TACACS+

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

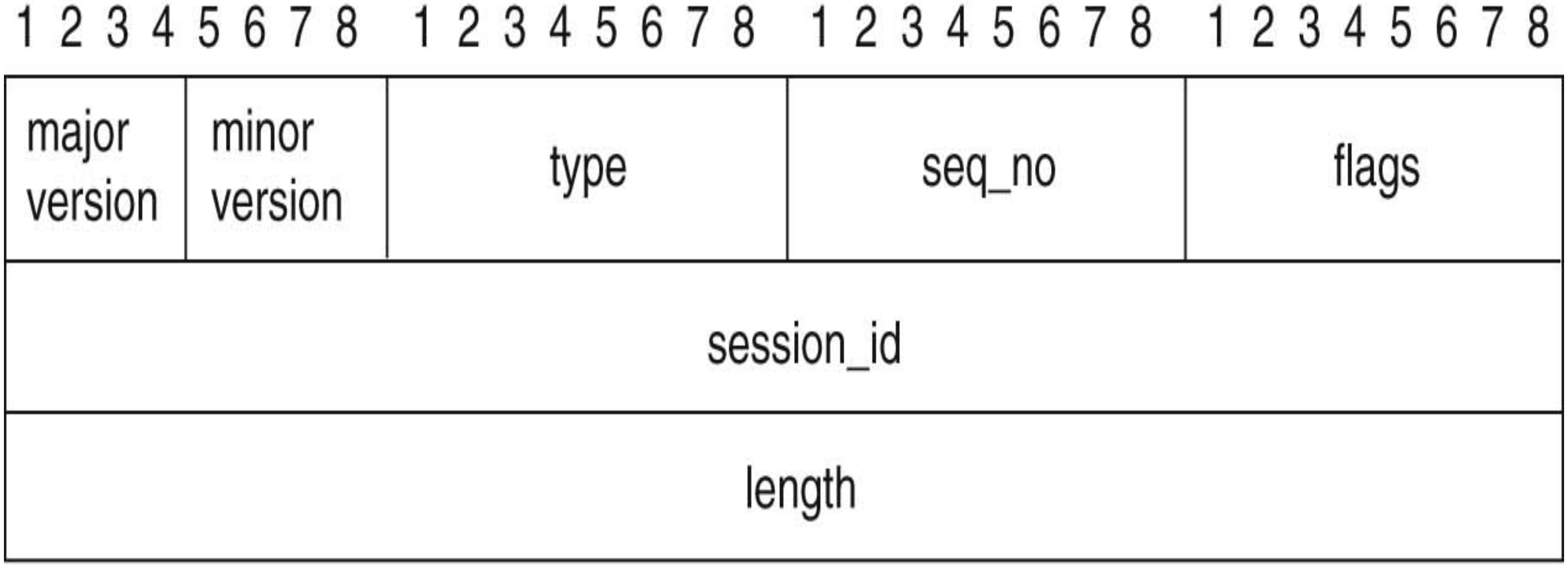
TACACS+

- Terminal Access Controller Access Control System
- Protocol and software used to provide AAA services to an access server or router
- TACACS+ protocol used in communication from NAS and the TACACS+ daemon running on a security server

TACACS+ Architecture

- Uses TCP port 49 to communicate
- Cisco proprietary
- Outgrowth of TACACS (RFC 1492)

TACACS+
Packet Header Format



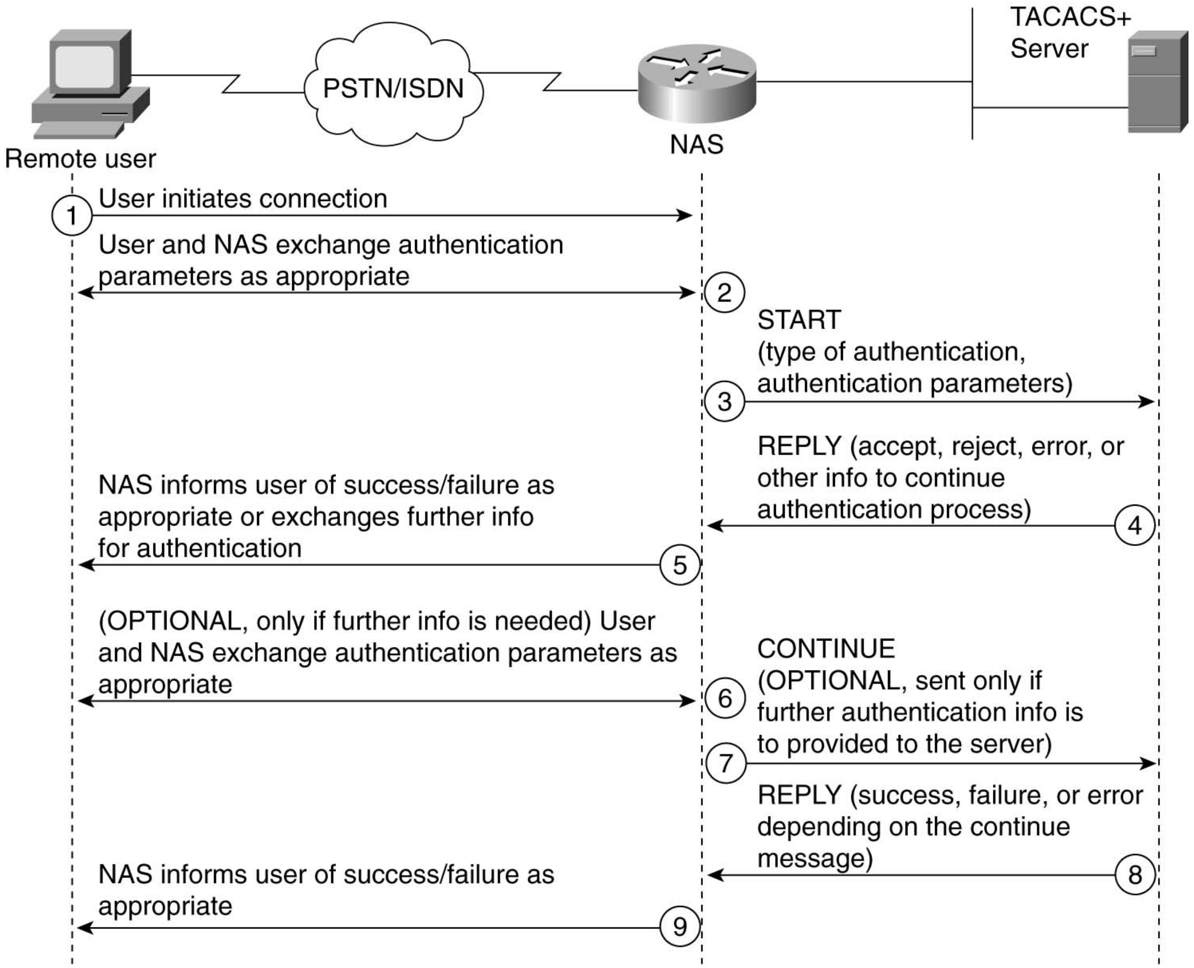
1 2 3 4	5 6 7 8	1 2 3 4 5 6 7 8	1 2 3 4 5 6 7 8	1 2 3 4 5 6 7 8
major version	minor version	type	seq_no	flags
session_id				
length				

- type field used to differentiate authentication, authorization, and accounting packets
- seq_no increments starting from 1 in any given session
- session_id’ is a randomly generated value used during entire session

TACACS+ Packet Encryption

- Entire packet after the TACACS+ header is encrypted
- Relies on a preshared secret stored on both NAS and AAA server
- Cipher text generated by XOR clear-text with concatenated MD5 hashes of session_id, preshared key, version number, and sequence number

TACACS+ Authentication



1 User initiates connection

2 User and NAS exchange authentication parameters as appropriate

3 START (type of authentication, authentication parameters)

4 REPLY (accept, reject, error, or other info to continue authentication process)

5 NAS informs user of success/failure as appropriate or exchanges further info for authentication

6 (OPTIONAL, only if further info is needed) User and NAS exchange authentication parameters as appropriate

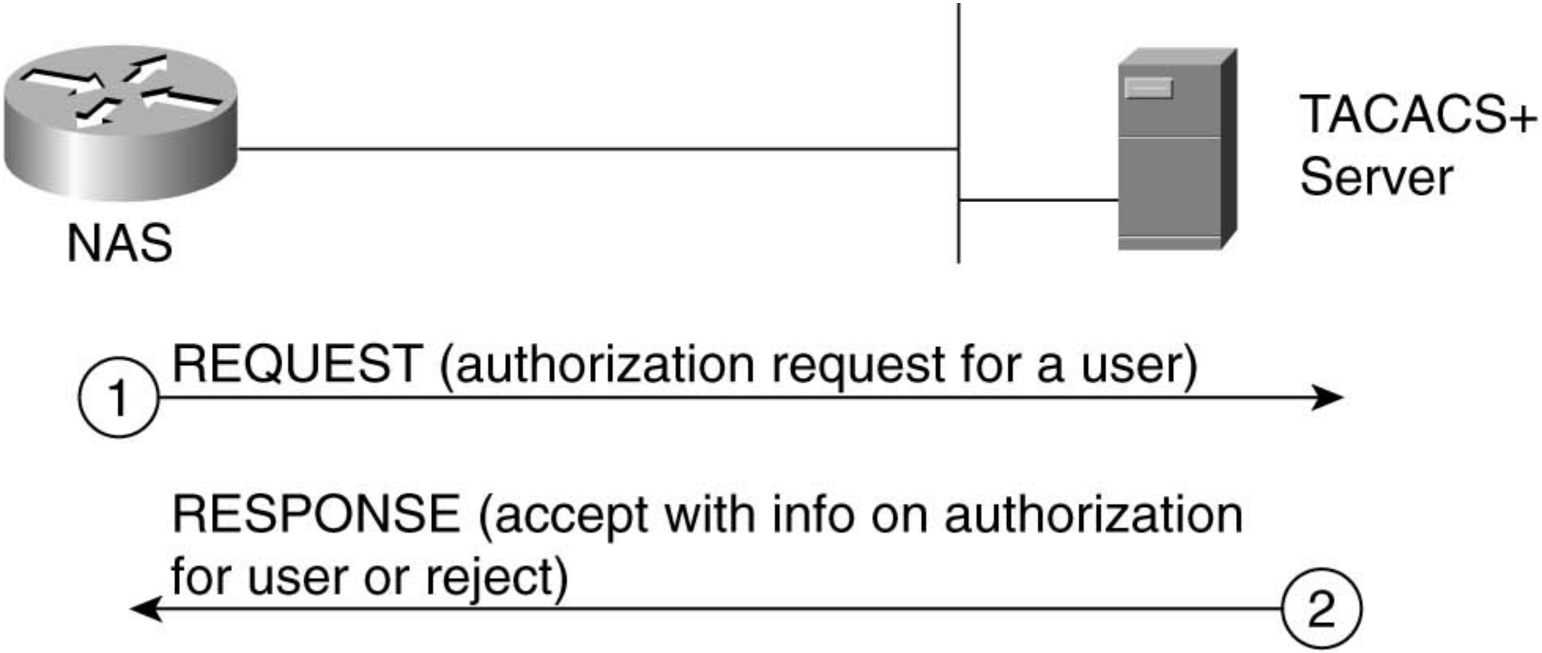
7 CONTINUE (OPTIONAL, sent only if further authentication info is to provided to the server)

8 REPLY (success, failure, or error depending on the continue message)

9 NAS informs user of success/failure as appropriate

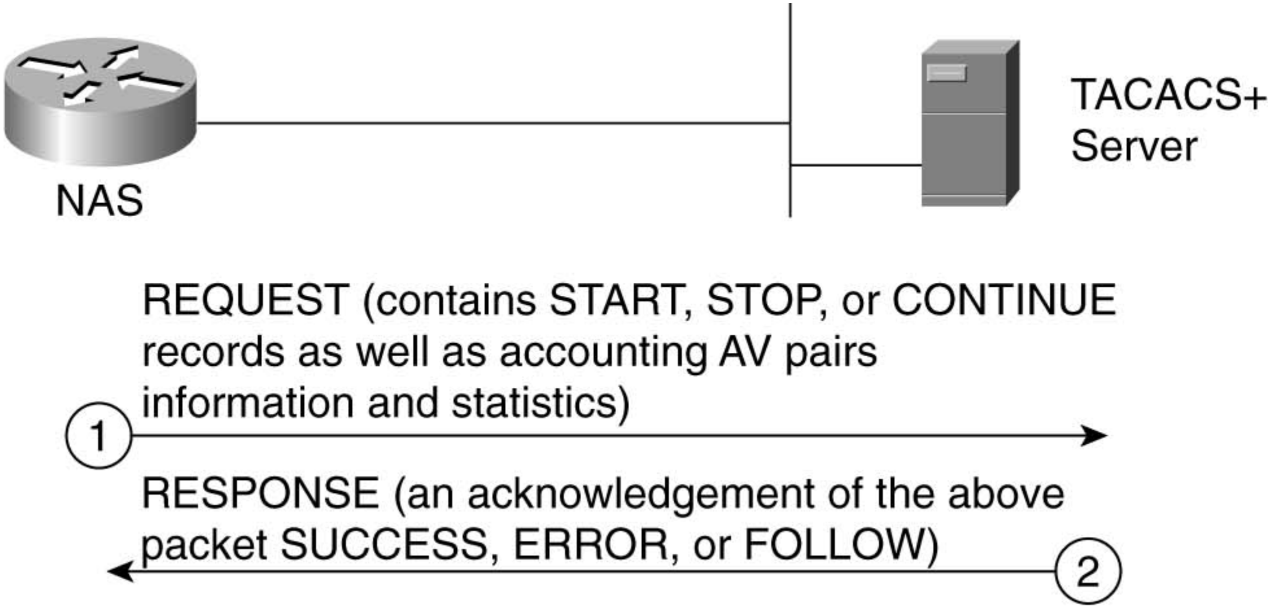
- uses ‘start’, ‘reply’, and ‘continue’ packets
- authentication results in ‘success’, ‘failure, or ‘error’

TACACS+ Authorization


NAS
TACACS+ Server
1
REQUEST (authorization request for a user)
RESPONSE (accept with info on authorization for user or reject)
2

- Request contains services or privileges needed to be authorized
- Response may contain fail, pass with additional attributes, pass with replacement attributes, error, or redirection to an alternate AAA server

TACACS+ Accounting



REQUEST (contains START, STOP, or CONTINUE records as well as accounting AV pairs information and statistics)

RESPONSE (an acknowledgement of the above packet SUCCESS, ERROR, or FOLLOW)

TACACS+ Accounting

- Request packet
  - 'Start' record indicates that a service is about to begin
  - 'Continue' record sent periodically while service is in progress
  - 'Stop' record sent when service has terminated
- Response packet
  - 'Success' status indicates that AAA server has received packet from NAS and has stored info into its database
  - 'Error' implies AAA server failed to commit record to its database
  - 'Follow' status indicates that NAS should send the records to another AAA server listed in packet data