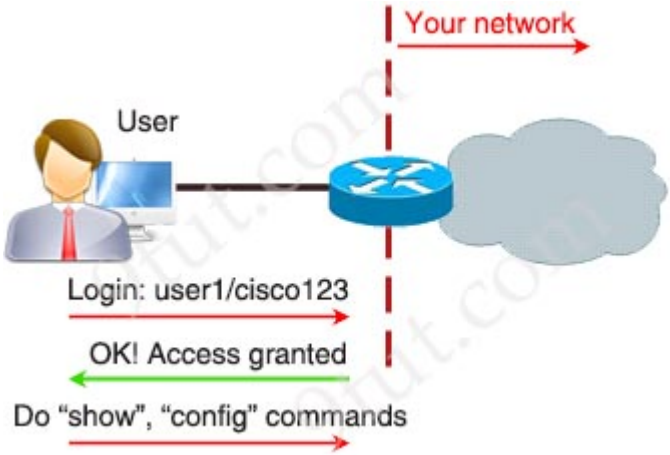
AAA TACACS+ and RADIUS Tutorial

October 18th, 2018 Go to comments

Nowadays, security plays an important role in a company. Without any security solution implementation on our network, a user can simply “plug and play” into our network. The user may simple pick up a valid IP address or be assigned one automatically via DHCP. It is convenient, but not a good way if your network contains sensitive data. Worse, this user may have all the rights to your network so he can do dangerous things.

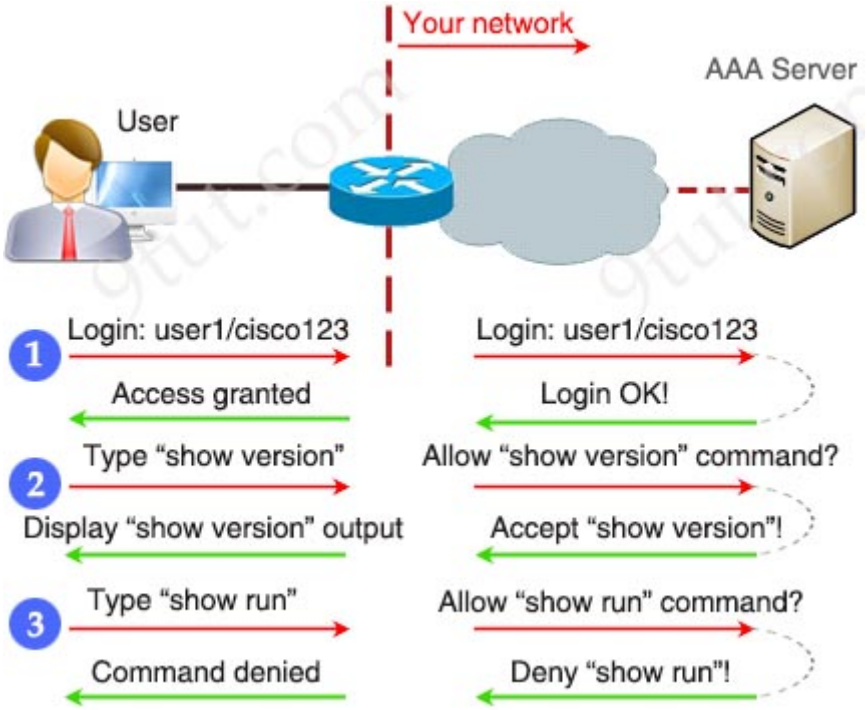
When your company grows bigger and bigger, there is a moment that you need to consider implementing security to your network. There are many ways to secure a network but AAA offers a complete solution. In this tutorial let’s find out about this security feature.

Before diving into AAA, let’s take an example of a user who wants to connect to our network.



This process uses a login and password on the access line. Although it is very easy to implement, but there are many disadvantages of using this method:
+ Insecure login method
+ Vulnerable to brute-force attacks
+ No accountability
+ Must be configured on each device manually
+ Store usernames & passwords locally on each device
+ Cannot limit which specific commands are not used

With AAA, now the process of a user connecting to our network is shown below:



Every action the users do must be submitted to the AAA server to determine if they are allowed or not. This process has many advantages:
+ Secure login (AAA server is not exposed to users and only some protocols are allowed to be sent initially)
+ Easy management at one or some centralized servers
+ Firewalls or other security devices can be placed before AAA servers to protect them
+ Can accept or reject specific commands
+ Every command typed by users can be logged for later analysis

Disadvantages:
+ Require powerful server (to handle all the traffic and requests)

AAA stands for Authentication, Authorization and Accounting.

+ **Authentication:** Specify who you are (usually via login username & password)
+ **Authorization**: Specify what actions you can do, what resource you can access
+ **Accounting**: Monitor what you do, how long you do it (can be used for billing and auditing)

An example of AAA is shown below:

+ **Authentication:** "I am a normal user. My username/password is **user_tom/learnforever**"
+ **Authorization**: "**user_tom** can access **LearnCCNA** server via **HTTP** and **FTP**"
+ **Accounting**: "**user_tom** accessed **LearnCCNA** server for **2 hours**". This user only uses "show" commands.

With AAA, users must authenticate before getting an IP address to access the network. Otherwise, they can only use specific protocols to continue authenticating

For authentication we can do via local database, 802.1x standard (which was developed to provide a method to authenticate devices attempting to access a switchport/LAN) or via remote AAA servers. There are two popular client/server AAA protocols to communicate between remote AAA servers and authenticating devices:

+ **RADIUS** (Remote Authentication Dial In User Service)
+ **TACACS+** (Terminal Access Controller Access-Control System)

The comparison of two protocols is listed below:

	RADIUS	**TACACS+**

Transportation & Ports	**UDP** port 1812/1645 (Authentication) 1813/1646 (Accounting)	**TCP** port 49
Encryption	only passwords	entire payload of each packet (leaving only the TACACS+ header in cleartext)
Standards	Open standard	Cisco proprietary (but actually now it is an open standard defined by RFC1492)
Operation	**Authentication and authorization are combined** in one function (packet)	**authentication, authorization and accounting are separated**
Logging	No command logging	Full command logging (commands typed by users can be recorded on the servers)

Note:
+ RADIUS is very old protocol (created around the early 1990s) and it was originally designed for dial-in modem connections. In these old days, security is not a strong concern so RADIUS encrypts only the authentication information (passwords) along the traffic path.
+ TACACS+ is a newer version of TACAS and XTACAS. It is the answer of Cisco to RADIUS.
+ Both RADIUS and TACACS+ support Extensible Authentication Protocol (EAP), which is an authentication framework frequently used in wireless networks and point-to-point connections
+ Both TACACS+ and RADIUS can run on either Windows or Unix/Linux servers
+ TACACS+ separates the authentication, authorization, and accounting steps. This architecture allows for separate authentication solutions while still using TACACS+ for authorization and accounting.
+ Authentication and authorization are not separated in a RADIUS transaction. When the authentication request is sent to a AAA server, the AAA client expects to have the authorization result sent back in reply.
+ TACACS+ supports access-level authorization for commands. That means you can assign privilege levels when a user logins successfully.

In the next part we will learn how to configure AAA.

1. Zoarexpro
   February 17th, 2020

   Glad to tell you PASSED my exam, 866 points, on 14th Feb 2020.
   lots of the questions from here but not entirely from here. there were many new technology infrastructure questions. Sims and drag and drop concepts are in here but still not exactly like what you see them in here. Exam time was sufficient. if you wisely use it, you can even be done before time. I had about 20 min answering my last questing.

2. Anonymous
   February 27th, 2020

   Hi Guys,

   Any advice for me as a beginner for this tutorial?
   what will be the first topic/s i need to study in order to understand the basic networking?

3. kevin
   July 14th, 2020

   Hello, In the book Official Cert Guide CCNA 200-301 there is no configuration for AAA TACACS+ and RADIUS, just a very brief introduction to them. Do you know if the configuration for AAA TACACS+ and RADIUS is still part of the exam?

4. miau
   March 5th, 2022

   miau?

Comment pages
« Previous 1 2 4228
Add a Comment
Name

Submit Comment
Subscribe to comments feed
Drag and Drop 4 CCNAv3 – New Questions

Premium Member Zone

Welcome Gurjeet singh!

- Welcome Premium Member
- CCNA – New Questions Part 5
- CCNA – New Questions Part 6
- CCNA – New Questions Part 7
- CCNA – New Questions Part 8
- CCNA – New Questions Part 9
- Composite Quizzes

- Logout

CCNA 200-301

- Basic Questions
- Topology Architecture Questions
- Cloud & Virtualization Questions
- CDP & LLDP Questions
- Switch Questions
- VLAN & Trunking Questions
- VLAN & Trunking Questions 2
- STP & VTP Questions
- EtherChannel Questions
- TCP & UDP Questions
- IP Address & Subnetting Questions
- IP Routing Questions
- IP Routing Questions 2
- OSPF Questions
- OSPF Questions 2

- EIGRP Questions
- NAT Questions
- NTP Questions
- Syslog Questions
- HSRP Questions
- Access-list Questions
- AAA Questions
- Security Questions
- Security Questions 2
- DAI Questions
- IPv6 Questions
- DNS Questions
- QoS Questions
- Port Security Questions
- Wireless Questions
- Wireless Questions 2
- SDN Questions
- DNA Center Questions
- Drag Drop Questions
- Drag Drop Questions 2
- Drag Drop Questions 3
- VPN Questions
- DHCP Questions
- Automation Questions
- Miscellaneous Questions
- CCNA FAQs & Tips
- Share your new CCNA Experience

CCNA Self-Study

- Practice CCNA GNS3 Labs
- CCNA Knowledge
- CCNA Lab Challenges
- Puppet Tutorial
- Chef Tutorial
- Ansible Tutorial
- JSON Tutorial
- Layer 2 Threats and Security Features
- AAA TACACS+ and RADIUS Tutorial
- STP Root Port Election Tutorial
- GRE Tunnel Tutorial
- Basic MPLS Tutorial
- TCP and UDP Tutorial
- Border Gateway Protocol BGP Tutorial
- Point to Point Protocol (PPP) Tutorial
- WAN Tutorial
- DHCP Tutorial
- Simple Network Management Protocol SNMP Tutorial
- Syslog Tutorial
- Gateway Load Balancing Protocol GLBP Tutorial
- EtherChannel Tutorial
- Hot Standby Router Protocol HSRP Tutorial
- InterVLAN Routing Tutorial
- Cisco Command Line Interface CLI
- Cisco Router Boot Sequence Tutorial
- OSI Model Tutorial
- Subnetting Tutorial – Subnetting Made Easy

- Frame Relay Tutorial
- Wireless Tutorial
- Virtual Local Area Network VLAN Tutorial
- VLAN Trunking Protocol VTP Tutorial
- IPv6 Tutorial
- Rapid Spanning Tree Protocol RSTP Tutorial
- Spanning Tree Protocol STP Tutorial
- Network Address Translation NAT Tutorial
- Access List Tutorial
- RIP Tutorial
- EIGRP Tutorial
- OSPF Tutorial

Network Resources

- Free Router Simulators
  - CCNA Website
  - ENCOR Website
  - ENSDWI Website
  - ENARSI Website
  - DevNet Website
  - CCIE R&S Website
  - Security Website
  - Wireless Website
  - Design Website
  - Data Center Website
  - Service Provider Website
  - Collaboration Website

Top