```
~# service freeradius debug
● freeradius.service - FreeRADIUS multi-protocol policy server
   Loaded: loaded (/lib/systemd/system/freeradius.service; enabled; vendor preset: enabled)
   Active: inactive (dead) since Tue 2021-08-10 15:34:52 CEST; 10min ago
     Docs: man:radiusd(8)
           man:radiusd.conf(5)
           http://wiki.freeradius.org/
           http://networkradius.com/doc/
  Process: 1097 ExecStart=/usr/sbin/freeradius $FREERADIUS_OPTIONS (code=exited, status=0/SUCCESS)
  Process: 758 ExecStartPre=/usr/sbin/freeradius $FREERADIUS_OPTIONS -Cxm -lstdout (code=exited, status=0/-
SUCCESS)
 Main PID: 1104 (code=exited, status=0/SUCCESS)

Aug 10 15:33:24 servergym.meineschule.lokal freeradius[758]: tls: Using cach…on
Aug 10 15:33:24 servergym.meineschule.lokal freeradius[758]: tls: Using cach…on
Aug 10 15:33:24 servergym.meineschule.lokal freeradius[758]: Ignoring "sql" …t)
Aug 10 15:33:24 servergym.meineschule.lokal freeradius[758]: Ignoring "ldap"…t)
Aug 10 15:33:24 servergym.meineschule.lokal freeradius[758]:  # Skipping con…32
Aug 10 15:33:24 servergym.meineschule.lokal freeradius[758]: radiusd: #### S…##
Aug 10 15:33:24 servergym.meineschule.lokal freeradius[758]: Configuration a…OK
Aug 10 15:33:24 servergym.meineschule.lokal systemd[1]: Started FreeRADIUS m…r.
Aug 10 15:34:52 servergym.meineschule.lokal systemd[1]: Stopping FreeRADIUS ….
Aug 10 15:34:52 servergym.meineschule.lokal systemd[1]: Stopped FreeRADIUS m…r.
Hint: Some lines were ellipsized, use -l to show in full.
FreeRADIUS Version 3.0.16
Copyright (C) 1999-2017 The FreeRADIUS server project and contributors
There is NO warranty; not even for MERCHANTABILITY or FITNESS FOR A
PARTICULAR PURPOSE
You may redistribute copies of FreeRADIUS under the terms of the
GNU General Public License
For more information about these matters, see the file named COPYRIGHT
Starting - reading configuration files ...
including dictionary file /usr/share/freeradius/dictionary
including dictionary file /usr/share/freeradius/dictionary.dhcp
including dictionary file /usr/share/freeradius/dictionary.vqp
including dictionary file /etc/freeradius/3.0/dictionary
including configuration file /etc/freeradius/3.0/radiusd.conf
including configuration file /etc/freeradius/3.0/proxy.conf
including configuration file /etc/freeradius/3.0/clients.conf
including files in directory /etc/freeradius/3.0/mods-enabled/
including configuration file /etc/freeradius/3.0/mods-enabled/cache_eap
including configuration file /etc/freeradius/3.0/mods-enabled/exec
including configuration file /etc/freeradius/3.0/mods-enabled/pap
including configuration file /etc/freeradius/3.0/mods-enabled/echo
including configuration file /etc/freeradius/3.0/mods-enabled/attr_filter
including configuration file /etc/freeradius/3.0/mods-enabled/radutmp
including configuration file /etc/freeradius/3.0/mods-enabled/dynamic_clients
including configuration file /etc/freeradius/3.0/mods-enabled/digest
including configuration file /etc/freeradius/3.0/mods-enabled/linelog
including configuration file /etc/freeradius/3.0/mods-enabled/files
including configuration file /etc/freeradius/3.0/mods-enabled/unix
including configuration file /etc/freeradius/3.0/mods-enabled/chap
including configuration file /etc/freeradius/3.0/mods-enabled/logintime
including configuration file /etc/freeradius/3.0/mods-enabled/ntlm_auth
including configuration file /etc/freeradius/3.0/mods-enabled/realm
including configuration file /etc/freeradius/3.0/mods-enabled/replicate
including configuration file /etc/freeradius/3.0/mods-enabled/expiration
including configuration file /etc/freeradius/3.0/mods-enabled/always
including configuration file /etc/freeradius/3.0/mods-enabled/unpack
including configuration file /etc/freeradius/3.0/mods-enabled/utf8
including configuration file /etc/freeradius/3.0/mods-enabled/detail.log
including configuration file /etc/freeradius/3.0/mods-enabled/soh
including configuration file /etc/freeradius/3.0/mods-enabled/sradutmp
including configuration file /etc/freeradius/3.0/mods-enabled/mschap
including configuration file /etc/freeradius/3.0/mods-enabled/eap
including configuration file /etc/freeradius/3.0/mods-enabled/preprocess
including configuration file /etc/freeradius/3.0/mods-enabled/expr
including configuration file /etc/freeradius/3.0/mods-enabled/passwd
including configuration file /etc/freeradius/3.0/mods-enabled/detail
including files in directory /etc/freeradius/3.0/policy.d/
including configuration file /etc/freeradius/3.0/policy.d/cui
including configuration file /etc/freeradius/3.0/policy.d/dhcp
including configuration file /etc/freeradius/3.0/policy.d/operator-name
including configuration file /etc/freeradius/3.0/policy.d/filter
including configuration file /etc/freeradius/3.0/policy.d/abfab-tr
including configuration file /etc/freeradius/3.0/policy.d/debug
including configuration file /etc/freeradius/3.0/policy.d/control
including configuration file /etc/freeradius/3.0/policy.d/accounting
including configuration file /etc/freeradius/3.0/policy.d/canonicalization
including configuration file /etc/freeradius/3.0/policy.d/eap
including configuration file /etc/freeradius/3.0/policy.d/moonshot-targeted-ids
including files in directory /etc/freeradius/3.0/sites-enabled/
including configuration file /etc/freeradius/3.0/sites-enabled/inner-tunnel
including configuration file /etc/freeradius/3.0/sites-enabled/default
main {
 security {
    user = "freerad"
    group = "freerad"
    allow_core_dumps = no
 }
    name = "freeradius"
    prefix = "/usr"
    localstatedir = "/var"
    logdir = "/var/log/freeradius"
    run_dir = "/var/run/freeradius"
}
main {
    name = "freeradius"
    prefix = "/usr"
    localstatedir = "/var"
    sbindir = "/usr/sbin"
    logdir = "/var/log/freeradius"
    run_dir = "/var/run/freeradius"
    libdir = "/usr/lib/freeradius"
    radacctdir = "/var/log/freeradius/radacct"
    hostname_lookups = no
    max_request_time = 30
    cleanup_delay = 5
    max_requests = 16384
    pidfile = "/var/run/freeradius/freeradius.pid"
    checkrad = "/usr/sbin/checkrad"
    debug_level = 0
    proxy_requests = yes
 log {
    stripped_names = no
    auth = no
    auth_badpass = no
    auth_goodpass = no
    colourise = yes
    msg_denied = "You are already logged in - access denied"
 }
 resources {
 }
 security {
    max_attributes = 200
    reject_delay = 1.000000
    status_server = yes
 }
}
radiusd: #### Loading Realms and Home Servers ####
 proxy server {
    retry_delay = 5
    retry_count = 3
    default_fallback = no
    dead_time = 120
    wake_all_if_all_dead = no
 }
 home_server localhost {
    ipaddr = 127.0.0.1
    port = 1812
    type = "auth"
    secret = <<< secret >>>
    response_window = 20.000000
    response_timeouts = 1
    max_outstanding = 65536
    zombie_period = 40
    status_check = "status-server"
    ping_interval = 30
    check_interval = 30
    check_timeout = 4
    num_answers_to_alive = 3
    revive_interval = 120
  limit {
    max_connections = 16
    max_requests = 0
    lifetime = 0
    idle_timeout = 0
  }
  coa {
    irt = 2
    mrt = 16
    mrc = 5
    mrd = 30
  }
 }
 home_server_pool my_auth_failover {
    type = fail-over
    home_server = localhost
 }
 realm example.com {
    auth_pool = my_auth_failover
 }
 realm LOCAL {
 }
radiusd: #### Loading Clients ####
 client localhost {
    ipaddr = 127.0.0.1
    require_message_authenticator = no
    secret = <<< secret >>>
    nas_type = "other"
    proto = "*"
  limit {
    max_connections = 16
    lifetime = 0
    idle_timeout = 30
  }
 }
 client localhost_ipv6 {
    ipv6addr = ::1
    require_message_authenticator = no
    secret = <<< secret >>>
  limit {
    max_connections = 16
    lifetime = 0
    idle_timeout = 30
  }
 }
 client WLC1 {
    ipaddr = 10.110.0.253
    require_message_authenticator = no
    secret = <<< secret >>>
  limit {
    max_connections = 16
    lifetime = 0
    idle_timeout = 30
  }
 }
 client WLC2 {
    ipaddr = 10.110.0.252
    require_message_authenticator = no
    secret = <<< secret >>>
  limit {
    max_connections = 16
    lifetime = 0
    idle_timeout = 30
  }
 }
 client server {
    ipaddr = 10.16.1.1
    require_message_authenticator = no
    secret = <<< secret >>>
  limit {
    max_connections = 16
    lifetime = 0
    idle_timeout = 30
  }
 }
Debugger not attached
 # Creating Auth-Type = ntlm_auth
 # Creating Auth-Type = mschap
 # Creating Auth-Type = eap
 # Creating Auth-Type = PAP
 # Creating Auth-Type = CHAP
 # Creating Auth-Type = MS-CHAP
 # Creating Auth-Type = digest
radiusd: #### Instantiating modules ####
 modules {
  # Loaded module rlm_cache
  # Loading module "cache_eap" from file /etc/freeradius/3.0/mods-enabled/cache_eap
  cache cache_eap {
    driver = "rlm_cache_rbtree"
    key = "%{%{control:State}:-%{%{reply:State}:-%{State}}}"
    ttl = 15
    max_entries = 0
    epoch = 0
    add_stats = no
  }
  # Loaded module rlm_exec
  # Loading module "exec" from file /etc/freeradius/3.0/mods-enabled/exec
  exec {
    wait = no
    input_pairs = "request"
    shell_escape = yes
    timeout = 10
  }
  # Loaded module rlm_pap
  # Loading module "pap" from file /etc/freeradius/3.0/mods-enabled/pap
  pap {
    normalise = yes
  }
  # Loading module "echo" from file /etc/freeradius/3.0/mods-enabled/echo
  exec echo {
    wait = yes
    program = "/bin/echo %{User-Name}"
    input_pairs = "request"
    output_pairs = "reply"
    shell_escape = yes
  }
  # Loaded module rlm_attr_filter
  # Loading module "attr_filter.post-proxy" from file /etc/freeradius/3.0/mods-enabled/attr_filter
  attr_filter attr_filter.post-proxy {
    filename = "/etc/freeradius/3.0/mods-config/attr_filter/post-proxy"
    key = "%{Realm}"
    relaxed = no
  }
  # Loading module "attr_filter.pre-proxy" from file /etc/freeradius/3.0/mods-enabled/attr_filter
  attr_filter attr_filter.pre-proxy {
    filename = "/etc/freeradius/3.0/mods-config/attr_filter/pre-proxy"
    key = "%{Realm}"
    relaxed = no
  }
  # Loading module "attr_filter.access_reject" from file /etc/freeradius/3.0/mods-enabled/attr_filter
  attr_filter attr_filter.access_reject {
    filename = "/etc/freeradius/3.0/mods-config/attr_filter/access_reject"
    key = "%{User-Name}"
    relaxed = no
  }
  # Loading module "attr_filter.access_challenge" from file /etc/freeradius/3.0/mods-enabled/attr_filter
  attr_filter attr_filter.access_challenge {
    filename = "/etc/freeradius/3.0/mods-config/attr_filter/access_challenge"
    key = "%{User-Name}"
    relaxed = no
  }
  # Loading module "attr_filter.accounting_response" from file /etc/freeradius/3.0/mods-enabled/attr_filter
  attr_filter attr_filter.accounting_response {
    filename = "/etc/freeradius/3.0/mods-config/attr_filter/accounting_response"
    key = "%{User-Name}"
    relaxed = no
  }
  # Loaded module rlm_radutmp
  # Loading module "radutmp" from file /etc/freeradius/3.0/mods-enabled/radutmp
  radutmp {
    filename = "/var/log/freeradius/radutmp"
    username = "%{User-Name}"
    case_sensitive = yes
    check_with_nas = yes
    permissions = 384
    caller_id = yes
  }
  # Loaded module rlm_dynamic_clients
  # Loading module "dynamic_clients" from file /etc/freeradius/3.0/mods-enabled/dynamic_clients
  # Loaded module rlm_digest
  # Loading module "digest" from file /etc/freeradius/3.0/mods-enabled/digest
  # Loaded module rlm_linelog
  # Loading module "linelog" from file /etc/freeradius/3.0/mods-enabled/linelog
  linelog {
    filename = "/var/log/freeradius/linelog"
    escape_filenames = no
    syslog_severity = "info"
    permissions = 384
    format = "This is a log message for %{User-Name}"
    reference = "messages.%{%{reply:Packet-Type}:-default}"
  }
  # Loading module "log_accounting" from file /etc/freeradius/3.0/mods-enabled/linelog
  linelog log_accounting {
    filename = "/var/log/freeradius/linelog-accounting"
    escape_filenames = no
    syslog_severity = "info"
    permissions = 384
    format = ""
    reference = "Accounting-Request.%{%{Acct-Status-Type}:-unknown}"
  }
  # Loaded module rlm_files
  # Loading module "files" from file /etc/freeradius/3.0/mods-enabled/files
  files {
    filename = "/etc/freeradius/3.0/mods-config/files/authorize"
    acctusersfile = "/etc/freeradius/3.0/mods-config/files/accounting"
    preproxy_usersfile = "/etc/freeradius/3.0/mods-config/files/pre-proxy"
  }
  # Loaded module rlm_unix
  # Loading module "unix" from file /etc/freeradius/3.0/mods-enabled/unix
  unix {
    radwtmp = "/var/log/freeradius/radwtmp"
  }
Creating attribute Unix-Group
  # Loaded module rlm_chap
  # Loading module "chap" from file /etc/freeradius/3.0/mods-enabled/chap
  # Loaded module rlm_logintime
  # Loading module "logintime" from file /etc/freeradius/3.0/mods-enabled/logintime
  logintime {
    minimum_timeout = 60
  }
  # Loading module "ntlm_auth" from file /etc/freeradius/3.0/mods-enabled/ntlm_auth
  exec ntlm_auth {
    wait = yes
    program = "/usr/bin/ntlm_auth --request-nt-key --domain=MEINESCHULE --username=%{mschap:User-Name} --
password=%{User-Password}"
    shell_escape = yes
  }
  # Loaded module rlm_realm
  # Loading module "IPASS" from file /etc/freeradius/3.0/mods-enabled/realm
  realm IPASS {
    format = "prefix"
    delimiter = "/"
    ignore_default = no
    ignore_null = no
  }
  # Loading module "suffix" from file /etc/freeradius/3.0/mods-enabled/realm
  realm suffix {
    format = "suffix"
    delimiter = "@"
    ignore_default = no
    ignore_null = no
  }
  # Loading module "realmpercent" from file /etc/freeradius/3.0/mods-enabled/realm
  realm realmpercent {
    format = "suffix"
    delimiter = "%"
    ignore_default = no
    ignore_null = no
  }
  # Loading module "ntdomain" from file /etc/freeradius/3.0/mods-enabled/realm
  realm ntdomain {
    format = "prefix"
    delimiter = "\\"
    ignore_default = no
    ignore_null = no
  }
  # Loaded module rlm_replicate
  # Loading module "replicate" from file /etc/freeradius/3.0/mods-enabled/replicate
  # Loaded module rlm_expiration
  # Loading module "expiration" from file /etc/freeradius/3.0/mods-enabled/expiration
  # Loaded module rlm_always
  # Loading module "reject" from file /etc/freeradius/3.0/mods-enabled/always
  always reject {
    rcode = "reject"
    simulcount = 0
    mpp = no
  }
  # Loading module "fail" from file /etc/freeradius/3.0/mods-enabled/always
  always fail {
    rcode = "fail"
    simulcount = 0
    mpp = no
  }
  # Loading module "ok" from file /etc/freeradius/3.0/mods-enabled/always
  always ok {
    rcode = "ok"
    simulcount = 0
    mpp = no
  }
  # Loading module "handled" from file /etc/freeradius/3.0/mods-enabled/always
  always handled {
    rcode = "handled"
    simulcount = 0
    mpp = no
  }
  # Loading module "invalid" from file /etc/freeradius/3.0/mods-enabled/always
  always invalid {
    rcode = "invalid"
    simulcount = 0
    mpp = no
  }
  # Loading module "userlock" from file /etc/freeradius/3.0/mods-enabled/always
  always userlock {
    rcode = "userlock"
    simulcount = 0
    mpp = no
  }
  # Loading module "notfound" from file /etc/freeradius/3.0/mods-enabled/always
  always notfound {
    rcode = "notfound"
    simulcount = 0
    mpp = no
  }
  # Loading module "noop" from file /etc/freeradius/3.0/mods-enabled/always
  always noop {
    rcode = "noop"
    simulcount = 0
    mpp = no
  }
  # Loading module "updated" from file /etc/freeradius/3.0/mods-enabled/always
  always updated {
    rcode = "updated"
```

```
    simulcount = 0
    mpp = no
  }
  # Loaded module rlm_unpack
  # Loading module "unpack" from file /etc/freeradius/3.0/mods-enabled/unpack
  # Loaded module rlm_utf8
  # Loading module "utf8" from file /etc/freeradius/3.0/mods-enabled/utf8
  # Loaded module rlm_detail
  # Loading module "auth_log" from file /etc/freeradius/3.0/mods-enabled/detail.log
  detail auth_log {
    filename = "/var/log/freeradius/radacct/%{%{Packet-Src-IP-Address}:-%{Packet-Src-IPv6-Address}}/auth-
detail-%Y%m%d"
    header = "%t"
    permissions = 384
    locking = no
    escape_filenames = no
    log_packet_header = no
  }
  # Loading module "reply_log" from file /etc/freeradius/3.0/mods-enabled/detail.log
  detail reply_log {
    filename = "/var/log/freeradius/radacct/%{%{Packet-Src-IP-Address}:-%{Packet-Src-IPv6-Address}}/reply-
detail-%Y%m%d"
    header = "%t"
    permissions = 384
    locking = no
    escape_filenames = no
    log_packet_header = no
  }
  # Loading module "pre_proxy_log" from file /etc/freeradius/3.0/mods-enabled/detail.log
  detail pre_proxy_log {
    filename = "/var/log/freeradius/radacct/%{%{Packet-Src-IP-Address}:-%{Packet-Src-IPv6-Address}}/pre-proxy-
detail-%Y%m%d"
    header = "%t"
    permissions = 384
    locking = no
    escape_filenames = no
    log_packet_header = no
  }
  # Loading module "post_proxy_log" from file /etc/freeradius/3.0/mods-enabled/detail.log
  detail post_proxy_log {
    filename = "/var/log/freeradius/radacct/%{%{Packet-Src-IP-Address}:-%{Packet-Src-IPv6-Address}}/post-proxy-
detail-%Y%m%d"
    header = "%t"
    permissions = 384
    locking = no
    escape_filenames = no
    log_packet_header = no
  }
  # Loaded module rlm_soh
  # Loading module "soh" from file /etc/freeradius/3.0/mods-enabled/soh
  soh {
    dhcp = yes
  }
  # Loading module "sradutmp" from file /etc/freeradius/3.0/mods-enabled/sradutmp
  radutmp sradutmp {
    filename = "/var/log/freeradius/sradutmp"
    username = "%{User-Name}"
    case_sensitive = yes
    check_with_nas = yes
    permissions = 420
    caller_id = no
  }
  # Loaded module rlm_mschap
  # Loading module "mschap" from file /etc/freeradius/3.0/mods-enabled/mschap
  mschap {
    use_mppe = yes
    require_encryption = no
    require_strong = no
    with_ntdomain_hack = yes
   passchange {
    ntlm_auth = "/usr/bin/ntlm_auth --request-nt-key --domain=MEINESCHULE  --username=%{%{Stripped-User-Name}:-
%{%{User-Name}:-None}} --challenge=%{%{mschap:Challenge}:-00} --nt-response=%{%{mschap:NT-Response}:-00}"
   }
    allow_retry = yes
    winbind_retry_with_normalised_username = no
  }
  # Loaded module rlm_eap
  # Loading module "eap" from file /etc/freeradius/3.0/mods-enabled/eap
  eap {
    default_eap_type = "md5"
    timer_expire = 60
    ignore_unknown_eap_types = no
    cisco_accounting_username_bug = no
    max_sessions = 16384
  }
  # Loaded module rlm_preprocess
  # Loading module "preprocess" from file /etc/freeradius/3.0/mods-enabled/preprocess
  preprocess {
    huntgroups = "/etc/freeradius/3.0/mods-config/preprocess/huntgroups"
    hints = "/etc/freeradius/3.0/mods-config/preprocess/hints"
    with_ascend_hack = no
    ascend_channels_per_line = 23
    with_ntdomain_hack = no
    with_specialix_jetstream_hack = no
    with_cisco_vsa_hack = no
    with_alvarion_vsa_hack = no
  }
  # Loaded module rlm_expr
  # Loading module "expr" from file /etc/freeradius/3.0/mods-enabled/expr
  expr {
    safe_characters = "@abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789.-_: /
äéöüàâæçèéêëîïôœùûüaÿÄÉÖÜßÀÂÆÇÈÉÊËÎÏÔŒÙÛÜŸ"
  }
  # Loaded module rlm_passwd
  # Loading module "etc_passwd" from file /etc/freeradius/3.0/mods-enabled/passwd
  passwd etc_passwd {
    filename = "/etc/passwd"
    format = "*User-Name:Crypt-Password:"
    delimiter = ":"
    ignore_nislike = no
    ignore_empty = yes
    allow_multiple_keys = no
    hash_size = 100
  }
  # Loading module "detail" from file /etc/freeradius/3.0/mods-enabled/detail
  detail {
    filename = "/var/log/freeradius/radacct/%{%{Packet-Src-IP-Address}:-%{Packet-Src-IPv6-Address}}/detail-
%Y%m%d"
    header = "%t"
    permissions = 384
    locking = no
    escape_filenames = no
    log_packet_header = no
  }
  instantiate {
  }
  # Instantiating module "cache_eap" from file /etc/freeradius/3.0/mods-enabled/cache_eap
rlm_cache (cache_eap): Driver rlm_cache_rbtree (module rlm_cache_rbtree) loaded and linked
  # Instantiating module "pap" from file /etc/freeradius/3.0/mods-enabled/pap
  # Instantiating module "attr_filter.post-proxy" from file /etc/freeradius/3.0/mods-enabled/attr_filter
reading pairlist file /etc/freeradius/3.0/mods-config/attr_filter/post-proxy
  # Instantiating module "attr_filter.pre-proxy" from file /etc/freeradius/3.0/mods-enabled/attr_filter
reading pairlist file /etc/freeradius/3.0/mods-config/attr_filter/pre-proxy
  # Instantiating module "attr_filter.access_reject" from file /etc/freeradius/3.0/mods-enabled/attr_filter
reading pairlist file /etc/freeradius/3.0/mods-config/attr_filter/access_reject
[/etc/freeradius/3.0/mods-config/attr_filter/access_reject]:11 Check item "FreeRADIUS-Response-Delay"   found
in filter list for realm "DEFAULT".
[/etc/freeradius/3.0/mods-config/attr_filter/access_reject]:11 Check item "FreeRADIUS-Response-Delay-USec"
found in filter list for realm "DEFAULT".
  # Instantiating module "attr_filter.access_challenge" from file /etc/freeradius/3.0/mods-enabled/attr_filter
reading pairlist file /etc/freeradius/3.0/mods-config/attr_filter/access_challenge
  # Instantiating module "attr_filter.accounting_response" from file /etc/freeradius/3.0/mods-enabled/-
attr_filter
reading pairlist file /etc/freeradius/3.0/mods-config/attr_filter/accounting_response
  # Instantiating module "linelog" from file /etc/freeradius/3.0/mods-enabled/linelog
  # Instantiating module "log_accounting" from file /etc/freeradius/3.0/mods-enabled/linelog
  # Instantiating module "files" from file /etc/freeradius/3.0/mods-enabled/files
reading pairlist file /etc/freeradius/3.0/mods-config/files/authorize
reading pairlist file /etc/freeradius/3.0/mods-config/files/accounting
reading pairlist file /etc/freeradius/3.0/mods-config/files/pre-proxy
  # Instantiating module "logintime" from file /etc/freeradius/3.0/mods-enabled/logintime
  # Instantiating module "IPASS" from file /etc/freeradius/3.0/mods-enabled/realm
  # Instantiating module "suffix" from file /etc/freeradius/3.0/mods-enabled/realm
  # Instantiating module "realmpercent" from file /etc/freeradius/3.0/mods-enabled/realm
  # Instantiating module "ntdomain" from file /etc/freeradius/3.0/mods-enabled/realm
  # Instantiating module "expiration" from file /etc/freeradius/3.0/mods-enabled/expiration
  # Instantiating module "reject" from file /etc/freeradius/3.0/mods-enabled/always
  # Instantiating module "fail" from file /etc/freeradius/3.0/mods-enabled/always
  # Instantiating module "ok" from file /etc/freeradius/3.0/mods-enabled/always
  # Instantiating module "handled" from file /etc/freeradius/3.0/mods-enabled/always
  # Instantiating module "invalid" from file /etc/freeradius/3.0/mods-enabled/always
  # Instantiating module "userlock" from file /etc/freeradius/3.0/mods-enabled/always
  # Instantiating module "notfound" from file /etc/freeradius/3.0/mods-enabled/always
  # Instantiating module "noop" from file /etc/freeradius/3.0/mods-enabled/always
  # Instantiating module "updated" from file /etc/freeradius/3.0/mods-enabled/always
  # Instantiating module "auth_log" from file /etc/freeradius/3.0/mods-enabled/detail.log
rlm_detail (auth_log): 'User-Password' suppressed, will not appear in detail output
  # Instantiating module "reply_log" from file /etc/freeradius/3.0/mods-enabled/detail.log
  # Instantiating module "pre_proxy_log" from file /etc/freeradius/3.0/mods-enabled/detail.log
  # Instantiating module "post_proxy_log" from file /etc/freeradius/3.0/mods-enabled/detail.log
  # Instantiating module "mschap" from file /etc/freeradius/3.0/mods-enabled/mschap
rlm_mschap (mschap): using internal authentication
  # Instantiating module "eap" from file /etc/freeradius/3.0/mods-enabled/eap
   # Linked to sub-module rlm_eap_md5
   # Linked to sub-module rlm_eap_leap
   # Linked to sub-module rlm_eap_gtc
   gtc {
    challenge = "Password: "
    auth_type = "PAP"
   }
   # Linked to sub-module rlm_eap_tls
   tls {
    tls = "tls-common"
   }
   tls-config tls-common {
    verify_depth = 0
    ca_path = "/etc/freeradius/3.0/certs"
    pem_file_type = yes
    private_key_file = "/etc/ssl/private/ssl-cert-snakeoil.key"
    certificate_file = "/etc/ssl/certs/ssl-cert-snakeoil.pem"
    ca_file = "/etc/ssl/certs/ca-certificates.crt"
    private_key_password = <<< secret >>>
    dh_file = "/etc/freeradius/3.0/certs/dh"
    fragment_size = 1024
    include_length = yes
    auto_chain = yes
    check_crl = no
    check_all_crl = no
    cipher_list = "DEFAULT"
    cipher_server_preference = no
    ecdh_curve = "prime256v1"
    tls_max_version = ""
    tls_min_version = "1.0"
    cache {
        enable = no
        lifetime = 24
        max_entries = 255
    }
    verify {
        skip_if_ocsp_ok = no
    }
    ocsp {
        enable = no
        override_cert_url = yes
        url = "http://127.0.0.1/ocsp/"
        use_nonce = yes
        timeout = 0
        softfail = no
    }
   }
   # Linked to sub-module rlm_eap_ttls
   ttls {
    tls = "tls-common"
    default_eap_type = "md5"
    copy_request_to_tunnel = no
    use_tunneled_reply = no
    virtual_server = "inner-tunnel"
    include_length = yes
    require_client_cert = no
   }
tls: Using cached TLS configuration from previous invocation
   # Linked to sub-module rlm_eap_peap
   peap {
    tls = "tls-common"
    default_eap_type = "mschapv2"
    copy_request_to_tunnel = no
    use_tunneled_reply = no
    proxy_tunneled_request_as_eap = yes
    virtual_server = "inner-tunnel"
    soh = no
    require_client_cert = no
   }
tls: Using cached TLS configuration from previous invocation
   # Linked to sub-module rlm_eap_mschapv2
   mschapv2 {
    with_ntdomain_hack = no
    send_error = no
   }
  # Instantiating module "preprocess" from file /etc/freeradius/3.0/mods-enabled/preprocess
reading pairlist file /etc/freeradius/3.0/mods-config/preprocess/huntgroups
reading pairlist file /etc/freeradius/3.0/mods-config/preprocess/hints
  # Instantiating module "etc_passwd" from file /etc/freeradius/3.0/mods-enabled/passwd
rlm_passwd: nfields: 3 keyfield 0(User-Name) listable: no
  # Instantiating module "detail" from file /etc/freeradius/3.0/mods-enabled/detail
 } # modules
radiusd: #### Loading Virtual Servers ####
server { # from file /etc/freeradius/3.0/radiusd.conf
} # server
server inner-tunnel { # from file /etc/freeradius/3.0/sites-enabled/inner-tunnel
 # Loading authenticate {...}
 # Loading authorize {...}
Ignoring "sql" (see raddb/mods-available/README.rst)
Ignoring "ldap" (see raddb/mods-available/README.rst)
 # Loading session {...}
 # Loading post-proxy {...}
 # Loading post-auth {...}
 # Skipping contents of 'if' as it is always 'false' -- /etc/freeradius/3.0/sites-enabled/inner-tunnel:332
} # server inner-tunnel
server default { # from file /etc/freeradius/3.0/sites-enabled/default
 # Loading authenticate {...}
 # Loading authorize {...}
 # Loading preacct {...}
 # Loading accounting {...}
 # Loading post-proxy {...}
 # Loading post-auth {...}
} # server default
radiusd: #### Opening IP addresses and Ports ####
listen {
    type = "auth"
    ipaddr = 127.0.0.1
    port = 18120
}
listen {
    type = "auth"
    ipaddr = *
    port = 0
   limit {
    max_connections = 16
    lifetime = 0
    idle_timeout = 30
   }
}
listen {
    type = "acct"
    ipaddr = *
    port = 0
   limit {
    max_connections = 16
    lifetime = 0
    idle_timeout = 30
   }
}
listen {
    type = "auth"
    ipv6addr = ::
    port = 0
   limit {
    max_connections = 16
    lifetime = 0
    idle_timeout = 30
   }
}
listen {
    type = "acct"
    ipv6addr = ::
    port = 0
   limit {
    max_connections = 16
    lifetime = 0
    idle_timeout = 30
   }
}
Listening on auth address 127.0.0.1 port 18120 bound to server inner-tunnel
Listening on auth address * port 1812 bound to server default
Listening on acct address * port 1813 bound to server default
Listening on auth address :: port 1812 bound to server default
Listening on acct address :: port 1813 bound to server default
Listening on proxy address * port 41418
Listening on proxy address :: port 36491
Ready to process requests
(0) Received Access-Request Id 196 from 10.110.0.253:8234 to 10.16.1.1:1812 length 231
(0)   User-Name = "testBenutzer"
(0)   NAS-Identifier = "WLC-Meineschule-1"
(0)   LCS-Orig-NAS-Identifier = "00A057604255"
(0)   Called-Station-Id = "0E-A0-57-60-42-58:gym-lehrer"
(0)   NAS-Port-Type = Wireless-802.11
(0)   Service-Type = Framed-User
(0)   Calling-Station-Id = "6C-C7-EC-60-61-34"
(0)   Connect-Info = "CONNECT"
(0)   Acct-Session-Id = "6A9B660E04CEDD34"
(0)   Acct-Multi-Session-Id = "A0100112F84B93E3"
(0)   WLAN-Pairwise-Cipher = 1027076
(0)   WLAN-Group-Cipher = 1027076
(0)   WLAN-AKM-Suite = 1027073
(0)   Framed-MTU = 1400
(0)   EAP-Message = 0x02ec000c01736368756c7465
(0)   Message-Authenticator = 0xb08528876284122a9a618e4af0a55de0
(0) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/default
(0)   authorize {
(0)     policy filter_username {
(0)       if (&User-Name) {
(0)       if (&User-Name)  -> TRUE
(0)       if (&User-Name)  {
(0)         if (&User-Name =~ / /) {
(0)         if (&User-Name =~ / /)  -> FALSE
(0)         if (&User-Name =~ /@[^@]*@/ ) {
(0)         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(0)         if (&User-Name =~ /\.\./ ) {
(0)         if (&User-Name =~ /\.\./ )  -> FALSE
(0)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))  {
(0)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))   -> FALSE
(0)         if (&User-Name =~ /\.$/)  {
(0)         if (&User-Name =~ /\.$/)   -> FALSE
(0)         if (&User-Name =~ /@\./)  {
(0)         if (&User-Name =~ /@\./)   -> FALSE
(0)       } # if (&User-Name)  = notfound
(0)     } # policy filter_username = notfound
(0)     [preprocess] = ok
(0)     [chap] = noop
(0)     [mschap] = noop
```

```
(0)     [digest] = noop
(0) suffix: Checking for suffix after "@"
(0) suffix: No '@' in User-Name = "testBenutzer", looking up realm NULL
(0) suffix: No such realm "NULL"
(0)     [suffix] = noop
(0) eap: Peer sent EAP Response (code 2) ID 236 length 12
(0) eap: EAP-Identity reply, returning 'ok' so we can short-circuit the rest of authorize
(0)     [eap] = ok
(0)   } # authorize = ok
(0) Found Auth-Type = eap
(0) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(0)   authenticate {
(0) eap: Peer sent packet with method EAP Identity (1)
(0) eap: Calling submodule eap_md5 to process data
(0) eap_md5: Issuing MD5 Challenge
(0) eap: Sending EAP Request (code 1) ID 237 length 22
(0) eap: EAP session adding &reply:State = 0xcfa27713cf4f7300
(0)     [eap] = handled
(0)   } # authenticate = handled
(0) Using Post-Auth-Type Challenge
(0) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(0)   Challenge { ... } # empty sub-section is ignored
(0) Sent Access-Challenge Id 196 from 10.16.1.1:1812 to 10.110.0.253:8234 length 0
(0)   EAP-Message = 0x01ed0016041061d864ed1a023647d3c4b5e0a6c73978
(0)   Message-Authenticator = 0x00000000000000000000000000000000
(0)   State = 0xcfa27713cf4f730013767f5546bb62c5
(0) Finished request
Waking up in 4.9 seconds.
(1) Received Access-Request Id 197 from 10.110.0.253:12633 to 10.16.1.1:1812 length 243
(1)   User-Name = "testBenutzer"
(1)   NAS-Identifier = "WLC-Meineschule-1"
(1)   LCS-Orig-NAS-Identifier = "00A057604255"
(1)   Called-Station-Id = "0E-A0-57-60-42-58:gym-lehrer"
(1)   NAS-Port-Type = Wireless-802.11
(1)   Service-Type = Framed-User
(1)   Calling-Station-Id = "6C-C7-EC-60-61-34"
(1)   Connect-Info = "CONNECT"
(1)   Acct-Session-Id = "6A9B660E04CEDD34"
(1)   Acct-Multi-Session-Id = "A0100112F84B93E3"
(1)   WLAN-Pairwise-Cipher = 1027076
(1)   WLAN-Group-Cipher = 1027076
(1)   WLAN-AKM-Suite = 1027073
(1)   Framed-MTU = 1400
(1)   EAP-Message = 0x02ed00060319
(1)   State = 0xcfa27713cf4f730013767f5546bb62c5
(1)   Message-Authenticator = 0x3e498a830986b35511ecd44c696d14b0
(1) session-state: No cached attributes
(1) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/default
(1)   authorize {
(1)     policy filter_username {
(1)       if (&User-Name) {
(1)       if (&User-Name)  -> TRUE
(1)       if (&User-Name)  {
(1)         if (&User-Name =~ / /) {
(1)         if (&User-Name =~ / /)  -> FALSE
(1)         if (&User-Name =~ /@[^@]*@/ ) {
(1)         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(1)         if (&User-Name =~ /\.\./ ) {
(1)         if (&User-Name =~ /\.\./ )  -> FALSE
(1)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))  {
(1)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))   -> FALSE
(1)         if (&User-Name =~ /\.$/)  {
(1)         if (&User-Name =~ /\.$/)   -> FALSE
(1)         if (&User-Name =~ /@\./)  {
(1)         if (&User-Name =~ /@\./)   -> FALSE
(1)       } # if (&User-Name)  = notfound
(1)     } # policy filter_username = notfound
(1)     [preprocess] = ok
(1)     [chap] = noop
(1)     [mschap] = noop
(1)     [digest] = noop
(1) suffix: Checking for suffix after "@"
(1) suffix: No '@' in User-Name = "testBenutzer", looking up realm NULL
(1) suffix: No such realm "NULL"
```

```
(1)     [suffix] = noop
(1) eap: Peer sent EAP Response (code 2) ID 237 length 6
(1) eap: No EAP Start, assuming it's an on-going EAP conversation
(1)     [eap] = updated
(1) files: users: Matched entry DEFAULT at line 1
(1)     [files] = ok
(1)     [expiration] = noop
(1)     [logintime] = noop
(1) pap: WARNING: No "known good" password found for the user.  Not setting Auth-Type
(1) pap: WARNING: Authentication will fail unless a "known good" password is available
(1)     [pap] = noop
(1)   } # authorize = updated
(1) Found Auth-Type = eap
(1) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(1)   authenticate {
(1) eap: Expiring EAP session with state 0xcfa27713cf4f7300
(1) eap: Finished EAP session with state 0xcfa27713cf4f7300
(1) eap: Previous EAP request found for state 0xcfa27713cf4f7300, released from the list
(1) eap: Peer sent packet with method EAP NAK (3)
(1) eap: Found mutually acceptable type PEAP (25)
(1) eap: Calling submodule eap_peap to process data
(1) eap_peap: Initiating new EAP-TLS session
(1) eap_peap: [eaptls start] = request
(1) eap: Sending EAP Request (code 1) ID 238 length 6
(1) eap: EAP session adding &reply:State = 0xcfa27713ce4c6e00
(1)     [eap] = handled
(1)   } # authenticate = handled
(1) Using Post-Auth-Type Challenge
(1) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(1)   Challenge { ... } # empty sub-section is ignored
(1) Sent Access-Challenge Id 197 from 10.16.1.1:1812 to 10.110.0.253:12633 length 0
(1)   EAP-Message = 0x01ee00061920
(1)   Message-Authenticator = 0x00000000000000000000000000000000
(1)   State = 0xcfa27713ce4c6e0013767f5546bb62c5
(1) Finished request
Waking up in 4.8 seconds.
(2) Received Access-Request Id 198 from 10.110.0.253:14835 to 10.16.1.1:1812 length 404
(2)   User-Name = "testBenutzer"
(2)   NAS-Identifier = "WLC-Meineschule-1"
(2)   LCS-Orig-NAS-Identifier = "00A057604255"
(2)   Called-Station-Id = "0E-A0-57-60-42-58:gym-lehrer"
(2)   NAS-Port-Type = Wireless-802.11
(2)   Service-Type = Framed-User
(2)   Calling-Station-Id = "6C-C7-EC-60-61-34"
(2)   Connect-Info = "CONNECT"
(2)   Acct-Session-Id = "6A9B660E04CEDD34"
(2)   Acct-Multi-Session-Id = "A0100112F84B93E3"
(2)   WLAN-Pairwise-Cipher = 1027076
(2)   WLAN-Group-Cipher = 1027076
(2)   WLAN-AKM-Suite = 1027073
(2)   Framed-MTU = 1400
(2)   EAP-Message = 
0x02ee00a719800000009d160301009801000094 0303b4723035b2b1dc9da791a924aae8460804265072dcec797dbad4e01f2fc5916700003cc
(2)   State = 0xcfa27713ce4c6e0013767f5546bb62c5
(2)   Message-Authenticator = 0x57e553c044ba381d9ddd794f7a18f3c1
(2) session-state: No cached attributes
(2) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/default
(2)   authorize {
(2)     policy filter_username {
(2)       if (&User-Name) {
(2)       if (&User-Name)  -> TRUE
(2)       if (&User-Name)  {
(2)         if (&User-Name =~ / /) {
(2)         if (&User-Name =~ / /)  -> FALSE
(2)         if (&User-Name =~ /@[^@]*@/ ) {
(2)         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(2)         if (&User-Name =~ /\.\./ ) {
(2)         if (&User-Name =~ /\.\./ )  -> FALSE
(2)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))  {
(2)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))   -> FALSE
(2)         if (&User-Name =~ /\.$/)  {
(2)         if (&User-Name =~ /\.$/)   -> FALSE
(2)         if (&User-Name =~ /@\./)  {
(2)         if (&User-Name =~ /@\./)   -> FALSE
(2)       } # if (&User-Name)  = notfound
(2)     } # policy filter_username = notfound
(2)     [preprocess] = ok
(2)     [chap] = noop
(2)     [mschap] = noop
(2)     [digest] = noop
(2) suffix: Checking for suffix after "@"
(2) suffix: No '@' in User-Name = "testBenutzer", looking up realm NULL
(2) suffix: No such realm "NULL"
(2)     [suffix] = noop
(2) eap: Peer sent EAP Response (code 2) ID 238 length 167
(2) eap: Continuing tunnel setup
(2)     [eap] = ok
(2)   } # authorize = ok
(2) Found Auth-Type = eap
(2) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(2)   authenticate {
(2) eap: Expiring EAP session with state 0xcfa27713ce4c6e00
(2) eap: Finished EAP session with state 0xcfa27713ce4c6e00
(2) eap: Previous EAP request found for state 0xcfa27713ce4c6e00, released from the list
(2) eap: Peer sent packet with method EAP PEAP (25)
(2) eap: Calling submodule eap_peap to process data
(2) eap_peap: Continuing EAP-TLS
(2) eap_peap: Peer indicated complete TLS record size will be 157 bytes
(2) eap_peap: Got complete TLS record (157 bytes)
(2) eap_peap: [eaptls verify] = length included
(2) eap_peap: (other): before SSL initialization
(2) eap_peap: TLS_accept: before SSL initialization
(2) eap_peap: TLS_accept: before SSL initialization
(2) eap_peap: <<< recv UNKNOWN TLS VERSION ?0304? [length 0098]
(2) eap_peap: TLS_accept: SSLv3/TLS read client hello
(2) eap_peap: >>> send TLS 1.2  [length 003d]
(2) eap_peap: TLS_accept: SSLv3/TLS write server hello
(2) eap_peap: >>> send TLS 1.2  [length 02d3]
(2) eap_peap: TLS_accept: SSLv3/TLS write certificate
(2) eap_peap: >>> send TLS 1.2  [length 014d]
(2) eap_peap: TLS_accept: SSLv3/TLS write key exchange
(2) eap_peap: >>> send TLS 1.2  [length 0004]
(2) eap_peap: TLS_accept: SSLv3/TLS write server done
(2) eap_peap: TLS_accept: Need to read more data: SSLv3/TLS write server done
(2) eap_peap: In SSL Handshake Phase
(2) eap_peap: In SSL Accept mode
(2) eap_peap: [eaptls process] = handled
(2) eap: Sending EAP Request (code 1) ID 239 length 1004
(2) eap: EAP session adding &reply:State = 0xcfa27713cd4d6e00
(2)     [eap] = handled
(2)   } # authenticate = handled
(2) Using Post-Auth-Type Challenge
(2) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(2)   Challenge { ... } # empty sub-section is ignored
(2) Sent Access-Challenge Id 198 from 10.16.1.1:1812 to 10.110.0.253:14835 length 0
(2)   EAP-Message = 
0x01ef03ec19c000000475160303003d020000390303081e3e50e70bc6ac29390616b4f0547417e732ad228d62ae0d520f696c7b91f400c02f00
(2)   Message-Authenticator = 0x00000000000000000000000000000000
(2)   State = 0xcfa27713cd4d6e0013767f5546bb62c5
(2) Finished request
Waking up in 4.8 seconds.
(3) Received Access-Request Id 199 from 10.110.0.253:8667 to 10.16.1.1:1812 length 243
(3)   User-Name = "testBenutzer"
(3)   NAS-Identifier = "WLC-Meineschule-1"
(3)   LCS-Orig-NAS-Identifier = "00A057604255"
(3)   Called-Station-Id = "0E-A0-57-60-42-58:gym-lehrer"
(3)   NAS-Port-Type = Wireless-802.11
(3)   Service-Type = Framed-User
(3)   Calling-Station-Id = "6C-C7-EC-60-61-34"
(3)   Connect-Info = "CONNECT"
(3)   Acct-Session-Id = "6A9B660E04CEDD34"
(3)   Acct-Multi-Session-Id = "A0100112F84B93E3"
(3)   WLAN-Pairwise-Cipher = 1027076
(3)   WLAN-Group-Cipher = 1027076
(3)   WLAN-AKM-Suite = 1027073
(3)   Framed-MTU = 1400
(3)   EAP-Message = 0x02ef00061900
(3)   State = 0xcfa27713cd4d6e0013767f5546bb62c5
```

```
(3)   Message-Authenticator = 0xfa9a4cbfbc2065d0aea94728da268566
(3) session-state: No cached attributes
(3) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/default
(3)   authorize {
(3)     policy filter_username {
(3)       if (&User-Name) {
(3)       if (&User-Name)  -> TRUE
(3)       if (&User-Name)  {
(3)         if (&User-Name =~ / /) {
(3)         if (&User-Name =~ / /)  -> FALSE
(3)         if (&User-Name =~ /@[^@]*@/ ) {
(3)         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(3)         if (&User-Name =~ /\.\./ ) {
(3)         if (&User-Name =~ /\.\./ )  -> FALSE
(3)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))  {
(3)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))   -> FALSE
(3)         if (&User-Name =~ /\.$/)  {
(3)         if (&User-Name =~ /\.$/)   -> FALSE
(3)         if (&User-Name =~ /@\./)  {
(3)         if (&User-Name =~ /@\./)   -> FALSE
(3)       } # if (&User-Name)  = notfound
(3)     } # policy filter_username = notfound
(3)     [preprocess] = ok
(3)     [chap] = noop
(3)     [mschap] = noop
(3)     [digest] = noop
(3) suffix: Checking for suffix after "@"
(3) suffix: No '@' in User-Name = "testBenutzer", looking up realm NULL
(3) suffix: No such realm "NULL"
(3)     [suffix] = noop
(3) eap: Peer sent EAP Response (code 2) ID 239 length 6
(3) eap: Continuing tunnel setup
(3)     [eap] = ok
(3)   } # authorize = ok
(3) Found Auth-Type = eap
(3) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(3)   authenticate {
(3) eap: Expiring EAP session with state 0xcfa27713cd4d6e00
(3) eap: Finished EAP session with state 0xcfa27713cd4d6e00
(3) eap: Previous EAP request found for state 0xcfa27713cd4d6e00, released from the list
(3) eap: Peer sent packet with method EAP PEAP (25)
(3) eap: Calling submodule eap_peap to process data
(3) eap_peap: Continuing EAP-TLS
(3) eap_peap: Peer ACKed our handshake fragment
(3) eap_peap: [eaptls verify] = request
(3) eap_peap: [eaptls process] = handled
(3) eap: Sending EAP Request (code 1) ID 240 length 153
(3) eap: EAP session adding &reply:State = 0xcfa27713cc526e00
(3)     [eap] = handled
(3)   } # authenticate = handled
(3) Using Post-Auth-Type Challenge
(3) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(3)   Challenge { ... } # empty sub-section is ignored
(3) Sent Access-Challenge Id 199 from 10.16.1.1:1812 to 10.110.0.253:8667 length 0
(3)   EAP-Message = 
0x01f0009919003c8c3a72cfba96ce0fb38205db6138126cca3ca2a6e0ef0e6bb5e259891c10995bd9083d67bfe417d11f6fd5b40fc3cdb402b6
(3)   Message-Authenticator = 0x00000000000000000000000000000000
(3)   State = 0xcfa27713cc526e0013767f5546bb62c5
(3) Finished request
Waking up in 4.7 seconds.
(0) Cleaning up request packet ID 196 with timestamp +45
Waking up in 0.1 seconds.
(1) Cleaning up request packet ID 197 with timestamp +45
(2) Cleaning up request packet ID 198 with timestamp +45
Waking up in 0.1 seconds.
(3) Cleaning up request packet ID 199 with timestamp +45
Ready to process requests
(4) Received Access-Request Id 200 from 10.110.0.253:8364 to 10.16.1.1:1812 length 231
(4)   User-Name = "testBenutzer"
(4)   NAS-Identifier = "WLC-Meineschule-1"
(4)   LCS-Orig-NAS-Identifier = "00A057604249"
(4)   Called-Station-Id = "12-A0-57-60-42-4C:gym-lehrer"
(4)   NAS-Port-Type = Wireless-802.11
(4)   Service-Type = Framed-User
```

```
(4)   Calling-Station-Id = "6C-C7-EC-60-61-34"
(4)   Connect-Info = "CONNECT"
(4)   Acct-Session-Id = "01E8C32B02BC44A4"
(4)   Acct-Multi-Session-Id = "949304E139FEEDD5"
(4)   WLAN-Pairwise-Cipher = 1027076
(4)   WLAN-Group-Cipher = 1027076
(4)   WLAN-AKM-Suite = 1027073
(4)   Framed-MTU = 1400
(4)   EAP-Message = 0x0282000c01736368756c7465
(4)   Message-Authenticator = 0x65217c733682d9ebc1aa037e63368590
(4) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/default
(4)   authorize {
(4)     policy filter_username {
(4)       if (&User-Name) {
(4)       if (&User-Name)  -> TRUE
(4)       if (&User-Name)  {
(4)         if (&User-Name =~ / /) {
(4)         if (&User-Name =~ / /)  -> FALSE
(4)         if (&User-Name =~ /@[^@]*@/ ) {
(4)         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(4)         if (&User-Name =~ /\.\./ ) {
(4)         if (&User-Name =~ /\.\./ )  -> FALSE
(4)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))  {
(4)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))   -> FALSE
(4)         if (&User-Name =~ /\.$/)  {
(4)         if (&User-Name =~ /\.$/)   -> FALSE
(4)         if (&User-Name =~ /@\./)  {
(4)         if (&User-Name =~ /@\./)   -> FALSE
(4)       } # if (&User-Name)  = notfound
(4)     } # policy filter_username = notfound
(4)     [preprocess] = ok
(4)     [chap] = noop
(4)     [mschap] = noop
(4)     [digest] = noop
(4) suffix: Checking for suffix after "@"
(4) suffix: No '@' in User-Name = "testBenutzer", looking up realm NULL
(4) suffix: No such realm "NULL"
(4)     [suffix] = noop
(4) eap: Peer sent EAP Response (code 2) ID 130 length 12
(4) eap: EAP-Identity reply, returning 'ok' so we can short-circuit the rest of authorize
(4)     [eap] = ok
(4)   } # authorize = ok
(4) Found Auth-Type = eap
(4) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(4)   authenticate {
(4) eap: Peer sent packet with method EAP Identity (1)
(4) eap: Calling submodule eap_md5 to process data
(4) eap_md5: Issuing MD5 Challenge
(4) eap: Sending EAP Request (code 1) ID 131 length 22
(4) eap: EAP session adding &reply:State = 0x0d91bdf20d12b9f8
(4)     [eap] = handled
(4)   } # authenticate = handled
(4) Using Post-Auth-Type Challenge
(4) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(4)   Challenge { ... } # empty sub-section is ignored
(4) Sent Access-Challenge Id 200 from 10.16.1.1:1812 to 10.110.0.253:8364 length 0
(4)   EAP-Message = 0x01830016041019301edfc2acb7f7fe95ed8b4cc7f01c
(4)   Message-Authenticator = 0x00000000000000000000000000000000
(4)   State = 0x0d91bdf20d12b9f898d0f9067dab6a40
(4) Finished request
Waking up in 4.9 seconds.
(5) Received Access-Request Id 201 from 10.110.0.253:8646 to 10.16.1.1:1812 length 243
(5)   User-Name = "testBenutzer"
(5)   NAS-Identifier = "WLC-Meineschule-1"
(5)   LCS-Orig-NAS-Identifier = "00A057604249"
(5)   Called-Station-Id = "12-A0-57-60-42-4C:gym-lehrer"
(5)   NAS-Port-Type = Wireless-802.11
(5)   Service-Type = Framed-User
(5)   Calling-Station-Id = "6C-C7-EC-60-61-34"
(5)   Connect-Info = "CONNECT"
(5)   Acct-Session-Id = "01E8C32B02BC44A4"
(5)   Acct-Multi-Session-Id = "949304E139FEEDD5"
(5)   WLAN-Pairwise-Cipher = 1027076
(5)   WLAN-Group-Cipher = 1027076
```

```
(5)   WLAN-AKM-Suite = 1027073
(5)   Framed-MTU = 1400
(5)   EAP-Message = 0x028300060319
(5)   State = 0x0d91bdf20d12b9f898d0f9067dab6a40
(5)   Message-Authenticator = 0x2c1024caa4ff7794eba7f0756baf37eb
(5) session-state: No cached attributes
(5) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/default
(5)   authorize {
(5)     policy filter_username {
(5)       if (&User-Name) {
(5)       if (&User-Name)  -> TRUE
(5)       if (&User-Name)  {
(5)         if (&User-Name =~ / /) {
(5)         if (&User-Name =~ / /)  -> FALSE
(5)         if (&User-Name =~ /@[^@]*@/ ) {
(5)         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(5)         if (&User-Name =~ /\.\./ ) {
(5)         if (&User-Name =~ /\.\./ )  -> FALSE
(5)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))  {
(5)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))   -> FALSE
(5)         if (&User-Name =~ /\.$/)  {
(5)         if (&User-Name =~ /\.$/)   -> FALSE
(5)         if (&User-Name =~ /@\./)  {
(5)         if (&User-Name =~ /@\./)   -> FALSE
(5)       } # if (&User-Name)  = notfound
(5)     } # policy filter_username = notfound
(5)     [preprocess] = ok
(5)     [chap] = noop
(5)     [mschap] = noop
(5)     [digest] = noop
(5) suffix: Checking for suffix after "@"
(5) suffix: No '@' in User-Name = "testBenutzer", looking up realm NULL
(5) suffix: No such realm "NULL"
(5)     [suffix] = noop
(5) eap: Peer sent EAP Response (code 2) ID 131 length 6
(5) eap: No EAP Start, assuming it's an on-going EAP conversation
(5)     [eap] = updated
(5) files: users: Matched entry DEFAULT at line 1
(5)     [files] = ok
(5)     [expiration] = noop
(5)     [logintime] = noop
(5) pap: WARNING: No "known good" password found for the user.  Not setting Auth-Type
(5) pap: WARNING: Authentication will fail unless a "known good" password is available
(5)     [pap] = noop
(5)   } # authorize = updated
(5) Found Auth-Type = eap
(5) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(5)   authenticate {
(5) eap: Expiring EAP session with state 0xcfa27713cc526e00
(5) eap: Finished EAP session with state 0x0d91bdf20d12b9f8
(5) eap: Previous EAP request found for state 0x0d91bdf20d12b9f8, released from the list
(5) eap: Peer sent packet with method EAP NAK (3)
(5) eap: Found mutually acceptable type PEAP (25)
(5) eap: Calling submodule eap_peap to process data
(5) eap_peap: Initiating new EAP-TLS session
(5) eap_peap: [eaptls start] = request
(5) eap: Sending EAP Request (code 1) ID 132 length 6
(5) eap: EAP session adding &reply:State = 0x0d91bdf20c15a4f8
(5)     [eap] = handled
(5)   } # authenticate = handled
(5) Using Post-Auth-Type Challenge
(5) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(5)   Challenge { ... } # empty sub-section is ignored
(5) Sent Access-Challenge Id 201 from 10.16.1.1:1812 to 10.110.0.253:8646 length 0
(5)   EAP-Message = 0x018400061920
(5)   Message-Authenticator = 0x00000000000000000000000000000000
(5)   State = 0x0d91bdf20c15a4f898d0f9067dab6a40
(5) Finished request
Waking up in 4.9 seconds.
(6) Received Access-Request Id 202 from 10.110.0.253:15626 to 10.16.1.1:1812 length 404
(6)   User-Name = "testBenutzer"
(6)   NAS-Identifier = "WLC-Meineschule-1"
(6)   LCS-Orig-NAS-Identifier = "00A057604249"
(6)   Called-Station-Id = "12-A0-57-60-42-4C:gym-lehrer"
```

```
(6)   NAS-Port-Type = Wireless-802.11
(6)   Service-Type = Framed-User
(6)   Calling-Station-Id = "6C-C7-EC-60-61-34"
(6)   Connect-Info = "CONNECT"
(6)   Acct-Session-Id = "01E8C32B02BC44A4"
(6)   Acct-Multi-Session-Id = "949304E139FEEDD5"
(6)   WLAN-Pairwise-Cipher = 1027076
(6)   WLAN-Group-Cipher = 1027076
(6)   WLAN-AKM-Suite = 1027073
(6)   Framed-MTU = 1400
(6)   EAP-Message =
0x028400a719800000009d16030100980100009403030bdf80fb6114b6a5d177f44fe5da178a1ea3fb92ee7dd6de9ead8df06b8af2e2b00003cc0
(6)   State = 0x0d91bdf20c15a4f898d0f9067dab6a40
(6)   Message-Authenticator = 0xd13b18f30ac991993be798688c0a32aa
(6) session-state: No cached attributes
(6) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/default
(6)   authorize {
(6)     policy filter_username {
(6)       if (&User-Name) {
(6)       if (&User-Name)  -> TRUE
(6)       if (&User-Name)  {
(6)         if (&User-Name =~ / /) {
(6)         if (&User-Name =~ / /)  -> FALSE
(6)         if (&User-Name =~ /@[^@]*@/ ) {
(6)         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(6)         if (&User-Name =~ /\.\./ ) {
(6)         if (&User-Name =~ /\.\./ )  -> FALSE
(6)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))  {
(6)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))   -> FALSE
(6)         if (&User-Name =~ /\.$/)  {
(6)         if (&User-Name =~ /\.$/)   -> FALSE
(6)         if (&User-Name =~ /@\./)  {
(6)         if (&User-Name =~ /@\./)   -> FALSE
(6)       } # if (&User-Name)  = notfound
(6)     } # policy filter_username = notfound
(6)     [preprocess] = ok
(6)     [chap] = noop
(6)     [mschap] = noop
(6)     [digest] = noop
(6) suffix: Checking for suffix after "@"
(6) suffix: No '@' in User-Name = "testBenutzer", looking up realm NULL
(6) suffix: No such realm "NULL"
(6)     [suffix] = noop
(6) eap: Peer sent EAP Response (code 2) ID 132 length 167
(6) eap: Continuing tunnel setup
(6)     [eap] = ok
(6)   } # authorize = ok
(6) Found Auth-Type = eap
(6) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(6)   authenticate {
(6) eap: Expiring EAP session with state 0xcfa27713cc526e00
(6) eap: Finished EAP session with state 0x0d91bdf20c15a4f8
(6) eap: Previous EAP request found for state 0x0d91bdf20c15a4f8, released from the list
(6) eap: Peer sent packet with method EAP PEAP (25)
(6) eap: Calling submodule eap_peap to process data
(6) eap_peap: Continuing EAP-TLS
(6) eap_peap: Peer indicated complete TLS record size will be 157 bytes
(6) eap_peap: Got complete TLS record (157 bytes)
(6) eap_peap: [eaptls verify] = length included
(6) eap_peap: (other): before SSL initialization
(6) eap_peap: TLS_accept: before SSL initialization
(6) eap_peap: TLS_accept: before SSL initialization
(6) eap_peap: <<< recv UNKNOWN TLS VERSION ?0304? [length 0098]
(6) eap_peap: TLS_accept: SSLv3/TLS read client hello
(6) eap_peap: >>> send TLS 1.2  [length 003d]
(6) eap_peap: TLS_accept: SSLv3/TLS write server hello
(6) eap_peap: >>> send TLS 1.2  [length 02d3]
(6) eap_peap: TLS_accept: SSLv3/TLS write certificate
(6) eap_peap: >>> send TLS 1.2  [length 014d]
(6) eap_peap: TLS_accept: SSLv3/TLS write key exchange
(6) eap_peap: >>> send TLS 1.2  [length 0004]
(6) eap_peap: TLS_accept: SSLv3/TLS write server done
(6) eap_peap: TLS_accept: Need to read more data: SSLv3/TLS write server done
(6) eap_peap: In SSL Handshake Phase
```

```
(6) eap_peap: In SSL Accept mode
(6) eap_peap: [eaptls process] = handled
(6) eap: Sending EAP Request (code 1) ID 133 length 1004
(6) eap: EAP session adding &reply:State = 0x0d91bdf20f14a4f8
(6)     [eap] = handled
(6)   } # authenticate = handled
(6) Using Post-Auth-Type Challenge
(6) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(6)   Challenge { ... } # empty sub-section is ignored
(6) Sent Access-Challenge Id 202 from 10.16.1.1:1812 to 10.110.0.253:15626 length 0
(6)   EAP-Message =
0x018503ec19c000000475160303003d02000039030371cf1c7b9df11ffe5da72442a38f7a53d69752c446e76234e6e4ad8a57ad268b00c02f00
(6)   Message-Authenticator = 0x00000000000000000000000000000000
(6)   State = 0x0d91bdf20f14a4f898d0f9067dab6a40
(6) Finished request
Waking up in 4.9 seconds.
(7) Received Access-Request Id 203 from 10.110.0.253:13475 to 10.16.1.1:1812 length 243
(7)   User-Name = "testBenutzer"
(7)   NAS-Identifier = "WLC-Meineschule-1"
(7)   LCS-Orig-NAS-Identifier = "00A057604249"
(7)   Called-Station-Id = "12-A0-57-60-42-4C:gym-lehrer"
(7)   NAS-Port-Type = Wireless-802.11
(7)   Service-Type = Framed-User
(7)   Calling-Station-Id = "6C-C7-EC-60-61-34"
(7)   Connect-Info = "CONNECT"
(7)   Acct-Session-Id = "01E8C32B02BC44A4"
(7)   Acct-Multi-Session-Id = "949304E139FEEDD5"
(7)   WLAN-Pairwise-Cipher = 1027076
(7)   WLAN-Group-Cipher = 1027076
(7)   WLAN-AKM-Suite = 1027073
(7)   Framed-MTU = 1400
(7)   EAP-Message = 0x028500061900
(7)   State = 0x0d91bdf20f14a4f898d0f9067dab6a40
(7)   Message-Authenticator = 0x047241047b45187d19bcb5d0ea84f3a1
(7) session-state: No cached attributes
(7) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/default
(7)   authorize {
(7)     policy filter_username {
(7)       if (&User-Name) {
(7)       if (&User-Name)  -> TRUE
(7)       if (&User-Name)  {
(7)         if (&User-Name =~ / /) {
(7)         if (&User-Name =~ / /)  -> FALSE
(7)         if (&User-Name =~ /@[^@]*@/ ) {
(7)         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(7)         if (&User-Name =~ /\.\./ ) {
(7)         if (&User-Name =~ /\.\./ )  -> FALSE
(7)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))  {
(7)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))   -> FALSE
(7)         if (&User-Name =~ /\.$/)  {
(7)         if (&User-Name =~ /\.$/)   -> FALSE
(7)         if (&User-Name =~ /@\./)  {
(7)         if (&User-Name =~ /@\./)   -> FALSE
(7)       } # if (&User-Name)  = notfound
(7)     } # policy filter_username = notfound
(7)     [preprocess] = ok
(7)     [chap] = noop
(7)     [mschap] = noop
(7)     [digest] = noop
(7) suffix: Checking for suffix after "@"
(7) suffix: No '@' in User-Name = "testBenutzer", looking up realm NULL
(7) suffix: No such realm "NULL"
(7)     [suffix] = noop
(7) eap: Peer sent EAP Response (code 2) ID 133 length 6
(7) eap: Continuing tunnel setup
(7)     [eap] = ok
(7)   } # authorize = ok
(7) Found Auth-Type = eap
(7) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(7)   authenticate {
(7) eap: Expiring EAP session with state 0xcfa27713cc526e00
(7) eap: Finished EAP session with state 0x0d91bdf20f14a4f8
(7) eap: Previous EAP request found for state 0x0d91bdf20f14a4f8, released from the list
(7) eap: Peer sent packet with method EAP PEAP (25)
```

```
(7) eap: Calling submodule eap_peap to process data
(7) eap_peap: Continuing EAP-TLS
(7) eap_peap: Peer ACKed our handshake fragment
(7) eap_peap: [eaptls verify] = request
(7) eap_peap: [eaptls process] = handled
(7) eap: Sending EAP Request (code 1) ID 134 length 153
(7) eap: EAP session adding &reply:State = 0x0d91bdf20e17a4f8
(7)     [eap] = handled
(7)   } # authenticate = handled
(7) Using Post-Auth-Type Challenge
(7) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(7)   Challenge { ... } # empty sub-section is ignored
(7) Sent Access-Challenge Id 203 from 10.16.1.1:1812 to 10.110.0.253:13475 length 0
(7)   EAP-Message =
0x018600991900dc09f7599c32584feeba31f89701cc0f0009192c90e0d37973ef39ef88111c39802be2d9a469f754d6c6425824a7205b811be0
(7)   Message-Authenticator = 0x00000000000000000000000000000000
(7)   State = 0x0d91bdf20e17a4f898d0f9067dab6a40
(7) Finished request
Waking up in 4.9 seconds.
(4) Cleaning up request packet ID 200 with timestamp +51
(5) Cleaning up request packet ID 201 with timestamp +51
(6) Cleaning up request packet ID 202 with timestamp +51
(7) Cleaning up request packet ID 203 with timestamp +51
Ready to process requests
(8) Received Access-Request Id 204 from 10.110.0.253:8362 to 10.16.1.1:1812 length 231
(8)   User-Name = "testBenutzer"
(8)   NAS-Identifier = "WLC-Meineschule-1"
(8)   LCS-Orig-NAS-Identifier = "00A057604349"
(8)   Called-Station-Id = "0E-A0-57-60-43-4C:gym-lehrer"
(8)   NAS-Port-Type = Wireless-802.11
(8)   Service-Type = Framed-User
(8)   Calling-Station-Id = "6C-C7-EC-60-61-34"
(8)   Connect-Info = "CONNECT"
(8)   Acct-Session-Id = "B42DB9D0899ACF18"
(8)   Acct-Multi-Session-Id = "05430C7B820DAC3B"
(8)   WLAN-Pairwise-Cipher = 1027076
(8)   WLAN-Group-Cipher = 1027076
(8)   WLAN-AKM-Suite = 1027073
(8)   Framed-MTU = 1400
(8)   EAP-Message = 0x02fe000c01736368756c7465
(8)   Message-Authenticator = 0x9082e393966af3853c239f06b9d43a91
(8) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/default
(8)   authorize {
(8)     policy filter_username {
(8)       if (&User-Name) {
(8)       if (&User-Name)  -> TRUE
(8)       if (&User-Name)  {
(8)         if (&User-Name =~ / /) {
(8)         if (&User-Name =~ / /)  -> FALSE
(8)         if (&User-Name =~ /@[^@]*@/ ) {
(8)         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(8)         if (&User-Name =~ /\.\./ ) {
(8)         if (&User-Name =~ /\.\./ )  -> FALSE
(8)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))  {
(8)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))   -> FALSE
(8)         if (&User-Name =~ /\.$/)  {
(8)         if (&User-Name =~ /\.$/)   -> FALSE
(8)         if (&User-Name =~ /@\./)  {
(8)         if (&User-Name =~ /@\./)   -> FALSE
(8)       } # if (&User-Name)  = notfound
(8)     } # policy filter_username = notfound
(8)     [preprocess] = ok
(8)     [chap] = noop
(8)     [mschap] = noop
(8)     [digest] = noop
(8) suffix: Checking for suffix after "@"
(8) suffix: No '@' in User-Name = "testBenutzer", looking up realm NULL
(8) suffix: No such realm "NULL"
(8)     [suffix] = noop
(8) eap: Peer sent EAP Response (code 2) ID 254 length 12
(8) eap: EAP-Identity reply, returning 'ok' so we can short-circuit the rest of authorize
(8)     [eap] = ok
(8)   } # authorize = ok
(8) Found Auth-Type = eap
```

```
(8) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(8)   authenticate {
(8) eap: Peer sent packet with method EAP Identity (1)
(8) eap: Calling submodule eap_md5 to process data
(8) eap_md5: Issuing MD5 Challenge
(8) eap: Sending EAP Request (code 1) ID 255 length 22
(8) eap: EAP session adding &reply:State = 0x1682c78c167dc33c
(8)     [eap] = handled
(8)   } # authenticate = handled
(8) Using Post-Auth-Type Challenge
(8) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(8)   Challenge { ... } # empty sub-section is ignored
(8) Sent Access-Challenge Id 204 from 10.16.1.1:1812 to 10.110.0.253:8362 length 0
(8)   EAP-Message = 0x01ff00160410f9717cdad3580878f50b2698926f9bbb
(8)   Message-Authenticator = 0x00000000000000000000000000000000
(8)   State = 0x1682c78c167dc33c204caa76a5e89391
(8) Finished request
Waking up in 4.9 seconds.
(9) Received Access-Request Id 205 from 10.110.0.253:14531 to 10.16.1.1:1812 length 243
(9)   User-Name = "testBenutzer"
(9)   NAS-Identifier = "WLC-Meineschule-1"
(9)   LCS-Orig-NAS-Identifier = "00A057604349"
(9)   Called-Station-Id = "0E-A0-57-60-43-4C:gym-lehrer"
(9)   NAS-Port-Type = Wireless-802.11
(9)   Service-Type = Framed-User
(9)   Calling-Station-Id = "6C-C7-EC-60-61-34"
(9)   Connect-Info = "CONNECT"
(9)   Acct-Session-Id = "B42DB9D0899ACF18"
(9)   Acct-Multi-Session-Id = "05430C7B820DAC3B"
(9)   WLAN-Pairwise-Cipher = 1027076
(9)   WLAN-Group-Cipher = 1027076
(9)   WLAN-AKM-Suite = 1027073
(9)   Framed-MTU = 1400
(9)   EAP-Message = 0x02ff00060319
(9)   State = 0x1682c78c167dc33c204caa76a5e89391
(9)   Message-Authenticator = 0xd6313514a04e3b8518c0463ff395adbc
(9) session-state: No cached attributes
(9) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/default
(9)   authorize {
(9)     policy filter_username {
(9)       if (&User-Name) {
(9)       if (&User-Name)  -> TRUE
(9)       if (&User-Name)  {
(9)         if (&User-Name =~ / /) {
(9)         if (&User-Name =~ / /)  -> FALSE
(9)         if (&User-Name =~ /@[^@]*@/ ) {
(9)         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(9)         if (&User-Name =~ /\.\./ ) {
(9)         if (&User-Name =~ /\.\./ )  -> FALSE
(9)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))  {
(9)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))   -> FALSE
(9)         if (&User-Name =~ /\.$/)  {
(9)         if (&User-Name =~ /\.$/)   -> FALSE
(9)         if (&User-Name =~ /@\./)  {
(9)         if (&User-Name =~ /@\./)   -> FALSE
(9)       } # if (&User-Name)  = notfound
(9)     } # policy filter_username = notfound
(9)     [preprocess] = ok
(9)     [chap] = noop
(9)     [mschap] = noop
(9)     [digest] = noop
(9) suffix: Checking for suffix after "@"
(9) suffix: No '@' in User-Name = "testBenutzer", looking up realm NULL
(9) suffix: No such realm "NULL"
(9)     [suffix] = noop
(9) eap: Peer sent EAP Response (code 2) ID 255 length 6
(9) eap: No EAP Start, assuming it's an on-going EAP conversation
(9)     [eap] = updated
(9) files: users: Matched entry DEFAULT at line 1
(9)     [files] = ok
(9)     [expiration] = noop
(9)     [logintime] = noop
(9) pap: WARNING: No "known good" password found for the user.  Not setting Auth-Type
(9) pap: WARNING: Authentication will fail unless a "known good" password is available
```

```
(9)     [pap] = noop
(9)   } # authorize = updated
(9) Found Auth-Type = eap
(9) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(9)   authenticate {
(9) eap: Expiring EAP session with state 0xcfa27713cc526e00
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!! EAP session with state 0xcfa27713cc526e0013767f5546bb62c5 did not finish!                  !!
!! Please read http://wiki.freeradius.org/guide/Certificate_Compatibility      !!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
(9) eap: Expiring EAP session with state 0x0d91bdf20e17a4f8
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!! EAP session with state 0x0d91bdf20e17a4f898d0f9067dab6a40 did not finish!                  !!
!! Please read http://wiki.freeradius.org/guide/Certificate_Compatibility      !!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
(9) eap: Expiring EAP session with state 0x1682c78c167dc33c
(9) eap: Finished EAP session with state 0x1682c78c167dc33c
(9) eap: Previous EAP request found for state 0x1682c78c167dc33c, released from the list
(9) eap: Peer sent packet with method EAP NAK (3)
(9) eap: Found mutually acceptable type PEAP (25)
(9) eap: Calling submodule eap_peap to process data
(9) eap_peap: Initiating new EAP-TLS session
(9) eap_peap: [eaptls start] = request
(9) eap: Sending EAP Request (code 1) ID 0 length 6
(9) eap: EAP session adding &reply:State = 0x1682c78c1782de3c
(9)     [eap] = handled
(9)   } # authenticate = handled
(9) Using Post-Auth-Type Challenge
(9) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(9)   Challenge { ... } # empty sub-section is ignored
(9) Sent Access-Challenge Id 205 from 10.16.1.1:1812 to 10.110.0.253:14531 length 0
(9)   EAP-Message = 0x010000061920
(9)   Message-Authenticator = 0x00000000000000000000000000000000
(9)   State = 0x1682c78c1782de3c204caa76a5e89391
(9) Finished request
Waking up in 4.8 seconds.
(10) Received Access-Request Id 206 from 10.110.0.253:13188 to 10.16.1.1:1812 length 404
(10)   User-Name = "testBenutzer"
(10)   NAS-Identifier = "WLC-Meineschule-1"
(10)   LCS-Orig-NAS-Identifier = "00A057604349"
(10)   Called-Station-Id = "0E-A0-57-60-43-4C:gym-lehrer"
(10)   NAS-Port-Type = Wireless-802.11
(10)   Service-Type = Framed-User
(10)   Calling-Station-Id = "6C-C7-EC-60-61-34"
(10)   Connect-Info = "CONNECT"
(10)   Acct-Session-Id = "B42DB9D0899ACF18"
(10)   Acct-Multi-Session-Id = "05430C7B820DAC3B"
(10)   WLAN-Pairwise-Cipher = 1027076
(10)   WLAN-Group-Cipher = 1027076
(10)   WLAN-AKM-Suite = 1027073
(10)   Framed-MTU = 1400
(10)   EAP-Message =
0x020000a719800000009d16030100980100009403030d08953e40a6f163738c4ca5744248605bda34b046744b398bc97796287b2cd8100003cc
(10)   State = 0x1682c78c1782de3c204caa76a5e89391
(10)   Message-Authenticator = 0x0ace5dd7324e440f1f4903b1cdb58781
(10) session-state: No cached attributes
(10) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/default
(10)   authorize {
(10)     policy filter_username {
(10)       if (&User-Name) {
(10)       if (&User-Name)  -> TRUE
(10)       if (&User-Name)  {
(10)         if (&User-Name =~ / /) {
(10)         if (&User-Name =~ / /)  -> FALSE
(10)         if (&User-Name =~ /@[^@]*@/ ) {
(10)         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(10)         if (&User-Name =~ /\.\./ ) {
(10)         if (&User-Name =~ /\.\./ )  -> FALSE
(10)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))  {
(10)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))   -> FALSE
(10)         if (&User-Name =~ /\.$/)  {
(10)         if (&User-Name =~ /\.$/)   -> FALSE
(10)         if (&User-Name =~ /@\./)  {
(10)         if (&User-Name =~ /@\./)   -> FALSE
(10)       } # if (&User-Name)  = notfound
(10)     } # policy filter_username = notfound
(10)     [preprocess] = ok
(10)     [chap] = noop
(10)     [mschap] = noop
(10)     [digest] = noop
(10) suffix: Checking for suffix after "@"
(10) suffix: No '@' in User-Name = "testBenutzer", looking up realm NULL
(10) suffix: No such realm "NULL"
(10)     [suffix] = noop
(10) eap: Peer sent EAP Response (code 2) ID 0 length 167
(10) eap: Continuing tunnel setup
(10)     [eap] = ok
(10)   } # authorize = ok
(10) Found Auth-Type = eap
(10) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(10)   authenticate {
(10) eap: Expiring EAP session with state 0x1682c78c1782de3c
(10) eap: Finished EAP session with state 0x1682c78c1782de3c
(10) eap: Previous EAP request found for state 0x1682c78c1782de3c, released from the list
(10) eap: Peer sent packet with method EAP PEAP (25)
(10) eap: Calling submodule eap_peap to process data
(10) eap_peap: Continuing EAP-TLS
(10) eap_peap: Peer indicated complete TLS record size will be 157 bytes
(10) eap_peap: Got complete TLS record (157 bytes)
(10) eap_peap: [eaptls verify] = length included
(10) eap_peap: (other): before SSL initialization
(10) eap_peap: TLS_accept: before SSL initialization
(10) eap_peap: TLS_accept: before SSL initialization
(10) eap_peap: <<< recv UNKNOWN TLS VERSION ?0304? [length 0098]
(10) eap_peap: TLS_accept: SSLv3/TLS read client hello
(10) eap_peap: >>> send TLS 1.2  [length 003d]
(10) eap_peap: TLS_accept: SSLv3/TLS write server hello
(10) eap_peap: >>> send TLS 1.2  [length 02d3]
(10) eap_peap: TLS_accept: SSLv3/TLS write certificate
(10) eap_peap: >>> send TLS 1.2  [length 014d]
(10) eap_peap: TLS_accept: SSLv3/TLS write key exchange
(10) eap_peap: >>> send TLS 1.2  [length 0004]
(10) eap_peap: TLS_accept: SSLv3/TLS write server done
(10) eap_peap: TLS_accept: Need to read more data: SSLv3/TLS write server done
(10) eap_peap: In SSL Handshake Phase
(10) eap_peap: In SSL Accept mode
(10) eap_peap: [eaptls process] = handled
(10) eap: Sending EAP Request (code 1) ID 1 length 1004
(10) eap: EAP session adding &reply:State = 0x1682c78c1483de3c
(10)     [eap] = handled
(10)   } # authenticate = handled
(10) Using Post-Auth-Type Challenge
(10) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(10)   Challenge { ... } # empty sub-section is ignored
(10) Sent Access-Challenge Id 206 from 10.16.1.1:1812 to 10.110.0.253:13188 length 0
(10)   EAP-Message =
0x010103ec19c000000475160303003d020000390303bca6cfce39426ebf026f4503a156d7a54e737ad43685450fd65ec293faf5b2cd00c02f00
(10)   Message-Authenticator = 0x00000000000000000000000000000000
(10)   State = 0x1682c78c1483de3c204caa76a5e89391
(10) Finished request
Waking up in 4.8 seconds.
(11) Received Access-Request Id 207 from 10.110.0.253:8482 to 10.16.1.1:1812 length 243
(11)   User-Name = "testBenutzer"
(11)   NAS-Identifier = "WLC-Meineschule-1"
(11)   LCS-Orig-NAS-Identifier = "00A057604349"
(11)   Called-Station-Id = "0E-A0-57-60-43-4C:gym-lehrer"
(11)   NAS-Port-Type = Wireless-802.11
(11)   Service-Type = Framed-User
(11)   Calling-Station-Id = "6C-C7-EC-60-61-34"
(11)   Connect-Info = "CONNECT"
(11)   Acct-Session-Id = "B42DB9D0899ACF18"
(11)   Acct-Multi-Session-Id = "05430C7B820DAC3B"
(11)   WLAN-Pairwise-Cipher = 1027076
(11)   WLAN-Group-Cipher = 1027076
(11)   WLAN-AKM-Suite = 1027073
(11)   Framed-MTU = 1400
(11)   EAP-Message = 0x020100061900
(11)   State = 0x1682c78c1483de3c204caa76a5e89391
```

```
(11)   Message-Authenticator = 0x1828872a9ae29a769401a2fa8afd97a9
(11) session-state: No cached attributes
(11) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/default
(11)   authorize {
(11)     policy filter_username {
(11)       if (&User-Name) {
(11)       if (&User-Name)  -> TRUE
(11)       if (&User-Name)  {
(11)         if (&User-Name =~ / /) {
(11)         if (&User-Name =~ / /)  -> FALSE
(11)         if (&User-Name =~ /@[^@]*@/ ) {
(11)         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(11)         if (&User-Name =~ /\.\./ ) {
(11)         if (&User-Name =~ /\.\./ )  -> FALSE
(11)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))  {
(11)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))   -> FALSE
(11)         if (&User-Name =~ /\.$/)  {
(11)         if (&User-Name =~ /\.$/)   -> FALSE
(11)         if (&User-Name =~ /@\./)  {
(11)         if (&User-Name =~ /@\./)   -> FALSE
(11)       } # if (&User-Name)  = notfound
(11)     } # policy filter_username = notfound
(11)     [preprocess] = ok
(11)     [chap] = noop
(11)     [mschap] = noop
(11)     [digest] = noop
(11) suffix: Checking for suffix after "@"
(11) suffix: No '@' in User-Name = "testBenutzer", looking up realm NULL
(11) suffix: No such realm "NULL"
(11)     [suffix] = noop
(11) eap: Peer sent EAP Response (code 2) ID 1 length 6
(11) eap: Continuing tunnel setup
(11)     [eap] = ok
(11)   } # authorize = ok
(11) Found Auth-Type = eap
(11) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(11)   authenticate {
(11) eap: Expiring EAP session with state 0x1682c78c1483de3c
(11) eap: Finished EAP session with state 0x1682c78c1483de3c
(11) eap: Previous EAP request found for state 0x1682c78c1483de3c, released from the list
(11) eap: Peer sent packet with method EAP PEAP (25)
(11) eap: Calling submodule eap_peap to process data
(11) eap_peap: Continuing EAP-TLS
(11) eap_peap: Peer ACKed our handshake fragment
(11) eap_peap: [eaptls verify] = request
(11) eap_peap: [eaptls process] = handled
(11) eap: Sending EAP Request (code 1) ID 2 length 153
(11) eap: EAP session adding &reply:State = 0x1682c78c1580de3c
(11)     [eap] = handled
(11)   } # authenticate = handled
(11) Using Post-Auth-Type Challenge
(11) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(11)   Challenge { ... } # empty sub-section is ignored
(11) Sent Access-Challenge Id 207 from 10.16.1.1:1812 to 10.110.0.253:8482 length 0
(11)   EAP-Message =
0x010200991900e2bd5c4f91afe6fdd9c54fcff8cfd4a0eff402b72c60b82ad376790df756355ab0248ee5012748ad4382495018adc2e38b7d5
(11)   Message-Authenticator = 0x00000000000000000000000000000000
(11)   State = 0x1682c78c1580de3c204caa76a5e89391
(11) Finished request
Waking up in 1.8 seconds.
(12) Received Access-Request Id 208 from 10.110.0.253:16243 to 10.16.1.1:1812 length 373
(12)   User-Name = "testBenutzer"
(12)   NAS-Identifier = "WLC-Meineschule-1"
(12)   LCS-Orig-NAS-Identifier = "00A057604349"
(12)   Called-Station-Id = "0E-A0-57-60-43-4C:gym-lehrer"
(12)   NAS-Port-Type = Wireless-802.11
(12)   Service-Type = Framed-User
(12)   Calling-Station-Id = "6C-C7-EC-60-61-34"
(12)   Connect-Info = "CONNECT"
(12)   Acct-Session-Id = "B42DB9D0899ACF18"
(12)   Acct-Multi-Session-Id = "05430C7B820DAC3B"
(12)   WLAN-Pairwise-Cipher = 1027076
(12)   WLAN-Group-Cipher = 1027076
(12)   WLAN-AKM-Suite = 1027073
```

```
(12)   Framed-MTU = 1400
(12)   EAP-Message =
0x0202008819800000007e16030300461000004241104d9e83a8e5ce2f3cbdd51b3e7a1d9a2154a898bdd75e8d81cba8b84057c8ef4107c5eb477
(12)   State = 0x1682c78c1580de3c204caa76a5e89391
(12)   Message-Authenticator = 0xe2226c563c321c58da45f5fd8f28d32f
(12) session-state: No cached attributes
(12) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/default
(12)   authorize {
(12)     policy filter_username {
(12)       if (&User-Name) {
(12)       if (&User-Name)  -> TRUE
(12)       if (&User-Name)  {
(12)         if (&User-Name =~ / /) {
(12)         if (&User-Name =~ / /)  -> FALSE
(12)         if (&User-Name =~ /@[^@]*@/ ) {
(12)         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(12)         if (&User-Name =~ /\.\./ ) {
(12)         if (&User-Name =~ /\.\./ )  -> FALSE
(12)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))  {
(12)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))   -> FALSE
(12)         if (&User-Name =~ /\.$/)  {
(12)         if (&User-Name =~ /\.$/)   -> FALSE
(12)         if (&User-Name =~ /@\./)  {
(12)         if (&User-Name =~ /@\./)   -> FALSE
(12)       } # if (&User-Name)  = notfound
(12)     } # policy filter_username = notfound
(12)     [preprocess] = ok
(12)     [chap] = noop
(12)     [mschap] = noop
(12)     [digest] = noop
(12) suffix: Checking for suffix after "@"
(12) suffix: No '@' in User-Name = "testBenutzer", looking up realm NULL
(12) suffix: No such realm "NULL"
(12)     [suffix] = noop
(12) eap: Peer sent EAP Response (code 2) ID 2 length 136
(12) eap: Continuing tunnel setup
(12)     [eap] = ok
(12)   } # authorize = ok
(12) Found Auth-Type = eap
(12) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(12)   authenticate {
(12) eap: Expiring EAP session with state 0x1682c78c1580de3c
(12) eap: Finished EAP session with state 0x1682c78c1580de3c
(12) eap: Previous EAP request found for state 0x1682c78c1580de3c, released from the list
(12) eap: Peer sent packet with method EAP PEAP (25)
(12) eap: Calling submodule eap_peap to process data
(12) eap_peap: Continuing EAP-TLS
(12) eap_peap: Peer indicated complete TLS record size will be 126 bytes
(12) eap_peap: Got complete TLS record (126 bytes)
(12) eap_peap: [eaptls verify] = length included
(12) eap_peap: TLS_accept: SSLv3/TLS write server done
(12) eap_peap: <<< recv TLS 1.2  [length 0046]
(12) eap_peap: TLS_accept: SSLv3/TLS read client key exchange
(12) eap_peap: TLS_accept: SSLv3/TLS read change cipher spec
(12) eap_peap: <<< recv TLS 1.2  [length 0010]
(12) eap_peap: TLS_accept: SSLv3/TLS read finished
(12) eap_peap: >>> send TLS 1.2  [length 0001]
(12) eap_peap: TLS_accept: SSLv3/TLS write change cipher spec
(12) eap_peap: >>> send TLS 1.2  [length 0010]
(12) eap_peap: TLS_accept: SSLv3/TLS write finished
(12) eap_peap: (other): SSL negotiation finished successfully
(12) eap_peap: SSL Connection Established
(12) eap_peap: [eaptls process] = handled
(12) eap: Sending EAP Request (code 1) ID 3 length 57
(12) eap: EAP session adding &reply:State = 0x1682c78c1281de3c
(12)     [eap] = handled
(12)   } # authenticate = handled
(12) Using Post-Auth-Type Challenge
(12) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(12)   Challenge { ... } # empty sub-section is ignored
(12) Sent Access-Challenge Id 208 from 10.16.1.1:1812 to 10.110.0.253:16243 length 0
(12)   EAP-Message =
0x010300391900140303000101160303002 8ab9cdd8b2e98b542b499ad0135f38a49be80b5da9fd2c26253d157b4e081147a1e194bf76aecec43
(12)   Message-Authenticator = 0x00000000000000000000000000000000
```

```
(12)   State = 0x1682c78c1281de3c204caa76a5e89391
(12) Finished request
Waking up in 1.8 seconds.
(8) Cleaning up request packet ID 204 with timestamp +211
Waking up in 0.1 seconds.
(9) Cleaning up request packet ID 205 with timestamp +211
(10) Cleaning up request packet ID 206 with timestamp +211
Waking up in 2.9 seconds.
(13) Received Access-Request Id 209 from 10.110.0.253:11747 to 10.16.1.1:1812 length 243
(13)   User-Name = "testBenutzer"
(13)   NAS-Identifier = "WLC-Meineschule-1"
(13)   LCS-Orig-NAS-Identifier = "00A057604349"
(13)   Called-Station-Id = "0E-A0-57-60-43-4C:gym-lehrer"
(13)   NAS-Port-Type = Wireless-802.11
(13)   Service-Type = Framed-User
(13)   Calling-Station-Id = "6C-C7-EC-60-61-34"
(13)   Connect-Info = "CONNECT"
(13)   Acct-Session-Id = "B42DB9D0899ACF18"
(13)   Acct-Multi-Session-Id = "05430C7B820DAC3B"
(13)   WLAN-Pairwise-Cipher = 1027076
(13)   WLAN-Group-Cipher = 1027076
(13)   WLAN-AKM-Suite = 1027073
(13)   Framed-MTU = 1400
(13)   EAP-Message = 0x020300061900
(13)   State = 0x1682c78c1281de3c204caa76a5e89391
(13)   Message-Authenticator = 0xd4e11e0940f908911e547ae784b6e9c5
(13) session-state: No cached attributes
(13) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/default
(13)   authorize {
(13)     policy filter_username {
(13)       if (&User-Name) {
(13)       if (&User-Name)  -> TRUE
(13)       if (&User-Name)  {
(13)         if (&User-Name =~ / /) {
(13)         if (&User-Name =~ / /)  -> FALSE
(13)         if (&User-Name =~ /@[^@]*@/ ) {
(13)         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(13)         if (&User-Name =~ /\.\./ ) {
(13)         if (&User-Name =~ /\.\./ )  -> FALSE
(13)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))  {
(13)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))   -> FALSE
(13)         if (&User-Name =~ /\.$/)  {
(13)         if (&User-Name =~ /\.$/)   -> FALSE
(13)         if (&User-Name =~ /@\./)  {
(13)         if (&User-Name =~ /@\./)   -> FALSE
(13)       } # if (&User-Name)  = notfound
(13)     } # policy filter_username = notfound
(13)     [preprocess] = ok
(13)     [chap] = noop
(13)     [mschap] = noop
(13)     [digest] = noop
(13) suffix: Checking for suffix after "@"
(13) suffix: No '@' in User-Name = "testBenutzer", looking up realm NULL
(13) suffix: No such realm "NULL"
(13)     [suffix] = noop
(13) eap: Peer sent EAP Response (code 2) ID 3 length 6
(13) eap: Continuing tunnel setup
(13)     [eap] = ok
(13)   } # authorize = ok
(13) Found Auth-Type = eap
(13) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(13)   authenticate {
(13) eap: Expiring EAP session with state 0x1682c78c1281de3c
(13) eap: Finished EAP session with state 0x1682c78c1281de3c
(13) eap: Previous EAP request found for state 0x1682c78c1281de3c, released from the list
(13) eap: Peer sent packet with method EAP PEAP (25)
(13) eap: Calling submodule eap_peap to process data
(13) eap_peap: Continuing EAP-TLS
(13) eap_peap: Peer ACKed our handshake fragment.  handshake is finished
(13) eap_peap: [eaptls verify] = success
(13) eap_peap: [eaptls process] = success
(13) eap_peap: Session established.  Decoding tunneled attributes
(13) eap_peap: PEAP state TUNNEL ESTABLISHED
(13) eap: Sending EAP Request (code 1) ID 4 length 40
```

```
(13) eap: EAP session adding &reply:State = 0x1682c78c1386de3c
(13)     [eap] = handled
(13)   } # authenticate = handled
(13) Using Post-Auth-Type Challenge
(13) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(13)   Challenge { ... } # empty sub-section is ignored
(13) Sent Access-Challenge Id 209 from 10.16.1.1:1812 to 10.110.0.253:11747 length 0
(13)   EAP-Message = 0x010400281900170303001dab9cdd8b2e98b54386904d0c72e5ba412df525927dd3b91befa7dea700
(13)   Message-Authenticator = 0x00000000000000000000000000000000
(13)   State = 0x1682c78c1386de3c204caa76a5e89391
(13) Finished request
Waking up in 2.0 seconds.
(14) Received Access-Request Id 210 from 10.110.0.253:15035 to 10.16.1.1:1812 length 280
(14)   User-Name = "testBenutzer"
(14)   NAS-Identifier = "WLC-Meineschule-1"
(14)   LCS-Orig-NAS-Identifier = "00A057604349"
(14)   Called-Station-Id = "0E-A0-57-60-43-4C:gym-lehrer"
(14)   NAS-Port-Type = Wireless-802.11
(14)   Service-Type = Framed-User
(14)   Calling-Station-Id = "6C-C7-EC-60-61-34"
(14)   Connect-Info = "CONNECT"
(14)   Acct-Session-Id = "B42DB9D0899ACF18"
(14)   Acct-Multi-Session-Id = "05430C7B820DAC3B"
(14)   WLAN-Pairwise-Cipher = 1027076
(14)   WLAN-Group-Cipher = 1027076
(14)   WLAN-AKM-Suite = 1027073
(14)   Framed-MTU = 1400
(14)   EAP-Message = 0x0204002b190017030300200000000000000000001543bc7e27ed0e6ce8c031f5314290c54b1ceec7cc8f29d91
(14)   State = 0x1682c78c1386de3c204caa76a5e89391
(14)   Message-Authenticator = 0xc3ed89aaabe59cfd5ff2895c304a3995
(14) session-state: No cached attributes
(14) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/default
(14)   authorize {
(14)     policy filter_username {
(14)       if (&User-Name) {
(14)       if (&User-Name)  -> TRUE
(14)       if (&User-Name)  {
(14)         if (&User-Name =~ / /) {
(14)         if (&User-Name =~ / /)  -> FALSE
(14)         if (&User-Name =~ /@[^@]*@/ ) {
(14)         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(14)         if (&User-Name =~ /\.\./ ) {
(14)         if (&User-Name =~ /\.\./ )  -> FALSE
(14)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))  {
(14)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))   -> FALSE
(14)         if (&User-Name =~ /\.$/)  {
(14)         if (&User-Name =~ /\.$/)   -> FALSE
(14)         if (&User-Name =~ /@\./)  {
(14)         if (&User-Name =~ /@\./)   -> FALSE
(14)       } # if (&User-Name)  = notfound
(14)     } # policy filter_username = notfound
(14)     [preprocess] = ok
(14)     [chap] = noop
(14)     [mschap] = noop
(14)     [digest] = noop
(14) suffix: Checking for suffix after "@"
(14) suffix: No '@' in User-Name = "testBenutzer", looking up realm NULL
(14) suffix: No such realm "NULL"
(14)     [suffix] = noop
(14) eap: Peer sent EAP Response (code 2) ID 4 length 43
(14) eap: Continuing tunnel setup
(14)     [eap] = ok
(14)   } # authorize = ok
(14) Found Auth-Type = eap
(14) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(14)   authenticate {
(14) eap: Expiring EAP session with state 0x1682c78c1386de3c
(14) eap: Finished EAP session with state 0x1682c78c1386de3c
(14) eap: Previous EAP request found for state 0x1682c78c1386de3c, released from the list
(14) eap: Peer sent packet with method EAP PEAP (25)
(14) eap: Calling submodule eap_peap to process data
(14) eap_peap: Continuing EAP-TLS
(14) eap_peap: [eaptls verify] = ok
(14) eap_peap: Done initial handshake
```

```
(14) eap_peap: [eaptls process] = ok
(14) eap_peap: Session established.  Decoding tunneled attributes
(14) eap_peap: PEAP state WAITING FOR INNER IDENTITY
(14) eap_peap: Identity - testBenutzer
(14) eap_peap: Got inner identity 'testBenutzer'
(14) eap_peap: Setting default EAP type for tunneled EAP session
(14) eap_peap: Got tunneled request
(14) eap_peap:   EAP-Message = 0x0204000c01736368756c7465
(14) eap_peap: Setting User-Name to testBenutzer
(14) eap_peap: Sending tunneled request to inner-tunnel
(14) eap_peap:   EAP-Message = 0x0204000c01736368756c7465
(14) eap_peap:   FreeRADIUS-Proxied-To = 127.0.0.1
(14) eap_peap:   User-Name = "testBenutzer"
(14) Virtual server inner-tunnel received request
(14)   EAP-Message = 0x0204000c01736368756c7465
(14)   FreeRADIUS-Proxied-To = 127.0.0.1
(14)   User-Name = "testBenutzer"
(14) WARNING: Outer and inner identities are the same.  User privacy is compromised.
(14) server inner-tunnel {
(14)   # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/inner-tunnel
(14)     authorize {
(14)       policy filter_username {
(14)         if (&User-Name) {
(14)         if (&User-Name)  -> TRUE
(14)         if (&User-Name)  {
(14)           if (&User-Name =~ / /) {
(14)           if (&User-Name =~ / /)  -> FALSE
(14)           if (&User-Name =~ /@[^@]*@/ ) {
(14)           if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(14)           if (&User-Name =~ /\.\./ ) {
(14)           if (&User-Name =~ /\.\./ )  -> FALSE
(14)           if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))  {
(14)           if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))   -> FALSE
(14)           if (&User-Name =~ /\.$/)  {
(14)           if (&User-Name =~ /\.$/)   -> FALSE
(14)           if (&User-Name =~ /@\./)  {
(14)           if (&User-Name =~ /@\./)   -> FALSE
(14)         } # if (&User-Name)  = notfound
(14)       } # policy filter_username = notfound
(14)       [chap] = noop
(14)       [mschap] = noop
(14) suffix: Checking for suffix after "@"
(14) suffix: No '@' in User-Name = "testBenutzer", looking up realm NULL
(14) suffix: No such realm "NULL"
(14)       [suffix] = noop
(14)       update control {
(14)         &Proxy-To-Realm := LOCAL
(14)       } # update control = noop
(14) eap: Peer sent EAP Response (code 2) ID 4 length 12
(14) eap: EAP-Identity reply, returning 'ok' so we can short-circuit the rest of authorize
(14)       [eap] = ok
(14)     } # authorize = ok
(14)   Found Auth-Type = eap
(14)   # Executing group from file /etc/freeradius/3.0/sites-enabled/inner-tunnel
(14)     authenticate {
(14) eap: Peer sent packet with method EAP Identity (1)
(14) eap: Calling submodule eap_mschapv2 to process data
(14) eap_mschapv2: Issuing Challenge
(14) eap: Sending EAP Request (code 1) ID 5 length 43
(14) eap: EAP session adding &reply:State = 0xdd167b72dd1361b8
(14)       [eap] = handled
(14)     } # authenticate = handled
(14) } # server inner-tunnel
(14) Virtual server sending reply
(14)   EAP-Message = 0x0105002b1a01050026104fd75d00cf1b1ee23a43eb533a2b55e36672656572616469757 32d332e302e3136
(14)   Message-Authenticator = 0x00000000000000000000000000000000
(14)   State = 0xdd167b72dd1361b882db11b1ea4461c2
(14) eap_peap: Got tunneled reply code 11
(14) eap_peap:   EAP-Message = 
0x0105002b1a01050026104fd75d00cf1b1ee23a43eb533a2b55e366726565726164697573 2d332e302e3136
(14) eap_peap:   Message-Authenticator = 0x00000000000000000000000000000000
(14) eap_peap:   State = 0xdd167b72dd1361b882db11b1ea4461c2
(14) eap_peap: Got tunneled reply RADIUS code 11
(14) eap_peap:   EAP-Message = 
0x0105002b1a01050026104fd75d00cf1b1ee23a43eb533a2b55e36672656572616469757 32d332e302e3136
(14) eap_peap:   Message-Authenticator = 0x00000000000000000000000000000000
(14) eap_peap:   State = 0xdd167b72dd1361b882db11b1ea4461c2
(14) eap_peap: Got tunneled Access-Challenge
(14) eap: Sending EAP Request (code 1) ID 5 length 74
(14) eap: EAP session adding &reply:State = 0x1682c78c1087de3c
(14)     [eap] = handled
(14)   } # authenticate = handled
(14) Using Post-Auth-Type Challenge
(14) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(14)   Challenge { ... } # empty sub-section is ignored
(14) Sent Access-Challenge Id 210 from 10.16.1.1:1812 to 10.110.0.253:15035 length 0
(14)   EAP-Message =
0x0105004a1900170303003fab9cdd8b2e98b5447b988d9a58da55ef1537be89fa021f813185899ec852de378e28cb85260c6df4e30af3b3eaa
(14)   Message-Authenticator = 0x00000000000000000000000000000000
(14)   State = 0x1682c78c1087de3c204caa76a5e89391
(14) Finished request
Waking up in 2.0 seconds.
(15) Received Access-Request Id 211 from 10.110.0.253:15552 to 10.16.1.1:1812 length 334
(15)   User-Name = "testBenutzer"
(15)   NAS-Identifier = "WLC-Meineschule-1"
(15)   LCS-Orig-NAS-Identifier = "00A057604349"
(15)   Called-Station-Id = "0E-A0-57-60-43-4C:gym-lehrer"
(15)   NAS-Port-Type = Wireless-802.11
(15)   Service-Type = Framed-User
(15)   Calling-Station-Id = "6C-C7-EC-60-61-34"
(15)   Connect-Info = "CONNECT"
(15)   Acct-Session-Id = "B42DB9D0899ACF18"
(15)   Acct-Multi-Session-Id = "05430C7B820DAC3B"
(15)   WLAN-Pairwise-Cipher = 1027076
(15)   WLAN-Group-Cipher = 1027076
(15)   WLAN-AKM-Suite = 1027073
(15)   Framed-MTU = 1400
(15)   EAP-Message =
0x020500611900170303005600000000000000000277746100b664cad1fef5869f50827a3c9713a8792442c76351695030625d7a7f41cf37fd0ca
(15)   State = 0x1682c78c1087de3c204caa76a5e89391
(15)   Message-Authenticator = 0x6866dc0cd50563cf516b33f2882bacb6
(15) session-state: No cached attributes
(15) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/default
(15)   authorize {
(15)     policy filter_username {
(15)       if (&User-Name) {
(15)       if (&User-Name)  -> TRUE
(15)       if (&User-Name)  {
(15)         if (&User-Name =~ / /) {
(15)         if (&User-Name =~ / /)  -> FALSE
(15)         if (&User-Name =~ /@[^@]*@/ ) {
(15)         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(15)         if (&User-Name =~ /\.\./ ) {
(15)         if (&User-Name =~ /\.\./ )  -> FALSE
(15)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))  {
(15)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))   -> FALSE
(15)         if (&User-Name =~ /\.$/)  {
(15)         if (&User-Name =~ /\.$/)   -> FALSE
(15)         if (&User-Name =~ /@\./)  {
(15)         if (&User-Name =~ /@\./)   -> FALSE
(15)       } # if (&User-Name)  = notfound
(15)     } # policy filter_username = notfound
(15)     [preprocess] = ok
(15)     [chap] = noop
(15)     [mschap] = noop
(15)     [digest] = noop
(15) suffix: Checking for suffix after "@"
(15) suffix: No '@' in User-Name = "testBenutzer", looking up realm NULL
(15) suffix: No such realm "NULL"
(15)     [suffix] = noop
(15) eap: Peer sent EAP Response (code 2) ID 5 length 97
(15) eap: Continuing tunnel setup
(15)     [eap] = ok
(15)   } # authorize = ok
(15) Found Auth-Type = eap
(15) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(15)   authenticate {
(15) eap: Expiring EAP session with state 0xdd167b72dd1361b8
```

```
(15) eap: Finished EAP session with state 0x1682c78c1087de3c
(15) eap: Previous EAP request found for state 0x1682c78c1087de3c, released from the list
(15) eap: Peer sent packet with method EAP PEAP (25)
(15) eap: Calling submodule eap_peap to process data
(15) eap_peap: Continuing EAP-TLS
(15) eap_peap: [eaptls verify] = ok
(15) eap_peap: Done initial handshake
(15) eap_peap: [eaptls process] = ok
(15) eap_peap: Session established.  Decoding tunneled attributes
(15) eap_peap: PEAP state phase2
(15) eap_peap: EAP method MSCHAPv2 (26)
(15) eap_peap: Got tunneled request
(15) eap_peap:   EAP-Message = 
0x020500421a0205003d317bcc572d2470a9780e65e01eff641d1f0000000000000000f96cd34c798762c624de34864cf98360e577ebf0158eb3
(15) eap_peap: Setting User-Name to testBenutzer
(15) eap_peap: Sending tunneled request to inner-tunnel
(15) eap_peap:   EAP-Message = 
0x020500421a0205003d317bcc572d2470a9780e65e01eff641d1f0000000000000000f96cd34c798762c624de34864cf98360e577ebf0158eb3
(15) eap_peap:   FreeRADIUS-Proxied-To = 127.0.0.1
(15) eap_peap:   User-Name = "testBenutzer"
(15) eap_peap:   State = 0xdd167b72dd1361b882db11b1ea4461c2
(15) Virtual server inner-tunnel received request
(15)   EAP-Message = 
0x020500421a0205003d317bcc572d2470a9780e65e01eff641d1f0000000000000000f96cd34c798762c624de34864cf98360e577ebf0158eb3
(15)   FreeRADIUS-Proxied-To = 127.0.0.1
(15)   User-Name = "testBenutzer"
(15)   State = 0xdd167b72dd1361b882db11b1ea4461c2
(15) WARNING: Outer and inner identities are the same.  User privacy is compromised.
(15) server inner-tunnel {
(15)   session-state: No cached attributes
(15)   # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/inner-tunnel
(15)     authorize {
(15)       policy filter_username {
(15)         if (&User-Name) {
(15)         if (&User-Name)  -> TRUE
(15)         if (&User-Name)  {
(15)           if (&User-Name =~ / /) {
(15)           if (&User-Name =~ / /)  -> FALSE
(15)           if (&User-Name =~ /@[^@]*@/ ) {
(15)           if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(15)           if (&User-Name =~ /\.\./ ) {
(15)           if (&User-Name =~ /\.\./ )  -> FALSE
(15)           if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))  {
(15)           if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))   -> FALSE
(15)           if (&User-Name =~ /\.$/)  {
(15)           if (&User-Name =~ /\.$/)   -> FALSE
(15)           if (&User-Name =~ /@\./)  {
(15)           if (&User-Name =~ /@\./)   -> FALSE
(15)         } # if (&User-Name)  = notfound
(15)       } # policy filter_username = notfound
(15)       [chap] = noop
(15)       [mschap] = noop
(15) suffix: Checking for suffix after "@"
(15) suffix: No '@' in User-Name = "testBenutzer", looking up realm NULL
(15) suffix: No such realm "NULL"
(15)       [suffix] = noop
(15)       update control {
(15)         &Proxy-To-Realm := LOCAL
(15)       } # update control = noop
(15) eap: Peer sent EAP Response (code 2) ID 5 length 66
(15) eap: No EAP Start, assuming it's an on-going EAP conversation
(15)       [eap] = updated
(15) files: users: Matched entry DEFAULT at line 1
(15)       [files] = ok
(15)       [expiration] = noop
(15)       [logintime] = noop
(15)       [pap] = noop
(15)     } # authorize = updated
(15)   Found Auth-Type = eap
(15)   # Executing group from file /etc/freeradius/3.0/sites-enabled/inner-tunnel
(15)     authenticate {
(15) eap: Expiring EAP session with state 0xdd167b72dd1361b8
(15) eap: Finished EAP session with state 0xdd167b72dd1361b8
(15) eap: Previous EAP request found for state 0xdd167b72dd1361b8, released from the list
(15) eap: Peer sent packet with method EAP MSCHAPv2 (26)
(15) eap: Calling submodule eap_mschapv2 to process data
(15) eap_mschapv2: # Executing group from file /etc/freeradius/3.0/sites-enabled/inner-tunnel
(15) eap_mschapv2:   authenticate {
(15) mschap: WARNING: No Cleartext-Password configured.  Cannot create NT-Password
(15) mschap: WARNING: No Cleartext-Password configured.  Cannot create LM-Password
(15) mschap: Creating challenge hash with username: testBenutzer
(15) mschap: Client is using MS-CHAPv2
(15) mschap: ERROR: FAILED: No NT/LM-Password.  Cannot perform authentication
(15) mschap: ERROR: MS-CHAP2-Response is incorrect
(15)     [mschap] = reject
(15)   } # authenticate = reject
(15) eap: Sending EAP Failure (code 4) ID 5 length 4
(15) eap: Freeing handler
(15)       [eap] = reject
(15)     } # authenticate = reject
(15)   Failed to authenticate the user
(15)   Using Post-Auth-Type Reject
(15)   # Executing group from file /etc/freeradius/3.0/sites-enabled/inner-tunnel
(15)     Post-Auth-Type REJECT {
(15) attr_filter.access_reject: EXPAND %{User-Name}
(15) attr_filter.access_reject:    --> testBenutzer
(15) attr_filter.access_reject: Matched entry DEFAULT at line 11
(15)       [attr_filter.access_reject] = updated
(15)       update outer.session-state {
(15)         &Module-Failure-Message := &request:Module-Failure-Message -> 'mschap: FAILED: No NT/LM-
Password.  Cannot perform authentication'
(15)       } # update outer.session-state = noop
(15)     } # Post-Auth-Type REJECT = updated
(15) } # server inner-tunnel
(15) Virtual server sending reply
(15)   MS-CHAP-Error = "\005E=691 R=1 C=75b17bfd8896142985e4b7a242629a54 V=3 M=Authentication rejected"
(15)   EAP-Message = 0x04050004
(15)   Message-Authenticator = 0x00000000000000000000000000000000
(15) eap_peap: Got tunneled reply code 3
(15) eap_peap:   MS-CHAP-Error = "\005E=691 R=1 C=75b17bfd8896142985e4b7a242629a54 V=3 M=Authentication
rejected"
(15) eap_peap:   EAP-Message = 0x04050004
(15) eap_peap:   Message-Authenticator = 0x00000000000000000000000000000000
(15) eap_peap: Got tunneled reply RADIUS code 3
(15) eap_peap:   MS-CHAP-Error = "\005E=691 R=1 C=75b17bfd8896142985e4b7a242629a54 V=3 M=Authentication
rejected"
(15) eap_peap:   EAP-Message = 0x04050004
(15) eap_peap:   Message-Authenticator = 0x00000000000000000000000000000000
(15) eap_peap: Tunneled authentication was rejected
(15) eap_peap: FAILURE
(15) eap: Sending EAP Request (code 1) ID 6 length 46
(15) eap: EAP session adding &reply:State = 0x1682c78c1184de3c
(15)     [eap] = handled
(15)   } # authenticate = handled
(15) Using Post-Auth-Type Challenge
(15) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(15)   Challenge { ... } # empty sub-section is ignored
(15) session-state: Saving cached attributes
(15)   Module-Failure-Message := "mschap: FAILED: No NT/LM-Password.  Cannot perform authentication"
(15) Sent Access-Challenge Id 211 from 10.16.1.1:1812 to 10.110.0.253:15552 length 0
(15)   EAP-Message =
0x0106002e19001703030023ab9cdd8b2e98b545f06564f06110fdb32b829b88b9751c8388f293f93b0e7c62253b57
(15)   Message-Authenticator = 0x00000000000000000000000000000000
(15)   State = 0x1682c78c1184de3c204caa76a5e89391
(15) Finished request
Waking up in 1.9 seconds.
(11) Cleaning up request packet ID 207 with timestamp +214
(12) Cleaning up request packet ID 208 with timestamp +214
Waking up in 2.9 seconds.
(13) Cleaning up request packet ID 209 with timestamp +217
(14) Cleaning up request packet ID 210 with timestamp +217
(15) Cleaning up request packet ID 211 with timestamp +217
Ready to process requests
(16) Received Access-Request Id 212 from 10.110.0.253:15670 to 10.16.1.1:1812 length 283
(16)   User-Name = "testBenutzer"
(16)   NAS-Identifier = "WLC-Meineschule-1"
(16)   LCS-Orig-NAS-Identifier = "00A057604349"
(16)   Called-Station-Id = "0E-A0-57-60-43-4C:gym-lehrer"
```

```
(16)   NAS-Port-Type = Wireless-802.11
(16)   Service-Type = Framed-User
(16)   Calling-Station-Id = "6C-C7-EC-60-61-34"
(16)   Connect-Info = "CONNECT"
(16)   Acct-Session-Id = "B42DB9D0899ACF18"
(16)   Acct-Multi-Session-Id = "05430C7B820DAC3B"
(16)   WLAN-Pairwise-Cipher = 1027076
(16)   WLAN-Group-Cipher = 1027076
(16)   WLAN-AKM-Suite = 1027073
(16)   Framed-MTU = 1400
(16)   EAP-Message = 
0x0206002e19001703030023000000000000000030b01656f4052754085af2ce7a0de27d49ebfbe5dc8536b32fcaced
(16)   State = 0x1682c78c1184de3c204caa76a5e89391
(16)   Message-Authenticator = 0x3ffdedf7a1bff2606b97be1544a74312
(16) Restoring &session-state
(16)   &session-state:Module-Failure-Message := "mschap: FAILED: No NT/LM-Password.  Cannot perform 
authentication"
(16) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/default
(16)   authorize {
(16)     policy filter_username {
(16)       if (&User-Name) {
(16)       if (&User-Name)  -> TRUE
(16)       if (&User-Name)  {
(16)         if (&User-Name =~ / /) {
(16)         if (&User-Name =~ / /)  -> FALSE
(16)         if (&User-Name =~ /@[^@]*@/ ) {
(16)         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(16)         if (&User-Name =~ /\.\./ ) {
(16)         if (&User-Name =~ /\.\./ )  -> FALSE
(16)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))  {
(16)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))   -> FALSE
(16)         if (&User-Name =~ /\.$/)  {
(16)         if (&User-Name =~ /\.$/)   -> FALSE
(16)         if (&User-Name =~ /@\./)  {
(16)         if (&User-Name =~ /@\./)   -> FALSE
(16)       } # if (&User-Name)  = notfound
(16)     } # policy filter_username = notfound
(16)     [preprocess] = ok
(16)     [chap] = noop
(16)     [mschap] = noop
(16)     [digest] = noop
(16) suffix: Checking for suffix after "@"
(16) suffix: No '@' in User-Name = "testBenutzer", looking up realm NULL
(16) suffix: No such realm "NULL"
(16)     [suffix] = noop
(16) eap: Peer sent EAP Response (code 2) ID 6 length 46
(16) eap: Continuing tunnel setup
(16)     [eap] = ok
(16)   } # authorize = ok
(16) Found Auth-Type = eap
(16) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(16)   authenticate {
(16) eap: Expiring EAP session with state 0x1682c78c1184de3c
(16) eap: Finished EAP session with state 0x1682c78c1184de3c
(16) eap: Previous EAP request found for state 0x1682c78c1184de3c, released from the list
(16) eap: Peer sent packet with method EAP PEAP (25)
(16) eap: Calling submodule eap_peap to process data
(16) eap_peap: Continuing EAP-TLS
(16) eap_peap: [eaptls verify] = ok
(16) eap_peap: Done initial handshake
(16) eap_peap: [eaptls process] = ok
(16) eap_peap: Session established.  Decoding tunneled attributes
(16) eap_peap: PEAP state send tlv failure
(16) eap_peap: Received EAP-TLV response
(16) eap_peap:   ERROR: The users session was previously rejected: returning reject (again.)
(16) eap_peap:   This means you need to read the PREVIOUS messages in the debug output
(16) eap_peap:   to find out the reason why the user was rejected
(16) eap_peap:   Look for "reject" or "fail".  Those earlier messages will tell you
(16) eap_peap:   what went wrong, and how to fix the problem
(16) eap: ERROR: Failed continuing EAP PEAP (25) session.  EAP sub-module failed
(16) eap: Sending EAP Failure (code 4) ID 6 length 4
(16) eap: Failed in EAP select
(16)     [eap] = invalid
(16)   } # authenticate = invalid
```

```
(16) Failed to authenticate the user
(16) Using Post-Auth-Type Reject
(16) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(16)   Post-Auth-Type REJECT {
(16) attr_filter.access_reject: EXPAND %{User-Name}
(16) attr_filter.access_reject:    --> testBenutzer
(16) attr_filter.access_reject: Matched entry DEFAULT at line 11
(16)     [attr_filter.access_reject] = updated
(16)     [eap] = noop
(16)     policy remove_reply_message_if_eap {
(16)       if (&reply:EAP-Message && &reply:Reply-Message) {
(16)       if (&reply:EAP-Message && &reply:Reply-Message)  -> FALSE
(16)       else {
(16)         [noop] = noop
(16)       } # else = noop
(16)     } # policy remove_reply_message_if_eap = noop
(16)   } # Post-Auth-Type REJECT = updated
(16) Delaying response for 1.000000 seconds
Waking up in 0.3 seconds.
Waking up in 0.6 seconds.
(16) Sending delayed response
(16) Sent Access-Reject Id 212 from 10.16.1.1:1812 to 10.110.0.253:15670 length 44
(16)   EAP-Message = 0x04060004
(16)   Message-Authenticator = 0x00000000000000000000000000000000
Waking up in 3.9 seconds.
(16) Cleaning up request packet ID 212 with timestamp +226
Ready to process requests
(17) Received Access-Request Id 213 from 10.110.0.253:15599 to 10.16.1.1:1812 length 231
(17)   User-Name = "testBenutzer"
(17)   NAS-Identifier = "WLC-Meineschule-1"
(17)   LCS-Orig-NAS-Identifier = "00A057604255"
(17)   Called-Station-Id = "0E-A0-57-60-42-58:gym-lehrer"
(17)   NAS-Port-Type = Wireless-802.11
(17)   Service-Type = Framed-User
(17)   Calling-Station-Id = "6C-C7-EC-60-61-34"
(17)   Connect-Info = "CONNECT"
(17)   Acct-Session-Id = "80AB5154C1B6824B"
(17)   Acct-Multi-Session-Id = "E08BCFEFC9B6F9DF"
(17)   WLAN-Pairwise-Cipher = 1027076
(17)   WLAN-Group-Cipher = 1027076
(17)   WLAN-AKM-Suite = 1027073
(17)   Framed-MTU = 1400
(17)   EAP-Message = 0x0234000c01736368756c7465
(17)   Message-Authenticator = 0x20561b95c2ee6bc5261cc44114b33458
(17) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/default
(17)   authorize {
(17)     policy filter_username {
(17)       if (&User-Name) {
(17)       if (&User-Name)  -> TRUE
(17)       if (&User-Name)  {
(17)         if (&User-Name =~ / /) {
(17)         if (&User-Name =~ / /)  -> FALSE
(17)         if (&User-Name =~ /@[^@]*@/ ) {
(17)         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(17)         if (&User-Name =~ /\.\./ ) {
(17)         if (&User-Name =~ /\.\./ )  -> FALSE
(17)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))  {
(17)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))   -> FALSE
(17)         if (&User-Name =~ /\.$/)  {
(17)         if (&User-Name =~ /\.$/)   -> FALSE
(17)         if (&User-Name =~ /@\./)  {
(17)         if (&User-Name =~ /@\./)   -> FALSE
(17)       } # if (&User-Name)  = notfound
(17)     } # policy filter_username = notfound
(17)     [preprocess] = ok
(17)     [chap] = noop
(17)     [mschap] = noop
(17)     [digest] = noop
(17) suffix: Checking for suffix after "@"
(17) suffix: No '@' in User-Name = "testBenutzer", looking up realm NULL
(17) suffix: No such realm "NULL"
(17)     [suffix] = noop
(17) eap: Peer sent EAP Response (code 2) ID 52 length 12
(17) eap: EAP-Identity reply, returning 'ok' so we can short-circuit the rest of authorize
```

```
(17)     [eap] = ok
(17)   } # authorize = ok
(17) Found Auth-Type = eap
(17) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(17)   authenticate {
(17) eap: Peer sent packet with method EAP Identity (1)
(17) eap: Calling submodule eap_md5 to process data
(17) eap_md5: Issuing MD5 Challenge
(17) eap: Sending EAP Request (code 1) ID 53 length 22
(17) eap: EAP session adding &reply:State = 0x8db105c88d84013b
(17)     [eap] = handled
(17)   } # authenticate = handled
(17) Using Post-Auth-Type Challenge
(17) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(17)   Challenge { ... } # empty sub-section is ignored
(17) Sent Access-Challenge Id 213 from 10.16.1.1:1812 to 10.110.0.253:15599 length 0
(17)   EAP-Message = 0x0135001604107b09f4f274a4124b52bbc856ac9b8a6a
(17)   Message-Authenticator = 0x00000000000000000000000000000000
(17)   State = 0x8db105c88d84013b038a302aed8b6639
(17) Finished request
Waking up in 4.9 seconds.
(18) Received Access-Request Id 214 from 10.110.0.253:16143 to 10.16.1.1:1812 length 243
(18)   User-Name = "testBenutzer"
(18)   NAS-Identifier = "WLC-Meineschule-1"
(18)   LCS-Orig-NAS-Identifier = "00A057604255"
(18)   Called-Station-Id = "0E-A0-57-60-42-58:gym-lehrer"
(18)   NAS-Port-Type = Wireless-802.11
(18)   Service-Type = Framed-User
(18)   Calling-Station-Id = "6C-C7-EC-60-61-34"
(18)   Connect-Info = "CONNECT"
(18)   Acct-Session-Id = "80AB5154C1B6824B"
(18)   Acct-Multi-Session-Id = "E08BCFEFC9B6F9DF"
(18)   WLAN-Pairwise-Cipher = 1027076
(18)   WLAN-Group-Cipher = 1027076
(18)   WLAN-AKM-Suite = 1027073
(18)   Framed-MTU = 1400
(18)   EAP-Message = 0x023500060319
(18)   State = 0x8db105c88d84013b038a302aed8b6639
(18)   Message-Authenticator = 0xb82353e991d17896319de88f90657208
(18) session-state: No cached attributes
(18) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/default
(18)   authorize {
(18)     policy filter_username {
(18)       if (&User-Name) {
(18)       if (&User-Name)  -> TRUE
(18)       if (&User-Name)  {
(18)         if (&User-Name =~ / /) {
(18)         if (&User-Name =~ / /)  -> FALSE
(18)         if (&User-Name =~ /@[^@]*@/ ) {
(18)         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(18)         if (&User-Name =~ /\.\./ ) {
(18)         if (&User-Name =~ /\.\./ )  -> FALSE
(18)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))  {
(18)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))   -> FALSE
(18)         if (&User-Name =~ /\.$/)  {
(18)         if (&User-Name =~ /\.$/)   -> FALSE
(18)         if (&User-Name =~ /@\./)  {
(18)         if (&User-Name =~ /@\./)   -> FALSE
(18)       } # if (&User-Name)  = notfound
(18)     } # policy filter_username = notfound
(18)     [preprocess] = ok
(18)     [chap] = noop
(18)     [mschap] = noop
(18)     [digest] = noop
(18) suffix: Checking for suffix after "@"
(18) suffix: No '@' in User-Name = "testBenutzer", looking up realm NULL
(18) suffix: No such realm "NULL"
(18)     [suffix] = noop
(18) eap: Peer sent EAP Response (code 2) ID 53 length 6
(18) eap: No EAP Start, assuming it's an on-going EAP conversation
(18)     [eap] = updated
(18) files: users: Matched entry DEFAULT at line 1
(18)     [files] = ok
(18)     [expiration] = noop
```

```
(18)     [logintime] = noop
(18) pap: WARNING: No "known good" password found for the user.  Not setting Auth-Type
(18) pap: WARNING: Authentication will fail unless a "known good" password is available
(18)     [pap] = noop
(18)   } # authorize = updated
(18) Found Auth-Type = eap
(18) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(18)   authenticate {
(18) eap: Expiring EAP session with state 0x8db105c88d84013b
(18) eap: Finished EAP session with state 0x8db105c88d84013b
(18) eap: Previous EAP request found for state 0x8db105c88d84013b, released from the list
(18) eap: Peer sent packet with method EAP NAK (3)
(18) eap: Found mutually acceptable type PEAP (25)
(18) eap: Calling submodule eap_peap to process data
(18) eap_peap: Initiating new EAP-TLS session
(18) eap_peap: [eaptls start] = request
(18) eap: Sending EAP Request (code 1) ID 54 length 6
(18) eap: EAP session adding &reply:State = 0x8db105c88c871c3b
(18)     [eap] = handled
(18)   } # authenticate = handled
(18) Using Post-Auth-Type Challenge
(18) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(18)   Challenge { ... } # empty sub-section is ignored
(18) Sent Access-Challenge Id 214 from 10.16.1.1:1812 to 10.110.0.253:16143 length 0
(18)   EAP-Message = 0x013600061920
(18)   Message-Authenticator = 0x00000000000000000000000000000000
(18)   State = 0x8db105c88c871c3b038a302aed8b6639
(18) Finished request
Waking up in 4.9 seconds.
(19) Received Access-Request Id 215 from 10.110.0.253:14101 to 10.16.1.1:1812 length 404
(19)   User-Name = "testBenutzer"
(19)   NAS-Identifier = "WLC-Meineschule-1"
(19)   LCS-Orig-NAS-Identifier = "00A057604255"
(19)   Called-Station-Id = "0E-A0-57-60-42-58:gym-lehrer"
(19)   NAS-Port-Type = Wireless-802.11
(19)   Service-Type = Framed-User
(19)   Calling-Station-Id = "6C-C7-EC-60-61-34"
(19)   Connect-Info = "CONNECT"
(19)   Acct-Session-Id = "80AB5154C1B6824B"
(19)   Acct-Multi-Session-Id = "E08BCFEFC9B6F9DF"
(19)   WLAN-Pairwise-Cipher = 1027076
(19)   WLAN-Group-Cipher = 1027076
(19)   WLAN-AKM-Suite = 1027073
(19)   Framed-MTU = 1400
(19)   EAP-Message = 
0x023600a719800000009d16030100980100009403033351ec4acca45fcc13c2363921026ed26209ae25e3104e6b3a147058dc9be65ad00003cc
(19)   State = 0x8db105c88c871c3b038a302aed8b6639
(19)   Message-Authenticator = 0x379e457b1a7f0d8edf05c391dcba6f22
(19) session-state: No cached attributes
(19) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/default
(19)   authorize {
(19)     policy filter_username {
(19)       if (&User-Name) {
(19)       if (&User-Name)  -> TRUE
(19)       if (&User-Name)  {
(19)         if (&User-Name =~ / /) {
(19)         if (&User-Name =~ / /)  -> FALSE
(19)         if (&User-Name =~ /@[^@]*@/ ) {
(19)         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(19)         if (&User-Name =~ /\.\./ ) {
(19)         if (&User-Name =~ /\.\./ )  -> FALSE
(19)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))  {
(19)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))   -> FALSE
(19)         if (&User-Name =~ /\.$/)  {
(19)         if (&User-Name =~ /\.$/)   -> FALSE
(19)         if (&User-Name =~ /@\./)  {
(19)         if (&User-Name =~ /@\./)   -> FALSE
(19)       } # if (&User-Name)  = notfound
(19)     } # policy filter_username = notfound
(19)     [preprocess] = ok
(19)     [chap] = noop
(19)     [mschap] = noop
(19)     [digest] = noop
(19) suffix: Checking for suffix after "@"
```

```
(19) suffix: No '@' in User-Name = "testBenutzer", looking up realm NULL
(19) suffix: No such realm "NULL"
(19)     [suffix] = noop
(19) eap: Peer sent EAP Response (code 2) ID 54 length 167
(19) eap: Continuing tunnel setup
(19)     [eap] = ok
(19)   } # authorize = ok
(19) Found Auth-Type = eap
(19) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(19)   authenticate {
(19) eap: Expiring EAP session with state 0x8db105c88c871c3b
(19) eap: Finished EAP session with state 0x8db105c88c871c3b
(19) eap: Previous EAP request found for state 0x8db105c88c871c3b, released from the list
(19) eap: Peer sent packet with method EAP PEAP (25)
(19) eap: Calling submodule eap_peap to process data
(19) eap_peap: Continuing EAP-TLS
(19) eap_peap: Peer indicated complete TLS record size will be 157 bytes
(19) eap_peap: Got complete TLS record (157 bytes)
(19) eap_peap: [eaptls verify] = length included
(19) eap_peap: (other): before SSL initialization
(19) eap_peap: TLS_accept: before SSL initialization
(19) eap_peap: TLS_accept: before SSL initialization
(19) eap_peap: <<< recv UNKNOWN TLS VERSION ?0304? [length 0098]
(19) eap_peap: TLS_accept: SSLv3/TLS read client hello
(19) eap_peap: >>> send TLS 1.2  [length 003d]
(19) eap_peap: TLS_accept: SSLv3/TLS write server hello
(19) eap_peap: >>> send TLS 1.2  [length 02d3]
(19) eap_peap: TLS_accept: SSLv3/TLS write certificate
(19) eap_peap: >>> send TLS 1.2  [length 014d]
(19) eap_peap: TLS_accept: SSLv3/TLS write key exchange
(19) eap_peap: >>> send TLS 1.2  [length 0004]
(19) eap_peap: TLS_accept: SSLv3/TLS write server done
(19) eap_peap: TLS_accept: Need to read more data: SSLv3/TLS write server done
(19) eap_peap: In SSL Handshake Phase
(19) eap_peap: In SSL Accept mode
(19) eap_peap: [eaptls process] = handled
(19) eap: Sending EAP Request (code 1) ID 55 length 1004
(19) eap: EAP session adding &reply:State = 0x8db105c88f861c3b
(19)     [eap] = handled
(19)   } # authenticate = handled
(19) Using Post-Auth-Type Challenge
(19) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(19)   Challenge { ... } # empty sub-section is ignored
(19) Sent Access-Challenge Id 215 from 10.16.1.1:1812 to 10.110.0.253:14101 length 0
(19)   EAP-Message =
0x013703ec19c000000475160303003d02000039030301bbc826a6f2e9bc79f70abd7d236d11e02be8d7ee64e52a2977cc6c2bba0cfa00c02f00
(19)   Message-Authenticator = 0x00000000000000000000000000000000
(19)   State = 0x8db105c88f861c3b038a302aed8b6639
(19) Finished request
Waking up in 1.9 seconds.
(20) Received Access-Request Id 216 from 10.110.0.253:8557 to 10.16.1.1:1812 length 243
(20)   User-Name = "testBenutzer"
(20)   NAS-Identifier = "WLC-Meineschule-1"
(20)   LCS-Orig-NAS-Identifier = "00A057604255"
(20)   Called-Station-Id = "0E-A0-57-60-42-58:gym-lehrer"
(20)   NAS-Port-Type = Wireless-802.11
(20)   Service-Type = Framed-User
(20)   Calling-Station-Id = "6C-C7-EC-60-61-34"
(20)   Connect-Info = "CONNECT"
(20)   Acct-Session-Id = "80AB5154C1B6824B"
(20)   Acct-Multi-Session-Id = "E08BCFEFC9B6F9DF"
(20)   WLAN-Pairwise-Cipher = 1027076
(20)   WLAN-Group-Cipher = 1027076
(20)   WLAN-AKM-Suite = 1027073
(20)   Framed-MTU = 1400
(20)   EAP-Message = 0x023700061900
(20)   State = 0x8db105c88f861c3b038a302aed8b6639
(20)   Message-Authenticator = 0xd8644e2bd27609edf3aa9601aa93a6fe
(20) session-state: No cached attributes
(20) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/default
(20)   authorize {
(20)     policy filter_username {
(20)       if (&User-Name) {
(20)       if (&User-Name)  -> TRUE
```

```
(20)        if (&User-Name)  {
(20)          if (&User-Name =~ / /) {
(20)          if (&User-Name =~ / /)  -> FALSE
(20)          if (&User-Name =~ /@[^@]*@/ ) {
(20)          if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(20)          if (&User-Name =~ /\.\./ ) {
(20)          if (&User-Name =~ /\.\./ )  -> FALSE
(20)          if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))  {
(20)          if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))   -> FALSE
(20)          if (&User-Name =~ /\.$/)  {
(20)          if (&User-Name =~ /\.$/)   -> FALSE
(20)          if (&User-Name =~ /@\./)  {
(20)          if (&User-Name =~ /@\./)   -> FALSE
(20)        } # if (&User-Name)  = notfound
(20)      } # policy filter_username = notfound
(20)      [preprocess] = ok
(20)      [chap] = noop
(20)      [mschap] = noop
(20)      [digest] = noop
(20) suffix: Checking for suffix after "@"
(20) suffix: No '@' in User-Name = "testBenutzer", looking up realm NULL
(20) suffix: No such realm "NULL"
(20)      [suffix] = noop
(20) eap: Peer sent EAP Response (code 2) ID 55 length 6
(20) eap: Continuing tunnel setup
(20)      [eap] = ok
(20)    } # authorize = ok
(20) Found Auth-Type = eap
(20) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(20)    authenticate {
(20) eap: Expiring EAP session with state 0x8db105c88f861c3b
(20) eap: Finished EAP session with state 0x8db105c88f861c3b
(20) eap: Previous EAP request found for state 0x8db105c88f861c3b, released from the list
(20) eap: Peer sent packet with method EAP PEAP (25)
(20) eap: Calling submodule eap_peap to process data
(20) eap_peap: Continuing EAP-TLS
(20) eap_peap: Peer ACKed our handshake fragment
(20) eap_peap: [eaptls verify] = request
(20) eap_peap: [eaptls process] = handled
(20) eap: Sending EAP Request (code 1) ID 56 length 153
(20) eap: EAP session adding &reply:State = 0x8db105c88e891c3b
(20)      [eap] = handled
(20)    } # authenticate = handled
(20) Using Post-Auth-Type Challenge
(20) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(20)    Challenge { ... } # empty sub-section is ignored
(20) Sent Access-Challenge Id 216 from 10.16.1.1:1812 to 10.110.0.253:8557 length 0
(20)    EAP-Message =
0x013800991900d47f7d56905ae0c4c393b3cb7d35f6a69577f2bfe989754042a8a7935536c44bb24247db2ddf5340a089f4acce564094d9e17
(20)    Message-Authenticator = 0x00000000000000000000000000000000
(20)    State = 0x8db105c88e891c3b038a302aed8b6639
(20) Finished request
Waking up in 1.8 seconds.
(17) Cleaning up request packet ID 213 with timestamp +331
(18) Cleaning up request packet ID 214 with timestamp +331
Waking up in 3.0 seconds.
(21) Received Access-Request Id 217 from 10.110.0.253:8227 to 10.16.1.1:1812 length 373
(21)    User-Name = "testBenutzer"
(21)    NAS-Identifier = "WLC-Meineschule-1"
(21)    LCS-Orig-NAS-Identifier = "00A057604255"
(21)    Called-Station-Id = "0E-A0-57-60-42-58:gym-lehrer"
(21)    NAS-Port-Type = Wireless-802.11
(21)    Service-Type = Framed-User
(21)    Calling-Station-Id = "6C-C7-EC-60-61-34"
(21)    Connect-Info = "CONNECT"
(21)    Acct-Session-Id = "80AB5154C1B6824B"
(21)    Acct-Multi-Session-Id = "E08BCFEFC9B6F9DF"
(21)    WLAN-Pairwise-Cipher = 1027076
(21)    WLAN-Group-Cipher = 1027076
(21)    WLAN-AKM-Suite = 1027073
(21)    Framed-MTU = 1400
(21)    EAP-Message =
0x0238008819800000007e16030300461000004241040376d129ac1ceff609854c4cdc0c461616923ea04588dd5be121f7cd73c80571ddfb7a8
(21)    State = 0x8db105c88e891c3b038a302aed8b6639
```

```
(21)   Message-Authenticator = 0x35f4ddba5780b413737c5338aa86e45f
(21) session-state: No cached attributes
(21) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/default
(21)   authorize {
(21)     policy filter_username {
(21)       if (&User-Name) {
(21)       if (&User-Name)  -> TRUE
(21)       if (&User-Name)  {
(21)         if (&User-Name =~ / /) {
(21)         if (&User-Name =~ / /)  -> FALSE
(21)         if (&User-Name =~ /@[^@]*@/ ) {
(21)         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(21)         if (&User-Name =~ /\.\./ ) {
(21)         if (&User-Name =~ /\.\./ )  -> FALSE
(21)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))  {
(21)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))   -> FALSE
(21)         if (&User-Name =~ /\.$/)  {
(21)         if (&User-Name =~ /\.$/)   -> FALSE
(21)         if (&User-Name =~ /@\./)  {
(21)         if (&User-Name =~ /@\./)   -> FALSE
(21)       } # if (&User-Name)  = notfound
(21)     } # policy filter_username = notfound
(21)     [preprocess] = ok
(21)     [chap] = noop
(21)     [mschap] = noop
(21)     [digest] = noop
(21) suffix: Checking for suffix after "@"
(21) suffix: No '@' in User-Name = "testBenutzer", looking up realm NULL
(21) suffix: No such realm "NULL"
(21)     [suffix] = noop
(21) eap: Peer sent EAP Response (code 2) ID 56 length 136
(21) eap: Continuing tunnel setup
(21)     [eap] = ok
(21)   } # authorize = ok
(21) Found Auth-Type = eap
(21) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(21)   authenticate {
(21) eap: Expiring EAP session with state 0x8db105c88e891c3b
(21) eap: Finished EAP session with state 0x8db105c88e891c3b
(21) eap: Previous EAP request found for state 0x8db105c88e891c3b, released from the list
(21) eap: Peer sent packet with method EAP PEAP (25)
(21) eap: Calling submodule eap_peap to process data
(21) eap_peap: Continuing EAP-TLS
(21) eap_peap: Peer indicated complete TLS record size will be 126 bytes
(21) eap_peap: Got complete TLS record (126 bytes)
(21) eap_peap: [eaptls verify] = length included
(21) eap_peap: TLS_accept: SSLv3/TLS write server done
(21) eap_peap: <<< recv TLS 1.2  [length 0046]
(21) eap_peap: TLS_accept: SSLv3/TLS read client key exchange
(21) eap_peap: TLS_accept: SSLv3/TLS read change cipher spec
(21) eap_peap: <<< recv TLS 1.2  [length 0010]
(21) eap_peap: TLS_accept: SSLv3/TLS read finished
(21) eap_peap: >>> send TLS 1.2  [length 0001]
(21) eap_peap: TLS_accept: SSLv3/TLS write change cipher spec
(21) eap_peap: >>> send TLS 1.2  [length 0010]
(21) eap_peap: TLS_accept: SSLv3/TLS write finished
(21) eap_peap: (other): SSL negotiation finished successfully
(21) eap_peap: SSL Connection Established
(21) eap_peap: [eaptls process] = handled
(21) eap: Sending EAP Request (code 1) ID 57 length 57
(21) eap: EAP session adding &reply:State = 0x8db105c889881c3b
(21)     [eap] = handled
(21)   } # authenticate = handled
(21) Using Post-Auth-Type Challenge
(21) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(21)   Challenge { ... } # empty sub-section is ignored
(21) Sent Access-Challenge Id 217 from 10.16.1.1:1812 to 10.110.0.253:8227 length 0
(21)   EAP-Message =
0x0139003919001403030001011603030028 51a2884ce9c90687e36d7ad86583af69dd71b031a6fdf1e08d3684edc20cb3028ff77c7f296f9d5b
(21)   Message-Authenticator = 0x00000000000000000000000000000000
(21)   State = 0x8db105c889881c3b038a302aed8b6639
(21) Finished request
Waking up in 2.0 seconds.
(22) Received Access-Request Id 218 from 10.110.0.253:11717 to 10.16.1.1:1812 length 243
```

```
(22)   User-Name = "testBenutzer"
(22)   NAS-Identifier = "WLC-Meineschule-1"
(22)   LCS-Orig-NAS-Identifier = "00A057604255"
(22)   Called-Station-Id = "0E-A0-57-60-42-58:gym-lehrer"
(22)   NAS-Port-Type = Wireless-802.11
(22)   Service-Type = Framed-User
(22)   Calling-Station-Id = "6C-C7-EC-60-61-34"
(22)   Connect-Info = "CONNECT"
(22)   Acct-Session-Id = "80AB5154C1B6824B"
(22)   Acct-Multi-Session-Id = "E08BCFEFC9B6F9DF"
(22)   WLAN-Pairwise-Cipher = 1027076
(22)   WLAN-Group-Cipher = 1027076
(22)   WLAN-AKM-Suite = 1027073
(22)   Framed-MTU = 1400
(22)   EAP-Message = 0x023900061900
(22)   State = 0x8db105c889881c3b038a302aed8b6639
(22)   Message-Authenticator = 0x709d03611998f462119e8d7b106d8312
(22) session-state: No cached attributes
(22) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/default
(22)   authorize {
(22)     policy filter_username {
(22)       if (&User-Name) {
(22)       if (&User-Name)  -> TRUE
(22)       if (&User-Name)  {
(22)         if (&User-Name =~ / /) {
(22)         if (&User-Name =~ / /)  -> FALSE
(22)         if (&User-Name =~ /@[^@]*@/ ) {
(22)         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(22)         if (&User-Name =~ /\.\./ ) {
(22)         if (&User-Name =~ /\.\./ )  -> FALSE
(22)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))  {
(22)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))   -> FALSE
(22)         if (&User-Name =~ /\.$/)  {
(22)         if (&User-Name =~ /\.$/)   -> FALSE
(22)         if (&User-Name =~ /@\./)  {
(22)         if (&User-Name =~ /@\./)   -> FALSE
(22)       } # if (&User-Name)  = notfound
(22)     } # policy filter_username = notfound
(22)     [preprocess] = ok
(22)     [chap] = noop
(22)     [mschap] = noop
(22)     [digest] = noop
(22) suffix: Checking for suffix after "@"
(22) suffix: No '@' in User-Name = "testBenutzer", looking up realm NULL
(22) suffix: No such realm "NULL"
(22)     [suffix] = noop
(22) eap: Peer sent EAP Response (code 2) ID 57 length 6
(22) eap: Continuing tunnel setup
(22)     [eap] = ok
(22)   } # authorize = ok
(22) Found Auth-Type = eap
(22) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(22)   authenticate {
(22) eap: Expiring EAP session with state 0x8db105c889881c3b
(22) eap: Finished EAP session with state 0x8db105c889881c3b
(22) eap: Previous EAP request found for state 0x8db105c889881c3b, released from the list
(22) eap: Peer sent packet with method EAP PEAP (25)
(22) eap: Calling submodule eap_peap to process data
(22) eap_peap: Continuing EAP-TLS
(22) eap_peap: Peer ACKed our handshake fragment.  handshake is finished
(22) eap_peap: [eaptls verify] = success
(22) eap_peap: [eaptls process] = success
(22) eap_peap: Session established.  Decoding tunneled attributes
(22) eap_peap: PEAP state TUNNEL ESTABLISHED
(22) eap: Sending EAP Request (code 1) ID 58 length 40
(22) eap: EAP session adding &reply:State = 0x8db105c8888b1c3b
(22)     [eap] = handled
(22)   } # authenticate = handled
(22) Using Post-Auth-Type Challenge
(22) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(22)   Challenge { ... } # empty sub-section is ignored
(22) Sent Access-Challenge Id 218 from 10.16.1.1:1812 to 10.110.0.253:11717 length 0
(22)   EAP-Message = 0x013a00281900170303001d51a2884ce9c90688165bf84f3edac240783169fe10f494bb7ad50c0df5
(22)   Message-Authenticator = 0x00000000000000000000000000000000
```

```
(22)   State = 0x8db105c8888b1c3b038a302aed8b6639
(22) Finished request
Waking up in 1.9 seconds.
(19) Cleaning up request packet ID 215 with timestamp +334
(20) Cleaning up request packet ID 216 with timestamp +334
Waking up in 2.8 seconds.
(23) Received Access-Request Id 219 from 10.110.0.253:8895 to 10.16.1.1:1812 length 280
(23)   User-Name = "testBenutzer"
(23)   NAS-Identifier = "WLC-Meineschule-1"
(23)   LCS-Orig-NAS-Identifier = "00A057604255"
(23)   Called-Station-Id = "0E-A0-57-60-42-58:gym-lehrer"
(23)   NAS-Port-Type = Wireless-802.11
(23)   Service-Type = Framed-User
(23)   Calling-Station-Id = "6C-C7-EC-60-61-34"
(23)   Connect-Info = "CONNECT"
(23)   Acct-Session-Id = "80AB5154C1B6824B"
(23)   Acct-Multi-Session-Id = "E08BCFEFC9B6F9DF"
(23)   WLAN-Pairwise-Cipher = 1027076
(23)   WLAN-Group-Cipher = 1027076
(23)   WLAN-AKM-Suite = 1027073
(23)   Framed-MTU = 1400
(23)   EAP-Message = 0x023a002b1900170303002000000000000000001219236f618e383c2adf0b7b3f8ea71926d179991c2028514
(23)   State = 0x8db105c8888b1c3b038a302aed8b6639
(23)   Message-Authenticator = 0x647df73791032346e265d768a17e3ad1
(23) session-state: No cached attributes
(23) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/default
(23)   authorize {
(23)     policy filter_username {
(23)       if (&User-Name) {
(23)       if (&User-Name)  -> TRUE
(23)       if (&User-Name)  {
(23)         if (&User-Name =~ / /) {
(23)         if (&User-Name =~ / /)  -> FALSE
(23)         if (&User-Name =~ /@[^@]*@/ ) {
(23)         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(23)         if (&User-Name =~ /\.\./ ) {
(23)         if (&User-Name =~ /\.\./ )  -> FALSE
(23)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))  {
(23)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))   -> FALSE
(23)         if (&User-Name =~ /\.$/)  {
(23)         if (&User-Name =~ /\.$/)   -> FALSE
(23)         if (&User-Name =~ /@\./)  {
(23)         if (&User-Name =~ /@\./)   -> FALSE
(23)       } # if (&User-Name)  = notfound
(23)     } # policy filter_username = notfound
(23)     [preprocess] = ok
(23)     [chap] = noop
(23)     [mschap] = noop
(23)     [digest] = noop
(23) suffix: Checking for suffix after "@"
(23) suffix: No '@' in User-Name = "testBenutzer", looking up realm NULL
(23) suffix: No such realm "NULL"
(23)     [suffix] = noop
(23) eap: Peer sent EAP Response (code 2) ID 58 length 43
(23) eap: Continuing tunnel setup
(23)     [eap] = ok
(23)   } # authorize = ok
(23) Found Auth-Type = eap
(23) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(23)   authenticate {
(23) eap: Expiring EAP session with state 0x8db105c8888b1c3b
(23) eap: Finished EAP session with state 0x8db105c8888b1c3b
(23) eap: Previous EAP request found for state 0x8db105c8888b1c3b, released from the list
(23) eap: Peer sent packet with method EAP PEAP (25)
(23) eap: Calling submodule eap_peap to process data
(23) eap_peap: Continuing EAP-TLS
(23) eap_peap: [eaptls verify] = ok
(23) eap_peap: Done initial handshake
(23) eap_peap: [eaptls process] = ok
(23) eap_peap: Session established.  Decoding tunneled attributes
(23) eap_peap: PEAP state WAITING FOR INNER IDENTITY
(23) eap_peap: Identity - testBenutzer
(23) eap_peap: Got inner identity 'testBenutzer'
(23) eap_peap: Setting default EAP type for tunneled EAP session
```

```
(23) eap_peap: Got tunneled request
(23) eap_peap:   EAP-Message = 0x023a000c01736368756c7465
(23) eap_peap: Setting User-Name to testBenutzer
(23) eap_peap: Sending tunneled request to inner-tunnel
(23) eap_peap:   EAP-Message = 0x023a000c01736368756c7465
(23) eap_peap:   FreeRADIUS-Proxied-To = 127.0.0.1
(23) eap_peap:   User-Name = "testBenutzer"
(23) Virtual server inner-tunnel received request
(23)   EAP-Message = 0x023a000c01736368756c7465
(23)   FreeRADIUS-Proxied-To = 127.0.0.1
(23)   User-Name = "testBenutzer"
(23) WARNING: Outer and inner identities are the same.  User privacy is compromised.
(23) server inner-tunnel {
(23)   # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/inner-tunnel
(23)     authorize {
(23)       policy filter_username {
(23)         if (&User-Name) {
(23)         if (&User-Name)  -> TRUE
(23)         if (&User-Name)  {
(23)           if (&User-Name =~ / /) {
(23)           if (&User-Name =~ / /)  -> FALSE
(23)           if (&User-Name =~ /@[^@]*@/ ) {
(23)           if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(23)           if (&User-Name =~ /\.\./ ) {
(23)           if (&User-Name =~ /\.\./ )  -> FALSE
(23)           if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))  {
(23)           if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))   -> FALSE
(23)           if (&User-Name =~ /\.$/)  {
(23)           if (&User-Name =~ /\.$/)   -> FALSE
(23)           if (&User-Name =~ /@\./)  {
(23)           if (&User-Name =~ /@\./)   -> FALSE
(23)         } # if (&User-Name)  = notfound
(23)       } # policy filter_username = notfound
(23)       [chap] = noop
(23)       [mschap] = noop
(23) suffix: Checking for suffix after "@"
(23) suffix: No '@' in User-Name = "testBenutzer", looking up realm NULL
(23) suffix: No such realm "NULL"
(23)       [suffix] = noop
(23)       update control {
(23)         &Proxy-To-Realm := LOCAL
(23)       } # update control = noop
(23) eap: Peer sent EAP Response (code 2) ID 58 length 12
(23) eap: EAP-Identity reply, returning 'ok' so we can short-circuit the rest of authorize
(23)       [eap] = ok
(23)     } # authorize = ok
(23)   Found Auth-Type = eap
(23)   # Executing group from file /etc/freeradius/3.0/sites-enabled/inner-tunnel
(23)     authenticate {
(23) eap: Peer sent packet with method EAP Identity (1)
(23) eap: Calling submodule eap_mschapv2 to process data
(23) eap_mschapv2: Issuing Challenge
(23) eap: Sending EAP Request (code 1) ID 59 length 43
(23) eap: EAP session adding &reply:State = 0x16bf9d50168487e6
(23)       [eap] = handled
(23)     } # authenticate = handled
(23) } # server inner-tunnel
(23) Virtual server sending reply
(23)   EAP-Message = 0x013b002b1a013b002610e5730dd8d68dfb3180142ca87cd982a5667265657261646975732d332e302e3136
(23)   Message-Authenticator = 0x00000000000000000000000000000000
(23)   State = 0x16bf9d50168487e64b3498ddd081d5aa
(23) eap_peap: Got tunneled reply code 11
(23) eap_peap:   EAP-Message =
0x013b002b1a013b002610e5730dd8d68dfb3180142ca87cd982a5667265657261646975732d332e302e3136
(23) eap_peap:   Message-Authenticator = 0x00000000000000000000000000000000
(23) eap_peap:   State = 0x16bf9d50168487e64b3498ddd081d5aa
(23) eap_peap: Got tunneled reply RADIUS code 11
(23) eap_peap:   EAP-Message =
0x013b002b1a013b002610e5730dd8d68dfb3180142ca87cd982a5667265657261646975732d332e302e3136
(23) eap_peap:   Message-Authenticator = 0x00000000000000000000000000000000
(23) eap_peap:   State = 0x16bf9d50168487e64b3498ddd081d5aa
(23) eap_peap: Got tunneled Access-Challenge
(23) eap: Sending EAP Request (code 1) ID 59 length 74
(23) eap: EAP session adding &reply:State = 0x8db105c88b8a1c3b
```

```
(23)     [eap] = handled
(23)   } # authenticate = handled
(23) Using Post-Auth-Type Challenge
(23) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(23)   Challenge { ... } # empty sub-section is ignored
(23) Sent Access-Challenge Id 219 from 10.16.1.1:1812 to 10.110.0.253:8895 length 0
(23)   EAP-Message =
0x013b004a1900170303003f51a2884ce9c906899e80cbdc4074dcf8ddf67226a0139008c340b90f5092d12ccb65286051275ac13dcebe7f7154
(23)   Message-Authenticator = 0x00000000000000000000000000000000
(23)   State = 0x8db105c88b8a1c3b038a302aed8b6639
(23) Finished request
Waking up in 1.8 seconds.
(24) Received Access-Request Id 220 from 10.110.0.253:12905 to 10.16.1.1:1812 length 334
(24)   User-Name = "testBenutzer"
(24)   NAS-Identifier = "WLC-Meineschule-1"
(24)   LCS-Orig-NAS-Identifier = "00A057604255"
(24)   Called-Station-Id = "0E-A0-57-60-42-58:gym-lehrer"
(24)   NAS-Port-Type = Wireless-802.11
(24)   Service-Type = Framed-User
(24)   Calling-Station-Id = "6C-C7-EC-60-61-34"
(24)   Connect-Info = "CONNECT"
(24)   Acct-Session-Id = "80AB5154C1B6824B"
(24)   Acct-Multi-Session-Id = "E08BCFEFC9B6F9DF"
(24)   WLAN-Pairwise-Cipher = 1027076
(24)   WLAN-Group-Cipher = 1027076
(24)   WLAN-AKM-Suite = 1027073
(24)   Framed-MTU = 1400
(24)   EAP-Message =
0x023b0061190017030300560000000000000002 60e1964c6367454699f808c6dffd008b6a263c129580a04903b5db28b8f652c8e3aef0bf31eb
(24)   State = 0x8db105c88b8a1c3b038a302aed8b6639
(24)   Message-Authenticator = 0xd1a3241e77ac85c05d1c15cc73366940
(24) session-state: No cached attributes
(24) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/default
(24)   authorize {
(24)     policy filter_username {
(24)       if (&User-Name) {
(24)       if (&User-Name)  -> TRUE
(24)       if (&User-Name)  {
(24)         if (&User-Name =~ / /) {
(24)         if (&User-Name =~ / /)  -> FALSE
(24)         if (&User-Name =~ /@[^@]*@/ ) {
(24)         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(24)         if (&User-Name =~ /\.\./ ) {
(24)         if (&User-Name =~ /\.\./ )  -> FALSE
(24)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))  {
(24)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))   -> FALSE
(24)         if (&User-Name =~ /\.$/)  {
(24)         if (&User-Name =~ /\.$/)   -> FALSE
(24)         if (&User-Name =~ /@\./)  {
(24)         if (&User-Name =~ /@\./)   -> FALSE
(24)       } # if (&User-Name)  = notfound
(24)     } # policy filter_username = notfound
(24)     [preprocess] = ok
(24)     [chap] = noop
(24)     [mschap] = noop
(24)     [digest] = noop
(24) suffix: Checking for suffix after "@"
(24) suffix: No '@' in User-Name = "testBenutzer", looking up realm NULL
(24) suffix: No such realm "NULL"
(24)     [suffix] = noop
(24) eap: Peer sent EAP Response (code 2) ID 59 length 97
(24) eap: Continuing tunnel setup
(24)     [eap] = ok
(24)   } # authorize = ok
(24) Found Auth-Type = eap
(24) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(24)   authenticate {
(24) eap: Expiring EAP session with state 0x16bf9d50168487e6
(24) eap: Finished EAP session with state 0x8db105c88b8a1c3b
(24) eap: Previous EAP request found for state 0x8db105c88b8a1c3b, released from the list
(24) eap: Peer sent packet with method EAP PEAP (25)
(24) eap: Calling submodule eap_peap to process data
(24) eap_peap: Continuing EAP-TLS
(24) eap_peap: [eaptls verify] = ok
```

```
(24) eap_peap: Done initial handshake
(24) eap_peap: [eaptls process] = ok
(24) eap_peap: Session established.  Decoding tunneled attributes
(24) eap_peap: PEAP state phase2
(24) eap_peap: EAP method MSCHAPv2 (26)
(24) eap_peap: Got tunneled request
(24) eap_peap:   EAP-Message =
0x023b00421a023b003d317cdfab0ab960d5447b6d661ab57e092f0000000000000000394d5814c208ecf9f85da0cf1fafebf399cbe32814a3a9
(24) eap_peap: Setting User-Name to testBenutzer
(24) eap_peap: Sending tunneled request to inner-tunnel
(24) eap_peap:   EAP-Message =
0x023b00421a023b003d317cdfab0ab960d5447b6d661ab57e092f0000000000000000394d5814c208ecf9f85da0cf1fafebf399cbe32814a3a9
(24) eap_peap:   FreeRADIUS-Proxied-To = 127.0.0.1
(24) eap_peap:   User-Name = "testBenutzer"
(24) eap_peap:   State = 0x16bf9d50168487e64b3498ddd081d5aa
(24) Virtual server inner-tunnel received request
(24)   EAP-Message =
0x023b00421a023b003d317cdfab0ab960d5447b6d661ab57e092f0000000000000000394d5814c208ecf9f85da0cf1fafebf399cbe32814a3a9
(24)   FreeRADIUS-Proxied-To = 127.0.0.1
(24)   User-Name = "testBenutzer"
(24)   State = 0x16bf9d50168487e64b3498ddd081d5aa
(24) WARNING: Outer and inner identities are the same.  User privacy is compromised.
(24) server inner-tunnel {
(24)   session-state: No cached attributes
(24)   # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/inner-tunnel
(24)     authorize {
(24)       policy filter_username {
(24)         if (&User-Name) {
(24)         if (&User-Name)  -> TRUE
(24)         if (&User-Name)  {
(24)           if (&User-Name =~ / /) {
(24)           if (&User-Name =~ / /)  -> FALSE
(24)           if (&User-Name =~ /@[^@]*@/ ) {
(24)           if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(24)           if (&User-Name =~ /\.\./ ) {
(24)           if (&User-Name =~ /\.\./ )  -> FALSE
(24)           if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))  {
(24)           if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))   -> FALSE
(24)           if (&User-Name =~ /\.$/)  {
(24)           if (&User-Name =~ /\.$/)   -> FALSE
(24)           if (&User-Name =~ /@\./)  {
(24)           if (&User-Name =~ /@\./)   -> FALSE
(24)         } # if (&User-Name)  = notfound
(24)       } # policy filter_username = notfound
(24)       [chap] = noop
(24)       [mschap] = noop
(24) suffix: Checking for suffix after "@"
(24) suffix: No '@' in User-Name = "testBenutzer", looking up realm NULL
(24) suffix: No such realm "NULL"
(24)       [suffix] = noop
(24)       update control {
(24)         &Proxy-To-Realm := LOCAL
(24)       } # update control = noop
(24) eap: Peer sent EAP Response (code 2) ID 59 length 66
(24) eap: No EAP Start, assuming it's an on-going EAP conversation
(24)       [eap] = updated
(24) files: users: Matched entry DEFAULT at line 1
(24)       [files] = ok
(24)       [expiration] = noop
(24)       [logintime] = noop
(24)       [pap] = noop
(24)     } # authorize = updated
(24)   Found Auth-Type = eap
(24)   # Executing group from file /etc/freeradius/3.0/sites-enabled/inner-tunnel
(24)     authenticate {
(24) eap: Expiring EAP session with state 0x16bf9d50168487e6
(24) eap: Finished EAP session with state 0x16bf9d50168487e6
(24) eap: Previous EAP request found for state 0x16bf9d50168487e6, released from the list
(24) eap: Peer sent packet with method EAP MSCHAPv2 (26)
(24) eap: Calling submodule eap_mschapv2 to process data
(24) eap_mschapv2: # Executing group from file /etc/freeradius/3.0/sites-enabled/inner-tunnel
(24) eap_mschapv2:   authenticate {
(24) mschap: WARNING: No Cleartext-Password configured.  Cannot create NT-Password
(24) mschap: WARNING: No Cleartext-Password configured.  Cannot create LM-Password
(24) mschap: Creating challenge hash with username: testBenutzer
(24) mschap: Client is using MS-CHAPv2
(24) mschap: ERROR: FAILED: No NT/LM-Password.  Cannot perform authentication
(24) mschap: ERROR: MS-CHAP2-Response is incorrect
(24)     [mschap] = reject
(24)   } # authenticate = reject
(24) eap: Sending EAP Failure (code 4) ID 59 length 4
(24) eap: Freeing handler
(24)       [eap] = reject
(24)     } # authenticate = reject
(24)   Failed to authenticate the user
(24)   Using Post-Auth-Type Reject
(24)   # Executing group from file /etc/freeradius/3.0/sites-enabled/inner-tunnel
(24)     Post-Auth-Type REJECT {
(24) attr_filter.access_reject: EXPAND %{User-Name}
(24) attr_filter.access_reject:    --> testBenutzer
(24) attr_filter.access_reject: Matched entry DEFAULT at line 11
(24)       [attr_filter.access_reject] = updated
(24)       update outer.session-state {
(24)         &Module-Failure-Message := &request:Module-Failure-Message -> 'mschap: FAILED: No NT/LM-
Password.  Cannot perform authentication'
(24)       } # update outer.session-state = noop
(24)     } # Post-Auth-Type REJECT = updated
(24) } # server inner-tunnel
(24) Virtual server sending reply
(24)   MS-CHAP-Error = ";E=691 R=1 C=194b810c42eabdcdbfbfb07443aad403 V=3 M=Authentication rejected"
(24)   EAP-Message = 0x043b0004
(24)   Message-Authenticator = 0x00000000000000000000000000000000
(24) eap_peap: Got tunneled reply code 3
(24) eap_peap:   MS-CHAP-Error = ";E=691 R=1 C=194b810c42eabdcdbfbfb07443aad403 V=3 M=Authentication rejected"
(24) eap_peap:   EAP-Message = 0x043b0004
(24) eap_peap:   Message-Authenticator = 0x00000000000000000000000000000000
(24) eap_peap: Got tunneled reply RADIUS code 3
(24) eap_peap:   MS-CHAP-Error = ";E=691 R=1 C=194b810c42eabdcdbfbfb07443aad403 V=3 M=Authentication rejected"
(24) eap_peap:   EAP-Message = 0x043b0004
(24) eap_peap:   Message-Authenticator = 0x00000000000000000000000000000000
(24) eap_peap: Tunneled authentication was rejected
(24) eap_peap: FAILURE
(24) eap: Sending EAP Request (code 1) ID 60 length 46
(24) eap: EAP session adding &reply:State = 0x8db105c88a8d1c3b
(24)     [eap] = handled
(24)   } # authenticate = handled
(24) Using Post-Auth-Type Challenge
(24) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(24)   Challenge { ... } # empty sub-section is ignored
(24) session-state: Saving cached attributes
(24)   Module-Failure-Message := "mschap: FAILED: No NT/LM-Password.  Cannot perform authentication"
(24) Sent Access-Challenge Id 220 from 10.16.1.1:1812 to 10.110.0.253:12905 length 0
(24)   EAP-Message =
0x013c002e1900170303002351a2884ce9c9068a5b31e0bd19d31916402027224accf04167f896b9841b9bd358ed1b
(24)   Message-Authenticator = 0x00000000000000000000000000000000
(24)   State = 0x8db105c88a8d1c3b038a302aed8b6639
(24) Finished request
Waking up in 1.7 seconds.
(25) Received Access-Request Id 221 from 10.110.0.253:11058 to 10.16.1.1:1812 length 283
(25)   User-Name = "testBenutzer"
(25)   NAS-Identifier = "WLC-Meineschule-1"
(25)   LCS-Orig-NAS-Identifier = "00A057604255"
(25)   Called-Station-Id = "0E-A0-57-60-42-58:gym-lehrer"
(25)   NAS-Port-Type = Wireless-802.11
(25)   Service-Type = Framed-User
(25)   Calling-Station-Id = "6C-C7-EC-60-61-34"
(25)   Connect-Info = "CONNECT"
(25)   Acct-Session-Id = "80AB5154C1B6824B"
(25)   Acct-Multi-Session-Id = "E08BCFEFC9B6F9DF"
(25)   WLAN-Pairwise-Cipher = 1027076
(25)   WLAN-Group-Cipher = 1027076
(25)   WLAN-AKM-Suite = 1027073
(25)   Framed-MTU = 1400
(25)   EAP-Message =
0x023c002e19001703030023000000000000000003f64a35596376a0df131fb6056af04790881493aa3419740fba66a1
(25)   State = 0x8db105c88a8d1c3b038a302aed8b6639
(25)   Message-Authenticator = 0xf59fd3438571650d99338668442588a3
(25) Restoring &session-state
```

```
(25)   &session-state:Module-Failure-Message := "mschap: FAILED: No NT/LM-Password.  Cannot perform
authentication"
(25) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/default
(25)   authorize {
(25)     policy filter_username {
(25)       if (&User-Name) {
(25)       if (&User-Name)  -> TRUE
(25)       if (&User-Name)  {
(25)         if (&User-Name =~ / /) {
(25)         if (&User-Name =~ / /)  -> FALSE
(25)         if (&User-Name =~ /@[^@]*@/ ) {
(25)         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(25)         if (&User-Name =~ /\.\./ ) {
(25)         if (&User-Name =~ /\.\./ )  -> FALSE
(25)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))  {
(25)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))   -> FALSE
(25)         if (&User-Name =~ /\.$/)  {
(25)         if (&User-Name =~ /\.$/)   -> FALSE
(25)         if (&User-Name =~ /@\./)  {
(25)         if (&User-Name =~ /@\./)   -> FALSE
(25)       } # if (&User-Name)  = notfound
(25)     } # policy filter_username = notfound
(25)     [preprocess] = ok
(25)     [chap] = noop
(25)     [mschap] = noop
(25)     [digest] = noop
(25) suffix: Checking for suffix after "@"
(25) suffix: No '@' in User-Name = "testBenutzer", looking up realm NULL
(25) suffix: No such realm "NULL"
(25)     [suffix] = noop
(25) eap: Peer sent EAP Response (code 2) ID 60 length 46
(25) eap: Continuing tunnel setup
(25)     [eap] = ok
(25)   } # authorize = ok
(25) Found Auth-Type = eap
(25) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(25)   authenticate {
(25) eap: Expiring EAP session with state 0x8db105c88a8d1c3b
(25) eap: Finished EAP session with state 0x8db105c88a8d1c3b
(25) eap: Previous EAP request found for state 0x8db105c88a8d1c3b, released from the list
(25) eap: Peer sent packet with method EAP PEAP (25)
(25) eap: Calling submodule eap_peap to process data
(25) eap_peap: Continuing EAP-TLS
(25) eap_peap: [eaptls verify] = ok
(25) eap_peap: Done initial handshake
(25) eap_peap: [eaptls process] = ok
(25) eap_peap: Session established.  Decoding tunneled attributes
(25) eap_peap: PEAP state send tlv failure
(25) eap_peap: Received EAP-TLV response
(25) eap_peap:   ERROR: The users session was previously rejected: returning reject (again.)
(25) eap_peap:   This means you need to read the PREVIOUS messages in the debug output
(25) eap_peap:   to find out the reason why the user was rejected
(25) eap_peap:   Look for "reject" or "fail".  Those earlier messages will tell you
(25) eap_peap:   what went wrong, and how to fix the problem
(25) eap: ERROR: Failed continuing EAP PEAP (25) session.  EAP sub-module failed
(25) eap: Sending EAP Failure (code 4) ID 60 length 4
(25) eap: Failed in EAP select
(25)     [eap] = invalid
(25)   } # authenticate = invalid
(25) Failed to authenticate the user
(25) Using Post-Auth-Type Reject
(25) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(25)   Post-Auth-Type REJECT {
(25) attr_filter.access_reject: EXPAND %{User-Name}
(25) attr_filter.access_reject:    --> testBenutzer
(25) attr_filter.access_reject: Matched entry DEFAULT at line 11
(25)     [attr_filter.access_reject] = updated
(25)     [eap] = noop
(25)     policy remove_reply_message_if_eap {
(25)       if (&reply:EAP-Message && &reply:Reply-Message) {
(25)       if (&reply:EAP-Message && &reply:Reply-Message)  -> FALSE
(25)       else {
(25)         [noop] = noop
(25)       } # else = noop
(25)     } # policy remove_reply_message_if_eap = noop
(25)   } # Post-Auth-Type REJECT = updated
(25) Delaying response for 1.000000 seconds
Waking up in 0.3 seconds.
Waking up in 0.6 seconds.
(25) Sending delayed response
(25) Sent Access-Reject Id 221 from 10.16.1.1:1812 to 10.110.0.253:11058 length 44
(25)   EAP-Message = 0x043c0004
(25)   Message-Authenticator = 0x00000000000000000000000000000000
Waking up in 0.7 seconds.
(21) Cleaning up request packet ID 217 with timestamp +337
(22) Cleaning up request packet ID 218 with timestamp +337
Waking up in 3.0 seconds.
(23) Cleaning up request packet ID 219 with timestamp +340
(24) Cleaning up request packet ID 220 with timestamp +340
(25) Cleaning up request packet ID 221 with timestamp +340
Ready to process requests
```