NAS requirements

This page contains information about Network Access Server (NAS) requirements for connecting to SyCes.

SyCes uses a RADIUS server for centrally authenticating users and for accounting. Authentication of users against RADIUS is described in RFC2865. How accounting is done is described in RFC2866.

These are the specifications for implementing a Network Access Server (NAS) that communicates with SyCes. Within this document the two terms NAS and gateway are used in same meaning.

Captive Portal

A captive portal (CP) redirects unauthenticated users to a login form. Two different types (internal, external) of CPs may be implemented. At least one CP should be configurable per Gateway. In enterprise environments it should be possible to define multiple CPs and assign them to SSIDs (wireless), VLANs (wired) or physical interfaces.

Common Requirements

Independently of implemented CP type following features should be implemented.

- Idle Timeout
  Time in minutes after which a user should be disconnected if no data has been sent or received from WAN-connection. After disconnecting user has to login with his credentials again.
- Hard Timeout
  Time in minutes after which a user should be disconnected. After disconnecting user has to login with his credentials again.
- Reauthentication Time
  time in seconds after NAS reauthenticates user with given credentials automatically. If radius responds with an Access-Reject-Packet then user has to be disconnected, otherwise no change should be done. This feature is similar to CoA but is more secure as clients do not need incoming firewall rules. SyCes does not support CoA.
- Accounting Period
  time in seconds after which accounting packets will be sent to RADIUS-server
- Walled Garden Pages
  It should be possible to define multiple hosts and domains which should be accessible without authentication. This is required for payment process of self service portal
- Whitelist
  This list should contain MAC-Addresses which should have WAN access without authentication, e.g. VIPs
- Parallel Sessions
  It should be possible to configure a maximum number of parallel logins per username e.g. if a user wants to use his tablet and smartphone with same account.

Internal Captive Portal

This type of CP is located on the NAS. Users enter username and password and submit form to NAS. The NAS performs an authentication request to the configured RADIUS server. For internal captive portals following information needs to be stored on NAS:

- Domain
  Clients are distinguished by the domain. Inside SyCes every username has following format: user@domain
  For convenience gateway should add the postfix “@domain” to the username in every RADIUS-Request.
- Password
  If client wants to use the voucher system of syces it should be possible to configure the voucher password within the gateway. Users do not need to enter passwords any more, as all vouchers have same passwords.

External Captive Portal

This type of CP is located on SyCes-Server. Therefore we need only following information on Gateway:

- External Captive Portal URL
  URL where external CP is stored. SyCes provides appropriate information in administration frontend.

For external CPs an optionally API should be implemented which speeds up login process.

RADIUS configuration

- Radius-Server (authentication)
  Server, which is used for authentication. May be either a hostname or an ip-address. Hostnames are preferred over ip-addresses.
- Authentication-Port
  UDP-Port which is used for authentication on RADIUS-Server. [Default: 1812]
- Radius-Server (accounting)
  Server, which is used for accounting. May be either a hostname or an ip-address. Hostnames are preferred over ip-addresses. Different Servers are not required, but at least one Radius-Server (with 2 different ports) is required.
- Accounting-Port
  UDP-Port which is used for accounting on RADIUS-Server [Default: 1813]
- Shared-Secret
  Transactions between the client and RADIUS server are encrypted with a shared secret with a minimum length of 16 characters. It is used for both authentication and accounting.

Radius Packets

1. No Keep-Alives
   No Keep-Alive packets should be sent to test if the server is alive. This adds to load without

providing useful information.
Monitoring will be done by Synergy Systems GmbH. In case of a system crash the team willl start working on regaining the functionality anyway.

Use NAS tools like *radtest* to find out whether the radius server or your implementation causes problems.

Radius Authentication

Access Request

The access-request packet sent by the NAS needs the folllowing attributes :

- User-Name (RFC 2865 5.1)
  A maximum of 30 characters plus '@' plus a maximum of 19 characters for the domain (<username>@<domain>), makes a total of maximal 50 characters. Treated as case-insensitive.
- User-Password (RFC 2865 5.2)
  1 to 25 characters
- NAS-IP-Address (RFC 2865 5.4)
  External NAS IP-Address
- NAS-Identifier
  Name of NAS. Used for limit accounts to specific hosts
- NAS-Port (RFC 2865 5.5)
  physical port number
- NAS-Port-Type (RFC 2865 5.41)
  e.g
  15 : Ethernet
  19 : Wireless - IEEE 802.11
  see RFC

Any other attributes will currently be ignored.

Access Accept

In case of a successful authentication the radius server sends an acces-accept packet that may contain the following attributes::

- Session-Timeout (RFC 2865 5.27)
  session limit in seconds
- Reply-Message (RFC 2865 5.18)
  - XYM -volume limit in MiB

The NAS should use one of the following method:

1. Either use the received attributes to find out when to stop the session
   or

2. the NAS regularly retries to get users authenticated and stops the session when this fails

The manufacturer may decide which method to chose. The first one produces less traffic, but doesn't keep up to the frontend functionalities like a volume check. The second one is more flexible. The NAS can't rely on receiving one of the above attributes (see RFC2865 4.2. Access Accept). Other attributes are currently not used.

Access Reject

Radius Accounting

Accounting Start

The Accounting-Start packet needs to be generated right after a successful authentication.

It consists of an Accounting-Request (RFC 2866 4.1) with the following atttributes:

- Acct-Status-Type (RFC 2866 5.1)
  “Start”
- User-Name (RFC 2865 5.1)
  A maximum of 30 characters plus '@' plus a maximum of 19 characters for the domain (<username>@<domain>), makes a total of maximal 50 characters. Treated as case-insensitive.
- NAS-IP-Address (RFC 2865 5.4)
  External NAS IP-Address
- NAS-Port (RFC 2865 5.5)
  physical port number
- NAS-Port-Type (RFC 2865 5.41) (optional)
  e.g
  15 : Ethernet
  19 : Wireless - IEEE 802.11
  see RFC
- Framed-IP-Address (RFC 2865 5.8)
  User IP address (Client).
- Acct-Session-Id (RFC 2866 5.5)
  Unique Session-ID to identity the current session and update the counters
- Called-Station-Id (RFC 2865 5.30)
  other than in RFC: MAC address of gateway or wireless controller
- Calling-Station-Id (RFC 2865 5.31)
  other than in RFC: MAC address of client

Apart from the attributes marked as optional all other attributes have to be implemented due to §113 TKG.

Interim Update

With Interim Updates volume based accounts can be handled. They are optional, but recommended. With UDP protocol it is possible that packets get lost, therefore it is recommended to always send interim-update packets. And it is possible to contiunally inform the user about the reamining volume and time.

In an Accounting-Update packet the following attributes have to be sent:

- Acct-Status-Type (RFC 2866 5.1)
  “Interim-Update”
- User-Name (RFC 2865 5.1)
  A maximum of 30 characters plus '@' plus a maximum of 19 characters for the domain (<username>@<domain>), makes a total of maximal 50 characters. Treated as case-insensitive.
- NAS-IP-Address (RFC 2865 5.4)
  External NAS IP-Address
- Acct-Input-Octets (RFC 2866 5.3)
  Input volume in bytes within a user session.. According to RFC this should only be sent with a Stop-Packet, but SyCes also takes it into account in Interim-Update packets. NAS must always send the total volume from the beginning of the session, not only the volume since the last interim-update.
- Acct-Output-Octets (RFC 2866 5.4)
  Output volume in bytes within a user session.. According to RFC this should only be sent with a Stop-Packet, but SyCes also takes it into account in Interim-Update packets. NAS must always send the total volume from the beginning of the session, not only the volume since the last interim-update.
- Acct-Session-Id (RFC 2866 5.5)
  Unique Session-ID to identity the current session and update the counters
- Acct-Session-Time (RFC 2866 5.7)
  Duration of session in seconds. According to RFC this should only be sent with a Stop-Packet, but SyCes also takes it into account in Interim-Update packets. NAS must always send the total duration from the beginning of the session, not only the duration since the last interim-update.
- Called-Station-Id (RFC 2865 5.30)
  other than in RFC: MAC address of gateway or wireless controller
- Calling-Station-Id (RFC 2865 5.31)
  other than in RFC: MAC address of client
- Framed-IP-Address (RFC 2865 5.8)
  user IP address (Client).
- Vendor-Specific (RFC 2865 5.26)
  When this attribute is NOT sent the RADIUS-Server assumes that Acct-Session-Time, Acct-Output-Octets und Acct-Input-Octets contain deltas other to RFC.

Accounting Stop

The Accounting-Stop-Paket must be sent directly after session end. It consists of an accounting-Request (RFC 2866 4.1) with the following attributes:

- Acct-Status-Type (RFC 2866 5.1)
  “Stop”
- User-Name (RFC 2865 5.1)
  A maximum of 30 characters plus '@' plus a maximum of 19 characters for the domain (<username>@<domain>), makes a total of maximal 50 characters. Treated as case-insensitive.

- NAS-IP-Address (RFC 2865 5.4)
  External NAS IP-Address
- Acct-Input-Octets (RFC 2866 5.3)
  input volume in bytes within a session
- Acct-Output-Octets (RFC 2866 5.4)
  output volume in bytes within a session
- Acct-Session-Id (RFC 2866 5.5)
  Unique Session-ID to identity the current session and update the counters
- Acct-Session-Time (RFC 2866 5.7)
  duration in seconds
- Acct-Terminate-Cause (RFC 2866 5.10) (optional)
  Cause of session termination.
- Called-Station-Id (RFC 2865 5.30)
  other than in RFC: MAC address of gateway or wireless controller
- Calling-Station-Id (RFC 2865 5.31)
  other than in RFC: MAC address of client
- Framed-IP-Address (RFC 2865 5.8)
  user IP address (Client).

Apart from the attributes marked as optional all other attributes have to be implemented due to §113 TKG.