِد على المنافذ **PNAC: P**ort-based **N**etwork **A**ccess **C**ontrol)).

عند تفعيل التوثّق port-based authentication، لن يُمرِر منفذ المُبدّلة أي حركة بيانات حتى يتم التوثّق من المُستخدم بنجاح.

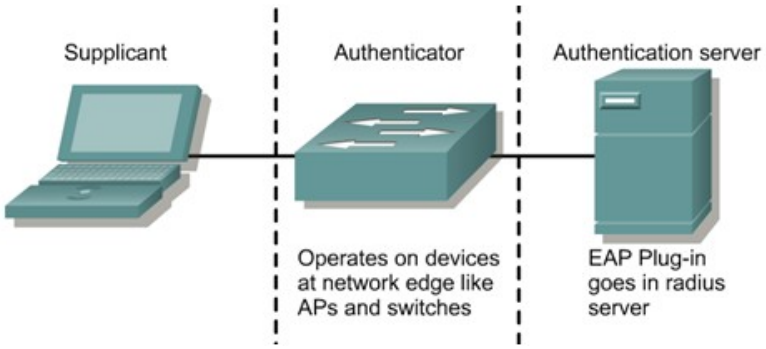


يجب أن يدعم كل من المُبدّلة وجهاز الحاسوب الخاص بالمستخدم النهائي معيار 802.1X ويكون ذلك باستخدام بروتوكول التوثّق القابل للتوسيع عبر الشبكة (Extensible Authentication Protocol over LAN (EAPOL)، وهو LAN بروتوكول طبقة ثانية (layer 2 protocol).

- **هناك نوعان من مُخدّمات التوثّق:**

1. RADIUS (Remote Authentication Dial In User Service): تم تقييسهُ بواسطة IETF.
2. TACACS + (Terminal Access Controller Access-Control System) يقوم بعمل مماثل لكنه مملوك من قِبل شركة Cisco.

✓ 802.1X Roles

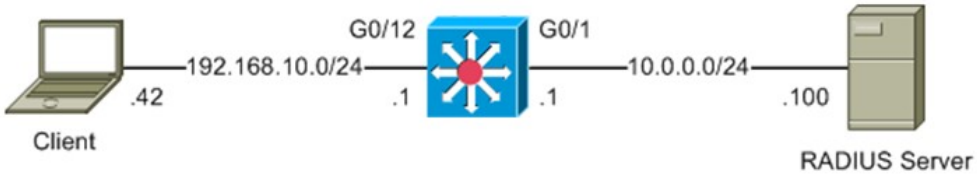


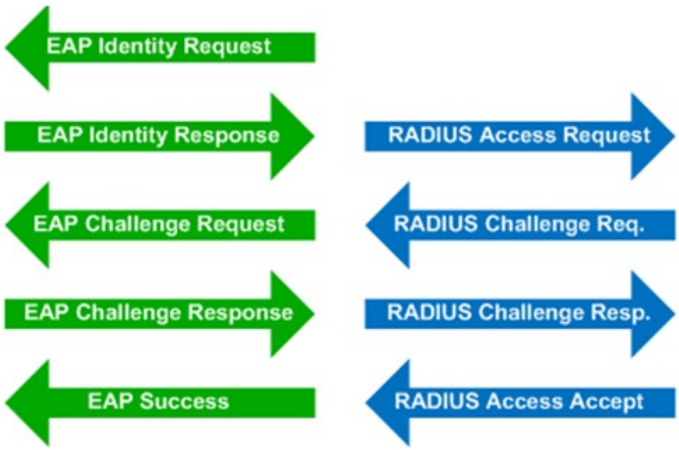
عند استخدام تقنية التحقّق من هوية المُستخدم من خلال المنفذ، يكون للأجهزة في الشبكة أدوار مُحددة، على النحو التالي:

1. **Client:** الجهاز (محطة العمل) الذي يطلب الوصول إلى الشبكة المحلية وخدمات المُبدّلة ثم يستجيب للطلبات الواردة من هذه المُبدّلة.
2. **مُخدّم التوثّق (Authentication Server):** يقوم بإجراء عملية التوثّق الفعلية للزبون Client. يقوم خادم المصادقة بالتحقق من هوية العميل وإخطار المُبدّلة بما إذا كان العميل مُصرّحًا له بالوصول إلى الشبكة المحلية أم لا.
   إنّ خدمة التوثّق تكون شفافة (غير مرئية) بالنسبة لل Client ذلك لإن المُبدّلة تعمل كوكيل (وسيط).
3. **Switch أو Router (يُطلق عليه أيضًا authenticator):** يتحكّم في الوصول الفيزيائيّ إلى الشبكة بناءً على حالة التوثّق من ال Client إذا كانت مسموحة أم لا.

- يتم هذا التوثّق عن طريق مُخدّم توثّق AAA Server وِفق المراحل التالية:

1. يقوم المُستخدم بتأسيس اتصال مع الموجّه أو المُبدّلة.
2. يقوم المُوجّه أو المُبدّلة بطلب اسم المستخدم وكلمة المرور.
3. يتم إرسال اسم المستخدم وكلمة المرور لمُخدّم التوثّق.
4. يقوم مُخدّم التوثّق بالتحقّق من صحة المعلومات المُدخلة.

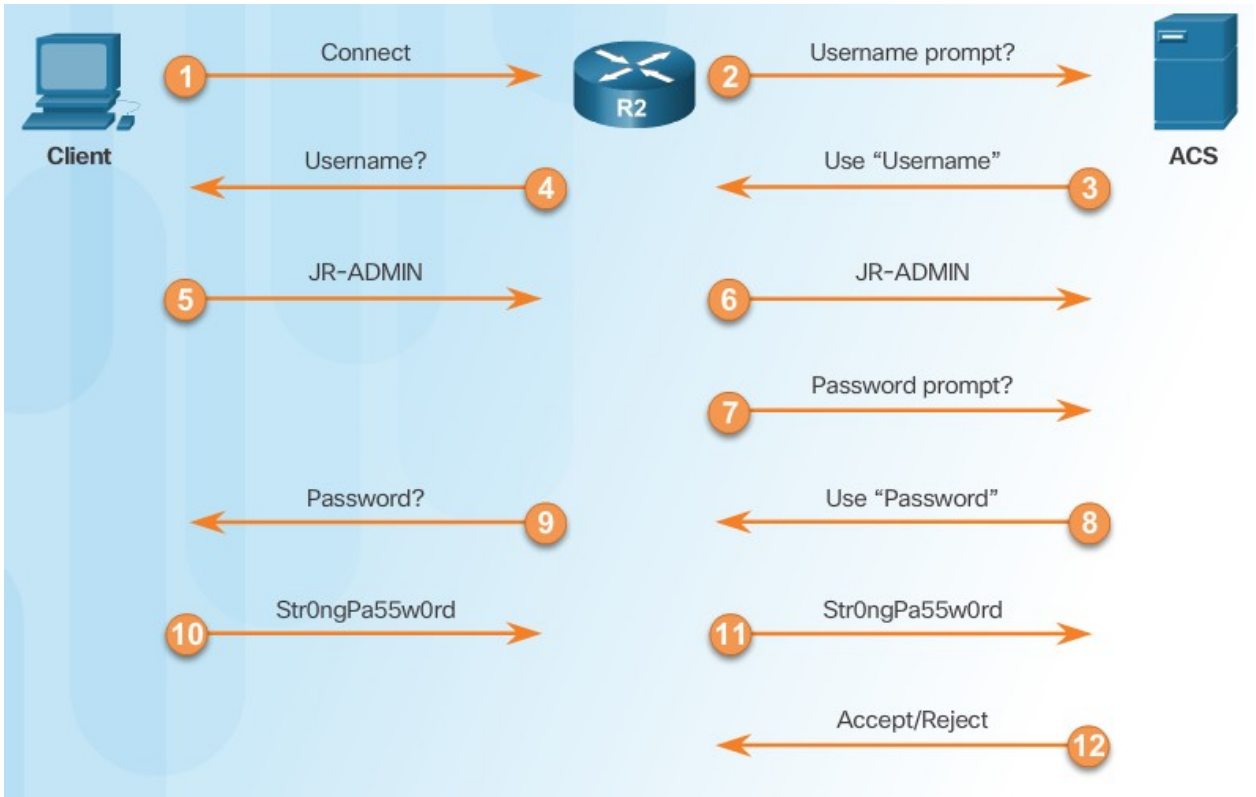




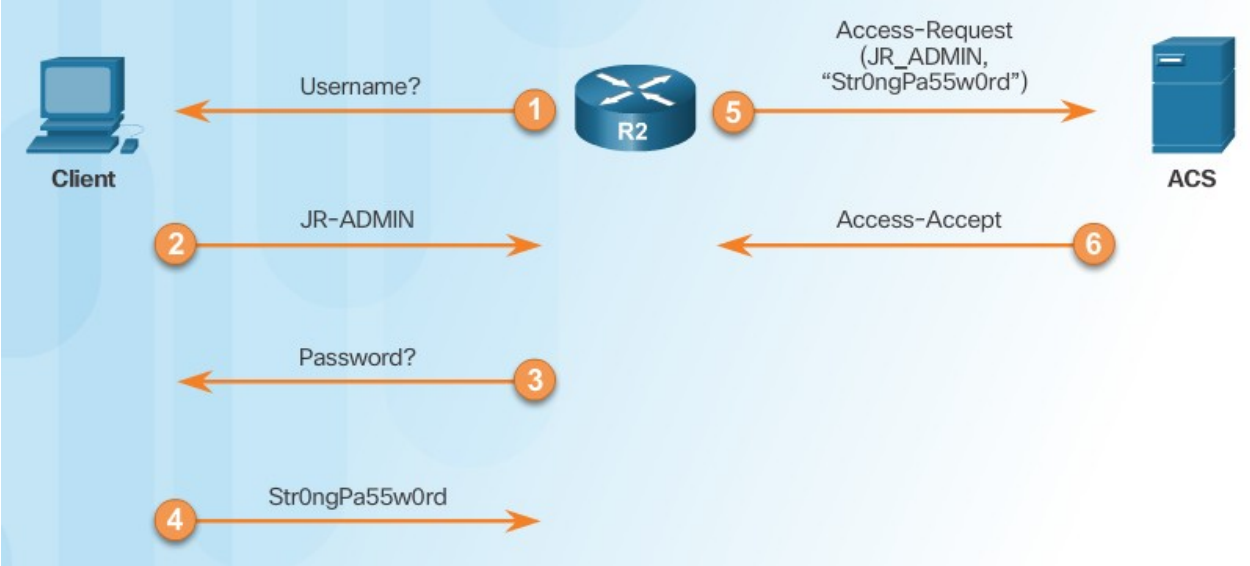
➢ أهم الفروقات بين AAA Servers

	TACACS+	RADIUS
Functionality	Separates AAA according to the AAA architecture, allowing modularity of the security server implementation	Combines authentication and authorization but separates accounting, allowing less flexibility in implementation than TACACS+
Standard	Mostly Cisco supported	Open/RFC standard
Transport Protocol	TCP	UDP
CHAP	Bidirectional challenge and response as used in Challenge Handshake Authentication Protocol (CHAP)	Unidirectional challenge and response from the RADIUS security server to the RADIUS client
Protocol Support	Multiprotocol support	No ARA, no NetBEUI
Confidentiality	Entire packet encrypted	Password encrypted
Customization	Provides authorization of router commands on a per-user or per-group basis	Has no option to authorize router commands on a per-user or per-group basis
Accounting	Limited	Extensive

- **سنوضّح بالصورتين التاليتين الفرق في طريقة التوثّق بين مُخدّمي TACACS+ وRADIUS.**

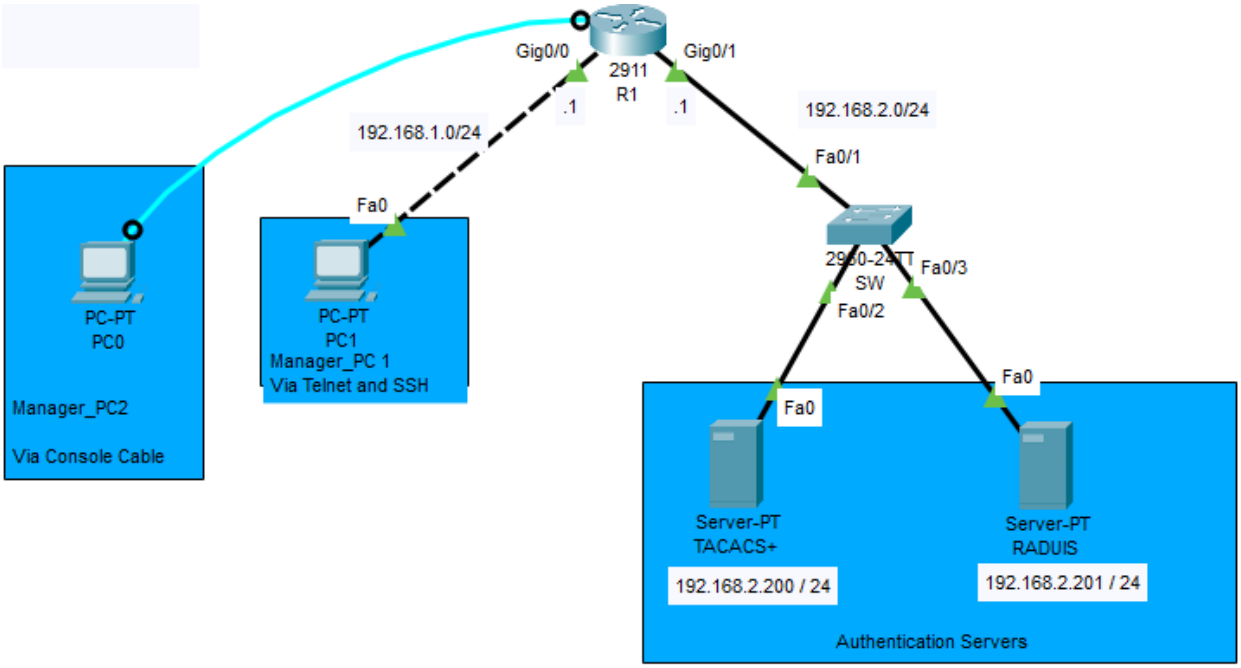


التوثّق عن طريق بروتوكول TACACS+



التوثّق عن طريق بروتوكول RADIUS

➢ التطبيق العملي



شكل طوبولوجيا الشبكة المستخدمة في الجزء العملي

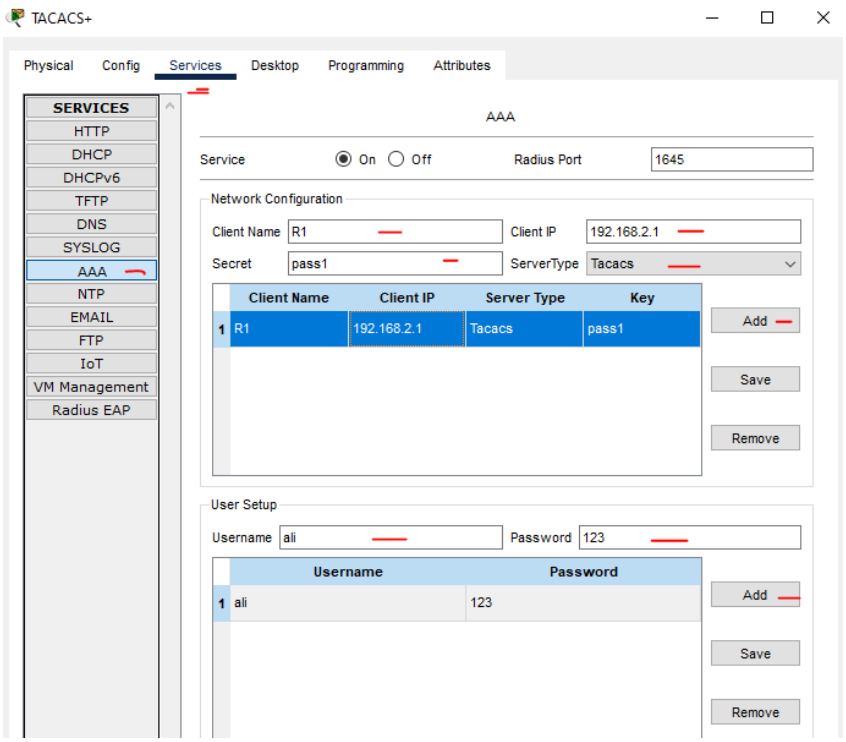
لتطبيق مُخدّم التوثّق على الجهاز الشبكي نقوم بالخطوات التالية:

1. تفعيل آلية التوثّق عن طريق مُخدّم.
2. تفعيل أحد بروتوكولي التوثّق (TACACS/RADIUS).
3. تعريف عنوان المخدم مع المفتاح المُشترك بين المُبدّلة والمُخدّم.
4. تعيين طريقة التوثق عند قيام المستخدمين بعملية Telnet أو SSH ويتم من خلالها التحقّق من اسم المستخدم وكلمة المرور.

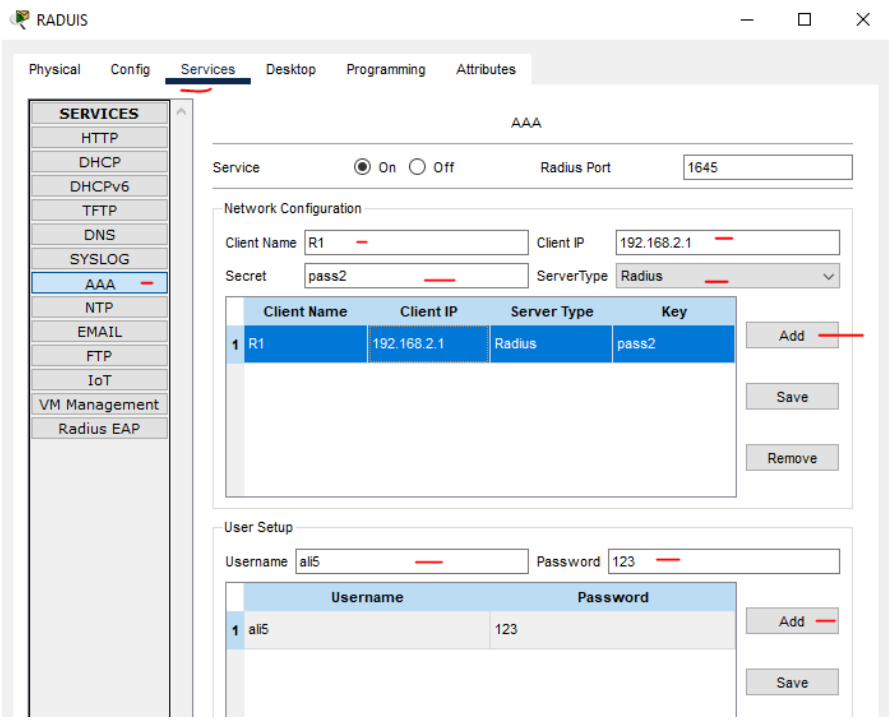
- **إعداد مُخدّمات AAA على المُحاكي Packet Tracer**

نقوم بما يلي لإعداد مُخدّم التوثّق لقبول الجهاز الشبكيّ كوكيل توثّق (Authenticator) وإعداد قاعدة بيانات التوثّق:

1. ننقر على المُخدّم المطلوب إما RADIUS أو TACACS ومن تبويب **services** نختار خدمة AAA ونقوم بتشغيل الخدمة.
2. نقوم بإدخال بيانات المُوجّه أو المُبدّلة (ال Authenticator) في حقول قسم إعدادات الشبكة **network configuration** مثل الاسم والعنوان المنطقي IP للجهاز والمفتاح المشترك الذي سنقوم **بتعيينه على المُوجّه أو المُبدّلة** أيضاً.
3. نذهب بعدها لحقل نوع الخدمة **service type** ونختار TACACS أو RADIUS.
4. يتم بعدها ضمن حقول إعدادات المُستخدم **user setup** إدخال معلومات المُستخدم المطلوبة لتسجيل الدخول مثل اسم المُستخدم وكلمة المرور.



إعداد مُخدّم AAA من نوع **TACACS+** على المُحاكي Packet Tracer



إعداد مُخدّم AAA من نوع **RADIUS** على المُحاكي Packet Tracer

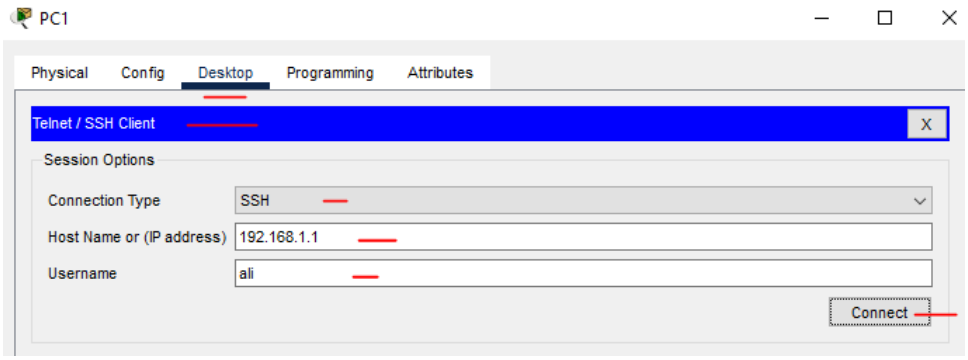
- **إعداد المُوجّه (أو المُبدّلة Authenticator) لاستخدام مُخدّمات AAA**

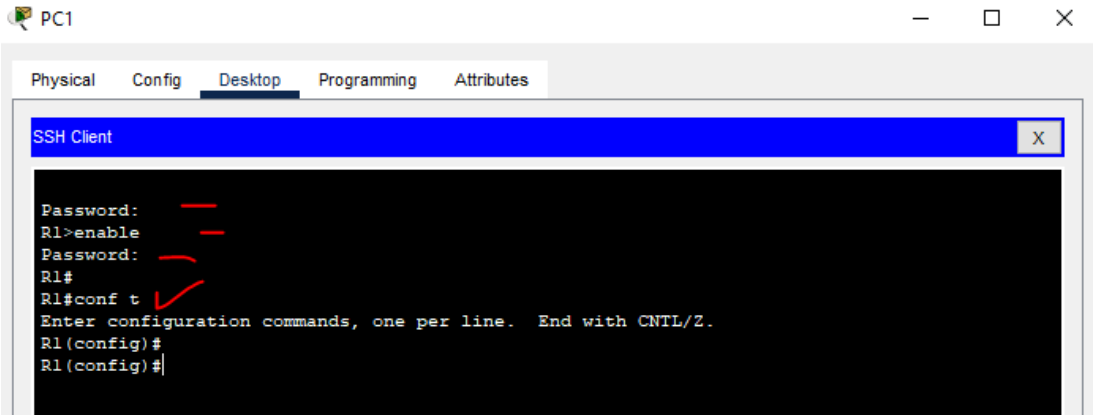
(On Packet Tracer 8.11)

```
enable password [password like 123] //set password for enable
aaa new-model
aaa authentication login auth group tacacs+ group radius
tacacs-server host 192.168.2.200 key pass1 // tacacs+ server IP and the shared key
radius server RADIUS // name the radius configurations any name you want
address 192.168.2.201 // radius server IP
key pass2
exit
line vty 0 4
transport input ssh // to enable ssh only (without telnet)
login authentication auth
```

ملاحظة: لا ننسى طبعاً تطبيق التوجيه المناسب وليكن توجيه ثابت (**Static Routing**) بين الشبكتين 192.168.1.0/24 و 192.168.2.0/24.

ندخل الى جهاز المستخدم ونقوم من تبويب **Desktop** (كما هو موضّح في الصورة التالية أدناه) بفتح **Telnet/SSH Client** ونُرسل طلب **ssh** الى المُوجّه ليقوم بدوره من التحقّق من المستخدم **عن طريق أول مُخدّم AAA مُتاح من المُخدّمات التي أعددناه مُسبقاً** وفتح جلسة اتصال عن بعد.

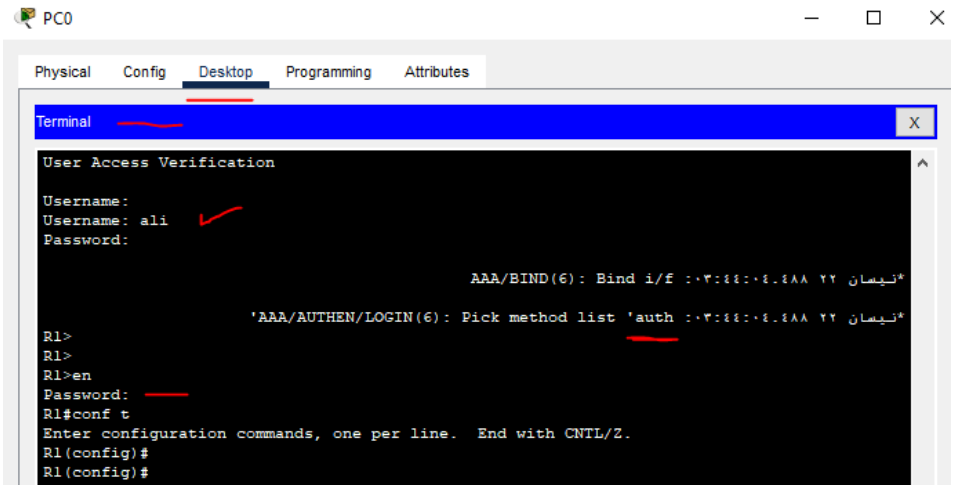




كما يمكن إعداد منفذ ال Console على الموجّه من أجل الدخول عبره (SSH حصراً) كالتالي:

```
R1(config)#line console 0
R1(config-line)#password 123
R1(config-line)#login authentication auth
R1(config-line)#transport output ssh
R1(config-line)#
R1(config-line)#do wr
Building configuration...
[OK]
```

ندخل الان إلى جهاز الحاسب PC0 (من الطوبولوجيا السابقة) ونختار من التبويب Desktop الخيار Terminal ونضغط Ok كي يفتح اتصال محلي Console مع المُوجّه ويُطالبنا باسم المستخدم وكلمة المرور ويتم التحقّق منهما من قبل مُخدّم التوثّق المُتاح:



- للتحقّق من عمل البروتوكول يُمكننا استخدام الأمر كما يلي:

```
debug aaa authentication
```

```
R1#debug aaa authentication
AAA Authentication debugging is on
```

Homework: ☺

Implementing and configuring the previous lab…

???Any Questions