(AAA)

Authentication / Authorization / Accounting

مقدمة:

تستخدم (AAA) في إدارةالمتصلين بالشبكة, ففي مجال الامن (Security) يكون، التحقق ، وتحديد الصلاحيات ، من العناصر المهمة.

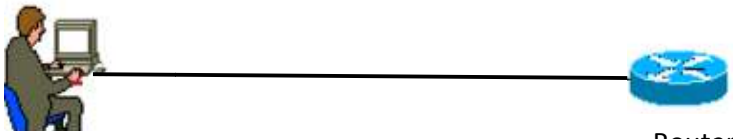
تعريف(AAA) :هي خاصية موجودة في الراوترات(Routers) ووظيفتها الرئيسية إعطاء التصاريح للدخول إلى الشبكة بالإضافة إلى تحديد الصلاحيات لكل شخص يدخل الى الراوتر.

شرح لهذه المفاهيم الهامة:

- Authentication: هي العملية الأولى في الدخول لأي نظام حيث يتم التحقق من اسم المستخدم وكلمة المرور ثم بعد أن يتأكد النظام من أنك مسجل به يسمح لك بالدخول.
- Authorization:في هذه العملية يتم تطبيق صلاحيات معينة على المستخدم (أي مُصرّح للمستخدم أن يفعل كذا ولا يفعل كذا مثل أن يمسح , يضيف , يعمل Show / Ping...الخ).
- Accounting: يتم التسجيل في الراوتر تحركات المستخدم (متى تم دخوله,الأعمال التي يقوم بها ..الخ).

- في عملية Authentication إما ان يدخل المستخدم بـــ

1. اسم المستخدم + كلمة المرورأو
2. كلمة المرور فقط (وهذه الطريقة غير آمنة لأن بمجرد معرفة كلمة المرور يتم الدخول للراوتر و في هذه الطريقة ايضاً اذا قام أي احد بتغيير الاعدادات في الراوتر و ارتكب خطأ ما في الشبكة لن يتم معرفته لمحاسبته)



تفعيل خدمة (AAA) على الراوتر:

- عندما يريد المستخدم الدخول الى الراوتر يرسل اسم المستخدم وكلمة المرور
- نفعل ميزة (AAA) على الراوتر ليتم التحقق من اسم المستخدم وكلمة المرور و معرفة صلاحيات المستخدمين حيث يحتوي الراوتر على قاعدة بيانات بداخلها أسماء المستخدمين و كلمات المرور الخاصة بهم بالإضافة الى صلاحياتهم .

لتفعيل (AAA) على الراوتر نتكتب الأوامر التالية :

```
R# config t
R(config)# username ahmad secret 1234        ------- 1
R(config)#aaa new-model                      --------2
R(config)#aaaauthentication login default local  -------3
R(config)#aaaauthentication attempt max fail 10 -------4
```

1. تم الدخول باسم مستخدم و كلمة المرور لمستخدم معين .
2. تفعيل ميزة (AAA) على الراوتر
3. يتم التحقق من اسم المستخدم وكلمة المرور بالرجوع الى قاعدة البيانات المحلية الموجودة في الراوتر .
4. عدد محاولات الدخول الخاطئة هي 10 محاولات

نقوم بتفعيل هذه الميزة على كل راوتر لكن المشكلة في حال كان لدي 100 راوتر هذا يعني انني سأقوم بتفعيل الميزة على 100 راوتر وسوف يكون لدينا 100 قاعدة بيانات وهذا أمر صعب ومرهق .

ومن هنا يأتي دور السيرفر(server) الـAAAهو عبارة عن برنامج يتم تنصيبه على الويندوز سيرفر،حيث تقدم سيسكو البرنامج الرائع

ACS (Access Control Server)فبعد عملية التنصيب،نبدء بربط الراوترات بهذا السيرفر وستكون الراوترات عبارة عن Clientsتضاف الى السيرفر .

ملاحظات هامة:

1. اذا كان المستخدم محلياً(local) يصل الى الراوتر عن طريق كبل .
2. اما اذا كان بعيد يدخل الى الراوتر عن طريق بروتوكولات (Telnet,SSH)
3. يتم التخاطب بين الراوتر والسيرفر المفعل عليه ACS عن طريق بروتوكولين هما :
   - Radius
   - Tacacs(Terminal Access ControlAccess Control System)

مقارنة بين البروتوكولين Radius وTacacs:

Radius	Tacacs
1. يمكن استخدامه مع جميع الأجهزة ومن بينها أجهزة سيسكو	1. خاص بأجهزة سيسكو فقط
2. يستخدم بروتوكول الـUDP	2. يستخدمبروتوكولالـTCP
3. يقوم بتشفير كلمةالمرور فقط	3. يقوم بتشفير عملية الإرسال بشكل كامل وهذا يشمل كل المعلومات المرسلة من وإلى السيرفر ومن بينها اسم المستخدم وكلمة المرور والتصاريح المرسلة
4. يقوم بدمج الـauthentication, authorizationبخطوةواحدة	4. يتعامل مع كل خاصية بشكل مستقل وهذا يشمل الخواص الثلاث
5. يعمل على البورت 1645او1812للـauthentication و1646او1813للـauthorization	5. يعمل على البورت 49فقط

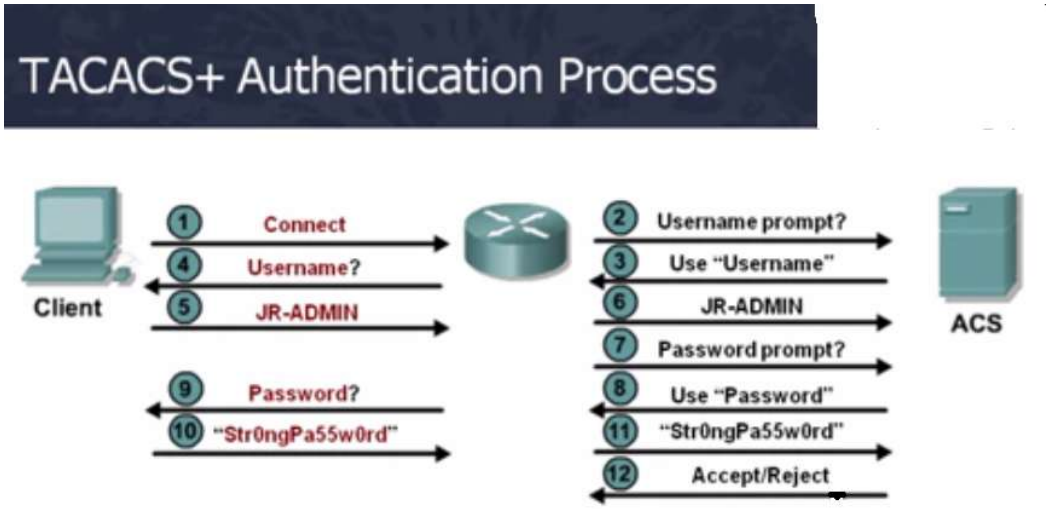
آلية الدخول باستخدام بروتوكول Radius:

1. عندما يريد المستخدم أن يتصل بالراوتر يرسل اسم المستخدم وكلمة المرور الى الراوتر ثم يرسل الراوتر بدوره هذه المعلومات الى السيرفر
2. السيرفر سيتحقق من صحة المعلومات المرسلة اذا كانت متوفرة سيسمح لهذا المستخدم بالوصول الى الراوتر ولكن ضمن صلاحيات محددة مسبقا من قبل نفس الراوتر ..

- Works in both local and roaming situations
- Uses UDP ports 1645 or 1812 for authentication and UDP ports 1646 or 1813 for accounting

آلية الدخول باستخدام بروتوكولTacacs:

1. يرسل المستخدم للراوتر اسم المستخدم أولا و الراوتر بدوره يرسله للسيرفر للتحقق منه
2. السيرفر يعيد للراوتر عن طريق بروتوكول Tacacsأنه تم التأكد من اسم المستخدم ثم الراوتر يعيده للمستخدم.
3. ثم يرسل المستخدم للراوتر كلمة المرور ثانياً و الراوتر بدوره يرسلها للسيرفر للتحقق منها
4. السيرفر يعيد للراوتر أنه تم التحقق من كلمة المرور ثم الراوتر يعيد ذلك للمستخدم.



- Provides separate AAA services
- Utilizes TCP port 49

بالتوفيق ...