Limitations of Local Security Configuration

- Configuring line level security or local usernames on each device has a serious scalability limitation
- If a password has to be added, changed or removed it needs to be done on all devices
- An external AAA server can be used to centralise this instead
- Multiple AAA servers can be implemented for redundancy

Authentication, Authorization & Accounting

- AAA servers provide Authentication, Authorization and Accounting.
- Authentication verifies somebody is who they say they are. This is most commonly achieved with a username and password.
- Authorization specifies what a particular user is allowed to do, such as running a particular command.
- Accounting keeps track of the actions a user has carried out.
- Authorization and Accounting are optional. Authentication is mandatory if Authorization and/or Accounting are used.

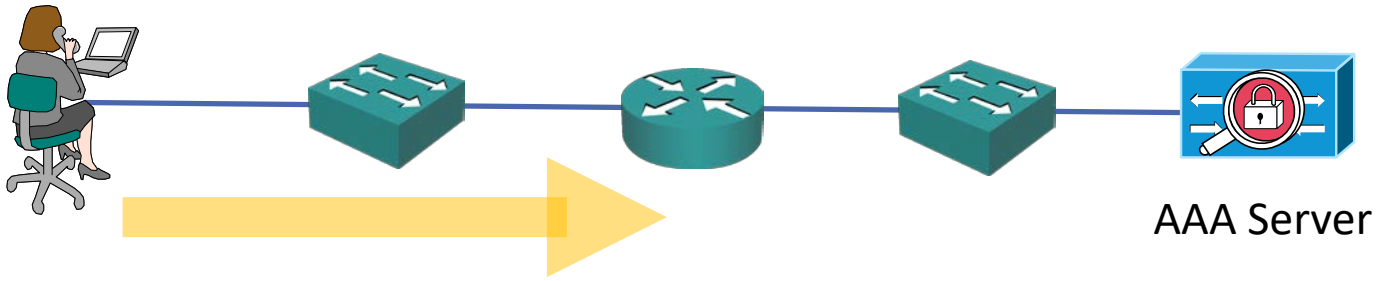
RADIUS and TACACS+

- The protocols which are used for AAA services are RADIUS and TACACS+
- Both are open standards, although vendors may add their own proprietary extensions
- Many vendor's AAA servers support both protocols
- RADIUS is commonly used for end user level services, such as VPN access
- TACACS+ is commonly used for administrator access on Cisco devices as it has more granular authorization capabilities

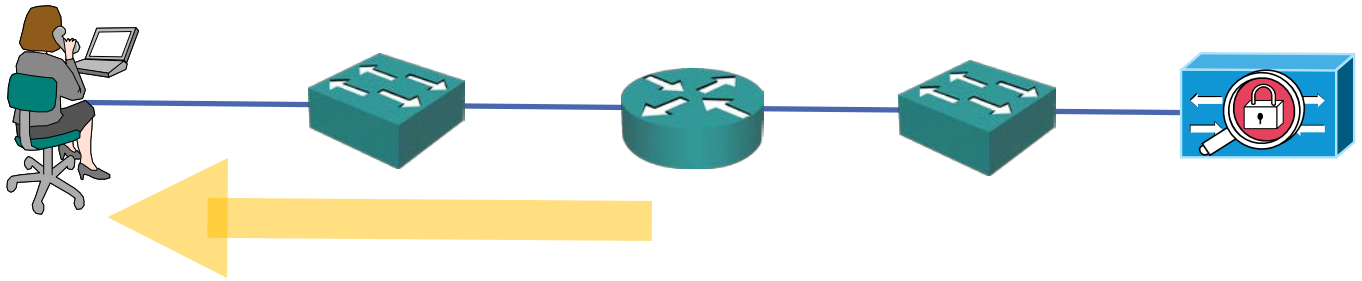
Cisco AAA Servers

- Cisco's AAA server is the Identity Services Engine (ISE)
- They also offered the Access Control Server (ACS) for a long time but it is now end of sale

How AAA Works

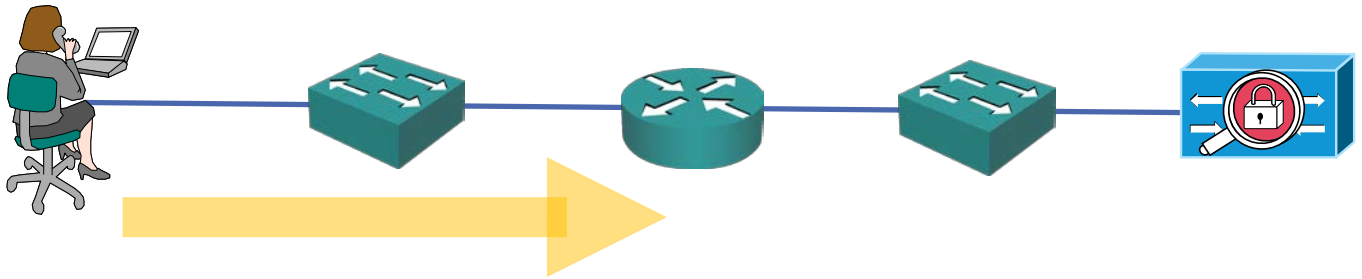


How AAA Works



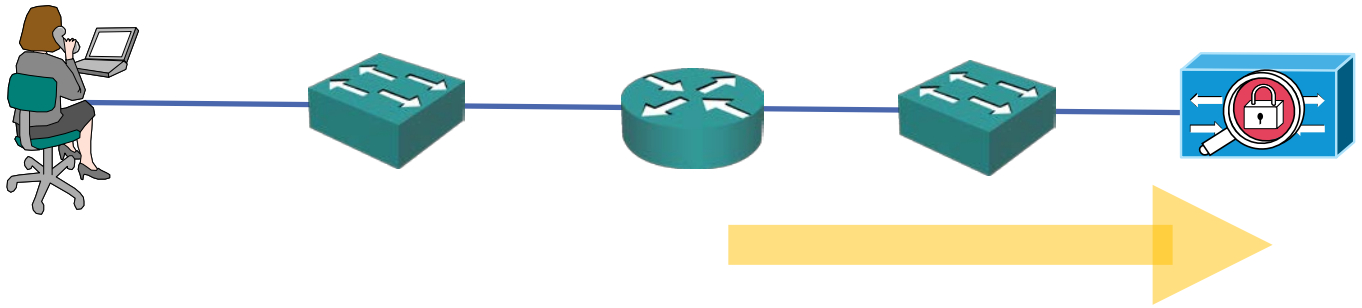
Challenge in
Telnet / SSH session

How AAA Works



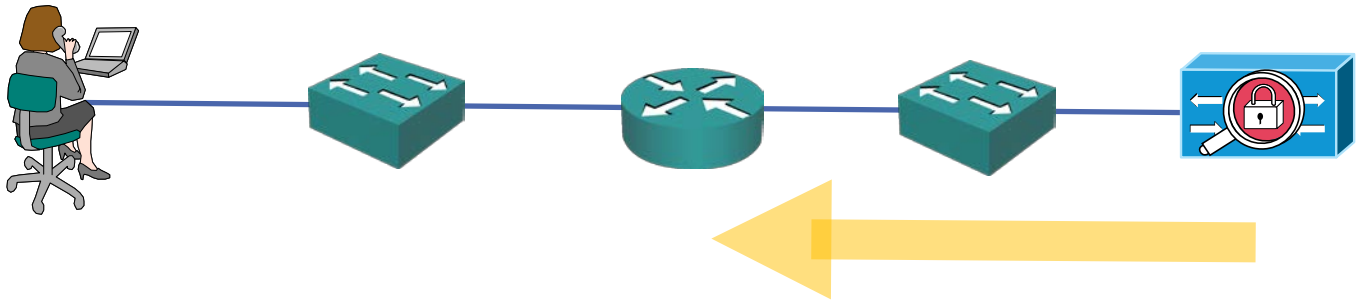
Username & Password

How AAA Works



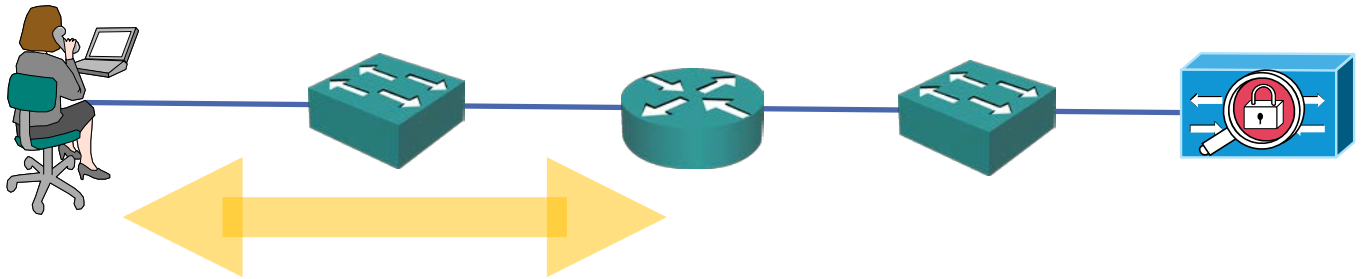
Username & Password
(RADIUS / TACACS+)

How AAA Works

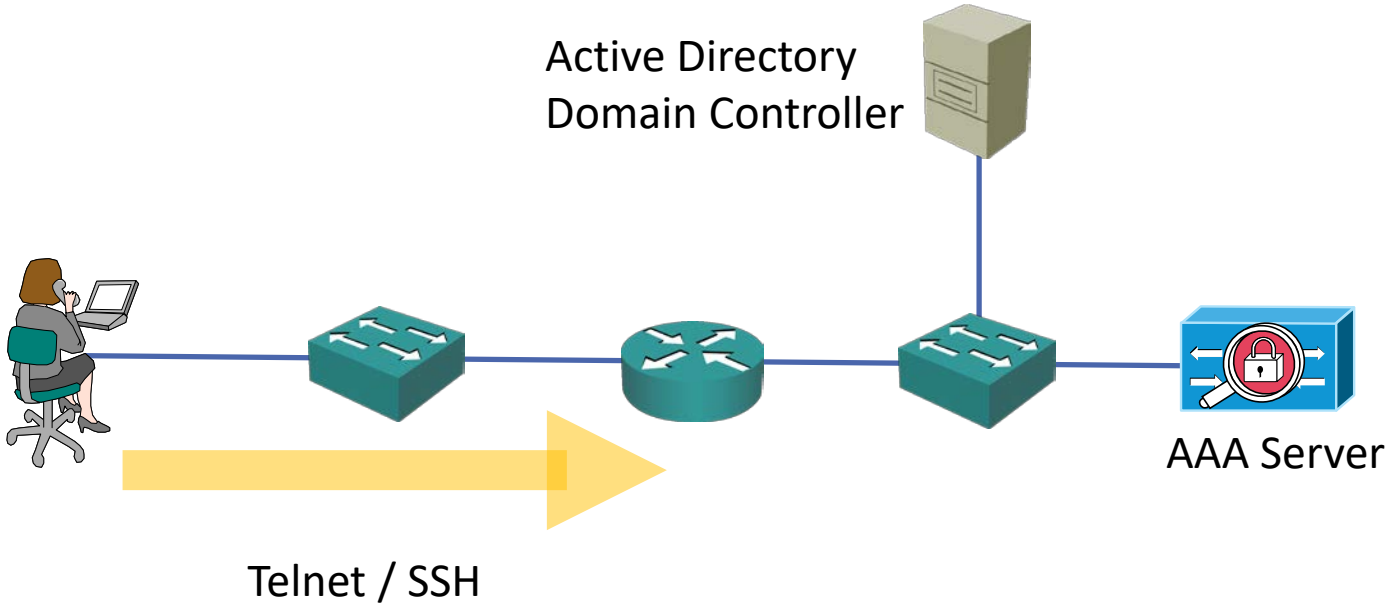


User Authenticated or Not
Optional Authorization Information

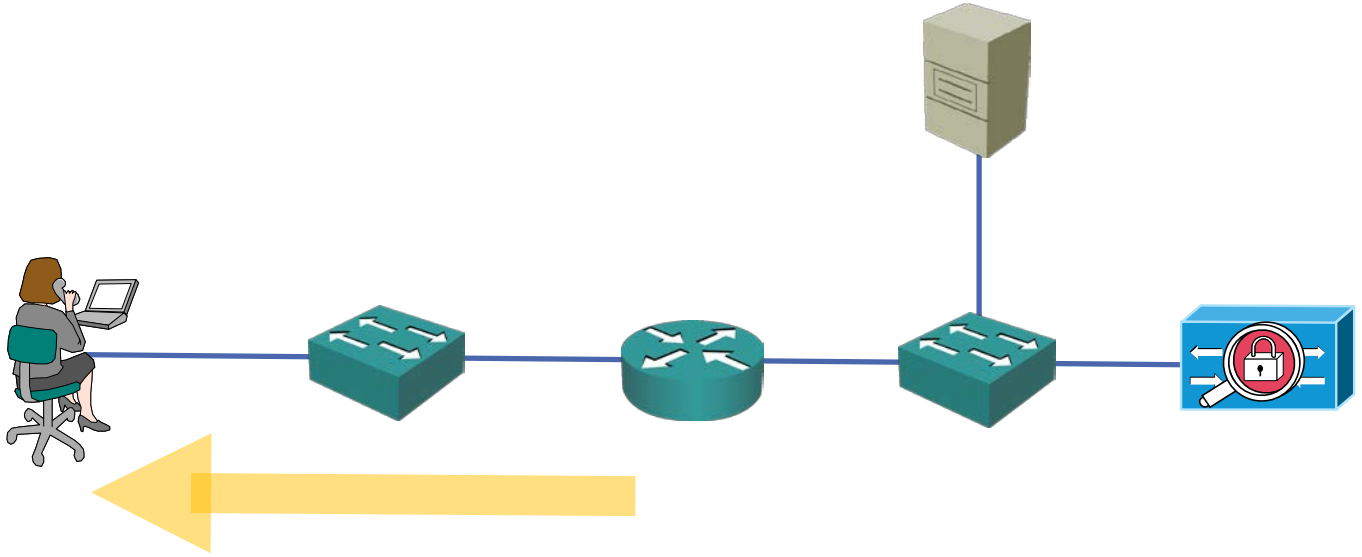
How AAA Works



Active Directory Integration

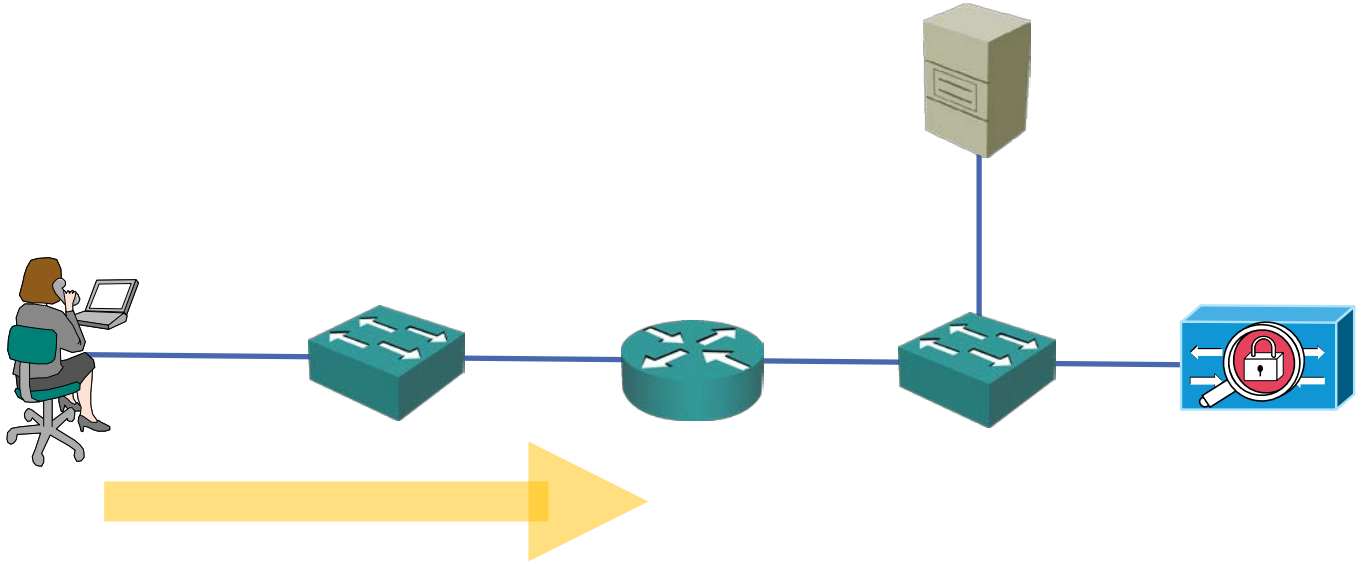


Active Directory Integration

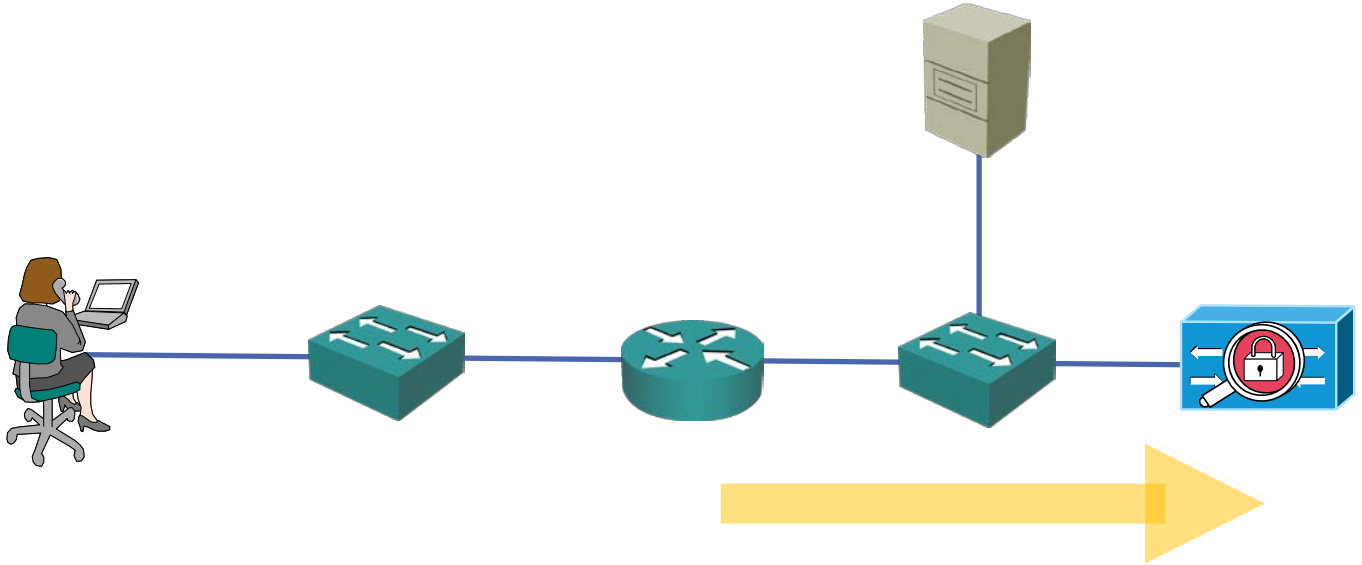


Challenge in
Telnet / SSH session

Active Directory Integration

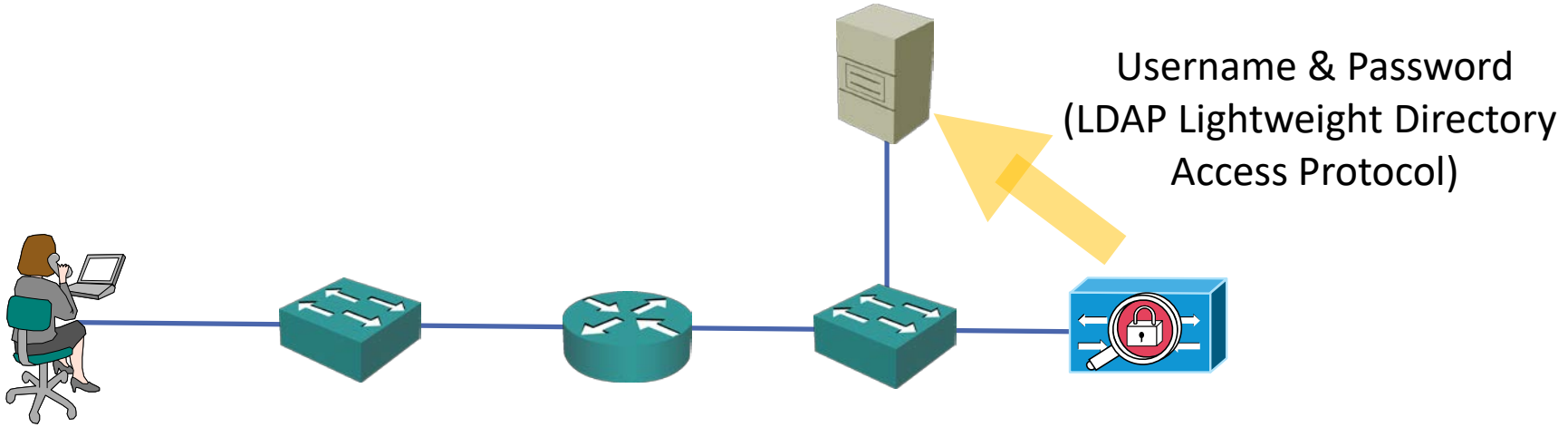


Active Directory Integration

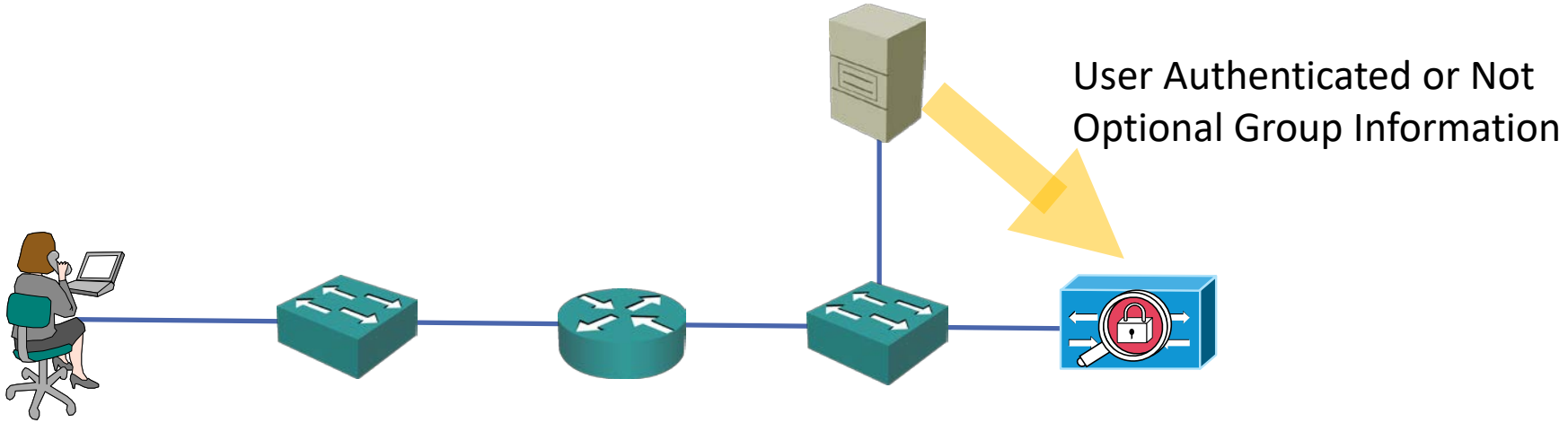


Username & Password
(RADIUS / TACACS+)

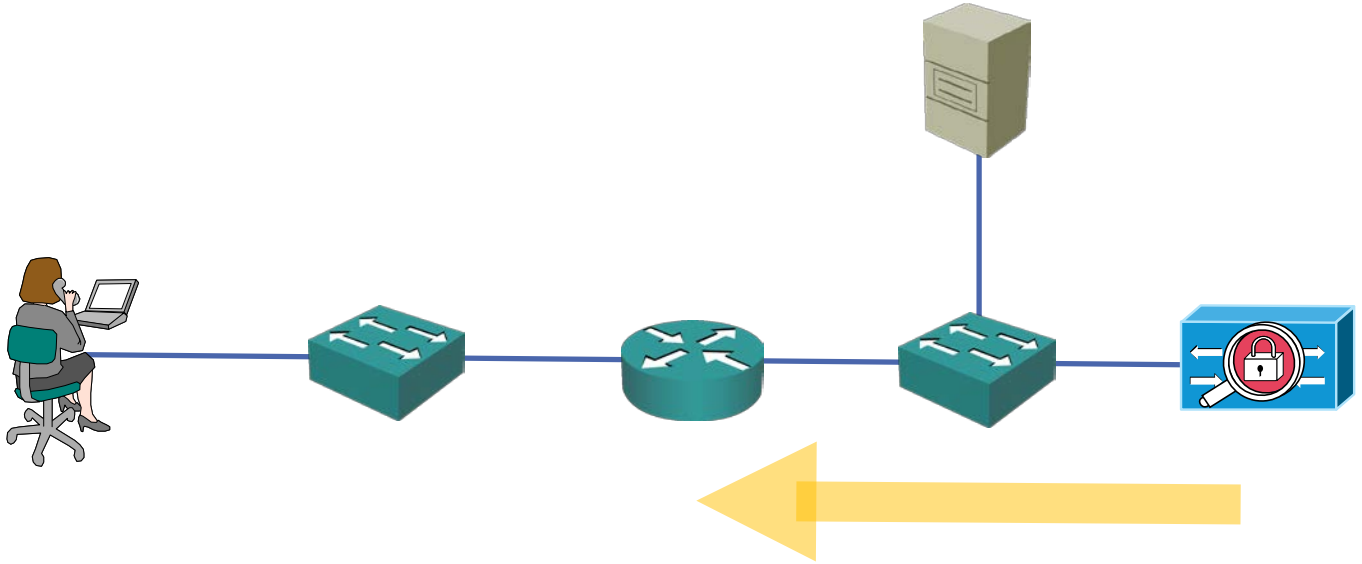
Active Directory Integration



Active Directory Integration

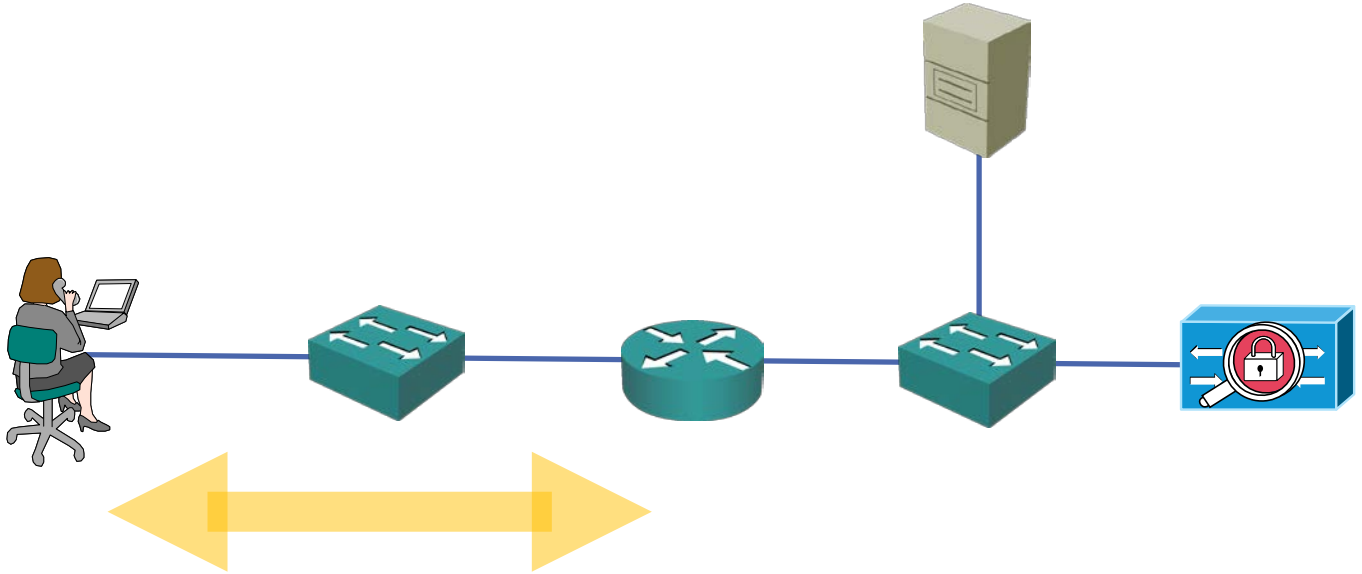


Active Directory Integration



User Authenticated or Not
Optional Authorization Information
based on AD group

Active Directory Integration



Telnet / SSH