Cisco Systems
Networking Academy

Cisco.com

Network Security 1

Module 4 – Trust and Identity Technology

CCNA CISCO CERTIFIED

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Cisco Systems
Networking Academy

Cisco.com

Module 1 – Trust and Identity Technology

4.1 AAA

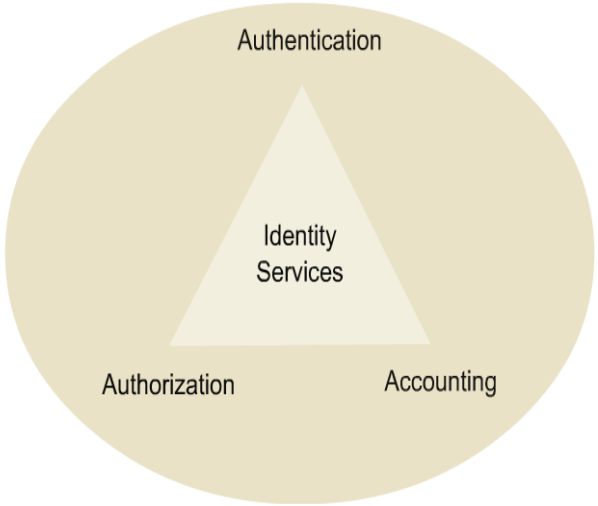
CCNA CISCO CERTIFIED™

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

AAA Model—
Network Security Architecture

Cisco.com

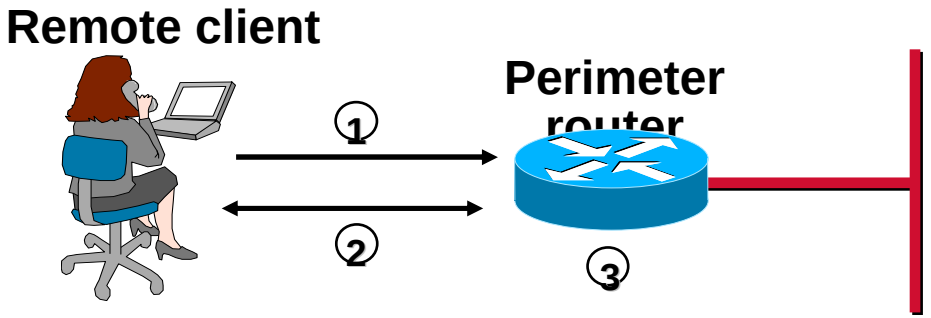
- Authentication
  - Who are you?
  - “I am user student and my password validateme proves it.”
- Authorization
  - What can you do? What can you access?
  - “I can access host 2000_Server with Telnet.”
- Accounting
  - What did you do? How long did you do it?
    How often did you do it?
  - “I accessed host 2000_Server with Telnet 15 times.”



Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Implementing AAA Using Local Services

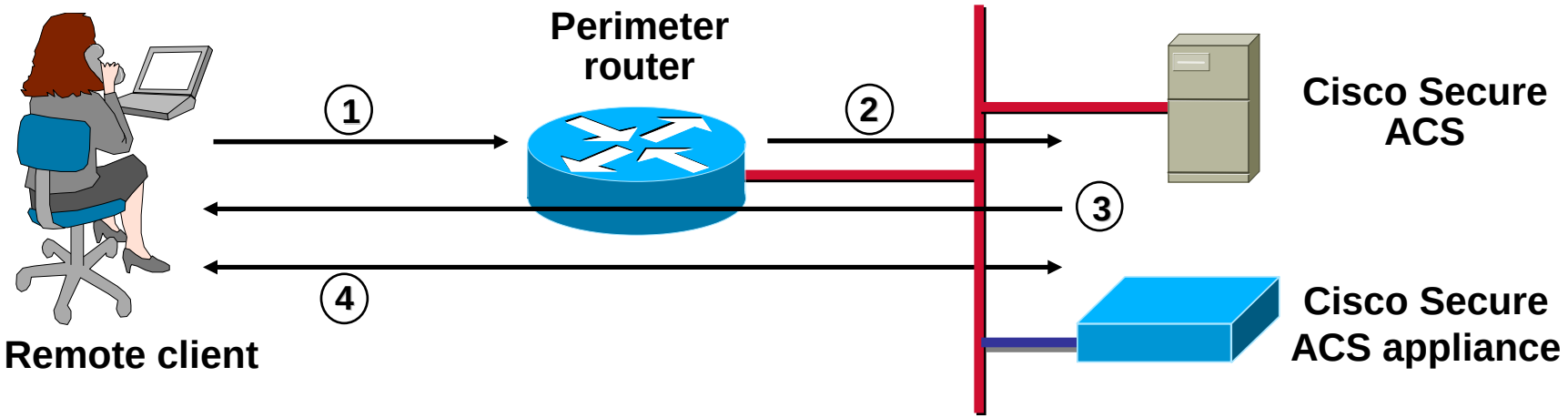
Cisco.com



1. The client establishes connection with the router.
2. The router prompts the user for their username and password.
3. The router authenticates the username and password in the local database. The user is authorized to access the network based on information in the local database.

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Implementing AAA Using External Servers



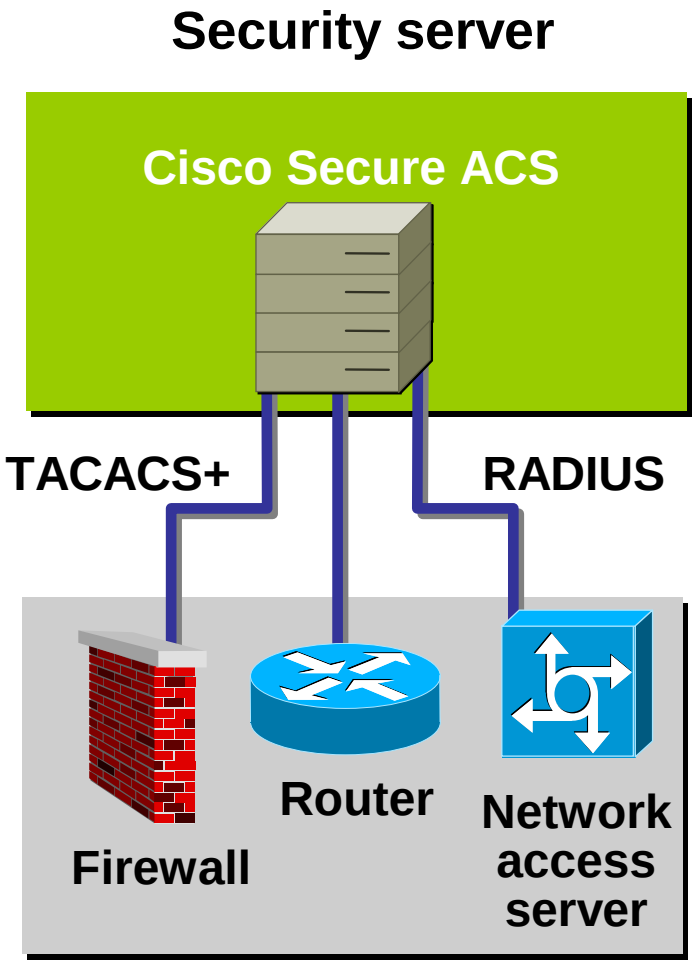
1. The client establishes a connection with the router.
2. The router communicates with the Cisco Secure ACS (server or appliance).
3. The Cisco Secure ACS prompts the user for their username and password.
4. The Cisco Secure ACS authenticates the user. The user is authorized to access the network based on information found in the Cisco Secure ACS database.

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

The TACACS+ and RADIUS AAA Protocols

Cisco.com

- Two different protocols are used to communicate between the AAA security servers and a router, NAS, or firewall.
- Cisco Secure ACS supports both TACACS+ and RADIUS:
  - TACACS+ remains more secure than RADIUS.
  - RADIUS has a robust API and strong accounting.



Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

The TACACS+ and RADIUS AAA Protocols

Cisco.com

	TACACS+	RADIUS
Functionality	Separates AAA	Combines Authentication/ Authorization
Transport Protocol	TCP	UDP
CHAP	Bidirectional	Unidirectional
Protocol Support	Multi-protocol support	No ARA No NetBEUI
Confidentiality	Entire Packet-Encrypted	Password-Encrypted
Accounting	Limited	Extensive

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Cisco Systems
Networking Academy

Cisco.com

Module 1 – Trust and Identity Technology

4.2 Authentication Technologies

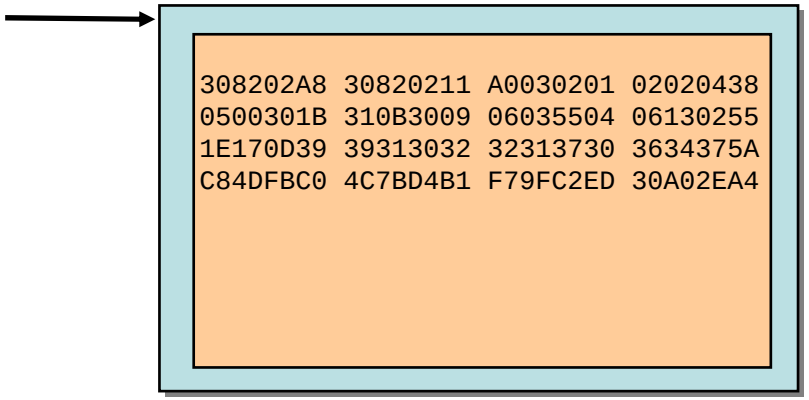
CCNA CISCO CERTIFIED ™

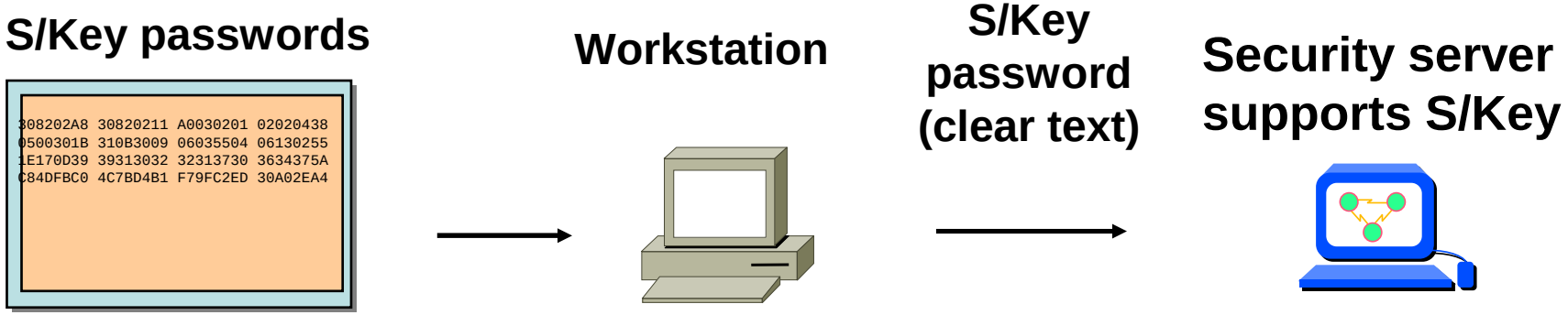
Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Authentication—
One-Time Passwords, S/Key

Cisco.com

- List of one-time passwords
- Generated by S/Key program hash function
- Sent in clear text over network
- Server must support S/Key





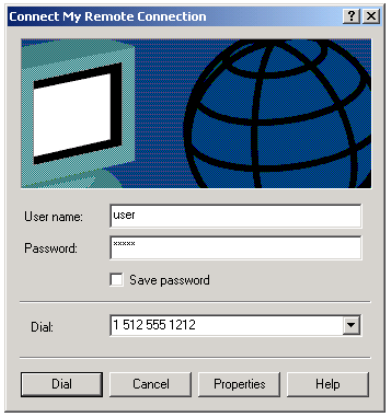
Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Authentication—
Token Cards and Servers

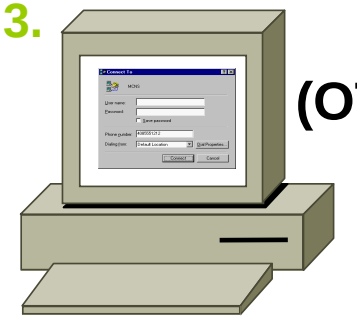
Cisco.com

1.

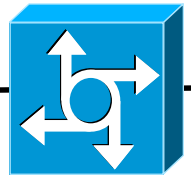
2.

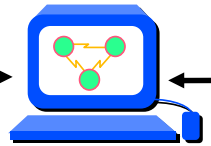


3.



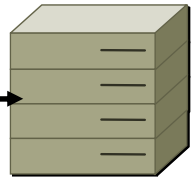
(OTP)





Cisco Secure ACS

4.

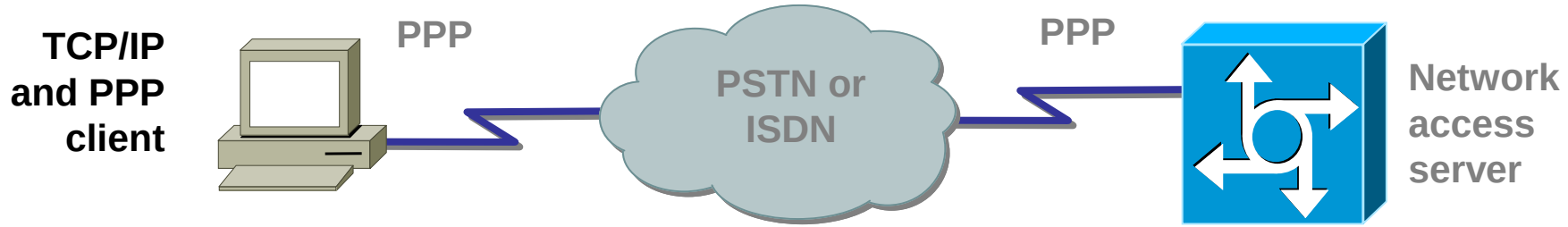


Token server

CCNA CISCO CERTIFIED™

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

AAA Example—Authentication Via PPP Link



- PAP—Password Authentication Protocol
  - Clear text, repeated password
  - Subject to eavesdropping and replay attacks
- CHAP—Challenge Handshake Authentication Protocol
  - Secret password, per remote user
  - Challenge sent on link (random number)
  - Challenge can be repeated periodically to prevent session hijacking
  - The CHAP response is an MD5 hash of (challenge + secret) provides authentication
  - Robust against sniffing and replay attacks
- MS-CHAP—Microsoft CHAP v1 (supported in IOS > 11.3) and v1 or v2 (supported in IOS > 12.2)

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Cisco Systems
Networking Academy

Cisco.com

Module 1 – Trust and Identity Technology

4.3 Identity Based Networking Services (IBNS)

CCNA CISCO CERTIFIED

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Identity Based Networking Services

Cisco.com

Features and Benefits:

- Intelligent adaptability for offering greater flexibility and mobility to stratified users
- A combination of authentication, access control, and user policies to secure network connectivity and resources
- User productivity gains and reduced operating costs

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

Cisco Systems
Networking Academy

Cisco.com

Module 1 – Trust and Identity Technology

4.4 Network Admission Control (NAC)

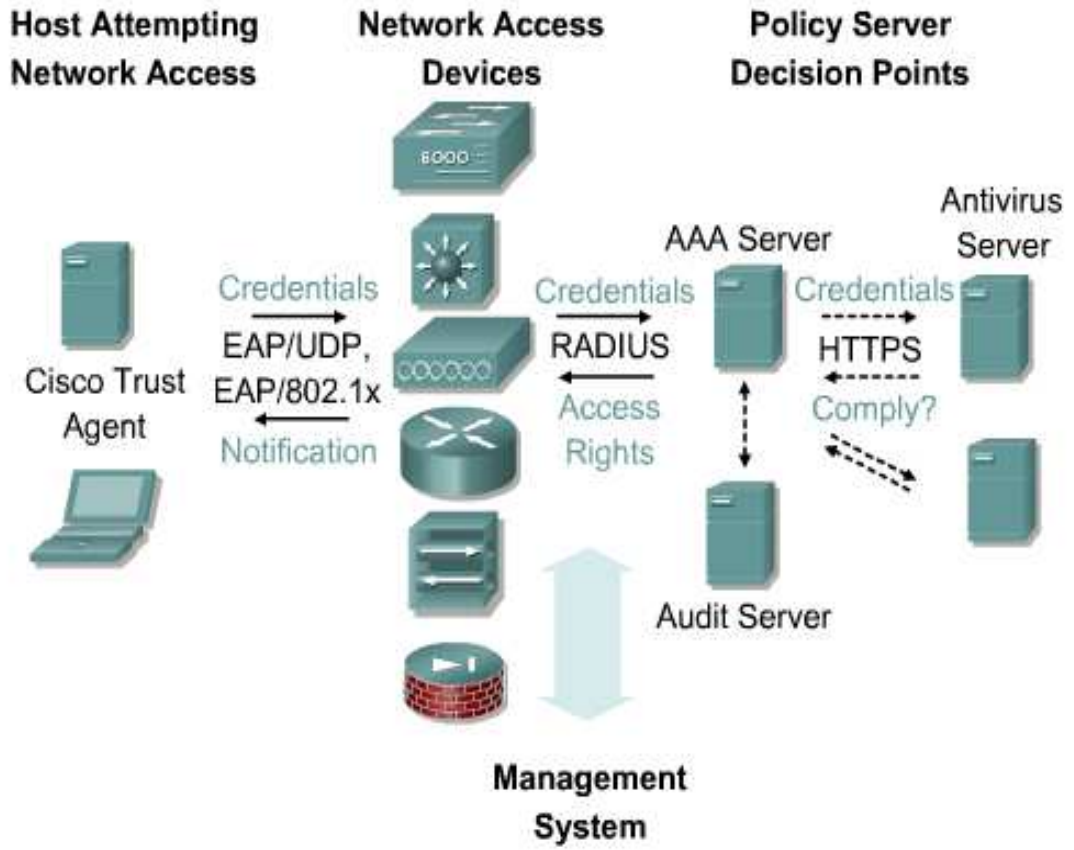
CCNA CISCO CERTIFIED

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

NAC Components

Cisco.com

The Four Components of the NAC System



Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se

NAC Vendor Participation

Cisco.com

NAC Enabled Applications	Vendor
eTrust AntiVirus, eTrust PestPatrol IBM - NAC enabled applications: Tivoli	Computer Associates International, Inc.
CyberGatekeeper Server 3.1 & CyberGatekeeper Policy Manager 3.1	InfoExpress
VirusScan 7.x and 8.0i	McAfee, Inc.
Symantec AntiVirus 9.0 & Symantec Client Security 2.0	Symantec
Trend Micro OfficeScan Corporate Edition 6.5	Trend Micro, Inc

Ola Lundh 070 69 86596
ola.lundh@edu.falkenberg.se