**Authentication**

Identification: process of providing the identity of a subject or user (providing a username, a passport, an IP address, or even pronouncing your name);

**Three categories of factors:**

* Knowledge: something the users knows
* Possession: something a user has
* Characteristics: something the user is

**Authentication by Knowledge**

* **Example:** it could bea user providing a password, a personal identification number PIN code, or an answer to a question
* The authentication strength of a password is a function of its length, complexity and unpredictability

**Authentication by ownership or possession**

**Examples:**

* **One time-passcode OTP:** set of characteristics that can be used to prove a subject’s identity one time and one time only; it is valid for only one access. OTP may be delivered via email, text message, or phone call to a predetermined address or phone number
* **A memory card:** is an authentication mechanism that holds user information within a magnetic strip and relies on a reader to process the information. The user inserts the card into the reader and enters a personal identification number (PIN).
* **A smartcard: i**nstead of a magnetic strip, it has a microprocessor  
  and integrated circuits. The user inserts the card into a reader, which has electrical contacts that interface with the card and power the processor. The user enters a PIN that unlocks the information. The card can hold the user’s private key, generate an OTP, or respond to a challenge-response.
* **Out-of-band authentication:** For example, a user enters her name and password at an application logon prompt (factor 1). The user then receives a call on her mobile phone; the user answers and provides a predetermined code (factor 2). For the authentication to be compromised, the attacker would have to have access to both the computer and the phone

**Authentication by Characteristic**

A system that uses authentication by characteristic authenticates the user based on some physical or behavioral characteristic, sometimes referred to as a biometric attribute. The most used physical or physiological characteristics are as follows:

* Fingerprints
* Face recognition
* Retina and iris
* Palm and hand geometry
* Blood and vascular information
* Voice recognition

**Multifactor Authentication:** Two or more factors are presented.

**Duo Security:**

* company acquired by cisco that develops a very popular multifactor authentication solution that is used by many small, medium, and large organizations
* protection of on-premises and cloud-based applications
* This is done by both preconfigured solutions and generic configurations RADIUS, Security Assertion Markup Language SAML, LDAP
* SAML: open standard for exchanging authentication and authorization data between identity providers.

**Duo Access Gateway:** another component of the duo solution that provides multifactor authenticator access to cloud applications

**Zero Trust security framework:** allows administrators to consistently enforce policy-based and maintain visibility of users and systems across the entire environment. It help you to prevent unauthorized access through your network. It is also providing detailed logs, reports, and alerts that can help security professionals better detect and respond to threats

**Single Sign On SSO**: help you to access dozens of applications throughout an enterprise network or even applications hosted in the cloud. The user only needs to authenticate one and he can access any other application that is a participant on the SSO implementation.

**Authorization**

Authorization is the process of assigning authenticated subjects permits to carry out a specific operation.

Authorization process would check the permissions associated with the subject/object pair so that the correct access right is provided

Trois principaux modèles d'autorisation sont : la capacité des objets, les étiquettes de sécurité et les ACL.

* La capacité d'un objet est utilisée de manière programmable et repose sur la combinaison d'une référence infalsifiable et d'un message opérationnel.
* (Security Labels) Les étiquettes de sécurité sont des contrôles d'accès obligatoires intégrés dans les propriétés des objets et des sujets.
* Les listes de contrôle d'accès (ACL) sont utilisées pour déterminer l'accès en fonction d'une combinaison de critères spécifiques, tels qu'un identifiant d'utilisateur, l'appartenance à un groupe, la classification, l'emplacement, l'adresse et la date.

**Authorization policy:**

Implicit deny: if no rule is specified for the transaction of the subject/object, the authorization policy should deny the transaction

Needed to know: A subject should be granted access to an object only if the access is needed to carry out the job of subject

Access controls categories

**Mandatory Access Control (MAC)**

Use in secure military and government systems that require a high degree of confidentiality.

Objects are assigned a security label that indicates the classification and category of the resource. Subjects are assigned a security label that indicates a clearance level and assigned categories. The operating system compares the object’s security label with the subject’s security label. The subject’s clearance must be equal to or greater than the object’s classification. The category must match.

**Discretionary Access control DAC**

Use in commercial operating systems

The object owner builds an ACL that allows or denies access to the object based on the user’s unique identity. The ACL can reference a user ID or a group that the user is a member of. Permission can be cumulative

**Role-based Access Control RBAC**

Access permissions are based on a specific role or function. Administrators grant access rights and permissions to roles. Ex: Engineer inherits all the permissions assigned to the engineer role.

**Rule-based Access Control**

Access is based on criteria that are independent of the user or group account. The rules are determined by the resource owner. Used criteria include source or destination address, geographic location, and time of day.

Attribute-based Access control ABAC (incompris)

**Accounting**

* Process of auditing and monitoring what user does once a specific resource is accessed

**Infrastructure Access Control**

This includes physical and logical network designs, border devices, communications mechanisms and host security settings.

**Access Control Mechanisms**

* **Access control list (ACL):** can apply to files, in routers, firewalls

In Cisco routers and firewalls an ACL is a collection of security rules or policies that allows or denies  
packets after looking at the packet headers and other attributes. Each permit or deny statement in the ACL is referred to as an access control entry (ACE)

* **Capability table**: collection of objects that a subject can access; together with the granted permissions
* **Access control matrix (ACM)**: includes three elements: the subject, the object, and the set of permissions. An ACM could be seen as a collection of access control list or a collection of capabilities table, depending on how you want to read it
* **Content-dependent access control:** uses the information (content) within a resource to make an authorization decision.

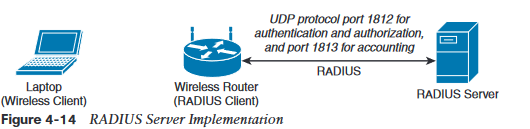
**AAA Protocols**

AAA protocols are used to grant access to networks or systems, provide information about  
access rights, and provide capabilities used to monitor, audit, and account for user actions  
once authenticated and authorized.

**AAA protocols: RADIUS, TACACS+, Diameter**

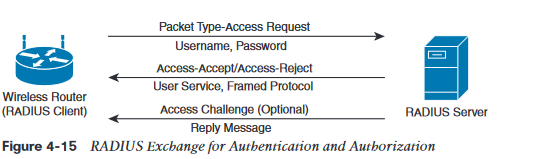
**RADIUS: Remote Authentication Dial-In User Service**

* Authentication and authorizations parts are specified in RFC 2865, accounting part is specified in RFC 2866
* Radius is a client-server protocol
* The client is an access server, which is the entity to which a user sends the access request
* Radius operates in most cases over UDP protocol port 1812 for authentication and authorization, and port 1813 for accounting



**Authentication and authorization phase:**

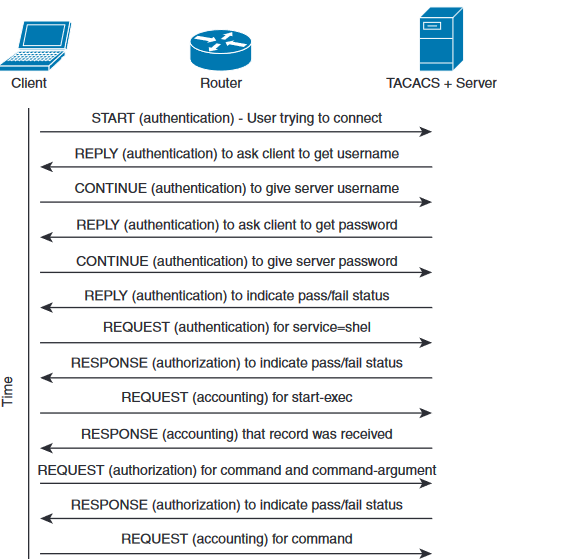
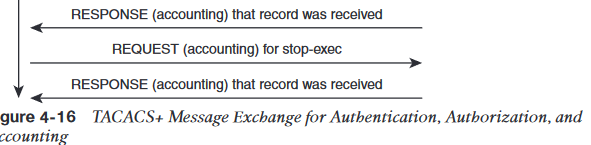
* Access server send an access-request to the radius server that includes the user identity, the password, and other information (ip address for example)
* Radius server may reply with three different messages:
* Access-accept if the user is authenticated
* Access-reject if access for the user is rejected
* Access-challenge if additional information is needed

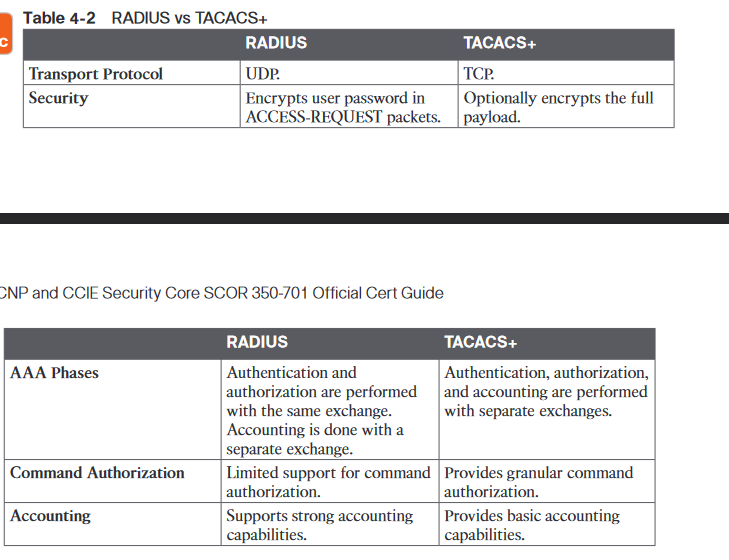


* Accounting exchange consists of two messages: accounting-request and accounting-response
* Radius exchange is authenticated by using a shared key between the access server and the radius server.
* Only the user password information in the access-request is encrypted. (the rest of the packets are sent in plaintext)

**TACACS+ Terminal Access Controller Access Control System Plus**

* Proprietary protocol developed by cisco
* Client server model
* Uses TCP as the transport protocol, and the TACACS+ server listens on port 49
* Using TCP ensure a more reliable connection and fault tolerance
* Tacacs+ use start, reply and continue packets during the authentication process, request and response during the authorization and accounting process

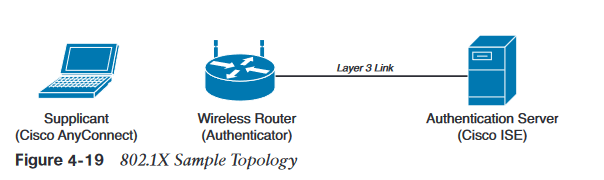
 



Diameter (A relire)

802.1X

* IEEE standard that is used to implement port-based access control
* 802.1X access device will allow traffic on the port only after the device has been authenticated and authorized
* Three main roles are defined:
  + Authentication server: entity that provides an authentication service to an authenticator (ex: Cisco Identity Service Engine ISE)
  + Supplicant: entity that seeks to be authenticated by an authenticator (ex: client laptop connected to a switch port)
  + Authenticator: entity that facilitates authentication of other entities attached to the same LAN. (ex: Cisco switches, wireless routers and access points)

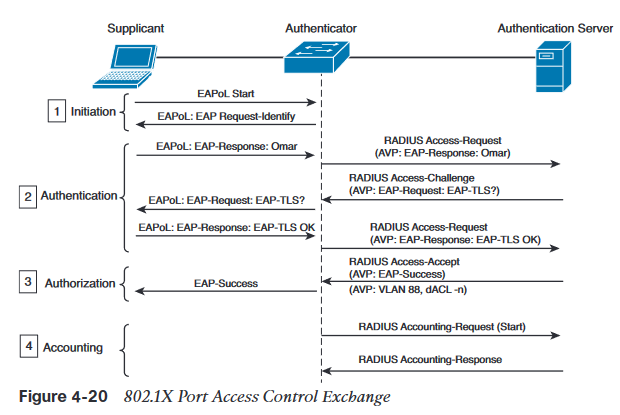


802.1X protocols

* EAP over LAN (EAPoL): encapsulation defined in 802.1X that’s used to encapsulated EAP packets to be transmitted from the supplicant to the authenticator
* Extensible Authentication Protocol (EAP): authentication protocol used between the supplicant and the server to transmit authentication information
* Radius or diameter: AAA protocol used for communication between the authenticator and authentication server

802.1X port-based access control includes four phases

* Session initiation: the session can be initiated either by the authenticator with an EAP-Request-Identity message or by the supplicant with an EAPoL-Start message
* Session authentication: the authenticator extracts the EAP message from the EAPoL frame and send a RADIUS Access-Request to the authentication server. The supplicant may provide a password, a certificate, a token, and so on.
* Session authorization:
* Session accounting:



**Networking Access Control List and Firewalling**

* **Network ACL** can be implemented at layer2, 3, 4
* **Vlan Acl:** used to limit the traffic within a specific vlan
* **Security group-**based ACL: is an ACL that impements access control based on the security group assigned to a user
* **Downloadable ACL:** the term downloadable stems from the fact that these ACLs are pushed from the authenticator server during the authorization phase

**Cisco Identity Services Engine ISE**

* It is the centralized AAA and policy engine solution from Cisco
* Allow you to maintain visibility of who and what is accessing your network, and to enforce access control consistently.

Cisco Platform Exchange Grid (pas compris)

**Cisco ISE Profiling Services**:

* this functionality allows you to dynamically detect and classify endpoints connected to the network.
* Cisco ISE uses Mac addresses as the unique identifier and captures various attributes for each network endpoint that are stored in an internal endpoint database. These attributes and setting are then correlated to an extensive library of profiles (laptop, ip phones, operating systems…)
* After the endpoint are classified, they can be authorized to the network and granted access based on their profile

**Cisco ISE Identity Services**

Identity and authentication information can be gathered in several ways:

* + 802.1X
  + VPN access with radius authentication
  + Cisco ASA identity firewall
  + Web authentication
  + MAC Authentication Bypass
  + TrustSec Security Group Tags
  + Unauthenticated or authenticated guest access

**Cisco TrustSec**

* Is a solution and architecture that provides the ability to perform network segmentation and enable access controls primarily based on the role of the user requesting access to the network
* Component of the cisco TrustSec Architecture:
  + Each device in a trustSec environment is authenticated by its peers, creating a trusted domain
  + Security group tag SGT is assigned to sources and destinations
  + 802.1AE Media Access Control Security MACSec is used to encrypt communication on each link

**Posture Assessment**

It includes a set of rules in a security policy that define a series of checks before an endpoint is granted access to the network

Posture assessment checks include the installation of operating system patches, host-based firewalls, antivirus and anti-malware…

Three agents can be used for posture assessment:

* **Temporal Agent**: no permanent software is installed on the endpoint. This is ideal for guest or contractor endpoints. It supports a limited number of posture conditions
* **Stealth AnyConnect:** does not provide any gui
* **AnyConnect:** provides support for most posture conditions, automatic, remediation and passive reassessment

**Change of Authorization CoA**

* RADIUS CoA is a feature that allow a Radius server to adjust an active client session.
* ISE can issue the CoA Radius attribute to an access device to force the session to be reauthenticated
* When a vulnerability event is received for an endpoint Cisco ISE can automatically trigger CoA for that endpoint.

TC-NAC (Threat Centric Network Access Control): feature enables you to have visibility into any vulnerable hosts on your network and to toke dynamic network quarantine actions when required.

Ex: the use of coa when the TCNAC detects a vulnerability

Terms

* **Network Access Server (NAS**): device providing access to the network
* **Dynamic Authorization Client (DAC):** entity originating the CoA Requests or Disconnect Requests. (Can be a co-resident within a RADIUS server)
* **Dynamic Authorization Server (DAS):** entity receiving CoA-Request or disconnect-Requests packets. The DAS may be a NAS or a Radius proxy