TACACS+ NG

Marc Huber

COLLABORATORS			
	TITLE : TACACS+ NG		
ACTION	*NAME*	*DATE*	*SIGNATURE*
WRITTEN BY	Marc Huber	August 28, 2022	

REVISION HISTORY			
NUMBER	DATE	DESCRIPTION	NAME

Contents

1 Introduction

tac_plus-ng is a TACACS+ daemon. It provides networking components like router and switches with authentication, authorisation and accounting services.

This version is a major rewrite of the original Cisco source code and is largely based on **tac_plus**, which comes with the same distribution. Key features include:

- NAS specific host keys, prompts, enable passwords
- Rule-based permission assignment
- Flexible external back-ends for user profiles (e.g. via PERL scripts or C; LDAP (including ActiveDirectory), RADIUS and others are included)
- Connection multiplexing (multiple concurrent NAS clients per process)
- Session multiplexing (multiple concurrent sessions per connection, *single-connection*)
- Scalable, no limit on users, clients or servers.
- CLI context aware.
- Full support for both IPv4 and IPv6
- Implements and auto-detects HAProxy protocol 2.
- Supports TLS
- Compliant to RFC8907
- Supports Linux VRFs

1.1 Download

Source and documentation are available from both the GitHub repository and https://www.pro-bono-publico.de/projects/.

2 Definitions and Terms

The following chapters utilize a couple of terms that may need further explanation:

NAC	A Network Access Client, e.g. the source host of a `telnet` connection.
NAS	A Network Access Server, e.g. a Cisco box, or any other client which makes TACACS+ authentication and authorization requests, or generates TACACS+ accounting packets.
Daemon	A program which services network requests for authentication and authorization, verifies identities, grants or denies authorizations, and logs accounting records.
AV pairs	Strings of text in the form `attribute=value`, sent between a NAS and a TACACS+ daemon as part of the TACACS+ protocol.

Since a *NAS* is sometimes referred to as a *server*, and a *daemon* is also often referred to as a *server*, the term *server* has been avoided here in favor of the less ambiguous terms *NAS* and *Daemon*.

3 Operation

This section gives a brief and basic overview how to run **tac_plus-ng**.

In earlier versions, **tac_plus** wasn't a standalone program but had to be invoked by **spawnd**. This has changed, as **spawnd** functionality is now part of the **tac_plus** binary. However, using a dedicated **spawnd** process is still possible and, more importantly, the **spawnd** configuration options and documentation remain valid.

tac_plus may use auxiliary **MAVIS** back-end modules for authentication and authorization.

3.1 Command line syntax

The only mandatory argument is the path to the configuration file:

```
tac_plus-ng [ -P ] [ -d level ] [ -i child_id ] configuration-file [ id ]
```

If the program was compiled with CURL support, *configuration-file* may be an URL.

Keep the `-P` option in mind - it is imperative that the configuration file supplied is syntactically correct, as the daemon won't start if there are any parsing errors.

The `-d` switch enables debugging. You most likely don't want to use this. Read the source if you need to.

The `-i` option is only honoured if the build-in **spawnd** functionality is used. In that case, it selects the configuration ID for **tac_plus**, while the optional last argument *id* sets the ID of the **spawnd** configuration section.

3.2 Signals

Both the master (that's the process running the **spawnd** code) and the child processes (running the **tac_plus-ng** code) intercept the `SIGHUP` signal:

- The master process will restart upon reception of `SIGHUP`, re-reading the configuration file. The child processes will recognize that the master process is no longer available. It will continue to serve the existing connections and terminate when idle.
- If `SIGHUP` is sent to a child process it will stop accepting new connections from its master process. It will continue to serve the existing connections and terminate when idle.

Sending `SIGUSR1` to the master process will cause it to abandon existing child processes (these will continue to serve the existing connections only) and start new child processes.

3.3 Event mechanism selection

Several level-triggered event mechanisms are supported. By default, the one best suited for your operating system will be used. However, you may set the environment variable `IO_POLL_MECHANISM` to select a specific one.

The following event mechanisms are supported (in order of preference):

- port (Sun Solaris 10 and higher only, `IO_POLL_MECHANISM=32`)
- kqueue (*BSD and Darwin only, `IO_POLL_MECHANISM=1`)
- /dev/poll (Sun Solaris only, `IO_POLL_MECHANISM=2`)
- epoll (Linux only, `IO_POLL_MECHANISM=4`)
- poll (`IO_POLL_MECHANISM=8`)
- select (`IO_POLL_MECHANISM=16`)

Environment variables can be set in the configuration file at top-level:

```
setenv IO_POLL_MECHANISM = 4
```

4 Configuration

The daemon is configured using a text file. Let's have a look at a sample configuration first, before digging into the various configuration directives.

4.1 Sample Configuration

A single configuration file is sufficient for configuring quite everything: the **spawnd** connection broker, **tac_plus-ng** and the *MAVIS* authentication and authorization back-end.

The daemon supports *shebang* syntax. If the configuration file is executable and starts with

```
#!/usr/local/sbin/tac_plus-ng
```

then it can be started directly.

The first step is to configure the **spawnd** portion to tell the daemon the addresses and TCP ports to listen on and to, eventually pass *realms*:

```
id = spawnd {
    listen { port = 49 }
    listen { port = 4949 }
    listen { address = ::0 port = 4950 realm = customer1 }
    listen { address = 10.0.0.1 port = 4951 realm = customer2 }
    # listen { address = 10.0.0.1 port = 4951 realm = customer2 tls = yes }
    #
    # See the spawnd configuration guide for further configuration options.
}
```

The thing that needs some explanation here is *realms*. A *realm* in **tac_plus-ng** summarizes a set of configuration options. Realms inherit configurations from their parent realm, including the parent ruleset, which will be evaluated if the local ruleset doesn't exist or doesn't return a verdict.

The default realm is internaly named `default`. Using *realms* is optional.

Now to the actual **tac_plus-ng** configuration which starts with

```
id = tac_plus-ng {
    # This is the top-level realm, actually.
```

The second line above starts a comment. Comments can appear anywhere in the configuration file, starting with the # character and extending to the end of the current line. Should you need to disable this special meaning of the # character, e.g. if you have a password containing a # character, simply enclose the string containing it within double quotes.

Typically, the next step is to define log destinations and tell the daemon to use them. This sample logs to disk, but other destinations (syslog, pipe) are available, too.

```
    log authzlog { destination = /var/log/tac_plus/authz/%Y/%m/%d.log }
    log authclog { destination = /var/log/tac_plus/authc/%Y/%m/%d.log }
    log acctlog  { destination = /var/log/tac_plus/acct/%Y/%m/%d.log }
    accounting log = acctlog
    authentication log = authclog
    authorization log log = authzlog
```

Logs are interited to sub-realms and while sub-realms can define their own logging that won't override the parent realm definitions.

You can specify a retire limit to have the server auto-terminate and restart its worker processes:

```
    retire limit = 1000
```

Then, there's the *MAVIS* part:

```
    mavis module = groups {
        resolve gids = yes
        groups filter = /^(guest|staff|ubuntu)$/
        script out = {
                # copy the already filtered UNIX group access list to TACMEMBER
                eval $GIDS =~ /^(.*)$/
```

```
            set $TACMEMBER = $1
        }
    }

    mavis module = external {
        exec = /usr/local/sbin/pammavis pammavis -s sshd
    }

    user backend = mavis
    login backend = mavis chpass
    pap backend = mavis
```

which defines interaction with external external back-ends.

You can define network objects for later use in ACLs:

```
    net outThere { address = 100.65.3.1 address = 100.66.0.0/16 }
```

Networks can be hierarchic, too:

```
    net all {
        net north {
            address = 100.67.0.0/16
        }
        net south {
            address = 100.68.0.0/16 }
    }
```

Now, define host objects for your network access devices. Just like realms and networks these can be hierarchic:

```
    host world {
        welcome banner = "\nHitherto shalt thou come, but no further. (Job 38.11)\n\n"
        key = QaWsEdRfTgY
        enable 15 = clear test
        address = ::/0
        host south {
            address = 100.99.0.0/16
        }
        host west {
            address = 100.100.0.0/16
        }
    }

    host localhost {
        address = 127.0.0.1
        prompt = "Welcome home\n"
        parent = world # for key and other definitions not set here
    }

    host rfc {
        address = 172.16.0.0/12
        prompt = "Welcome private\n"
        key = labKey
    }
```

Now, define some profiles. These will be assigned to users later:

```
    profile readwrite {
        script {
            if (service == shell) {
    if (cmd == "") {
        set priv-lvl = 15
```

```
                permit
            }
        }
    }
}

profile getconfig {
    script {
        if (service == shell) {
if (cmd == "") {
                set autocmd = "sho run"
                set priv-lvl = 15
                permit
      }
        }
    }
}

profile engineering {
    script {
        if (service == shell) {
if (cmd == "") {
                set priv-lvl = 7
                permit
            }
            if (cmd =~ /^ping/) deny
            permit
        }
    }
}

profile guest {
    script {
        if (service == shell) {
if (cmd == "") {
                set priv-lvl = 1
                permit
            }
        }
        permit
    }
}
```

Your can define groups to implement a role-based access control scheme ...

```
group admin {
    group north # "admin" is a member
    group south # of both
}

group engineering {
}

group guest {
}
```

... and add users:

```
user demo {
    password = clear demo
    groups = engineering,admin
}
```

```
    user readonly {
        password = clear readonly
        groups = guest
    }
```

Finally, implement a rule-set to assign profiles to users:

```
    ruleset {
        rule from-localhost {
            enabled = yes
            script {
                if (nas == localhost) {
                    if (group ==  admin) {
                        profile = admin
                        permit
                    }
                    if (group ==  engineering ) {
                        profile = engineering
                        permit
                    }
                }
          }
        }
        rule from-rfc {
            enabled = yes
            script {
                if (nas == rfc) {
                    if (group ==  south) {
                        profile = admin
                        permit
                    }
                    if (group ==  engineering ) {
                        profile = engineering
                        permit
                    }
                }
            }
        }
    }
}
```

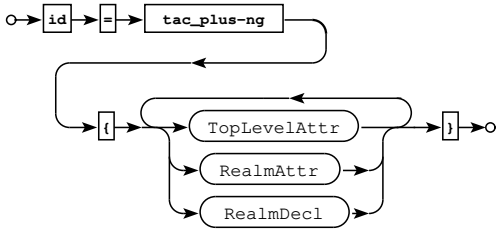
4.2 Configuration directives

Configuration options include

1. global options
2. realms
3. hosts
4. time specifications
5. profiles
6. groups
7. users
8. access lists

9. rules

The reasoning behind that non-random order is that parts of the configuration may use other parts, and these need to exist before being used.



Railroad diagram: TacPlusConfig

Including Files
Configuration files may refer to other configuration files:
`include = file`
will read and parse *file*. Shell wildcard patterns are expanded by `glob(3)`. The `include` statement will be accepted virtually everywhere (but not in comments or textual strings).

4.2.1 Global options

The global configuration section may contain the following configuration directives, plus the *realm* options detailed in the next section. *realm* confiurations at global level are implicitely assigned to the *default* realm and will be inherited by sub-realms.

4.2.1.1 Limits and timeouts

A number of global limits and timeouts may be specified exclusively at global level:

- `retire limit = n`

  The particular daemon instance will terminate after processing *n* requests. The **spawnd** instance will spawn a new instance if necessary.

  Default: unset

- `retire timeout = s`

  The particular daemon instance will terminate after *s* seconds. **spawnd** will spawn a new instance if necessary.

  Default: unset

Time units
Appending `s`, `m`, `h` or `d` to any timeout value will scale the value as expected.

4.2.1.2 DNS

tac_plus can make use of static DNS entries. The relevant global configuration options at global level are:

- `dns preload address` *address* = *hostname*

  Preload DNS cache with *address*-to-*hostname* mapping.

- `dns preload file` = *filename*

  Preload DNS cache with *address*-to-*hostname* mappings from *filename* (see your `hosts`(5) manpage for syntax). DNS lookups via lwresd are no longer supported.

  Example:

```
dns preload address 1.2.3.4 = router.example.com
dns preload file = /etc/hosts

host router.example.com {
    # "address = 1.2.3.4" is implied
    key = mykey
}
```

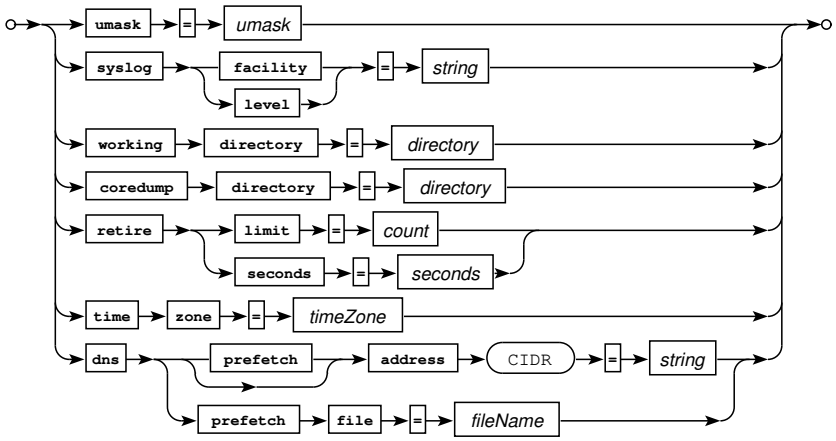
4.2.1.3 Process-specific options

There are a couple of process-specific options available:

- `coredump directory` = *directory*

  Dump cores to *directory*. You really shouldn't need this.

4.2.1.4 Railroad Diagrams



Railroad diagram: GlobalDecl

4.2.2 Realms

Bascially, realms are containers to logically separate configuration sets. At top-level, there's the default realm (called `default` internally). Realms pass on most configurations (e.g. logging, users (if there are no users defined in that realm scope), groups, profiles) to their sub-realms.

Realm selection is based on **spawnd** configuration:

```
spawnd = {
    listen { port = 49 }   # implied realm is "default"
    listen { port = 3939 } # implied realm is "default"
    listen { port = 4949 realm = realmOne }
    listen { port = 5959 realm = realmTwo }
}
```

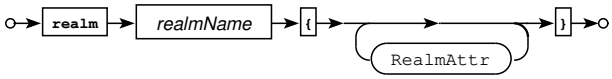
If *VRFs* are used and no `realm` is specified in the **spawnd** section, the daemon will try to use the *VRF name* as `realm` and fall back to the `default` realm if that "vrf realm" isn't defined.

The syntax to use (and define) realms is

```
realm realmName { ... }
```

at top configuration level. Realms cover hosts, users, groups, profiles, rulesets, timespecs, *MAVIS* configurations other configuration options.

4.2.2.1 Railroad Diagrams



Railroad diagram: RealmDecl

4.2.3 Realm attribtes

The following options may be specified at *realm* level. This includes the `default` *realm*:

4.2.3.1 Logging

Logging options defined in the top-level `default` realm will be shared with sub-realms unless the sub-realm has its own logging configuration. The software provides logs for

- Authentication

```
  authentication log = log_destination
```

- Authorization

```
  authorization log = log_destination
```

- Accounting

```
  accounting log = log_destination
```

- Connections

```
  connection log = log_destination
```

Logs may be written to multiple destinations:

Valid log destinations are "named":

```
log mylog {
  destination = 169.254.0.23                    # UDP syslog
  # or one of the following:
  # destination = [fe80::123:4567:89ab:cdef]:514 # IPv6 UDP, with non-standard UDP port
  # destination = "/tmp/x.log"                  # plain file, async writes
  # destination = ">/tmp/x.log"                 # plain file, sync writes
  # destination = "|my_script.sh"               # script
  # destination = syslog                        # syslog(3)
  #
  syslog facility = MAIL                        # sets log facility
  syslog level = DEBUG                          # sets log level
}
authentication log = mylog
accounting log = mylog
authorization log = mylog
```

Syslog
Logging non-session related output to `syslogd`*(8)* can be disabled using

```
syslog default = deny
```

Log destinations may contain `strftime(3)`-style character sequences, e.g.:

```
      destination = /var/log/tac_plus/%Y/%m/%d.auth
```

to automate time-based log file switching. By default, the daemon will use your local time zone for time conversion. You can switch to a different one by using the `time zone` option (see below).

A couple of other configuration options that may be useful in `log` context include:

- (`authentication` | `authorization` | `accounting`) `format` = *string*
  This defines the logging format. `strftime(3)` conversions are recognized. The following variables are resolved:

`${cmd}`, `${cmd,`*separator*`}`	values of `cmd=` and `cmd-arg=` attribute-value pairs, separated by whitespace or *separator*
`${args}`, `${args,`*separator*`}`	input attribute-value pairs, separated by whitespace or *separator*
`${rargs}`, `${rargs,`*separator*`}`	output attribute value pairs, separated by whitespace or *separator*
`${nas}`	NAS IP address
`${nac}`	NAC IP address
`${user}`	user name
`${profile}`	profile assigned to user
`${service}`	service type (e.g. `shell`)
`${result}`	typically `permit` or `deny`
`${port}`	NAS port
`${hint}`	`added`/`replaced` for authorization, informal text for accounting
`${host}`	Host name of matching host declaration
`${hostname}`	system hostname
`${msgid}`	A message ID, perhaps suitable for RFC5424 logs. These are listed somewhere below.
`${accttype}`	accounting type (`start`/`stop`/`update`)
`${priority}`	syslog priority
`${action}`	authentication info (e.g. `pap login`)
`${privlvl}`	privilege level
`${authen-action}`	`login` or `chpass`
`${authen-type}`	authorization type, e.g. `AUTHOR/PASS_ADD`
`${authen-service}`	`asciiascii`/`pap`/`chap`/`mschap`/`mschapv2`
`${authen-method}`	`krb5`/`line`/`enable`/`local`/`tacacs+`/`guest`/`radius`/`krb4`/`rcmd`
`${rule}`	Name of the matching rule.
`${label}`	Ruleset label, if any.
`${config-file}`	Configuration file name
`${config-line}`	Configuration file line number
`${vrf}`	Name of the current socket IPv4 vrf, supported on Linux (requires `sysctl net.ipv4.tcp_l3mdev_accept=1`) and possibly OpenBSD.
`${uid}`	UID from PAM backend
`${gid}`	GID from PAM backend
`${gids}`	GIDs from PAM backend
`${home}`	Home directory from PAM backend
`${shell}`	Shell from PAM backend
`${dn}`	Raw `dn` backend value, typically from LDAP
`${memberof}`	Raw `memberOf` backend value, typically from LDAP
`${tls-conn-version}`	TLS Connection Version (requires LibTLS)

${tls-conn-cipher}	TLS Connection Cipher (requires LibTLS)
${tls-peer-cert-issuer}	TLS Peer Certificate Issuer (requires LibTLS)
${tls-peer-cert-subject}	TLS Peer Certificate Subject (requires LibTLS)
${tls-conn-cipher-strength}	TLS Connection Cipher Strength (requires LibTLS)
${tls-peer-cn}	TLS peer certificate Common Name(requires LibTLS)

The built-in defaults as of writing this are:

```
# Accounting to file/pipe:
"%Y-%m-%d %H:%M:%S %z\t${nas}\t${user}\t${port}\t${nac}\t${acctttype}\t${service}\t${cmd}\n ↩
    "
# Accounting to UDP syslog:
"<${priority}>%Y-%m-%d %H:%M:%S %z ${hostname} ${nas}|${user}|${port}|${nac}|${acctttype}|$ ↩
    {service}|${args}"
# Accounting to syslog(3):
"${nas}|${user}|${port}|${nac}|${acctttype}|${service}|${args}"
# Authorization to file/pipe:
"%Y-%m-%d %H:%M:%S %z\t${nas}\t${user}\t${port}\t${nac}\t${profile}\t${result}\t${service ↩
    }\t${cmd}\n"
# Authorization to UDP syslog:
"<${priority}>%Y-%m-%d %H:%M:%S %z ${hostname} ${nas}|${user}|${port}|${nac}|${profile}|${ ↩
    result}|${service}|${cmd}"
# Authorization to syslog(3):
"${nas}|${user}|${port}|${nac}|${profile}|${result}|${service}|${cmd}"
# Authentication to file/pipe:
"%Y-%m-%d %H:%M:%S %z\t${nas}\t${user}\t${port}\t${nac}\t${action} ${hint}\n"
# Authentication to UDP syslog:
"<${priority}>%Y-%m-%d %H:%M:%S %z ${hostname} ${nas}|${user}|${port}|${nac}|${action} ${ ↩
    hint}"
# Authentication to syslog(3):
"${nas}|${user}|${port}|${nac}|${action} ${hint}"
# Connections to file/pipe:
"%Y-%m-%d %H:%M:%S %z\t${acctttype}\t${nas}\t${tls-conn-version}\t${tls-peer-cert-issuer}\ ↩
    t${tls-peer-cert-subject}\n"
# Connections to UDP syslog:
"<${priority}>%Y-%m-%d %H:%M:%S %z ${hostname} ${acctttype}|${nas}|${tls-conn-version}|${ ↩
    tls-peer-cert-issuer}|${tls-peer-cert-subject}"
# Connections to syslog(3):
"${acctttype}|${nas}|${tls-conn-version}|${tls-peer-cert-issuer}|${tls-peer-cert-subject}"
```

Message ID	**Description**
AUTHZPASS	authorization succeeded
AUTHZPASS-ADD	authorization succeeded, attribute-value-pairs were added
AUTHZPASS-REPL	authorization succeeded, attribute-value-pairs were replaced
AUTHZFAIL	authorization failed
AUTHCFAIL	generic authentication failure
AUTHCFAIL-ABORT	authentication was aborted
AUTHCFAIL-BACKEND	the authentication backend failed
AUTHCFAIL-BUG	authentication failed due some programming error
AUTHCFAIL-DENY	authentication was denied
AUTHCFAIL-WEAKPASSWORD	the password used didn't met minimum criteria
AUTHCFAIL-ACL	access was denied due to ruleset or acl
AUTHCFAIL-DENY-RETRY	the user tried the same wrong password once more
AUTHCFAIL-PASSWORD-NOT_TEXT	the password isn't specified as clear-text
AUTHCFAIL-BAD-CHALLENGE-LENGTH	the MSCHAP challenge length didn't match
AUTHCFAIL-NOPASS	there's no passwort set for the user
AUTHCPASS	authentication passed
ACCT-START	accounting start

Message ID	Description
ACCT-STOP	accounting stop
ACCT-UNKNOWN	unknown (non-compliant) accounting data
ACCT-UPDATE	accounting update/watchdog
CONN-REJECT	connection was rejected
CONN-START	connection was started
CONN-STOP	connection was terminated

- `time zone` = *time-zone*

  By default, the daemon uses your local system time zone to convert the internal system time to calendar time. This option sets the `TZ` environment variable to the *time-zone* argument. See your local `tzset` man page for details.

- `umask` = *mode*

  This sets the file creation mode mask. Example:

```
umask = 0640
```

4.2.3.1.1 Accounting

All accounting records are written, as text, to the file (or command) specified with the `accounting log` directive.

Accounting records are text lines containing tab-separated fields. The first 6 fields are always the same. These are:

- timestamp
- NAS address
- username
- port
- NAC address
- record type

Following these, a variable number of fields are written, depending on the accounting record type. All are of the form `attribute=valu`
There will always be a `task_id` field.

Attributes, as sent by the NAS, might be:

```
unknown service start_time port elapsed_time status priv_level cmd protocol cmd-arg bytes_
bytes_out paks_in paks_out address task_id callback-dialstring nocallback-verify callback-
callback-rotary
```

More may appear,. randomly..

Example records (lines wrapped for legibility) are thus:

```
1995-07-13 13:35:28 -0500  172.16.1.4  chein  tty5   198.51.100.141
        stop   task_id=12028  service=exec  port=5   elapsed_time=875
1995-07-13 13:37:04 -0500  172.16.1.4  lol    tty18  198.51.100.129
        stop   task_id=11613  service=exec  port=18  elapsed_time=909
1995-07-13 14:09:02 -0500  172.16.1.4  billw  tty18  198.51.100.152
        start  task_id=17150  service=exec  port=18
1995-07-13 14:09:02 -0500  172.16.1.4  billw  tty18  198.51.100.152
        start  task_id=17150  service=exec  port=18
```

Elapsed time is in seconds, and is the field most people are usually interested in.

4.2.3.1.2 Spoofing Syslog Packets

The script `tacspooflog.pl` (which comes bundled with this distribution) may be used to make `syslogd` believe that logs come straight from your router, not from `tac_plus`.

E.g., if your `syslogd` is listening on `127.0.0.1`, you may try:

```
access log = "|exec sudo /path/to/tacspooflog.pl 127.0.0.1"
```

This may be useful if you want to keep logs in a common place.

Please note that this will work for IPv4 destinations only.

4.2.3.2 Limits and timeouts

A number of global limits and timeouts may be specified at realm and global level:

- `connection timeout =` *s*

  Terminate a connection to a NAS after an idle period of at least *s* seconds.

  Default: 600

- `context timeout =` *s*

  Clears context cache entries after *s* seconds of inactivity. Default: 3600 seconds.

  Default: 3600

- `warning period =` *d*

  Set warning period for password expiry to *d* days.

  Default: 14

4.2.3.2.1 Authentication

- `password (acl =` *acl* `)`

  `password acl` may be used to perform simple compliance checks on user passwords. For example, to enforce a minimum password length of 6 characters you may try

```
acl password-compliance {
    if (password =~ /^....../)
        permit
    deny
}
password acl = password-compliance
```

  Authentications using passwords that fail the check will be rejected.

- `anonymous-enable = (permit | deny)`

  Several broken *TACACS+* implementations send no or an invalid username in `enable` packets. Setting this option to `deny` tries to enforce user authentication before enabling. This option defaults to `permit`.

  Alas, this may or may not work. In theory, the enable dialog should look somewhat like:

```
Router> enable
Username: me
Password: *******
Enable Password: **********
Router#
```

  However, some implementations may resend the user password at the `Enable Password:` prompt. In that case you've got only two options: Either try

```
    enable = login
```

at user profile level, which will omit the secondary password query and let the user enable with his login password, or permit anonymous `enable` (which is disabled by default) with

```
    anonymous-enable = permit
```

in host context to use the enable passwords defined there.

- `augmented-enable =( permit|deny )`

  For outdated *TACACS+* client implementations that send `$enable$` instead of the real username in an enable request, this will permit user specific authentication using a concatenation of username and login password, separated with a single space character:

```
> enable
Password: myusername mypassword
#
```

  `enable [ level ] = login` needs to be set in the users' profile for this option to take effect.

  Default: `augmented-enable = deny`

  `augmented-enable` will only take effect if the NAS tries to authenticate a username matching the regex

```
^\$enab..\$$
```

  (e.g.: `$enable$`, `$enab15$`). That matching criteria may be changed using an ACL:

```
acl custom_enable_acl { if (user =~ ^demo$) permit deny }
enable user acl = custom_enable_acl
```

4.2.3.2.2 User back-end options

These options are relevant for configuring the MAVIS user back-end:

- `pap password [ default ] =( login|pap )`

  When set to `login`, the PAP password default for new users will be set to use the login password.

- `pap password mapping =( login|pap )`

  When set to `login`, PAP authentication requests will be mapped to ASCII Login requests. You may wish to uses this for NEXUS devices.

  May be overridden at host level.

- `user backend = mavis`

  Get user data from the MAVIS back-end. Without that directive, only locally defined users will be available and the MAVIS back-end may be used for authenticating known users (with `password = mavis` or simlar) only.

- `pap backend = mavis [ prefetch ]`

  Verify PAP passwords using the MAVIS back-end. This needs to be set to either `mavis` or `prefetch` in order to authenticate PAP requests using the MAVIS back-end. If unset, the PAP password from the users' profile will be used.

  If `prefetch` is specified, the daemon will first retrieve the users' profile from the back-end and then authenticate the user based on information eventually found there.

  This directive implies `user backend = mavis`.

- `login backend = mavis [ prefetch ] [ chalresp [ noecho ] ] [ chpass ]`

  Verify Login passwords using the MAVIS back-end. This needs to be set to either `mavis` or `prefetch` in order to authenticate login requests using the MAVIS back-end. If unset, the login password from the users' profile will be used.

  If `prefetch` is specified, the daemon will first retrieve the users' profile from the back-end and then authenticate the user based on information eventually found there.

  This directive implies `user backend = mavis`.

  For use with OPIE-enabled MAVIS modules, add the `chalresp` keyword (and, optionally, add `noecho`, unless you want the typed-in response to display on the screen). Example:

```
login backend = mavis chalresp noecho
```

  For non-local users, if the `chpass` attribute is set and the user provides an empty password at login, the user is given the option to change his password. This requires appropriate support in the MAVIS back-end modules.

- `mavis module =` *module* `{ ... }`

  Load MAVIS module *module*. See the MAVIS documentation for configuration guidance.

- `mavis path =` *path*

  Add *path* to the search-path for MAVIS modules.

- `mavis cache timeout =` *s*

  Cache MAVIS authentication data for *s* seconds. If *s* is set to a value smaller than `11`, the dynamic user object is valid for the current TACACS+ session only. Default is `120` seconds.

- `mavis noauthcache`

  Disables password caching for MAVIS modules.

- `mavis user filter =` *acl*

  Query MAVIS user back-end only if *acl* matches. Defaults to:

```
acl __internal__username_acl__ { if (user =~ "[]<>/()|=[]+") deny permit }
mavis user filter = __internal__username_acl__
```

4.2.3.2.3 TLS

If compiled with LibTLS support the following configuration options are available:

- `tls cert-file =` *cert-file*

  Specifies the public part of a TLS server certificate in PEM format.

- `tls key-file =` *key-file*

  Specifies the private part (the key) of a TLS server certificate in PEM format.

- `tls passphrase =` *passphrase*

  Specifies the optional passphrase to decrypt *key-file*.

- `tls cafile =` *cafile*

  Specifies a file with the CAs to use.

Example:

```
id = spawnd {
    listen { port = 4949 realm = heck }
    listen { port = 4950 realm = heck tls = yes }
    spawn { instances min = 1 instances max = 32 }
    id = tac_plus-ng {
            ...
        realm heck {
            tls cert-file = /somewhere/tac-ca/server.tacacstest.crt
            tls key-file = /somewhere/tac-ca/server.key
            tls ca-file = /somewhere/tac-ca/ca.crt
            ...
        }
    }
}
```

4.2.3.2.4 Miscellaneous

In **spawnd listen** context,

- `haproxy = ( yes | no )`
  will will tell **tac_plus-ng** to auto-detect that a connection is proxied via HAProxy protocol 2.
  A suitable HAProxy configuration could look similar to:

```
frontend tacplus
    bind *:49
    mode tcp
    default_backend backendtacplus

backend backendtacplus
    balance source
    server tacserver1 127.0.0.1:4949 no-check send-proxy-v2
```

- `tls = ( yes | no )`
  will tell **tac_plus-ng** whether the connection is TLS encrypted.
- `vrf = (` *vrf-name* | *vrf-number*)
  will tell **spawnd listen** to *bind(2)* to the requested VRF (*vrf-name* on Linux, *vrf-number* on OpenBSD).

Example:

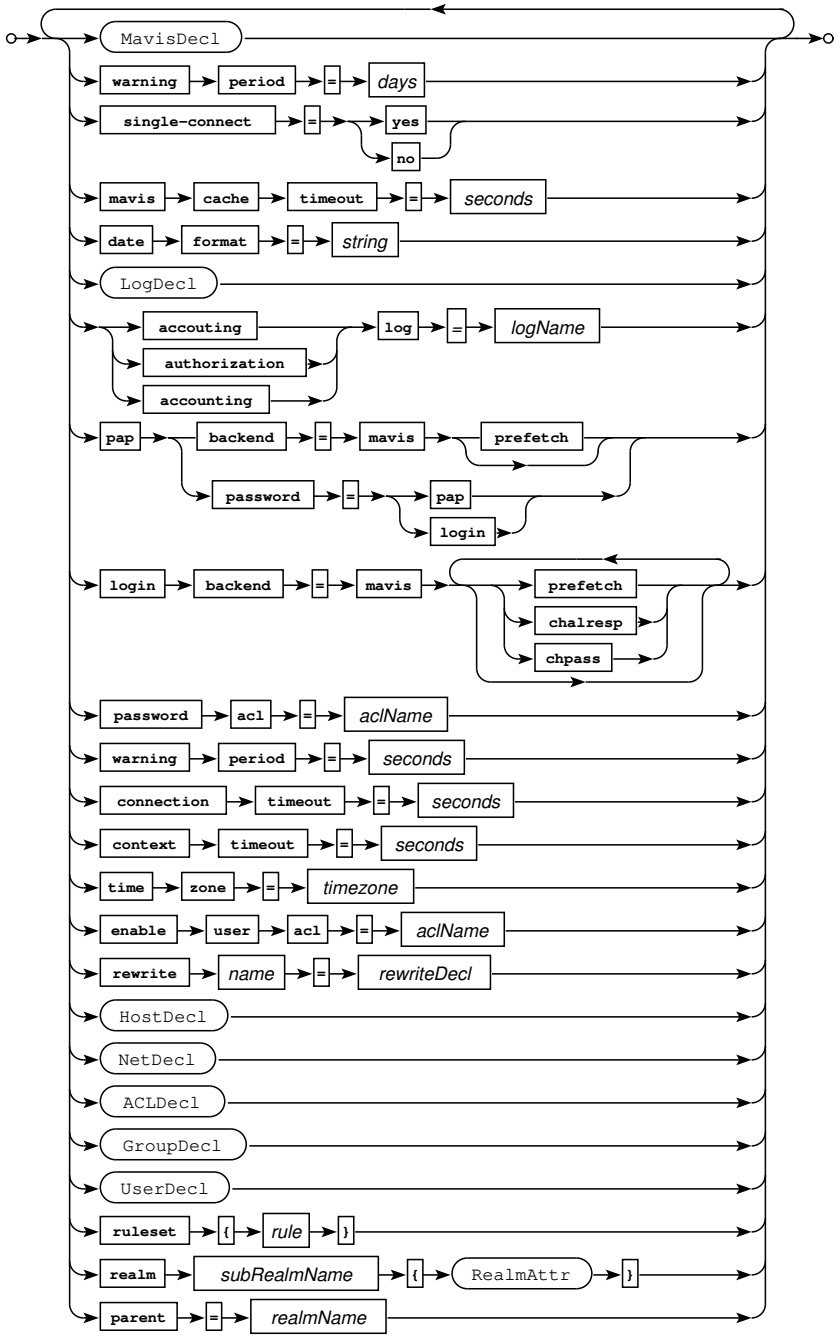
```
id = spawnd {
    ...
    listen {
        port = 49
        vrf = vrf-blue
        tls = true
        haproxy = true
    }
    ....
}
```

4.2.3.2.5 Realm Inheritance

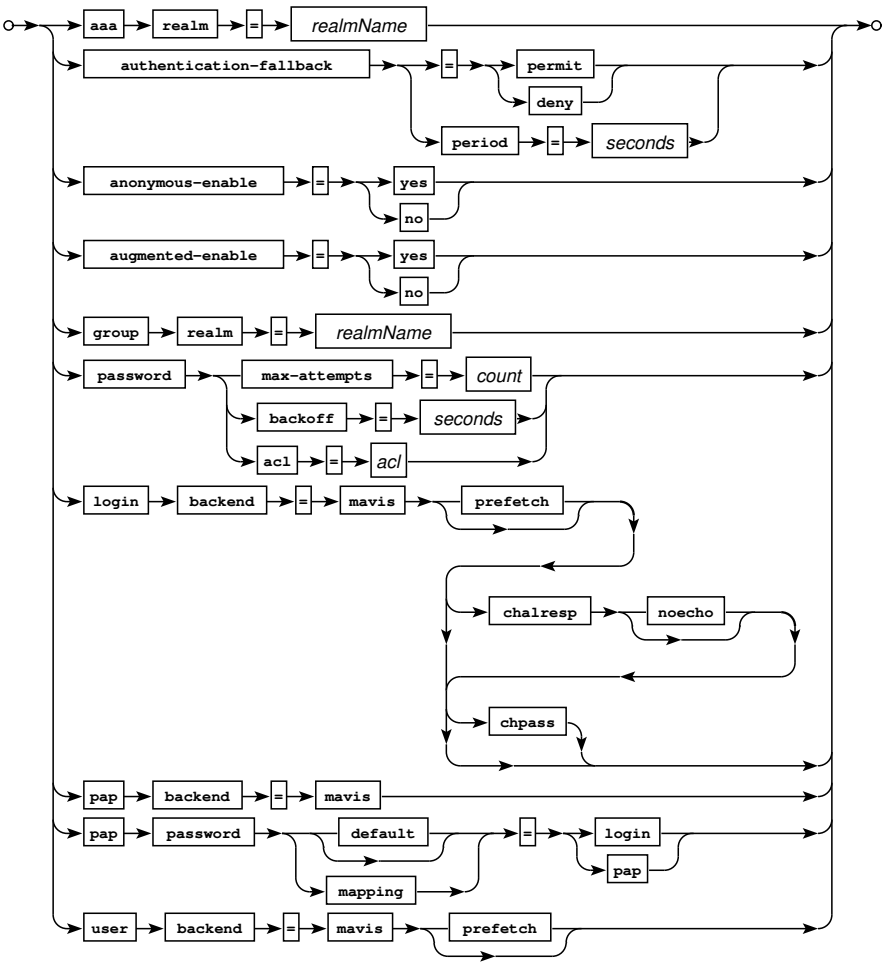
Realms inherit quite some configuration from their parent realm:

Declaration of ...	**is taken from parent realm ...**
acl	if not found in current realm
dns forward mapping	if not found in current realm
group	if not found in current realm
host (IP lookup)	if no hosts defined in current realm
host (name lookup)	if not found in current realm
log	always
mavis module	if not set and no users defined in current realm
network	if not found in current realm
profile	if not found in current realm
ruleset	if not set or undefined result in current realm
timespec	if not found in current realm
user	if no users defined in current realm

4.2.3.2.6 Railroad Diagrams



Railroad diagram: RealmAttr



Railroad diagram: RealmAttrAuthen

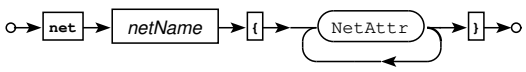
4.2.3.3 Networks

Networks consist of IP addresses or other networks. They may overlap. Networks can be used in ACLs. The parent of a network may be set either implicitly (by defining it it parent context) or explicitly.

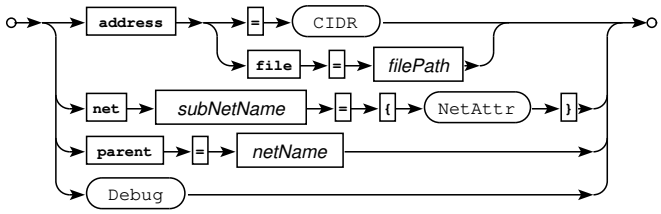
```
net home {
      address = 172.16.0.0/23
      net dev {
          address = 172.16.0.15
      }
      parent = ...

}
```

4.2.3.3.1 Railroad Diagrams



Railroad diagram: NetDecl



Railroad diagram: NetAttr

4.2.3.4 Hosts

The daemon will talk to known NAS addresses only. Connections from unknown addresses will be rejected.

If you want **tac_plus** to encrypt its packets (and you almost certainly *do* want this, as there can be usernames and passwords contained in there), then you'll have to specify an (non-empty) encryption key. The identical key must also be configured on any NAS which communicates with tac_plus.

To specify a global key, use a statement similar to

```
host world4 {
  key = "your key here"
  address = 0.0.0.0/0
}
```

(where `world` is *not* a keyword, but just some arbitrary character string).

Double Quotes

You only need double quotes on the daemon if your key contains spaces. Confusingly, even if your key does contain spaces, you should *never* use double quotes when you configure the matching key on the NAS.
The daemon will reject connections from hosts that have no encryption key defined.
Double quotes within double-quoted strings may be escaped using the backslash character `\` (which can be escaped by itself), e.g.:

```
key = "quo\\te me\"."
```

translates to the ASCII sequence

```
quo\te me".
```

Any CIDR range within a host definition needs to to be unique, and the most specific definition will match. The requirement for unambiguousness is quite simply based on the fact that certain host object attributes (key, prompt, enable passwords) may only exist once.

If compiled with TLS support, primary criteria for host object selection with TLS is no longer the NAS IP address but the certificate subject and/or the common name. E.g., `CN=server.tacacstest.demo,OU=org,OU=local` will check for host objects named `CN=server.tacacstest.demo,OU=org,OU=local`, `OU=org,OU=local`, `OU=local` and then for `server.tacacstest.demo`, `tacacstest.demo` and `demo` before falling back to IP based selection.

On the NAS, you also need to configure the *same* key. Do this by issuing the current variant of:

```
aaa new-model
tacacs-server host 192.168.0.1 single-connection key your key here
```

The optional `single-connection` parameter specifies that multiple sessions may use the same TCP/IP connection to the server.

Generally, the syntax for host declarations conforms to

`host` *name* { *key-value pairs* }

The key-value pairs permitted in host sections of the configuration file are explained below.

- `key` [`warn`] (*YYYY−MM−DD* | *s*)] = *string*

  This sets the key used for encrypting the communication between server and NAS. Multiple keys may be set, making key migration from one key to another pretty easy. If the `warn` keyword is specified, a warning message is logged when a NAS actually uses the key. Optionally, the `warn` keyword accepts a date argument that specifies when the warnings should start to appear in the logs.

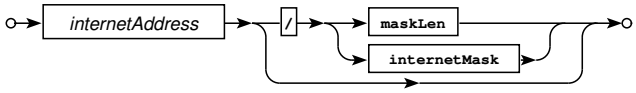
  During debugging, it may be convenient to temporarily switch off encryption by using an empty key:

```
key = ""
```

  Be careful to remember to switch encryption back on again after you've finished debugging.

- `address` = *cidr*

  Adds the address range specified by *cidr* to the current host definition.



Railroad diagram: CIDR

- `address file` = *file*

  Add the addresses from *file* to the current host definition. Shell wildcard patterns are expanded by `glob(3)`.

- `single-connection` (`may-close`) = (`yes` | `no`)

  This directive may be used to permit or deny the single-connection feature for a particular host object. The `may-close` keyword tells the daemon to close the connection if it's unused.

Caveat Emptor
There's a slight chance that single-connection doesn't work as expected. The single-connection implementation in your router or even the one implemented in this daemon (or possibly both) may be buggy. If you're noticing weird AAA behaviour that can't be explained otherwise, then try disabling single-connection on the router.

- `parent` = hostName

  This sets the the parent hosts. Definitions not found in the current host will be looked up there, recursively.

- `host` hostName `{` HostAttr `}`

  Hosts can be defined in host context, too.

- `script` `{` tacAction `}`

  Scripts can be used in host context. These are run before AAA and mey be used to permit or deny access, or to rewrite usernames.

4.2.3.4.1 Timeouts

The connection timeout may be specified:

- `connection timeout` = *s*

  Terminate a connection to this NAS after an idle period of at least *s* seconds. Defaults to the global option.

4.2.3.4.2 Authentication

The following authentication related directives are available at host object level:

- `pap password mapping =( login|pap )`

  When set to `login`, PAP authentication requests will be mapped to ASCII Login requests. You may wish to uses this for NEXUS devices.

- `enable [` *level* `] = (permit|deny|login|(clear|crypt)` *password* `)`

  This directive may be used to set host specific enable passwords, to use the *login* password, or to permit (without password) or refuse any enable attempt. *level* defaults to 15.

  Enable passwords specified at host level have a lower precedence as those defined at user or profile level.

  Password Hashes
  You can use the `openssl passwd` utility to compute password hashes.

  You can enable via TACACS+ by configuring on the NAS:

```
aaa authentication enable default group tacacs+ enable
```

- `anonymous-enable =( permit|deny )`

  Several broken *TACACS+* implementations send no or an invalid username in `enable` packets. Setting this option to `deny` enforces user authentication before enabling. Setting this option here has precedence over the global option.

- `augmented-enable =( permit|deny )`

  For *TACACS+* client implementations that send `$enable$` instead of the real username in an enable request, this will permit user specific authentication using a concatenation of username and login password, separated with a single space character. Setting this option here has precedence over the global option.

  `enable [` *level* `] = login` needs to be set in the users' profile for this option to take effect.

4.2.3.4.3 Authorization

The following authorization related directives are available at host object level:

- `permit if-authenticated =( yes|no )`

  This will cause authorization for users unknown to the daemon to succeed (e.g. when logging in locally while the daemon is down or while initially configuring TACACS+ support and messing up).

4.2.3.4.4 Banners and Messages

The daemon allows for various banners to be displayed to the user:

- `welcome banner (` *fallback* `) =` *string*
- `motd banner =` *string*
- `reject banner =` *string*

  The `reject banner` gets displayed in place of the welcome message if a connection was rejected by an `access` ACL defined at host, user or group level.

- `message =` *string*

The time when those texts get displayed largely depends on the actual login method:

Context	Directive	Telnet	SSHv1	SSHv2
`host`	`welcome banner`	displayed before `Username:`	not displayed	displayed before `Password:`
`host`	`reject banner`	displayed before closing connection	not displayed	not displayed
`host`	`motd banner`	displayed after successful login	not displayed	displayed after successful login
`host`	`failed authentication banner`	displayed after unsuccessful login	not displayed	displayed after unsuccessful login
`user` or `group`	`message`	displayed after `motd banner`	not displayed	displayed after `motd banner`

Neither the `motd banner` nor a `message` defined in the users' profile will be displayed if `hushlogin` is set for the user.

Both banners and messages support the same conversions as logs, unless specified as user level.

Example:

```
host ... {
  ...
  welcome banner = "Welcome. Today is %A.\n"
  ...
}
```

4.2.3.4.5 Workarounds for Client Bugs

The directive

`bug compatibility` = *value*

may improve compatibility with clients that violate the TACACS+ protocol. Currently, the following bit values (yes, you can use bitwise OR here) are recognized:

Bit	Value	Description
0	1	Ignore invalid AUTHEN/START data, seen with ZTE devices that put their MAC address there.
1	2	Accept version 1 for authorization and accounting packets, seen with Palo Alto systems.

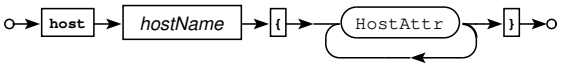
Example:

```
host ... {
  ...
  bug compatibility = 2
  ...
}
```

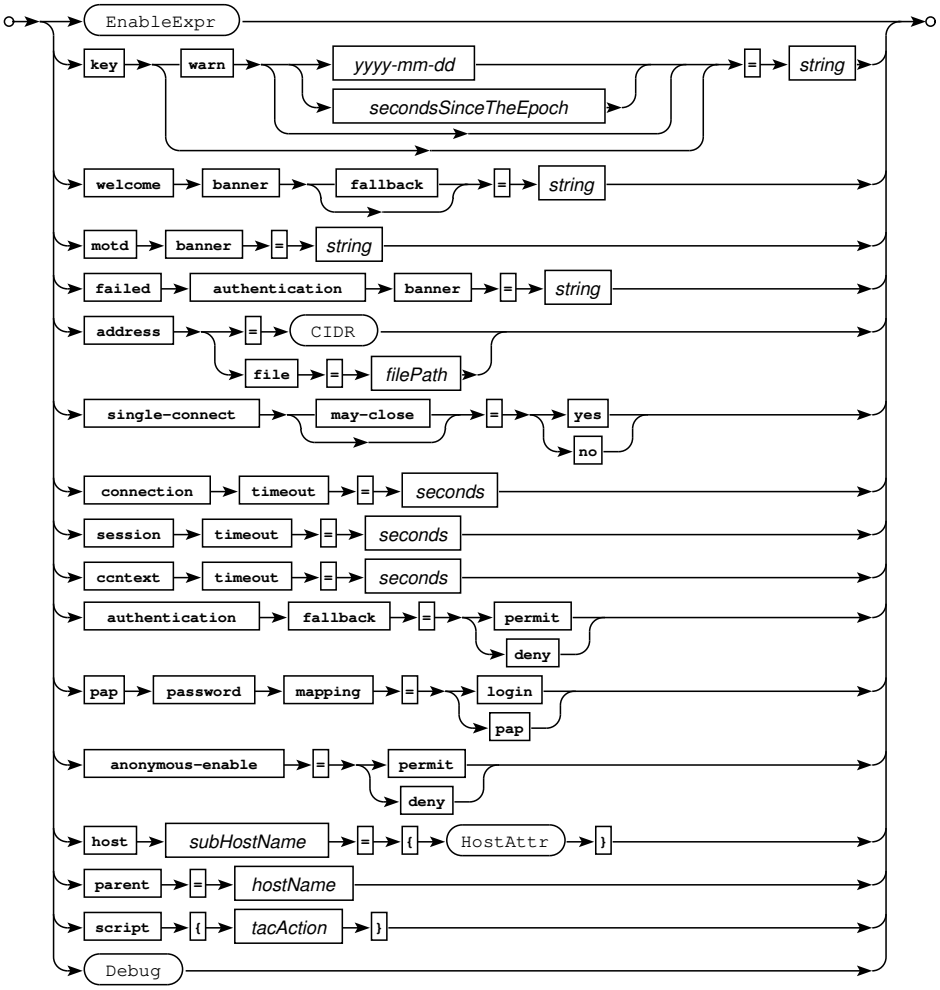
4.2.3.4.6 Inheritance and Hosts

For address based host lookups, the daemon looks for the most specific host definition. Values that aren't defined (if any) will be lookup up in the host's parent, which may be either set implicitely by defining a host in the context of it's parent host, or expliitely, using the `parent` statement.

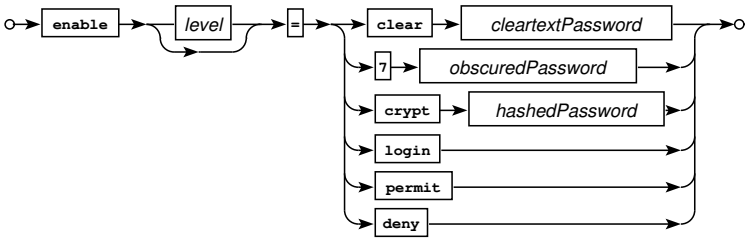
4.2.3.4.7 Railroad Diagrams



Railroad diagram: HostDecl



Railroad diagram: HostAttr



Railroad diagram: EnableExpr

4.2.3.4.8 Example

```
host = customer1 {
    address = 10.0.0.0/8
    key = "your key here"
    welcome banner = "\nHitherto shalt thou come, but no further. (Job 38.11)\n\n"
```

```
    enable 15 = clear whatever
}

host = test123 {
    address = 10.1.2.0/28
    address = 10.12.1.30/28
    address = 10.1.1.2
    # key/banners/enable will be inherited from 10.0.0.0/8 by default,
    # unless you specify "inherit = no"
    address file = /some/path/test123.cidr
    prompt = "\nGo away.\n\n"
}
```

4.2.3.5 Time Ranges

`timespec` objects may be used for time based profile assignments. Both `cron` and `Taylor-UUCP` syntax are supported; see you local `crontab(5)` and/or UUCP man pages for details. Syntax:

`timespec` = *timespec_name* { "*entry*" [...] }

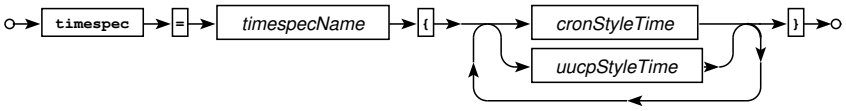
Example:

```
# Working hours are from Mo-Fr from 9 to 16:59, and
# on Saturdays from 9 to 12:59:
timespec workinghours {
    "* 9-16 * * 1-5"   # or: "* 9-16 * * Mon-Fri"
    "* 9-12 * * 6"     # or: "* 9-12 * * Sat"
}

timespec sunday { "* * * * 0" }

timespec example {
    Wk2305-0855,Sa,Su2305-1655
    Wk0905-2255,Su1705-2255
    Any
}
```

4.2.3.5.1 Railroad Diagrams



Railroad diagram: TimespecDecl

4.2.3.6 Access Control Lists

Access Control Lists (or, more exactly, Access Control Scripts) are the main component of ruleset evaluation.

Scripts may currently be used for ACLs, in service declaration scope and for rule sets:

- `acl` acl_name { tac_action ... }

  Example:

```
    acl myacl123 {
        if (nas == 1.2.3.4 || nac = SomeHostName || nac-dns =~ /\\.example\\.com$/) deny
    }
```

- `script = {` tac_action ... `}`

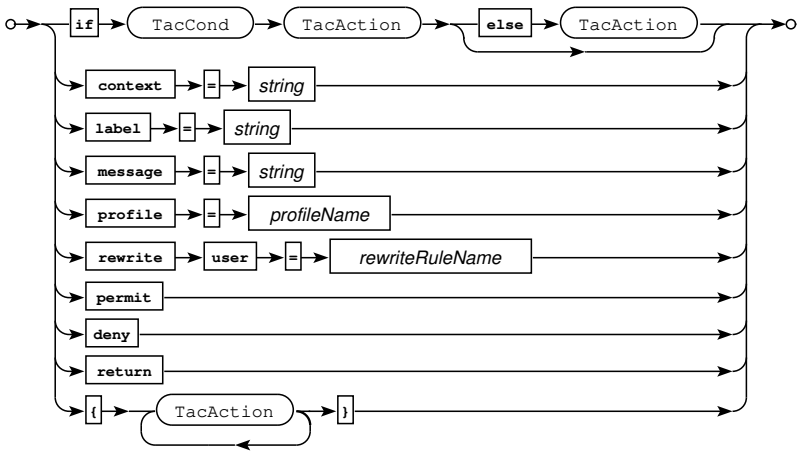
  Example:

```
profile messUp {
    service shell {
        script {
            if (cmd == "") permit # required for shell startup
            if (cmd =~ /^(no\s)?shutdown\s/) permit }
            deny
    }
}

user joe {
    password = ...
    member = ops
}
ruleset {
    rule opsRule {
        script {
            if (group == ops)
                profile = messUp
                permit
        }
    }
}
```

4.2.3.6.1 Syntax

A script consists of a series of actions:



Railroad diagram: TacAction

The actions `return`, `permit` and `deny` are final. At the end of a script, `return` is implied, at which the daemon continues processing the configured `cmd` statements in `shell` context) or standard ACLs (in ACL context). The assignment operations (`context =`, `message =`) do make sense in `shell` context only.

Setting the `context` variable makes sense in `shell` context only. See the example in the corresponding section.

Attribute-related directives are:

- `default attribute = (permit|deny)`

  This directive specifies whether the daemon is to accept or reject unknown attributes sent by the NAS (default: `deny`).

- `(set|add|optional)` *attribute* = *value*

  Defines mandatory and optional attribute-value pairs:

- `set` unconditionally returns a mandatory AV pair to the NAS
- `optional` returns a NAS-requested (and perhaps modified) optional AV pair to the NAS unless the attribute was already in the mandatory list
- `add` returns an optional AV pair to the client even if the client didn't request it (and it was neither in the mandatory nor optional list)

Example:

```
set priv-lvl = 15
```

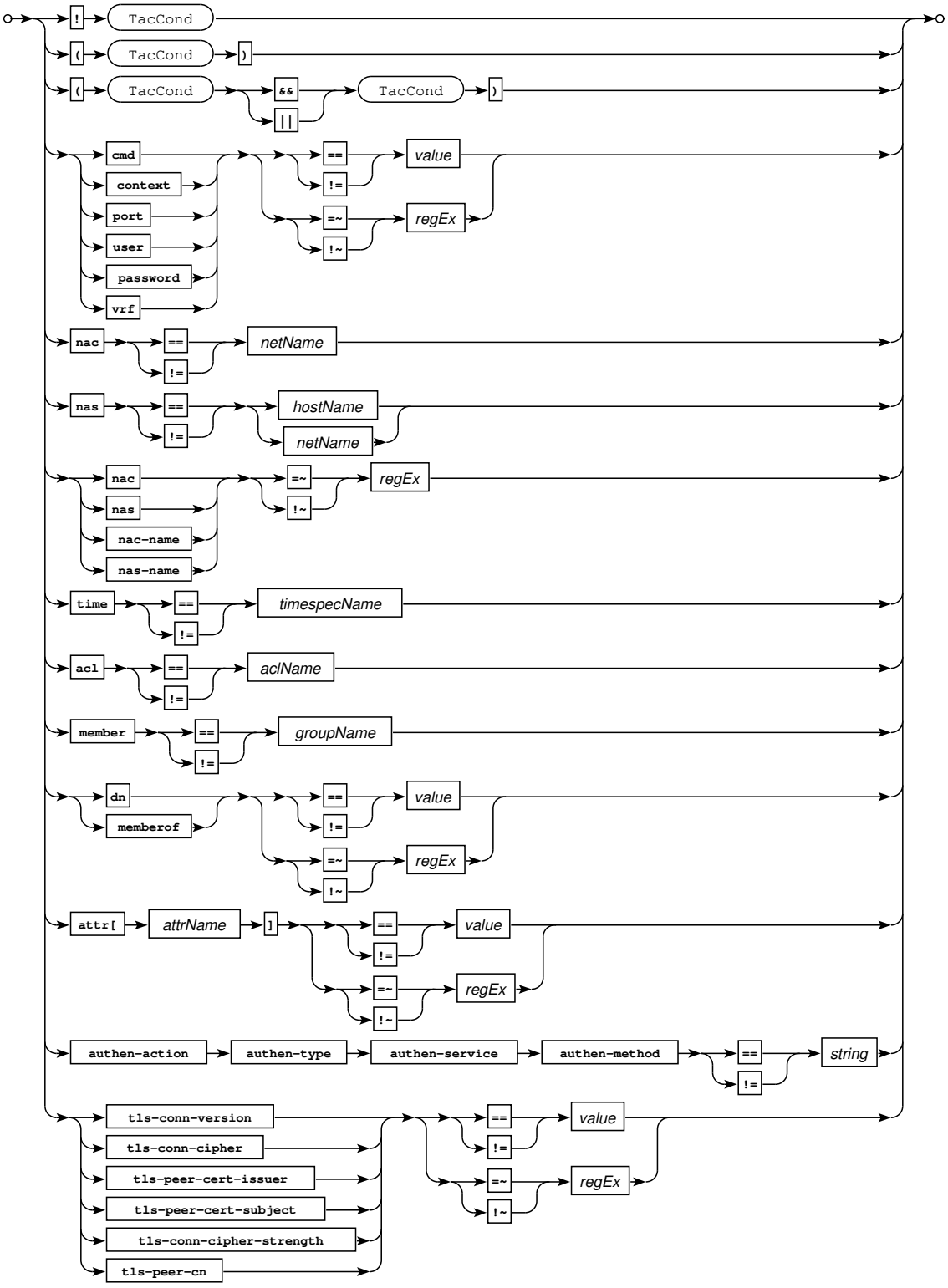
For a detailed description on mandatory and optional AV-pairs, see the "The Authorization Algorithm" section somewhere below.

Variables
The same variables supported for logging can be used as attribute values, too. Example: `set uid = "${uid}"`

- `return`

  Use the current service definition as-is. This stops the daemon from checking for the same service in the groups the current user (or group) is a member of.

Condition syntax is:



Railroad diagram: TacCond

`cmd` and `context` may be used in `shell` context only. `tls_*` conditions require *libtls*.

4.2.3.7 Rewriting User Names

This is experimental. It requires the binary to be built with PCRE v2 support (using the `--with-pcre2` configure option).

A host may refer to a rewrite profile defined at realm level to substitute user names. The following sample code will map both `admin` and `root` to `marc`, and convert all other usernames to lower-case:

```
rewrite rewriteRule {
    rewrite /^admin$/ jane.doe
    rewrite /^root$/ jane.doe
    rewrite /^.*$/ \L$0
}

host ... {
    ...
    # this is deprecated:
    rewrite user = rewriteRule
    # please use
    script { user = rewriteRule }
    # instead
    ...
}
```

Please keep in mind that this is experimental ...

4.2.3.8 Users

The basic form of a user declarations is

```
user username { ...  }
```

A user or group declaration may contain key-value pairs and service declarations.

The following declarations are valid in *user* context only:

- `password login = (( clear | crypt ) password | mavis | permit | deny )`

  The `login` password authenticates `shell` log-ins to the server.

  ```
  password login = crypt aFtFBT4e5muQE
  password login = clear Ci5c0
  ```

  For the argument after `crypt` you may use whatever hashes your *crypt(3)* implementation supports.

  If the `mavis` keyword is used instead, the password will be looked up via the **MAVIS** back-end. It will not be cached. This functionality may be useful if you want to authenticate at external systems, despite static user declarations in the configuration file.

- `password pap = (( clear | crypt ) password | login | mavis | permit | deny )`

  The `pap` authenticates PAP log-ins to the server. Just like with `login`, the password doesn't need to be in clear text, but may be hashed, or may be looked up via the **MAVIS** back-end. You can even map pap to login globally by configuring pap `password = login` in realm context.

- `password chap =( clear password | permit | deny )`

  For CHAP authentication, a cleartext password is required.

- `password ms-chap =( clear password | permit | deny )`

  For MS-CHAP authentication, a cleartext password is required.

- `password [ acl acl ] { ... }`

  This directive allows specification of ACL-dependent passwords. Example:

```
acl jumpstation { if (nac == 10.255.0.85) permit deny }

user marc {
    password acl jumpstation {
        login = permit
        pap = permit
    }
    password {
        login = clear myLoginPassword
        pap = clear myPapPassword
    }
}
```

- `enable` [*level*] `=` (`permit` | `deny` | `login` | (`clear` | `crypt`) *password*)

  This directive may be used to set user specific enable passwords, to use the *login* password, or to permit (without password) or refuse any enable attempt. Enable secrets defined at user level have precedence over those defined at host level. *level* defaults to 15.

  The default privilege level for an ordinary user on the NAS is usually 1. When a user enables, she can reset this level to a value between 0 and 15 by using the NAS `enable` command. If she doesn't specify a level, the default level she enables to is 15.

- `message` = *string*

  A message displayed to the user upon log-in.

- `hushlogin` = (`yes` | `no`)

  Setting `hushlogin` to `yes` keeps the daemon from displaying `motd` and `user` messages upon login.

- `valid from` = (*YYYY−MM−DD* | *s*)

  The user profile will be valid starting at the given date, which can be specified either in ISO8601 date format or as in seconds since January 1, 1970, UTC.

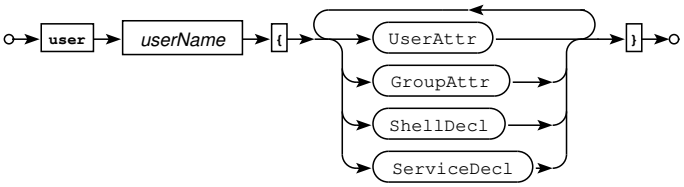
- `valid until` = (*YYYY−MM−DD* | *s*)

  The user profile will be invalid after the given date.

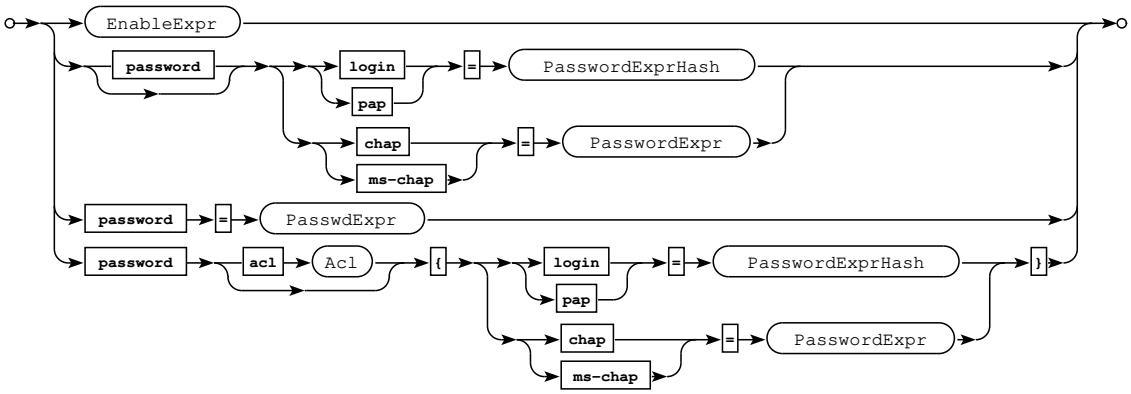
- `member` = *groupOne*[, *groupTwo*]*

  This specifies group membership. A user can be a member of multiple groups and groups can be members of a parent group.

4.2.3.8.1 Railroad Diagrams



Railroad diagram: UserDecl



Railroad diagram: ServiceDecl

4.2.3.9 Groups

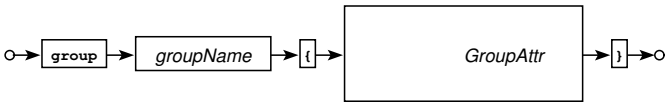
A user can be a member of multiple groups. A user that is a member of a group that comes with a parent group is a member of the latter, too. Group are defined using

```
group groupname {  ...  }
```

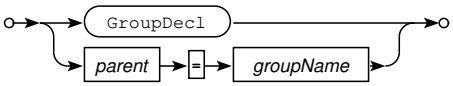
The following key-value pairs are valid for groups:

- `member =` *groupOne*[`,` *groupTwo*]*
  This specifies group membership.
- `parent =` groupName
  The parent of a group can be set explicitly.
- `group` groupName `{` GroupAttr `}`
  Groups may be parents of other groups.

4.2.3.9.1 Railroad Diagrams



Railroad diagram: GroupDecl



Railroad diagram: GroupAttr

4.2.3.10 Profiles

Profiles are collections of services that can be assigned to users via the policy rule-set. Syntax is

`profile` *profileName* `{` *profileAttr* `}`

Profiles are collections of services available to a user. A couple of configuration attributes are service specific and only valid in certain contexts:

SHELL (EXEC) Service

Shell startup should have an appropriate service

```
service shell { }
```

defined. Valid configuration directive within the curly brackets are:

- `message ( permit | deny ) =` *string*

  This specifies a message to be presented to the user on accepting or rejecting a command. Recognized string substitutions within *string* are `%c` for the command name, `%a` for the command arguments and `%C` for the currenly set context. Example:

  ```
  message permit "Permitted '%c %a'"
  message deny "Denied '%c %a'"
  ```

  This directive may appear in `cmd` sections, too, where it overrides the `service` section definitions.

- `script {` *tacAction* `}`

  Commands can be permitted or denied using script syntax:

  ```
  service shell
      script {
          if (cmd =~ /^write term/) deny
          if (cmd =~ /^configure /) deny
          permit
      }
  }
  ```

Have a look at the authorization log in case you're unsure what commands and arguments the router actually sends for verification. E.g.,

Non-Shell Services

E.g. for PPP, *protocol* definitions may be used:

```
service ppp {
    protocol = ip { set addr = 1.2.3.4 }
}
```

Use

```
    default protocol = permit
```

or

```
    default protocol = deny
```

to specify the default for protocols not explicitly defined within a service declaration. (default: `deny`).

For a Juniper Networks-specific authorization service, use:

```
service junos-exec {
   set local-user-name = NOC
   # see the Junos documentation for more attributes
}
```

Likewise, for Raritan Dominion SX IP Console Servers:

```
service dominionsx {
    set port-list = "1 3 4 15"
    set user-type = administator # or operator, or observer
}
```

Quotes
If your router expects double-quoted values (e.g. Cisco Nexus devices do), you can advise the parser to automatically add these:

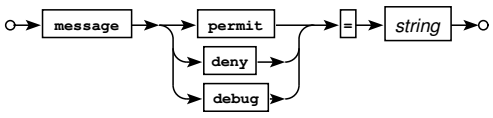
```
service shell {
    set shell:roles="\"network-admin\""
}
```

and

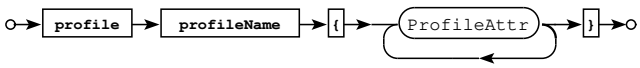
```
service shell {
    double-quote-values = yes
    set shell:roles="network-admin"
}
```

are equivalent, but the latter is more readable.

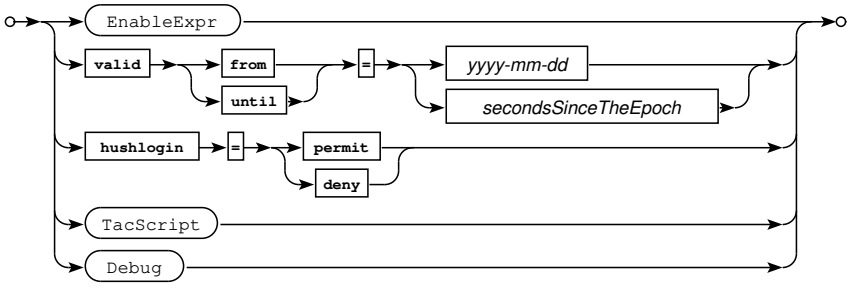
4.2.3.11 Railroad Diagrams



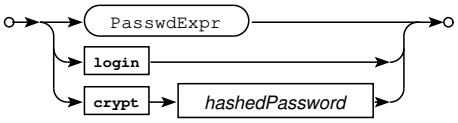
Railroad diagram: UserMessage



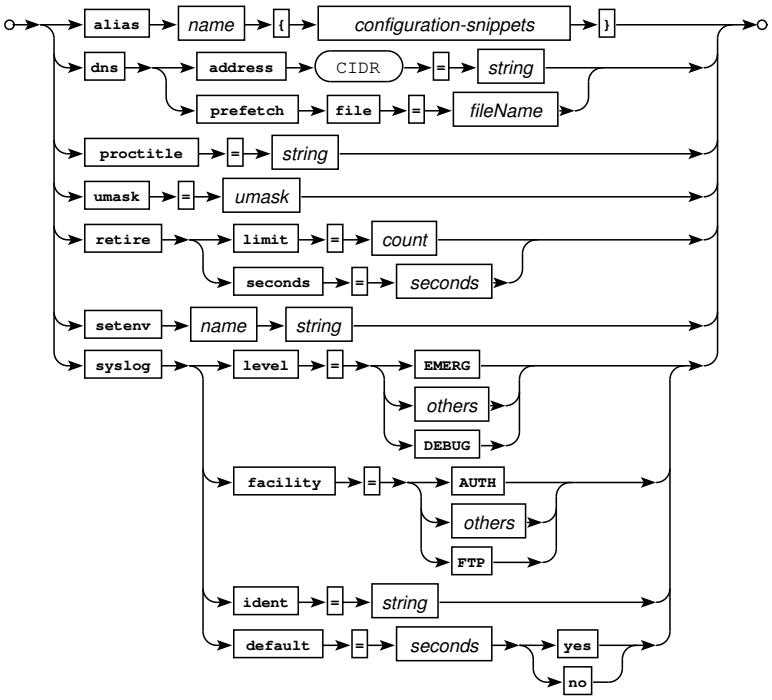
Railroad diagram: ProfileDecl



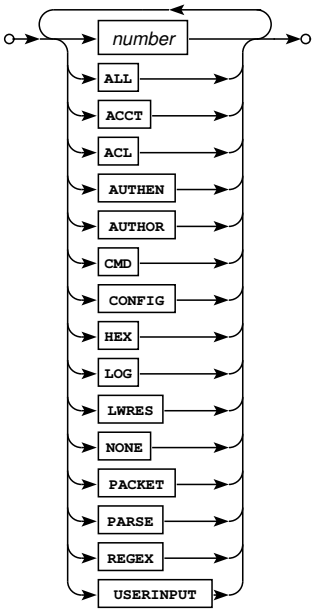
Railroad diagram: ProfileAttr



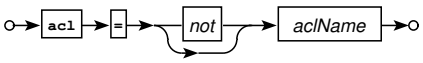
Railroad diagram: PasswordExprHash



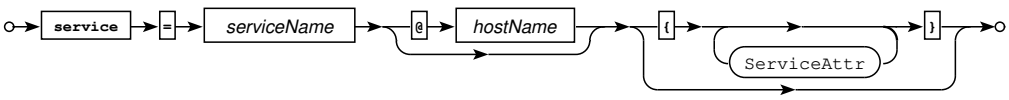
Railroad diagram: TopLevelAttr



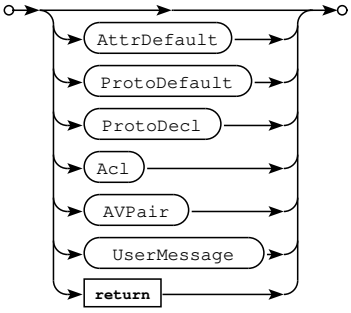
Railroad diagram: Debug



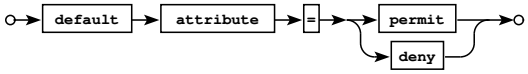
Railroad diagram: Acl



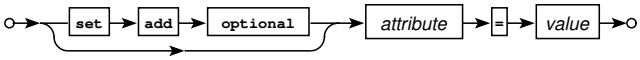
Railroad diagram: ServiceDecl



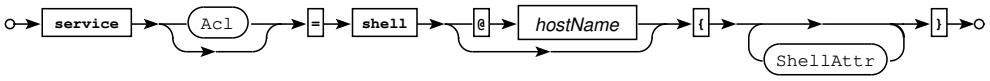
Railroad diagram: ServiceAttr



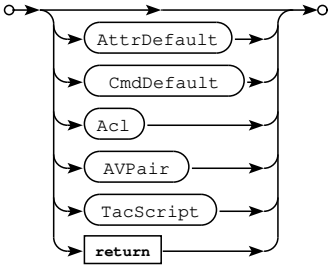
Railroad diagram: AttrDefault



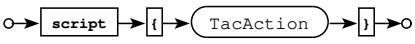
Railroad diagram: AVPair



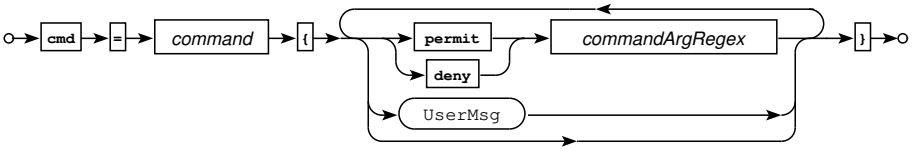
Railroad diagram: ShellDecl



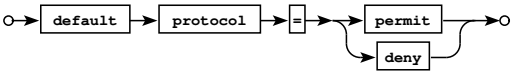
Railroad diagram: ShellAttr



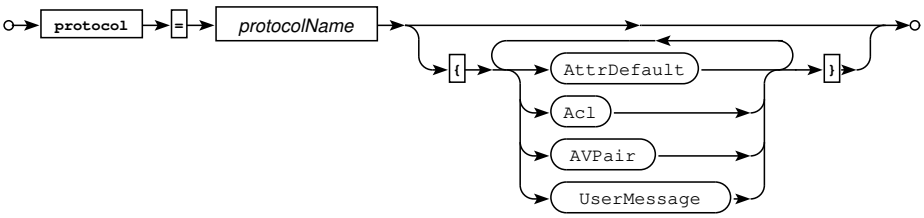
Railroad diagram: TacScript



Railroad diagram: ShellCommandDecl



Railroad diagram: ProtoDefault



Railroad diagram: ProtoDecl

4.2.3.12 Configuring Non-local Users via MAVIS

MAVIS configuration is optional. You don't need it if you're content with user configuration in the main configuration file.

MAVIS back-ends may dynamically create user entries, based, e.g., on LDAP information.

For PAP and LOGIN,

```
pap backend = mavis
login backend = mavis
```

in the global section delegate authentiation to the MAVIS sub-system. Statically defined users are still valid, and have a higher precedence.

By default, MAVIS user data will be cached for 120 seconds. You may change that period using

```
cache timeout = seconds
```

in the global configuration section.

4.2.3.13 Configuring Local Users for MAVIS authentication

Under certain circumstances you may wish to keep the user definitions in the plain text configuration file, but authenticate against some external system nevertheless, e.g. LDAP or RADIUS. To do so, just specify one of

```
    login = mavis
    pap = mavis
    password = mavis
```

in the corresponding user definition.

4.2.3.14 Configuring User Authentication

User Authentication can be specified separately for PAP, CHAP, and normal logins. CHAP and global user authentication must be given in clear text.

The following assigns the user mary five different passwords for inbound and outbound CHAP, inbound PAP, outbound PAP, and normal login respectively:

```
user mary {
    password chap = clear "chap password"
    password pap  = clear "inbound pap password"
    password login = crypt XQj4892fjk
}
```

If

```
user backend = mavis
```

is configured in the global section, users not found in the configuration file will be looked up by the MAVIS back-end. You should consider using this option in conjuction with the more sophisticated back-ends (LDAP and ActiveDirectory, in particular), or whenever you're not willing to duplicate your pre-existing database user data to the configuration file. For users looked up by the MAVIS back-end,

```
pap backend = mavis
```

and/or

```
login backend = mavis
```

(again, in the global section of the configuration file) will cause PAP and/or Login authentication to be performed by the MAVIS back-end (e.g. by performing an LDAP bind), ignoring any corresponding password definitions in the users' profile.

If you just want the users defined in your configuration file to authenticate using the MAVIS back-end, simply set the corresponding PAP or Login password field to `mavis` (there's no need to add the `user backend = mavis` directive in this case):

```
user mary { login = mavis }
```

4.2.3.15 Configuring Expiry Dates

An entry of the form:

```
user lol {
    valid until = YYYY-MM-DD
    password login = clear "bite me"
}
```

will cause the user profile to become invalid, starting after the `valid until` date. Valid date formats are both ISO8601 and the absolute number of seconds since 1970-01-01.

A expiry warning message is sent to the user when she logs in, by default starting at 14 days before the expiration date, but configurable via the `warning period` directive.

Complementary to profile expiry,

```
    valid from = YYYY-MM-DD
```

activates a profile at the given date.

4.2.3.16 Configuring Authentication on the NAS

On the NAS, to configure login authentication, try

```
aaa new-model
aaa authentication login default group tacacs+ local
```

(Alternatively, you can try a *named authentication list* instead of `default`. Please see the IOS documentation for details.)

Don't lock yourself out.
As soon as you issue this command, you will no longer be able to create new logins to your NAS without a functioning TACACS+ daemon appropriately configured with usernames and password, so make sure you have this ready.
As a safety measure while setting up, you should configure an enable secret and make it the last resort authentication method, so if your TACACS+ daemon fails to respond you will be able to use the NAS enable password to login. To do this, configure:

```
aaa authentication login default group tacacs+ enable
```

or, to if you have local accounts:

```
aaa authentication login default group tacacs+ local
```

If all else fails, and you find yourself locked out of the NAS due to a configuration problem, the section on *recovering from lost passwords* on Cisco's CCO web page will help you dig your way out.

4.2.3.17 Configuring Authorization

Authorization must be configured on both the NAS and the daemon to operate correctly. By default, the NAS will allow everything until you configure it to make authorization requests to the daemon.

On the daemon, the opposite is true: The daemon will, by default, deny authorization of anything that isn't explicitly permitted.

Authorization allows the daemon to deny commands and services outright, or to modify commands and services on a per-user basis. Authorization on the daemon is divided into two separate parts: commands and services.

4.2.3.18 Authorizing Commands

Exec commands are those commands which are typed at a NAS exec prompt. When authorization is requested by the NAS, the entire command is sent to the tac_plus daemon for authorization.

Command authorization is configured by telling the ruleset to apply a profile to the user. See the Profile section for details.

4.2.3.19 The Authorization Process

Authorizing a single session can result in multiple requests being sent to the daemon. For example, in order to authorize a dialin PPP user for IP, the following authorization requests will be made from the NAS:

1. An initial authorization request to startup PPP from the exec, using the AV pairs `service=ppp`, `protocol=ip`, will be made (Note: this initial request will be omitted if you are autoselecting PPP, since you won't know the username yet).

   This request is really done to find the address for dumb PPP (or SLIP) clients who can't do address negotiation. Instead, they expect you to tell them what address to use before PPP starts up, via a text message e.g. "Entering PPP. Your address is 1.2.3.4". They rely on parsing this address from the message to know their address.

2. Next, an authorization request is made from the PPP subsystem to see if PPP's LCP layer is authorized. LCP parameters can be set at this time (e.g. callback). This request contains the AV pairs `service=ppp`, `protocol=lcp`.

3. Next an authorization request to startup PPP's IPCP layer is made using the AV pairs `service=ppp`, `protocol=ipcp`. Any parameters returned by the daemon are cached.

4. Next, during PPP's address negotiation phase, each time the remote peer requests a specific address, if that address isn't in the cache obtained in step 3, a new authorization request is made to see if the peers requested address is allowable. This step can be repeated multiple times until both sides agree on the remote peer's address or until the NAS (or client) decide they're never going to agree and they shut down PPP instead.

4.2.3.20 Authorization Relies on Authentication

Since we pretty much rely on having a username in authorization requests to decide which addresses etc. to hand out, it is important to know where the username for a PPP user comes from. There are generally 2 possible sources:

1. You force the user to authenticate by making her login to the exec and you use that login name in authorization requests. This username isn't propagated to PPP by default. To have this happen, you generally need to configure the `if-needed` method, e.g.

```
aaa authentication login default tacacs+
aaa authentication ppp default if-needed
```

2. Alternatively, you can run an authentication protocol, PAP or CHAP (CHAP is much preferred), to identify the user. You don't need an explicit login step if you do this (so it's the only possibility if you are using autoselect). This authentication gets done before you see the first LCP authorization request of course. Typically you configure this by doing:

```
aaa authentication ppp default tacacs+
int async 1
  ppp authentication chap
```

If you omit either of these authentication schemes, you will start to see authorization requests in which the username is missing.

4.2.3.21 Configuring Service Authorization

A list of AV pairs is placed in the daemon's configuration file in order to authorize services. The daemon compares each NAS AV pair to its configured AV pairs and either allows or denies the service. If the service is allowed, the daemon may add, change or delete AV pairs before returning them to the NAS, thereby restricting what the user is permitted to do.

4.2.3.21.1 The Authorization Algorithm

The complete algorithm by which the daemon processes its configured AV pairs against the list the NAS sends, is given below.

Find the user (or group) entry for this service (and protocol), then for each AV pair sent from the NAS:

1. If the AV pair from the NAS is mandatory:
   (a) look for an exact attribute,value match in the user's mandatory list. If found, add the AV pair to the output.
   (b) If an exact match doesn't exist, look in the user's optional list for the first attribute match. If found, add the NAS AV pair to the output.
   (c) If no attribute match exists, deny the command if the default is to deny, or,
   (d) If the default is permit, add the NAS AV pair to the output.
2. If the AV pair from the NAS is optional:
   (a) look for an exact attribute,value match in the user's mandatory list. If found, add DAEMON's AV pair to output.
   (b) If not found, look for the first attribute match in the user's mandatory list. If found, add DAEMON's AV pair to output.
   (c) If no mandatory match exists, look for an exact attribute,value pair match among the daemon's optional AV pairs. If found add the DAEMON's matching AV pair to the output.
   (d) If no exact match exists, locate the first attribute match among the daemon's optional AV pairs. If found add the DAEMON's matching AV pair to the output.
   (e) If no match is found, delete the AV pair if the default is deny, or
   (f) If the default is permit add the NAS AV pair to the output.
3. After all AV pairs have been processed, for each mandatory DAEMON AV pair, if there is no attribute match already in the output list, add the AV pair (but add only ONE AV pair for each mandatory attribute).
4. After all AV pairs have been processed, for each optional unrequested DAEMON AV pair, if there is no attribute match already in the output list, add that AV pair (but add only ONE AV pair for each optional attribute).

4.3 MAVIS Backends

The distribution comes with various *MAVIS* modules, of which the *external* module is probably the most interesting, as it interacts with simple Perl scripts to authenticate and authorize requests. You'll find sample scripts in the `mavis/perl` directory. Have a close look at them, as you may (or will) need to perform some trivial customizations to make them match your local environment.

You should really have a look at the *MAVIS* documentation. It gives examples for RADIUS and PAM authentication, too.

4.3.1 LDAP Backends

`mavis_tacplus_ldap.pl` is an authentication/authorization back-end for the *external* module. It interfaces to various kinds of LDAP servers, e.g. OpenLDAP, Fedora DS and Active Directory. Its behaviour is controlled by a list of environmental variables:

Variable	Description
`LDAP_SERVER_TYPE`	One of: `generic`, `tacacs_schema`, `microsoft`. Default: `tacacs_schema`
`LDAP_HOSTS`	Space-separated list of LDAP URLs or IP addresses or hostnames Examples: `"ldap01 ldap02"`, `"ldaps://ads01:636 ldaps://ads02:636"`
`LDAP_SCOPE`	LDAP search scope (`base`, `one`, `sub`) Default: `sub`
`LDAP_BASE`	Base DN of your LDAP server Example: `dc=example,dc=com`

`LDAP_FILTER`	LDAP search filter. Defaults:
	• for `LDAP_SERVER_TYPE=generic`:
	`"(uid=%s)"`
	• for `LDAP_SERVER_TYPE=tacacs_schema`:
	`"(&(uid=%s)(objectClass=tacacsAccount))"`
	• for `LDAP_SERVER_TYPE=microsoft`:
	`"(&(objectclass=user)(sAMAccountName=%s))"`

`LDAP_FILTER_CHPW`	LDAP search filter for password changes. Defaults:
	• for `LDAP_SERVER_TYPE=generic`:
	`"(uid=%s)"`
	• for `LDAP_SERVER_TYPE=tacacs_schema`:
	`"(&(uid=%s)(objectClass=tacacsAccount)(!(tacacsFlag=staticpas`
	• for `LDAP_SERVER_TYPE=microsoft`:
	`"(&(objectclass=user)(sAMAccountName=%s))"`

`LDAP_USER`	User to use for LDAP bind if server doesn't permit anonymous searches. Default: unset
`LDAP_PASSWD`	Password for `LDAP_USER` Default: unset
`AD_GROUP_PREFIX`	An AD group starting with this prefix will be used as the user's TACACS+ group membership. The value of `AD_GROUP_PREFIX` will be stripped from the group name. Example: With `AD_GROUP_PREFIX` set to `tacacs` (which is actually the default), an AD group membership of `TacacsNOC` will assign the user to the `NOC` TACACS+ group. Note that TACACS+ group names are case-sensitive.

Variable	Description
REQUIRE_AD_GROUP_PREFIX	If set, user needs to be in one of the AD_GROUP_PREFIX groups. Default: unset
USE_TLS	If set, the server is required to support start_tls. Default: unset
FLAG_CHPW	Permit password changes via this back-end. Default: unset
FLAG_PWPOLICY	Try to enforce a simplicistic password policy. Default: unset
FLAG_CACHE_CONNECTION	Keep connection to LDAP server open. Default: unset
FLAG_FALLTHROUGH	If searching for the user in LDAP fails, try the next MAVIS module (if any). Default: unset
FLAG_USE_MEMBEROF	Use the memberOf attribute for determining group membership. Setting LDAP_SERVER_TYPE to microsoft implies this. May be used if you're running *OpenLDAP* with **memberof** overlay enabled. Default: unset

4.3.1.1 LDAP Custom Schema Backend

For LDAP_SERVER_TYPE set to tacacs_schema, the program expects the LDAP server to support the experimental ldap.schema included for OpenLDAP and Fedora-DS. The schema files are located in the mavis/perl directory.

The new schema allows for a *auxiliary* object class

```
objectClass: tacacsAccount
```

which introduces a couple of new attributes. A sample user entry could then look similar to the following LDIF snippet:

```
dn: uid=marc,ou=people,dc=example,dc=com
uid: marc
cn: Marc Huber
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: shadowAccount
objectClass: tacacsAccount
shadowMax: 10000
uidNumber: 1000
gecos: Marc Huber
givenName: Marc
sn: Huber
gidNumber: 500
shadowLastChange: 14012
loginShell: /bin/bash
homeDirectory: /Users/marc
mail: marc@example.com
userPassword:: abcdefghijklmnopqrstuvwxyz=
tacacsClient: 192.168.0.0/24
tacacsClient: management
tacacsMember: readonly,readwrite
tacacsProfile: { valid until = 2010-01-30 chap = clear ahzoi5Ue }
```

As tacacsProfile may (and most probably will) contain sensitive data, you should consider setting up LDAP ACLs to restrict access.

You should be pretty familiar with OpenLDAP (or, for that matter, Fedora-DS) if you're willing to go this route. For current versions of OpenLDAP: Use ldapadd to add tacacs_schema.ldif to the cn=config tree. For older versions, add tacacs.schema to the list of included schema and objectClass definitions in slapd.conf.

4.3.1.2 Active Directory Backend

If `LDAP_SERVER_TYPE` is set to `microsoft`, the script back-ends to AD servers. Sample configuration:

```
id = spawnd {
    listen = {
        port = 49
    }
    spawn = {
        instances min = 1
        instances max = 10
    }
    background = yes
}

id = tac_plus {

    mavis module = external {
        # Optionally:
        # script out = {
        #     # Require group membership:
        #     if (undef($TACMEMBER) && $RESULT == ACK) set $RESULT = NAK
        #
        #     # Don't cache passwords:
        #     if ($RESULT == ACK) set $PASSWORD_ONESHOT = 1
        # }

        setenv LDAP_SERVER_TYPE = "microsoft"
        # setenv LDAP_HOSTS = "ldaps://ads01:636 ldaps://ads02:636"
        setenv LDAP_HOSTS = "ads01:3268 ads02:3268"
        setenv LDAP_SCOPE = sub
        setenv LDAP_BASE = "dc=example,dc=com"
        setenv LDAP_FILTER = "(&(objectclass=user)(sAMAccountName=%s))";
        setenv LDAP_USER = tacacs@example.com
        setenv LDAP_PASSWD = Secret123
        setenv AD_GROUP_PREFIX = tacacs
        # setenv REQUIRE_AD_GROUP_PREFIX = 1
        setenv USE_TLS = 0
        exec = /usr/local/lib/mavis/mavis_tacplus_ldap.pl
    }

    login backend = mavis
    pap backend = mavis

    host world {
        address = ::/0
        welcome banner = "Welcome\n"
        key = demo
    }

    host helpdesklab {
        address = 192.168.34.16/28
        parent = world
    }

    # A user will be in the "admin" group if he's member of the
    # corresponding "tacacsadmin" ADS group.

    profile admin {
        default service = permit
        service shell {
            if (cmd == "") {
```

```
                set priv-lvl = 15
            }
            permit
        }
    }

    group helpdesk { }

    ruleset {
        rule help { if (member == helpdesk) profile = admin permit
    }
}
```

4.3.1.3 Generic LDAP Backend

If `LDAP_SERVER_TYPE` is set to `generic`, the script won't require any modification to your LDAP server, but only authenticates users (with `login = mavis`, `pap = mavis` or `password = mavis` declaration) defined in the configuration file. No authorization is done by this back-end.

4.3.2 PAM back-end

Example configuration for using *Pluggable Authentication Modules*:

```
id = spawnd { listen = { port = 49 } }

id = tac_plus {
  mavis module = groups {
    resolve gids = yes
    groups filter = /^(guest|staff)$/
    script out = {
      # copy the already filtered UNIX group access list to TACMEMBER
      eval $GIDS =~ /^(.*)$/
      set $TACMEMBER = $1
    }
  }
  mavis module = external {
    exec = /usr/local/sbin/pammavis pammavis -s sshd
  }
  user backend = mavis
  login backend = mavis
  host = global { address = 0.0.0.0/0 key = demo }

  profile staff {
    service shell {
      script {
          if (cmd == "") {
            set priv-lvl = 15
            permit
          }
    }
  }
  group = guest {
    service shell {
      script {
          set priv-lvl = 15
          if (cmd =~ ^/show /)
            permit
          deny
      }
```

```
    }
  }
}
```

4.3.3 System Password Backends

`mavis_tacplus_passwd.pl` authenticates against your local password database. Alas, to use this functionality, the script may have to run as root, as it needs access to the encrypted passwords. Primary and auxiliary UNIX group memberships will be mapped to TACACS+ groups.

`mavis_tacplus_opie.pl` is based on `mavis_tacplus_passwd.pl`, but uses OPIE one-time passwords for authentication.

4.3.4 Shadow Backend

`mavis_tacplus_shadow.pl` may be used to keep user passwords out of the **tac_plus**configuration file, enabling users to change their passwords via the password change dialog. Passwords are stored in an auxiliary, `/etc/shadow`-like ASCII file, one user per line:

```
username:encryptedPassword:lastChange:minAge:maxAge:reserved
```

`lastChange` is the number of days since 1970-01-01 when the password was last changed, and `minAge` and `maxAge` determine whether the password may/may not/needs to be changed. Setting `lastChange` to `0` enforces a password change upon first login.

Example shadow file:

```
marc:$1$q5/vUEsR$jVwHmEw8zAmgkjMShLBg/.:15218:0:99999:
newuser:$1$pQtQsMuj$GKpIr5r2GNaZNfDfnCBtw.:0:0:99999:
test:$1$pQtQsMuj$GKpIr5r2GNaZNfDfnCBtw.:15218:1:30:
```

Sample daemon configuration:

```
...
  id = tac_plus {
    ...
    mavis module = external {
      setenv SHADOWFILE = /path/to/shadow
      # setenv FLAG_PWPOLICY=y
      # setenv ci=/usr/bin/ci
      exec = /usr/local/lib/mavis/mavis_tacplus_shadow.pl
    }
    ...
    login backend = mavis chpass
    ...
    user marc {
      login = mavis
      ...
    }
  ...
  }
...
```

4.3.5 RADIUS Backends

`mavis_tacplus_radius.pl` authenticates against a RADIUS server. No authorization is done, unless the `RADIUS_GROUP_ATTR` environment variable is set (see below). This module may, for example, be useful if you have static user account definitions in

the configuration file, but authentication passwords should be verified by RADIUS. Use the `login = mavis` or `password = mavis` statement in the user profile for this to work.

If the `Authen::Radius` Perl module is installed, the value of the RADIUS attribute specified by `RADIUS_GROUP_ATTR` will be used to create a `TAC_MEMBER` definition which uses the attribute value as group membership. E.g., an attribute value of `Administrator` would result in a

```
  member = Administrator
```

declaration for the authenticated user, enabling authorization and omitting the need for static users in the configuration file.

Keep in mind that authorization will only work well if either

- the `tacplus_info_cache` module is being used (it will cache authentication AV pairs locally, so subsequent authorizations should work fine unless you're switching to a tac_plus server running elsewhere).

or

- `single-connection` is used and
- `mavis cache timeout` is set to a sufficiently high value that covers the user's (expected) maximum login time.

Alternatively to `mavis_tacplus_radius.pl` the `pamradius` program may called by the `external` module. Results should be roughly equivalent.

4.3.5.1 Sample Configuration

```
## Use tacinfo_cache to cache authorization data to disk:
mavis module = tacinfo_cache {
    directory = /tmp/tacinfo
}

## You can use either the Perl module ...
#mavis module = external {
#   exec = /usr/local/lib/mavis_tacplus_radius.pl
#   setenv RADIUS_HOST = 1.2.3.4:1812 # could add more hosts here, comma-separated
#   setenv RADIUS_SECRET = "mysecret"
#   setenv RADIUS_GROUP_ATTR = Class
#   setenv RADIUS_PASSWORD_ATTR = Password # defaults to: User-Password
# }
## ... or the freeradius-client based code:
mavis module = external {
    exec = /usr/local/sbin/radmavis radmavis "group_attribute=Class" "authserver ↩
        =1.2.3.4:1812:mysecret"
}
```

4.3.6 Experimental Backends

`mavis_tacplus_sms.pl` is a sample (skeleton) script to send One-Time Passwords via a SMS back-end.

4.3.7 Error Handling

If a back-end script fails due to an external problem (e.g. LDAP server unavailability), your router may or may not fall back to local authentication (if configured). Chances are, that the fallback doesn't work. If you still want to be able to authenticate via TACACS+ in that case, you can do so with a non-MAVIS user which will only be valid in case of a back-end error:

```
...
# set the time interval you want the user to be valid if the back-end fails:
authentication fallback period = 60 # that's actually the default value
...
# add a local user for emergencies:
user = cisco {
    ...
    fallback-only
    ...
}
```

To indicate that fallback mode is actually active, you may a display a different login prompt to your users:

```
host = ... {
    ...
    welcome banner = "Welcome\n"
    welcome banner fallback = "Welcome\nEmergency accounts are currently enabled.\n"
    ...
}
```

Fallback can be enabled/disabled globally an on a per-host basis. Default is enabled.

```
authentication fallback = permit
host = ... {
    ...
    authentication fallback = deny
    ...
}
```

5 Debugging

5.1 Debugging Configuration Files

When creating configuration files, it is convenient to check their syntax using the `-P` flag to `tac_plus`; e.g:

```
tac_plus -P config-file
```

will syntax check the configuration file and print any error messages on the terminal.

5.2 Trace Options

Trace (or debugging) options may be specified in *global*, *host*, *user* and *group* context. The current debugging level is a combination (read: `OR`) of all those. Generic syntax is:

```
debug = option ...
```

For example, getting command authorization to work in a predictable way can be tricky - the exact attributes the NAS sends to the daemon may depend on the IOS version, and may in general not match your expectations. If your regular expressions don't work, add

```
debug = REGEX
```

where appropriate, and the daemon may log some useful information to `syslog`.

Multiple trace options may be specified. Example:

```
debug = REGEX CMD
```

Trace options may be removed by prefixing them with−. Example:

```
debug = ALL -PARSE
```

The debugging options available are summarized in the following table:

Bit	Value	Name	Description
0	1	PARSE	Configuration file parsing
1	2	AUTHOR	Authorization related
2	4	AUTHEN	Authentication related
3	8	ACCT	Accounting related
4	16	CONFIG	Configuration related
5	32	PACKET	Packet dump
6	64	HEX	Packet hex-dump
7	128	LOCK	File locking
8	256	REGEX	Regular expressions
9	512	ACL	Access Control Lists
10	1024	RADIUS	unused
11	2048	CMD	Command lookups
12	4096	BUFFER	Buffer handling
13	8192	PROC	Procedural traces
14	16384	NET	Network related
15	32768	PATH	File system path related
16	65536	CONTROL	Control connection related
17	131072	INDEX	Directory index related
18	262144	AV	Attribute-Value pair handling
19	524288	MAVIS	MAVIS related
20	1048576	LWRES	DNS related
21	2097152	USERINPUT	Show user input (this may include passwords)
31	2147483648	NONE	Disable debugging

Some of those debugging options are not used and trigger no output at all.

Debugging User Input

The daemon will (starting with snapshot 202012051554) by default no longer outputs user input from authentication packets sent by the NAS. You can explicitly change this using the `USERINPUT` debug flag. Something like

```
debug = ALL
```

or using a numeric value will *not* work, it needs to be enabled explicitly, e.g.:

```
debug = ALL USERINPUT
```

Be prepared to see plain text user passwords if you enable this option.

---

6 Frequently Asked Questions

- **Is there a Graphical User Interface of any kind?**

  Old answer: No, unless your favourite text editor does qualify. The configuration syntax is too complex and flexible to be coverable using a GUI. If you're looking for a way to manage your user database then have a look at Webmin, ActiveDirectory, whatever. It's trivial to use those as authentication/authorization back-ends.

  Updated answer: Yes, various, and unrelated. Search for "tacacsgui". There are other adaptors, too.

- **I'm using the *single-connection* feature. How can I force my router to close the TCP connections to the TACACS+ server?**

On IOS, `show tcp brief` will display the TCP connections. Search for the ones terminating at your server, and kill them using `clear tcp tcb ...`. Example:

```
Router#sho tcp brief | incl 10.0.0.1.49
633BB794  10.0.0.2.17326              10.0.0.1.49                ESTAB
6287E4C4  10.0.0.2.24880              10.0.0.1.49                ESTAB
Router#clear tcp tcb 633BB794
[confirm]
 [OK]
Router#clear tcp tcb 6287E4C4
[confirm]
 [OK]
Router#
```

- **Is there any way to avoid having clear text versions of the CHAP secrets in the configuration file?**

  CHAP requires that the server knows the cleartext password (or equivalently, something from which the server can generate the cleartext password). Note that this is part of the definition of CHAP, not just the whim of some Cisco engineer who drank too much coffee late one night.

  If we encrypted the CHAP passwords in the database, then we'd need to keep a key around so that the server can decrypt them when CHAP needs them. So this only ends up being a slight obfuscation and not much more secure than the original scheme.

  In extended TACACS, the CHAP secrets were separated from the password file because the password file may be a system password file and hence world readable. But with TACACS+'s native database, there is no such requirement, so we think the best solution is to read-protect the files. Note that this is the same problem that a Kerberos server has. If your security is compromised on the Kerberos server, then your database is wide open. Kerberos does encrypt the database, but if you want your server to automatically restart, then you end up having to "kstash" the key in a file anyway and you're back to the same security problem.

  So storing the cleartext password on the security server is really an absolute requirement of the CHAP protocols, not something imposed by TACACS+.

  With the scheme choosen for newer TACACS+ protocol revisions, the NAS sends the challenge information to the TACACS+ daemon and the daemon uses the cleartext password to generate the response and returns that.

  The original TACACS+ protocol included specific protocol knowledge for CHAP. Please note that this version of the daemon implementation no longer supports SENDPASS, SENDAUTH and ARAP to comply to RFC8907.

  However, the above doesn't apply to PAP. You can keep an inbound PAP password DES- or MD5-encrypted, since all you need to do with it is verify that the password the principal gave you is correct.

- **How is the typical login authentication sequence done?**

  1. NAS sends START packet to daemon
  2. Daemon send GETUSER containing login prompt to NAS
  3. NAS prompts user for username
  4. NAS sends packet to daemon
  5. Daemon sends GETPASS containing password prompt to the NAS
  6. NAS prompts user for password
  7. NAS sends packet to daemon
  8. Daemon sends accept, reject or error to NAS

- **What does "`default service = permit`" really do?**

  When a request comes in to authorize exec startup, or ppp (with protocol lcp, ip, ipx), or slip or a specific command, the daemon looks for a matching declarations for the user (or groups the user is a member of).

  For exec startup, it looks for a `service=shell`.

  For PPP, it looks for a `service=ppp` and `protocol=` one of `lcp`, `ip`, `ipx`.

  For commands, the `script` defined must permit the command.

  If these aren't found, authorization will fail, *unless* you say `default service = permit`.

- **How do I limit the number of sessions a user can have?**

  With this version of the daemon you can't.

- **How can I configure time-outs on an interface via TACACS+?**

  Certain per-user/per-interface timeouts may be set by TACACS+ during authorization. As of 11.0, you can set an exec timeout. As of 11.1 you can also set an exec idle timeout.

  There are currently no settable timeouts for PPP or SLIP sessions, but there is a workaround which applies to ASYNC PPP/SLIP idle timeouts started via exec sessions only: This workaround is to set an EXEC (idletime) timeout on an exec session which is later used to start up PPP or SLIP (either via a TACACS+ autocommand or via the user explicitly invoking PPP or SLIP). In this case, the exec idle timeout will correctly terminate an idle PPP or SLIP session. Note that this workaround cannot be used for sessions which autoselect PPP or SLIP.

  An idle timeout terminates a connection when the interface is idle for a given period of time (this is equivalent to the "session-timeout" Cisco IOS configuration directive). The other timeouts are absolute. Of course, any timeouts set by TACACS+ apply only to the current connection.

```
profile ... {
    ...
    service shell {
        set idletime = 5 # disconnect lol if there is no traffic for 5 minutes
        set timeout = 60 # disconnect lol unconditionally after one hour
        ...
    }
}
```

  You also need to configure exec authorization on the NAS for the above timeouts, e.g.

```
aaa authorization exec default group tacacs+
```

  Note that these timeouts only work for async lines, not for ISDN currently.

  Note also that you cannot use the authorization `if-authenticated` option with these parameters, since that skips authorization if the user has successfully authenticated.

- **Can someone expand on the use of the `optional` keyword?**

  Most attributes are mandatory i.e. if the daemon sends them to the NAS, the NAS must obey them or deny the authorization. This is the default. It is possible to mark attributes as optional, in which case a NAS which cannot support the attribute is free to simply ignore it without causing the authorization to fail.

  This was intended to be useful in cutover situations where you have multiple NASes running different versions of IOS, some of which support more attributes than others. If you make the new attributes optional, older NASes could ignore the optional attributes while new NASes could apply them. Note that this weakens your security a little, since you are no longer guaranteed that attributes are always applied on successful authorization, so it should be used judiciously.

- **What about MSCHAP?**

  The daemon comes with mschap support. Mschap is configured the same way as chap, only using the `mschap` keyword in place of the `chap` keyword.

  MSCHAP requires DES support. Use the `--with-ssl` flag when configuring the package.

  Marc Huber thinks that MSCHAP relevance is less than zero and expects it to be removed from the standard, as nobody uses it anyway.

7 Bugs

- There may still be some nasty bugs lurking in the code. Please contact the author via the "Event-Driven Servers" Google Group at event-driven-servers@googlegroups.com or http://groups.google.com/group/event-driven-servers if you think you've found one.
- This documentation isn't well structured.

- The examples given are too IPv4-centric. However, the daemon handles IPv6 just fine.
- Some of the NAS configuration examples aren't recently tested. Refer to the IOS documentation for IOS configuration syntax guidance.

8 Multi-tenant setups

While using a dedictated tac_plus-ng installation per tenant is certainly possible it lacks some elegance. There are other ways:

A single daemon can tell tenants apart by

- host identity, either
  - by NAD IP address or
  - by certificate common name (currently irrelevant, as there's no NAD support)
- realms, which are determined
  - by tacacs+ destination port or
  - by VRF (Linux, mostly)

Using the IP-based host identity should be sufficient for simple setups, but these don't scale and don't handle IP address conflicts. Options to cope with the latter involve *realms*. A realm is most basicly a text string the tcp listener (spawnd) assigns to a connection based on TCP destination port:

```
id = spawnd {
    ...
    listen { port = 49001 realm = customer1 }
    listen { port = 49002 realm = customer2 }
    ...
}
```

In case VRFs aren't an option you can use HAProxy instances to transparently relay TACACS+ connections to tac_plus-ng:

```
id = spawnd {
    ...
    listen { port = 49001 realm = customer1 haproxy = yes }
    listen { port = 49002 realm = customer2 haproxy = yes }
    ....
}
```

tac_plus-ng will then take the NAD IP from the HAProxy protocol v2 header.

Otherwise, the "listen" directive can be limite to your locally defined VRFs:

```
id = spawnd {
    ...
    listen { port = 49000 realm = customer1 vrf = blue }
    listen { port = 49000 realm = customer2 vrf = red }
    ...
}
```

On Linux, if you set `net.ipv4.tcp_l3mdev_accept=1`, you can even get away with

```
id = spawnd { ... listen { port = 49000 } ... }
```

and the daemon will use the VRF name your clients did connect from as realm name.

8.1 AD, Realms and Tenants

The suggested setup for giving customers limited access to NADs is:

```
id = tac_plus-ng {
    mavis module = external { your AD configuration goes here }

    profile ... { ... }

    realm customer1 {

        net custsrc { the IP ranges the end customer may log in from  }

        rewrite normalizeCustomerAccount {
           rewrite /^.*$/ cust1-\L$0
        }

        net custnet { the IP ranges the end customer may log in from  }

        host customer1 {
            ....
            script {  if (nac == custsrc) rewrite user = normalizeCustomerAccount
        }

        ruleset {
            rule customer {
                if (nac == custnet) {
                   if (member == ...) { profile = ... permit }
                   deny
                }
               if (member == ...) profile = ... permit
               deny
        }
}
```

In this example, you can easily share your LDAP (or AD) server between your own admin users and multiple tenants. The daemon will automatically prefix the customer accounts with a prefix and convert them to lower case. Note that the username rewriting happens using a script in host context. Rewriting won't work in scripts anywhere else.

9 References

- draft-grant-tacacs-02.txt - The TACACS+ Protocol (Version 1.78)
- RFC8907: The Terminal Access Controller Access-Control System Plus (TACACS+) Protocol

10 Copyrights and Acknowledgements

Please see the source for copyright and licensing information of individual files.

- **The following applies if the software was compiled with OpenSSL support:**
  This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).
  This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).
- **MD4 algorithm:**
  The software uses the RSA Data Security, Inc. MD4 Message-Digest Algorithm.

- **MD5 algorithm:**

  The software uses the RSA Data Security, Inc. MD5 Message-Digest Algorithm.

- **If the software was compiled with PCRE (Perl Compatible Regular Expressions) support, the following applies:**

  Regular expression support is provided by the PCRE library package, which is open source software, written by Philip Hazel, and copyright by the University of Cambridge, England. (ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/).

- **The original tac_plus code (which this software and considerable parts of the documentation are based on) is distributed under the following license:**

  Copyright (c) 1995-1998 by Cisco systems, Inc.

  Permission to use, copy, modify, and distribute this software for any purpose and without fee is hereby granted, provided that this copyright and permission notice appear on all copies of the software and supporting documentation, the name of Cisco Systems, Inc. not be used in advertising or publicity pertaining to distribution of the program without specific prior permission, and notice be given in supporting documentation that modification, copying and distribution is by permission of Cisco Systems, Inc.

  Cisco Systems, Inc. makes no representations about the suitability of this software for any purpose. THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

- **The code written by Marc Huber is distributed under the following license:**

  Copyright (C) 1999-2022 Marc Huber (Marc.Huber@web.de). All rights reserved.

  Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

  1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
  2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
  3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment:

     This product includes software developed by Marc Huber (Marc.Huber@web.de).

     Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

  THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL ITS AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.