



A

AAA

- BootFlash considerations **B-1**
- case study overview (figure) **1-2**
- Cisco IOS 12.0(7)T command descriptions **A-13**
- defined **1-1**
- disabling **B-1**
- example configuration (NAS) **A-5, A-9**
- example configuration (router) **A-2**
- overview **1-1**
- security checklist (table) **1-12**
- task checklist (table) **1-14**
- aaa accounting command **A-13, A-14**
- aaa authentication command **A-13, A-14**
- aaa authorization command **A-13, A-14**
- aaa new-model key command **A-13, A-14**
- AAA server
 - creating a user profile (RADIUS authentication) **4-7**
 - creating a user profile (RADIUS authorization) **4-9**
 - creating a user profile (TACACS+ authentication) **4-3**
 - creating a user profile (TACACS+ authorization) **4-5**
 - negotiation process (flow diagram) **6-3**
 - restarting **3-10**
 - software version used in case study **xii**
 - verifying user configuration (RADIUS authentication) **4-8, 4-9**
 - verifying user configuration (TACACS+ authentication) **4-3**
 - verifying user configuration (TACACS+ authorization) **4-5**
- AAA servers
 - in network context **1-2**
- access list

- dialup PPP filtering **1-11**
- troubleshooting problems **6-14, 6-17**
- verification, show caller user command (server-based) **4-10, C6**
- verification, show line command (local-based) **2-8**
- accounting
 - configuring EXEC and command level (TACACS+) **5-4**
 - configuring NAS (TACACS+) **5-2**
 - configuring router (TACACS+) **5-4**
 - defined **1-1**
 - dial-based accounting (server) **5-1, 5-4**
 - monitored dialup PPP events **1-11**
 - monitored router administration events **1-11**
 - records policies **1-11**
 - server-based dial implementation **5-1**
 - server-based router implementation **5-4**
 - session timeout output example **5-3**
 - SQL query **5-2, 5-5**
 - TACACS+ dial implementation **5-1**
 - TACACS+ implementation (local-based) **2-12**
 - TACACS+ router implementation **5-4**
 - TACACS+ verification tests (local-based) **2-13**
 - TACACS+ verification tests (server-based) **5-2**
 - verifying from AAA server **5-2, 5-5**
- acknowledgements **xv**
- AddProfile command
 - adding basic user profile **3-11**
 - adding group profiles (TACACS+ authentication) **4-11**
 - adding group profiles (TACACS+ authorization) **4-17, 4-18**
 - adding user profiles (RADIUS authentication) **4-7**
 - adding user profiles (RADIUS authorization) **4-9**
 - adding user profiles (TACACS+ authentication) **4-3**

- adding user profiles (TACACS+ authorization) **4-5**
 - administrative control
 - authorization policy **1-11**
 - creating, router example **4-13**
 - privilege level 15 **1-11**
 - attribute-value pair
 - See AVPs
 - audience
 - defined **xi**
 - authentication
 - configuring NAS (RADIUS) **4-7**
 - configuring NAS (TACACS+) **4-3**
 - general process (flow diagram) **6-3**
 - RADIUS implementation **4-6**
 - RADIUS verification tests (server-based) **C4**
 - RADIUS vs. TACACS+ **1-5**
 - server-based implementation **4-2, 4-6, 4-10**
 - TACACS+ dialup, verifying by using csuslog **4-4**
 - TACACS+ implementation (local-based) **2-2, 2-8**
 - TACACS+ implementation (server-based) **4-2, 4-10**
 - TACACS+ verification tests (local-based) **2-3, 2-9**
 - TACACS+ verification tests (server-based) **C1, C7**
 - verifying PPP user authentication **4-4**
 - authentication, authorization, and accounting
 - See AAA
 - authorization
 - configuring NAS (RADIUS) **4-9**
 - configuring NAS (TACACS+) **4-4**
 - configuring routers **4-13**
 - defined **1-1**
 - general process (flow diagram) **6-3**
 - RADIUS implementation **4-8**
 - RADIUS verification tests (server-based) **C5**
 - RADIUS vs. TACACS+ **1-5**
 - server-based implementation **4-4, 4-8, 4-13**
 - TACACS+ dialup, verifying by using csuslog **4-5**
 - TACACS+ implementation (local-based) **2-5, 2-10**
 - TACACS+ implementation (server-based) **4-4, 4-13**
 - TACACS+ router, verifying by using csuslog **4-16, 4-18, 4-19**
 - TACACS+ verification tests (local-based) **2-6, 2-11**
 - TACACS+ verification tests (server-based) **C2, C9**
 - verifying access list **4-10**
 - verifying PPP user authorization **4-5**
 - verifying RADIUS authorization **4-9**
 - autocommand ppp negotiate command **1-11**
 - AVPs
 - adding group profiles (TACACS+ authentication) **4-11**
 - adding group profiles (TACACS+ authorization) **4-16, 4-17, 4-18**
 - defined **1-6**
 - dial access devices **1-11**
 - EXEC disabled implementation **6-6**
 - EXEC shell enabled (TACACS+) **6-5**
 - privilege level 15 enabled (TACACS+) **6-5**
 - RADIUS, user profile **4-7, 4-9**
 - RADIUS examples (table) **1-6**
 - TACACS+, user profile **4-3, 4-5**
 - TACACS+ authentication, group profile **4-11**
 - TACACS+ authorization, group profile **4-16, 4-17, 4-18**
 - TACACS+ examples (table) **1-6**
-
- ## B
- BootFlash images
 - AAA considerations **B-1**
-
- ## C
- case study
 - hardware **xii**
 - objectives **xi**
 - overview **1-1**
 - purpose **xi**
 - software **xii**
 - CCO
 - accessing **xiii**

- definition **xiii**
- CD-ROM
 - documentation **xiv**
- Challenge Handshake Authentication Protocol
 - See CHAP
- CHAP
 - ISDN authentication **1-10**
- checklists
 - AAA implementation tasks (table) **1-14**
 - AAA security (table) **1-12**
 - AAA service definition (table) **1-10**
 - general service definition (table) **1-9**
 - network services **1-9**
- Cisco 7206 VXR **xii**
- Cisco AS5300 **xii**
- Cisco AS5800 **xii**
- Cisco Connection Online
 - See CCO
- Cisco IOS 12.0(7)T **xii**
 - aaa accounting command **A-13, A-14**
 - aaa authentication command **A-13, A-14**
 - aaa authorization command **A-13, A-14**
 - AAA command descriptions (NAS) **A-13**
 - AAA command descriptions (router) **A-13**
 - aaa new-model command **A-13, A-14**
 - autocommand ppp negotiate command **1-11**
 - disabling AAA **B-1**
 - example configurations **A-1**
 - ip http command **A-13**
 - ip tacacs command **A-13**
 - local-based router example **A-2**
 - radius-server host command **A-15**
 - server-based NAS example **A-5, A-9**
 - tacacs-server host command **A-13, A-15**
 - tacacs-server key command **A-13**
 - version used in case study **xii**
- CiscoSecure for UNIX
 - See CSU
- commands
 - Cisco IOS 12.0(7)T (AAA) **A-13**
- configurations
 - Cisco IOS 12.0(7)T, NAS example **A-5, A-9**
 - Cisco IOS 12.0(7)T, router example **A-2**
 - CSU example **A-15**
 - example CSCConfig.ini listing **A-19**
 - example CSU.cfg listing **A-16**
 - examples, Cisco IOS 12.0(7)T **A-1**
 - local router **A-2**
 - RADIUS **A-9**
 - TACACS+ **A-5**
- conventions
 - command syntax **xiii**
 - document **xiii**
- CSCConfig.ini
 - example file listing **A-19**
- CSU
 - configuring CSU logging **3-9**
 - configuring debugging level **3-10**
 - creating csuslog file **3-9**
 - example configuration listings **A-15**
 - example CSCConfig.ini listing **A-19**
 - example CSU.cfg listing **A-16**
 - installation process **3-2**
 - installing **3-5**
 - log files listed **A-25**
 - minimum system specifications **xii**
 - pkgadd command **3-6**
 - restarting AAA server **3-10**
 - restarting syslog daemon **3-10**
 - software version used in case study **xii**
 - verifying Oracle account information **3-4**
 - version 2.3(3) **xii**
- CSU.cfg
 - example file listing **A-16**
- csuslog
 - configuring logging **3-9**
 - creating file **3-9**
 - TACACS+ dialup authentication **4-4**

TACACS+ dialup authorization **4-5**
 TACACS+ router authorization **4-16, 4-18, 4-19**
 using tail command (TACACS+ dialup authentication) **4-4**
 using tail command (TACACS+ PPP authorization) **4-5**
 using tail command (TACACS+ router authorization) **4-16, 4-18, 4-19**
 using the tail command **C1**

D

database
 verifying instance **3-3**

Data Encryption Standard
 See DES

debug command
 summary of relevant commands **6-7**
 using to troubleshoot AAA problems **6-7**

debug output
 accounting (server-based) **5-3, 5-5**
 accounting, TACACS+ (local-based) **2-13**
 authentication, RADIUS (server-based) **C4**
 authentication, TACACS+ (local-based) **2-3, 2-10**
 authentication, TACACS+ (server-based) **C1, C7**
 authorization, RADIUS (server-based) **C5**
 authorization, TACACS+ (local-based) **2-6, 2-11**
 authorization, TACACS+ (server-based) **C3, C9**

DES
 password support policy **1-13**
 router policy **1-10**

diagnostics
 using debug command output **C1**

directory environment variable
 verifying **3-3**

disconnect cause codes
 idle timeouts **5-2, 5-3**
 listed (table) **5-6**

E

encryption
 RADIUS **1-4**
 TACACS+ **1-5**

F

flow diagram
 general authentication and authorization **6-3**
 TACACS+, authentication and authorization **4-14**

G

groups
 defining administrative control **4-13**

H

hardware
 case study **xii**
 Cisco 7206 VXR **xii**
 Cisco AS5300 **xii**
 Cisco AS5800 **xii**
 Sun UltraSPARC **xii**

I

implementation
 AAA task checklist (table) **1-14**

interoperability
 RADIUS attribute support **1-6**

IP addresses
 static address policy **1-13**

ip http command **A-13**

ip tacacs command **A-13**

ISDN
 CHAP authentication **1-10**

L

- listener.ora
 - configuration listing **A-24**
- local-based access
 - compared with server-based access **1-6**
 - defined **1-6**
- local-based configuration
 - implementation overview **2-1**
 - TACACS+, accounting **2-12**
 - TACACS+, authentication **2-2, 2-8**
 - TACACS+, authorization **2-5, 2-10**
 - verification test results (TACACS+ accounting) **2-13**
 - verification test results (TACACS+ authentication) **2-3, 2-9**
 - verification test results (TACACS+ authorization) **2-6, 2-11**

M

- management policy
 - TACACS+ vs. RADIUS comparison **1-5**
- MD5
 - RFC link **1-2**
- multiprotocol support
 - TACACS+ vs. RADIUS comparison **1-5**

N

- NAS
 - versions used in case study **xii**
- NAS profile
 - RADIUS **4-7**
- network environment
 - equipment summary **1-13**
- network services
 - AAA checklist (table) **1-10**
 - accounting policy **1-11**
 - authentication policy **1-10**

- authorization policy **1-11**
- checklist **1-9**
- definitions and policies **1-10**
- dialup/shell AAA policy **1-10**
- general checklist (table) **1-9**

O

- objectives
 - case study **xi**
- online documentation
 - See CCO
- Oracle
 - accounting records policy **1-11**
 - confirming tnsnames service **3-4**
 - creating tablespace **3-2**
 - DB Client 7.3(4) **xii**
 - DB Server 7.3(4) **xii**
 - installation reference **3-2**
 - listener (lsnrctl) **3-3**
 - listener.ora listing **A-24**
 - Server Manager (svrmgrl) **3-3**
 - software version used in case study **xii**
 - user environment variable **A-23**
 - verifying account information **3-4**
 - verifying database instance **3-3**
 - verifying SMON operation **3-3**
 - verifying software directory environment variable **3-3**
- OS Solaris 2.5(1) **xii**
- overview
 - AAA case study **1-1**

P

- PAP
 - PPP authentication **1-10**
- Password Authentication Protocol
 - See PAP

passwords

- authentication policies **1-13**
- authentication policy **1-10**
- authorization policies **1-13**
- local access policy **1-10**

planning

- pre-deployment summary **1-9**
- site preparation **xi**

Point-to-Point Protocol

See PPP

policies

- accounting **1-11**
- accounting, PPP **1-11**
- accounting, router administration **1-11**
- authentication **1-10**
- authorization **1-11**
- dialup/shell AAA **1-10**
- privilege level 15 authorization **1-13**
- router, administrative control **1-11**
- router management **1-5**
- security considerations **1-12**

PPP

- PAP authentication **1-10**
- verifying TACACS+ authorization **4-5**
- verifying TACACS+ user authentication **4-4**

privilege level

- TACACS+ support **1-2**

privilege level 15

- accounting **1-11, 1-12**
- command authorization policy **1-13**
- local administration **1-12**
- router authorization policy **1-11**
- router command authorization **A-13**

privilege level 15 commands **4-13**

- configuring accounting **5-4**

problems

authentication

- AAA behavior configured incorrectly in NAS **6-9**
- AAA behavior configured incorrectly in router **6-20**

connection between NAS and AAA server down **6-12**

connection between router and AAA server down **6-23**

group profile password type does not match type in NAS **6-13**

incorrect AAA configuration in router **6-21, 6-24**

maximum number of users exceeded **6-12, 6-23**

shell initiated PPP session fails **6-9, 6-13**

TACACS+ key incorrect in router or AAA server **6-23**

TACACS+ or RADIUS key incorrect in NAS or AAA server **6-12**

user account disabled due to too many failed logins **6-10, 6-22**

user account password or profile expired **6-11, 6-22**

user enters invalid username or password **6-9, 6-20**

user enters password incorrectly **6-10, 6-22**

user exceeds the maximum number of concurrent sessions **6-11, 6-22**

user name not in server database **6-10, 6-22**

user profile configured incorrectly **6-10, 6-22**

user workstation configured incorrectly **6-11**

authorization

AAA authorization configured incorrectly in NAS **6-16**

AAA behavior incorrectly configured **6-26, 6-28**

AAA configuration error **6-25, 6-27**

access list assigned to user **6-14, 6-17**

authorization failed service **6-25, 6-27**

autocommand ppp negotiate assigned to user **6-26, 6-28**

AVPs not assigned **6-14, 6-17**

does not have PPP service assigned **6-16**

feature is not supported on console ports **6-28**

group lacks shell service assigned **6-16**

Idle-Timeout RADIUS AVP not configured on group profile **6-18**

idletime TACACS+ AVP not configured on group profile **6-18**

Lack of service=shell AVP **6-28**

user client configuration error **6-13**

- user exceeds the maximum number of concurrent sessions **6-19**
- user or group does not have User-Service-Type AVP assigned **6-19**
- user or group profile lacks proper AVP **6-18**
- user or group profile restricted **6-18**
- user or lacks service=shell AVP assigned **6-19**
- user profile configured incorrectly **6-28**
- user profile lacks appropriate enable level to perform command **6-25**
- user profile lacks appropriate enable privilege level to perform command **6-27**
- user profile lacks appropriate privilege level to perform command **6-25, 6-27**
- user profile restricted **6-14**
- profiles
 - assigning user to group profile (TACACS+ authentication) **4-11**
 - assigning user to group profile (TACACS+ authorization) **4-16, 4-17, 4-18**
 - creating basic user **3-11**
 - group, configuring router access **4-13**
 - group, verifying (TACACS+ authentication) **4-11**
 - group, verifying (TACACS+ authorization) **4-16, 4-17, 4-18**
 - group configuration, TACACS+ **4-14**
 - group permissions (table) **4-13**
 - user, defining access privileges **6-5**
 - user, RADIUS **4-7, 4-9**
 - user, TACACS+ **4-3, 4-5**
 - user, verifying (TACACS+ authentication) **4-12**
 - user, verifying (TACACS+ authorization) **4-16, 4-17, 4-18**
 - user, verifying basic **3-11**
 - user configuration (RADIUS authentication) **4-7**
 - user configuration (RADIUS authorization) **4-9**
 - user configuration (TACACS+ authentication) **4-3**
 - user configuration (TACACS+ authorization) **4-5**
- purpose
 - case study **xi**

R

RADIUS

- authentication tests (server-based) **C4**
- authorization tests (server-based) **C5**
- AVP examples (table) **1-6**
- compared with TACACS+ **1-4**
- compared with TACACS+ (table) **1-4**
- configuring authentication (server-based) **4-6**
- configuring authorization (server-based) **4-8**
- creating user profiles (authentication) **4-7**
- debug output, server-based authentication **C4**
- debug output, server-based authorization **C5**
- encryption **1-4**
- example configuration (NAS) **A-9**
- interoperability **1-6**
- NAS profile, creating **4-7**
- negotiation process (flow diagram) **6-4**
- RFC link **1-2**
- See also AVPs
- See also troubleshooting
- technology overview **1-3**
- troubleshooting scenario, authorization **6-36**
- troubleshooting symptom list, authentication **6-10**
- troubleshooting symptom list, authorization **6-15**
- verifying access list assignment **4-10**
- radius-server host command **A-15**
- Remote Authentication Dial-in User Service
 - See RADIUS
- Requests for Comments
 - See RFCs
- RFCs
 - reference links **1-2**
- router
 - administration, command and control policy **1-11**
 - administrative control, creating **4-13**
 - authorization, controlling **4-13**
 - management, RADIUS vs. TACACS+ **1-5**

S

scenario

- case study description **1-8**
- case study overview (figure) **1-2**

scenarios

- troubleshooting examples **6-29**

security

- policy considerations **1-12**

server-based access

- compared with local-based access **1-7**
- defined **1-7**

server-based configuration

- implementation overview (authentication and authorization) **4-1**
- verification test results (RADIUS authentication) **C4**
- verification test results (RADIUS authorization) **C5**
- verification test results (TACACS+ authentication) **C1, C7**
- verification test results (TACACS+ authorization) **C2, C9**
- verifying user (RADIUS authentication) **4-8, 4-9**
- verifying user (TACACS+ authentication) **4-3**
- verifying user (TACACS+ authorization) **4-5**

show caller user command

- access list verification output (server-based) **4-10, C6**
- session timeout disconnect example **5-3**

show line command

- verification output (local-based) **2-8**

site preparation **xi**

SMON

- verifying operation on Oracle server **3-3**

software

- case study listing **xii**

software components

- Cisco IOS 12.0(7)T **xii**
- Oracle DB Client 7.3(4) **xii**
- Oracle DB Server 7.3(4) **xii**
- OS Solaris 2.5(1) **xii**
- SQL*Plus Release 3.3.4.0.1 **xii**

SQL*Plus

- Release 3.3.4.0.1 **xii**

sqlplus

- verifying account information **3-4**

symptom list, troubleshooting AAA

- dial-based local authentication **6-9**
- dial-based local authorization **6-13**
- dial-based server authentication **6-10**
- dial-based server authorization **6-15**
- router-based local authentication **6-19**
- router-based local authorization **6-24**
- router-based server authentication **6-21**
- router-based server authorization **6-26**

syslog daemon

- restarting **3-10**

T

tablespace

- installing (Oracle) **3-2**
- size requirements **3-2**

TAC

- contacting **xiv**

TACACS

- RFC link **1-2**

TACACS+

- accounting tests (local-based) **2-13**
- assigning user to group profile (authentication) **4-11**
- assigning user to group profile (authorization) **4-16, 4-17, 4-18**
- authentication and authorization (figure) **4-14**
- authentication tests (local-based) **2-3, 2-9**
- authentication tests (server-based) **C1, C7**
- authorization tests (local-based) **2-6, 2-11**
- authorization tests (server-based) **C2, C9**
- AVP examples (table) **1-6**
- compared with RADIUS **1-4**
- compared with RADIUS (table) **1-4**
- configuring accounting (local-based) **2-12**

- configuring authentication (local-based) **2-2, 2-8**
- configuring authentication (server-based) **4-2, 4-10**
- configuring authorization (local-based) **2-5, 2-10**
- configuring authorization (server-based) **4-4, 4-13**
- configuring dial accounting (server-based) **5-1, 5-2**
- configuring router accounting (server-based) **5-4**
- creating user profiles (authentication) **4-3**
- debug output, server-based authentication **C1, C7**
- debug output, server-based authorization **C3, C9**
- encryption **1-5**
- example configuration (NAS) **A-5**
- multiprotocol support **1-5**
- negotiation process, EXEC disabled (flow diagram) **6-6**
- negotiation process, EXEC enabled (flow diagram) **6-5**
- privilege level support **1-2**
- RFC link **1-2**
- router management **1-5**
- See also AVPs
- See also troubleshooting
- service control **1-3**
- technology overview **1-2**
- troubleshooting scenario, authentication **6-29, 6-30, 6-31**
- troubleshooting scenario, authorization **6-33, 6-34, 6-35**
- troubleshooting symptom list, authentication **6-10, 6-21**
- troubleshooting symptom list, authorization **6-15, 6-24, 6-26**
- tacacs-server host command **A-13, A-15**
- tacacs-server key command **A-13**
- tail command
 - reading the csuslog file **C1**
 - verifying dialup authentication with csuslog (TACACS+) **4-4**
 - verifying PPP authorization with csuslog (TACACS+) **4-5**
 - verifying router authorization with csuslog (TACACS+) **4-16, 4-18, 4-19**
- Technical Assistance Center
 - See TAC
- technology

- AAA overview **1-1**
- Terminal Access Controller Access Control System Plus
 - See TACACS+
- tnsnames service
 - verifying with tnsping utility **3-4**
- tnsping
 - using to verify tnsnames service **3-4**
- troubleshooting
 - diagnostic overview **6-1**
 - example scenarios **6-29**
 - methodology overview **6-7**
 - RADIUS authorization scenario **6-36**
 - See also problems
 - See also RADIUS
 - See also symptom list, troubleshooting AAA
 - See also TACACS+
 - TACACS+ authentication scenario **6-29, 6-30, 6-31**
 - TACACS+ authorization scenario **6-33, 6-34, 6-35**

U

- UNIX
 - version used in case study **xii**
- user
 - creating profiles (RADIUS authentication) **4-7**
 - creating profiles (RADIUS authorization) **4-9**
 - creating profiles (TACACS+ authentication) **4-3**
 - creating profiles (TACACS+ authorization) **4-5**
- user environment variable
 - Oracle, listed **A-23**

V

- verification
 - accounting, TACACS+ (local-based) **2-13**
 - accounting, TACACS+ (server-based) **5-2**
 - authentication, RADIUS (server-based) **C4**
 - authentication, TACACS+ (local-based) **2-3, 2-9**

authentication, TACACS+ (server-based) **C1, C7**
authorization, RADIUS (server-based) **C5**
authorization, TACACS+ (local-based) **2-6, 2-11**
authorization, TACACS+ (server-based) **C2, C9**

verification tests

debug output, RADIUS authentication
(server-based) **C4**
debug output, RADIUS authorization
(server-based) **C5**
debug output, TACACS+ (local-based) **2-6, 2-11, 2-13**
debug output, TACACS+ (server-based
accounting) **5-3, 5-5**
debug output, TACACS+ authentication
(server-based) **C1, C7**
debug output, TACACS+ authorization
(server-based) **C3, C9**
SQL query (accounting) **5-2, 5-5**

ViewProfile command

verifying basic user configuration **3-11**
verifying user configuration (RADIUS
authentication) **4-8, 4-9**
verifying user configuration (TACACS+
authentication) **4-3**
verifying user configuration (TACACS+
authorization) **4-5**