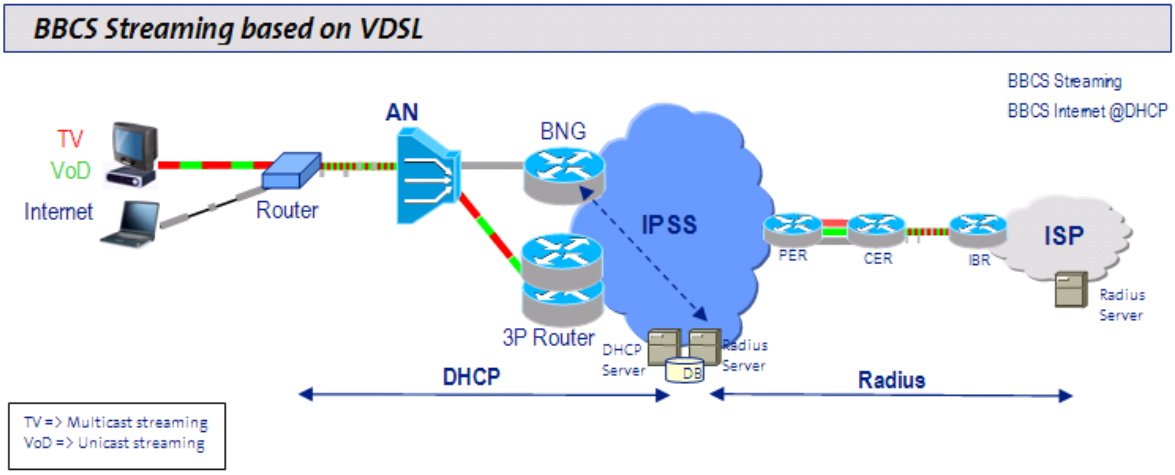
# Supporting Document DHCP

## INHALT

# 1 Class of Service

## 1.1 Streaming

BBCS Streaming allows the ISP to transfer video data in a continuous stream across the Swisscom backbone network. For BBCS Streaming, the streaming packets are prioritised above the internet packets in the Access Node (AN) both towards the End User and towards the ISP connectivity link. The service is based on the BBCS internet service (DHCP).




- The BBCS Streaming service is only offered with BBCS Private Internet access based on DHCP.
- The service supports all access technologies.
- BBCS Streaming is only available with the Premium Plus service level for the connectivity part.
- BBCS Streaming consists of the combination of an access and a connectivity part.
- The ISP is responsible for setting the correct bits in the packet.
- The BBCS Streaming service consists of 2 different types of Streaming Traffic.
- Multicast: The ISP converts the signal into digital IP packets at its head end. The IP video stream is transmitted in multicast over the Swisscom network.
- Unicast: In the case of unicast streaming, the ISP offers on-demand content and this traffic is delivered as a unicast IP stream.

## 1.2 Real time traffic

BBCS real-time traffic (formerly also known as Voice over Broadband or VoBB) allows the ISP to transfer voice traffic across the Swisscom backbone network. The voice packets are prioritised in the BNG both towards the AN and towards the ISP connectivity link. The ISP is responsible for setting the correct bits in the packet which are then queued in the BNG accordingly. The real time service is based on BBCS Internet with Service Termination DHCP.

A real time access enables the ISP to transport voice packets across the Swisscom backbone network with the highest priority. The real time service is only offered in conjunction with an existing BBCS Internet access connection. All types of access technology (ADSL, VDSL, BX, XGS-PON) are supported.

Real time is only available with the Premium Plus service level for the connectivity part. The real time product consists of the combination of an access and a connectivity part.

# 2 Connectivity

## 2.1 IP Pool Management

The ISP is responsible for providing Swisscom with a range of Public IP addresses or If the ISP wishes to use private IPv4 addresses in at least one of the two IP pools, Swisscom will allocate the corresponding range after consultation. The allocation of the IP addresses from these ranges to the end user will be managed by Swisscom. The ISP is also responsible to ensure that sufficient IP addresses are available in the pool.

The ISP has the possibility to manage this IPv4 ranges via WSG-IP Pool Management. Updates to IPv4 pool can be done via this access.

If the number of free IPv4 addresses is lower than 10 – 20%, the following will occur:

- Low IP threshold: The ISP receives a message by e-mail and SMS based on three ISP defined threshold values. The ISP is then responsible for defining new IPv4 address ranges via the WSG.
  → No impact on end user.
- IP shortage: Insufficient IPv4 addresses available to service all end users. The ISP is urgently requested by e-mail or SMS to define new address ranges using the WSG.
  → 'Surplus' End Users cannot log in.

For IPv6 Swisscom will receive once the "lifelong" range from the ISP in initial setup and deploy them.

## 2.2 Subscriber & service classes (IPv4 only)

The following subscriber classes are supported:

- Flat: 3P subscribers with the traditional model offering flat internet access

Every service class (internet, real time, unicast [i.e., retransmissions], multicast, etc.) is accounted in up- & downstream direction for each subscriber class.

Note:

Downstream: ISP -> Swisscom -> Subscriber

Upstream: Subscriber -> Swisscom -> ISP

## 2.3 Marking

The marking occurs on the connectivity link based on the source/destination IP addresses.

The customer must deliver the appropriate IP ranges for each of the services.

Therefore, the ISP must communicate the IP-address range of the different servers. Note that these ranges must not overlap.

All unknown IP packets (with unknown source address) are remarked to best effort traffic. This includes also all L2TP packets.

## 2.4 QoS in the IPSS network

In the Swisscom network, a transparent end-to-end QoS solution is implemented to ensure appropriate treatment of the different 3P traffic types. In this context, transparency means that any existing L3 packet markings (DSCP, IP precedence) are passed transparently (untouched) through the Swisscom network and do not have any influence upon the QoS treatment of the packet. This is achieved by solely using L2 packet markings on each network element.

Four main traffic classes are supported within the Swisscom network:

| Traffic Class | DSCP Value | Service |
|---|---|---|
| Best effort | Default | 3P Internet |
| Priority | AF31 | 3P VoD (Unicast, TCP) |
| High Priority | CS2 | 3P TV (Multicast) |
| Real Time | AF41 | 3P VoIP signalling, 3P Video Conference Signalling |
| | EF | 3P VoIP, 3P Video Conference |

Each of these four main traffic classes are mapped into its own queue within each network element.

Rather than allocating absolute bandwidths to each queue, the relative bandwidth is adjusted using ratios between the queues to achieve QoS differentiation.

The real-time class is always served first (strict priority). After this queue has been emptied, the high priority queue gets the majority of the remaining bandwidth, e.g. 80 %, the priority queue 18%, and the best effort queue gets whatever is left.

In addition to this queuing scheme, intelligent dropping mechanisms, such as WRED (Weighted Random Early Detect) are implemented (except for the real time queue and the high priority queue).

The 3-play classes are assigned to these queues as follows:

| | |
|---|---|
| Real time traffic (VoIP) | Real Time |
| Multicast (TV), Control | High Priority |
| VoIP signalling, VoD | Priority |
| uni- and multicast internet, L2TP | Best effort |

## 2.5 Port Filtering

To prevent dhcp Denial-of-Service attacks on the dhcp clients in Swisscom network, the following ports are blocked:

- UDP BOOTP client (68).
- UDP BOOTP server (67).

## 2.6 BGP routes for IPoX subscribers

### 2.6.1 Upstream traffic for Internet traffic (Swisscom -> ISP)

The hub & spoke design for subscribers terminated with dhcp ensures that every upstream packet is passed to the ISP's equipment. No direct peer-to-peer communication among subscribers is possible. This enables the ISP to offer value add services, such as firewalls.

For upstream unicast traffic the ISP must propagate the next-hop routes. No other routes are required for customers terminated with dhcp. No other route will be propagated into the ISP's VPN.

| Parameter | ISP |
|---|---|
| Next-hop route for "Flat subscribers" | 10.138.187.7 mask 255.255.255.255 |

Table 1: Upstream traffic for Internet traffic

By propagating these next-hop routes all upstream subscriber traffic will be delivered on the associated CER interface as long as the interface is up (policy-based routing).

### 2.6.2 Downstream traffic direction (ISP-> Swisscom)

For the subscriber downstream traffic, the ISP will get the summary routes of its IP address pools.

## 2.7 Multimedia traffic BGP routes

If the ISP provides triple play services, then he has to announce the summary address of the multimedia network.

## 2.8 BGP routes for RADIUS service for subscribers terminated by DHCP

The ISP must propagate its radius server addresses.

Swisscom will propagate the relevant radius addresses (proxy radius).

→ Please refer to the connectivity order form.

## 2.9 Redundancy and load balancing between PoPs

Connectivity via two PoPs provides redundancy for both unicast and multicast traffic.

Additionally, unicast traffic can be load balanced between the two connections.

Note that proactive load balancing of multicast traffic is not foreseen. The shortest path trees select the necessary PoP connection. In the case of a connectivity link failure the shortest path trees are reorganized and they use only the remaining connection.

Redundancy for DHCP subscribers is provided as follows:

Upstream traffic (Swisscom -> ISP):

- All traffic follows either the next-hop routes or the multimedia/real time routes that are propagated via both connectivity links (PoPs).
- In the upstream direction, BNG based load balancing is implemented. Load balancing is performed based on regional criteria.

Downstream traffic (ISP -> Swisscom):

- The pool addresses are announced via both PoP connections (eBGP).
- Downstream unicast load balancing is based on “AS-Path prepend”. The AS-Path will be prepended on one PoP for approximately 50% of the IP prefixes (addressing the IP-Pools configured on the BNG. On the companion PoP, the other half of IP prefixes will be assigned a prepended AS-Path. This results in equal load balancing if the ISP bases its routing decision on the AS-Path.

## 2.10 Policing of downstream real time traffic on the connectivity link

An ISP can order the real-time service only in combination with Premium Plus connectivity. Load balancing of real-time traffic will be handled in the same manner as described above. To ensure that VoIP traffic will be treated as real-time traffic in the network, it is necessary to limit the amount of EF marked traffic in the core network. As an extreme example, it is impossible to prioritise Voice traffic in a network with a load of 100% real-time traffic. Therefore, Swisscom has to protect its core network from an overload of Real-Time traffic.

## 2.11 Parallel L3 links for high bandwidth connections

If the service requires a bandwidth of more than one 10 Gbps (respectively more than 100 Gbps) Interface, Swisscom uses LACP bundle interfaces.

### 2.11.1 Multicast Implementation and Protocols (PIM v2, MSDP)

Both Swisscom and the ISP have to operate their own PIM sparse version 2 domain. The PIM border is the interface CER – IBR (ISP Border Router). Both domains are assigned their own Rendezvous Points (RPs).

The multicast sources are always located in the ISP's domain.

The multicast receivers are always BBCS subscribers. The Client of each subscriber may initiate IGMP Join/Leave messages that are forwarded by the CPE to the appropriate Swisscom equipment.

Normally, the ISP's sources are always transmitting and are therefore registered at the ISPs RPs. MSDP (Multicast Source Discovery Protocol) ensures communication of those active streaming sources from the ISP RPs towards the Swisscom RPs. MSDP propagates these active sources towards all configured MSDP Peers using SA (Source Active) messages.

Redundancy:

For redundancy Swisscom implements two identical RPs (same RP address on different routers). The ISP may also implement two identical RPs. It is required that each ISP_RP peers with each Swisscom_RP (full mesh between the two domains). Additionally, the ISP may implement "Anycast" between its RPs. Anycast is based on MSDP and ensures communication of active multicast sources (SA-Messages) between two ISP RPs which are configured with the same IP address.

Required MSDP sessions:

ISP_RP1 --- Swisscom_RP1

ISP_RP1 --- Swisscom_RP2

ISP_RP2 --- Swisscom_RP1

ISP_RP2 --- Swisscom_RP2

_____

ISP_RP1 --- ISP_:RP2 (Anycast)

As an important additional requirement, the sending MSDP peers of the ISP must always be the originating RP. No separation of RP and MSDP Peer is allowed. This is required by our network in order to avoid MSDP-RPF checks.

The multicast group address range the ISP may use is assigned by Swisscom.

The total number of multicast groups and the total multicast bandwidth is limited to the numbers agreed between Swisscom and the ISP.

| Parameter | ISP |
|---|---|
| range of multicast group addresses | 233.a.b.c – 233.d.e.f |
| number of multicast group addresses | tbd |
| multicast bandwidth | tbd |

Table 2: Multicast Implementation and Protocols

The necessary routing information between the ISP and Swisscom for correct multicast operation is listed in chapter 3.

### 2.11.2 Summary of BGP routes to be delivered by the ISP

- Next-hop addresses for upstream internet traffic
- Summary address of the real-time platform
- Summary address of the multimedia network
- Radius addresses for DHCP model
- MSDP peer addresses for SA messages
- RP address of the ISP
- MCast source addresses (for RPF check)
- Summary address(es) of the redundant server network(s) (DNS, NTP...)

### 2.11.3 Summary of BGP routes that will be delivered by Swisscom

- IP address pool prefixes for downstream subscriber traffic
- Proxy radius addresses for DHCP model
- MSDP peer addresses for SA messages

## 2.12 Security

### 2.12.1 Allowed Protocols to access the Swisscom Infrastructure

For correct operation the following protocols are allowed to access Swisscom infrastructure addresses:

- MSDP
- Radius

All other traffic to and from the infrastructure IP addresses will be blocked on the CER and on the BNG.

### 2.12.2 Port Filtering for the DHCP Subsrcibers

To prevent DHCP Denial-of-Service attacks to the DHCP clients in Swisscom network, the following ports are blocked on the ISP connectivity link:

- UDP BOOTP client (68)
- UDP BOOTP server (67)

# 3 Access Link

## 3.1 Overview

The Access Link uses either ADSL/VDSL/BX/XGS-PON. The BNG is responsible for the accounting updates through RADIUS client. The IP address assignment, in the encapsulation flavour will be done by the DHCP server.

Policing and shaping to enforce the traffic to the bought internet rate will be done on the BNG. Multimedia traffic is never shaped.

## 3.2 DHCP

### 3.2.1 Introduction

The session is always terminated by Swisscom. The IP addresses (of the ISP's pool) will be distributed by the DHCP Server which is also located at Swisscom.

### 3.2.2 DHCP Ruleset

The following are the guidelines for the successful operation of DHCP modems for the BBCS service:

- Clients: A maximum number of 1 client is permitted to send DHCP message requests towards the IPBB Infrastructure.

### 3.2.3 Add-on for TR-069 CPE Management support

#### 3.2.3.1 Introduction

Sending DHCP Options 43.1 and 43.2 to the CPE is supported in order to simplify ISP CPE management process using TR-069 standard.

The DHCP Option 43 is called "Vendor Specific Information" in RFC 2132.

DHCP Option 43 implementation is defined in TR-069_Amendment-2 for ACS Discovery.

TR-069 implementation requires Encapsulated Vendor-Specific Options that is also defined in RFC.

Swisscom DHCP server will ignore, not process or answer DHCP INFORM messages intended to re-discover the ACS URL.

#### 3.2.3.2 Attribute definition

Current implementation supports two encapsulated vendor-specific option numbers "1" (URL of the ACS) and "2" (Provisioning code) as required in TR-069 standard.

No other encapsulated vendor-specific option numbers can be used by ISP or are specified in TR-069.

According to TR-069 the URL of the ACS is defined as string (256) and provisioning code as string(64).

Null strings are not expected for both sub-options.

The URL of the ACS is configurable per ISP code, pool type and service model.

If an ISP has more than one service model activated for a particular ISP code it will be possible to configure separate URLs per service model.

An ISP is identified in BBCS by its ISP code. If a particular ISP uses more primary ISP codes, different URLs for each code are possible. Secondary ISP code will map - use the primary ISP code configuration.

If an ISP requests Option 43 activation for a specific ISP code all new subscriber CPEs will receive this DHCP option during the DORA or RENEW/REBIND process, it will not be possible to selectively activate this DHCP option per subscriber.

Swisscom will not restrict http or https usage for ACS URL. The http and https based URLs can't be combined for the same ISP code and Product technology.

The Provisioning code content is subscriber specific and it will be set to "<ISP Code>:<Vline ID>".

The option 43 must be implemented for all BBCS DHCP based products.

A CPE doesn't need to identify itself to the Swisscom DHCP server as supporting this method by including the string “dslforum.org” (dhcp-class-identifier set to all lower case) anywhere in the vendor class identifier (DHCP option 60). Swisscom DHCP server will not evaluate DHCP option 60 to identify if option 43 is to be send or not. The option 43 is send to every ISP CPE for a configured service model.

If an ISP doesn’t need TR-069 standard this functionality can be switched off. If an ISP doesn’t request activation the functionality is switched off per default.

#### 3.2.3.3 Attribute example

The following example can be used as a reference.

BBCS copper based access Pool1

Option 43.1 (option number 1) data item: **http://pool1-isp-defined-url.ch/pool1-isp-defined-path**

Option 43.2 (option number 2) data item: **100026:1234567890**

BBCS copper based access Pool2

Option 43.1 (option number 1) data item: **https://pool2-isp-defined-url.ch/pool2-isp-defined-path**

Option 43.2 (option number 2) data item: **100026:1234567890**

Note that ISP must inform Swisscom in advance which URLs must be configured. Changing an existing URL is also possible but it requires a planned data migration and agreed service window.

## 3.3 Downstream QoS

In the downstream direction, the traffic is shaped and prioritized according to the figure below.

The queues will be defined as required by the subscribed services. Only the best-effort and real-time queue will be built.

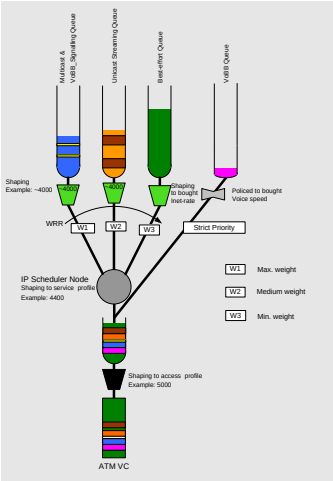



Figure 1: Egress QoS priorisation and shaping model on the BNG

Traffic will be classified and assigned to the shown queues according to the classification rules imposed on the ISP connectivity link.

Rather than allocating absolute bandwidth to each queue we will allocate relative bandwidth ratios between the queues in a Weighted Round Robin (WRR) Scheduler to achieve the desired traffic differentiation.

| Class | Queue | Relative weight |
|---|---|---|
| Real-time Traffic | Strict | Strict |
| Streaming Multicast &<br>Real-time Signalling | Queue 1 | Maximum |
| Streaming Unicast | Queue 2 | Medium |
| Internet Best-Effort | Queue 3 | Minimum |

Table 3: Downstream QoS of 3P Traffic Classes

During overload situations the following scheduling mechanism is applied:

- The Strict queue is always serviced (up to the subscribed real-time bandwidth). This is necessary in order to achieve minimal jitter.
- As long as there are no bytes in the strict queue, Queue 1, Queue 2 and Queue 3 are serviced in a weighted round robin manner up to the respective limits.

Care must be taken by the ISP to avoid that the situation whereby higher prioritized traffic classes starve out other queues. However, through the relative weights within the WRR Scheduler and the policing per class, a minimum bandwidth is always available for the low priority queues.

Note that real-time signalling traffic is assigned to the same queue as Mulitcast Streaming traffic. It is the ISP's responsibility to avoid congestion within that subscriber queue (as long as the Multicast, real-time signalling and real-time traffic do not exceed the profile's bandwidth no quality degradation can occur).

## 3.4 Upstream Classification, QoS, Filtering and Policing

The main bottle-neck in the upstream direction is the DSL line. The ISP is responsible for the necessary QoS implementation on the subscriber's CPE. It is strongly recommended for a real-time based VoIP service that the ISP implements at least two queues on the CPE: one strict priority queue (or heavy weighted/prioritized queue) for real-time and one for the rest of the traffic.

Note that the ISP is not requested to mark the upstream traffic. For the QoS implementation in the IPBB network, the upstream traffic is classified on the BNG based on the destination IP address and/or destination. L2-marking is used within the Swisscom network to achieve L3 TOS/DSCP transparency i.e. the Customer's TOS bits are not changed to fulfil the internal classification and prioritisation.

At the BNG, the upstream traffic is assigned to one of the following classes and rate-limited (policed) where necessary:

| Class | Classification Criteria |
|---|---|
| Real-time Traffic | destination address = voice GW |
| Real-time Signalling | destination address & protocol/port for voice signalling |
| Streaming Control | destination address of streaming platform |
| Internet Best-Effort | any other IP traffic |

Table 4: 3P Upstream Classification and Policing of the 3P Traffic Classes

Additionally, the following traffic policies are applied:

- Traffic with a Swisscom infrastructure address is blocked completely.
- Multicast packets, with the exception of IGMP messages, are blocked.
- Unicast traffic belonging to the Best-Effort Class that has passed the ingress filtering rules, is policed to the bought internet upstream rate and policy-routed towards the desired next-hop address 10.138.187.7 . This is to force unicast traffic to be always forwarded via the ISP as requested by the Hub&Spoke principle.
- Real-time or VoD traffic is routed to the respective destination addresses propagated by the ISP via BGP.

### 3.5 Multicast (IGMP)

Subscribers are requested to join the desired Multicast Group by means of IGMP.

IGMP is supported, version 2 and version 3 (no PIM-SSM). Swisscom will not prevent the subscribers from joining any available Multicast-Group. The ISP is requested to protect its Multicast streams via a DRM system to prevent Subscribers from extracting data from Multicast-Groups they have not paid for.

On the Swisscom side IGMP immediate-leave will be configured to allow for fast channel change times.

A Subscriber can join to a maximum of four Multicast-Groups concurrently.

In the upstream direction, no multicast data traffic will be accepted.

The multicast replication point will be the AN.

# 4 Subscriber Identification

## 4.1 Introduction

For PPP terminated DSL connections the ISP will still receive the username@realm.ch information in the access request. For DHCP based connections , the username information will have the following form: The User-Name will be set to the Vline-Id number.

The RADIUS password field will be set to a default value (in line with the appropriate RFC).

## 4.2 Indentifying IPoE subscribers

The DHCP option 82 will be used for authentication. Option 82 is encoded in the RADIUS attribute DHCP options [26-55]. Within this option the sub-option known as “circuit-identifier” will be used to authenticate the subscriber.

## 4.3 Interoperability Issues

The Swisscom RADIUS servers must communicate with many other systems including ISP RADIUS servers. Any misinterpretation or incompatibility in the information being passed will result in lost functionality, delays, and additional costs. It is highly recommended that extensive end-to-end testing and a beta test period be included in the overall project plan.

The Swisscom radius supports Load Balancing to improve the performance and the reliability of radius communication.

# 5 Radius

The ISP is responsible for all Lawful Interception Logs.

## 5.1 Subscriber Identification

The service subscriber is identified to the ISP using the User-Name AVP with the following values

a. Vline-Id for DHCP

## 5.2 Interoperability Issues

The Swisscom RADIUS servers must communicate with many other systems including ISP RADIUS servers. Any misinterpretation or incompatibility in the information being passed will result in lost functionality, delays, and costs to resolve. It is highly recommended that extensive end-to-end testing and a beta test period be included in the overall project plan.

## 5.3 Swisscom RADIUS Server Authentication and Authorization

All these AVPs can be optionally sent by the ISPs.

The Acct-Interim-Interval AVP determines how often ISP will receive accounting messages. The value to send should be an integer, this represents the number of seconds between each accounting records.

Interim accounting record forwarding can be enabled for Light and Flat users using different range of value. To disable this feature, the Acct-Interim-Interval AVP should be sent with a value set to zero.

Any invalid AVPs will be discarded.

Any invalid AVPs value for Acct-Interim-Interval will be replaced by the appropriate default value.

### 5.3.1 AVPs from ISP RADIUS Server for DHCP

| Radius Attribute | Accepted Values | |
|---|---|---|
| Unisphere-Ingress-Policy-Name | y1<br>y2<br>y3 | |
| Acct-Interim-Interval | 0<br>>= 10800 | disables interim accounting messages for the session<br>(Flat Users) seconds between interim accounting messages |

Table 5: AVPs from ISP RADIUS Server for DHCP over VDSL

### 5.3.2 Acct-Interim-Interval Values Applied by the Swisscom RADIUS Server

The Swisscom RADIUS server filters the Acct-Interim-Interval AVP to enforce the acceptable values and to apply default values as necessary. "AII" stands for Acct-Interim-Interval.

| **Subscription** | **Acct-Interim-Interval Value Sent by the ISP RADIUS Server** | | | | |
|---|---|---|---|---|---|
| | **No AII VSA** | **AII<=60** | **60<AII<=3600** | **3600<AII<10800** | **10800<AII** |
| Flat DHCP | 86100<br>(23h 55m) | 0 Disable | 3600<br>(1h) | 10800 (Default)<br>(3h) | Value from ISP RADIUS |

Table 6: Acct-Interim-Interval Values

### 5.3.3 Disabling Interim Accounting for DoA and DoV Cases

An Acct-Interim-Interval value of 0 should be in the Access-Accept to the Swisscom RADIUS Server in order to disable Interim Accounting for the corresponding subscriber. The disabling Interim Accounting may be subject to change in future BBCS releases due to Lawful Interception requirements.

### 5.3.4 Access-Accept AVP Disallowed from the ISP for DHCP

All AVPs from the ISP that are not on the allowed AVP lists will be filtered from the Access-Accept from the ISP.

## 5.4 Swisscom RADIUS Server Accounting

The BNG meters the sessions and services delivered to the end-user and then forwards the session information to the RADIUS server. Where required, the RADIUS server can also forward the RADIUS Accounting-Requests to other ISP RADIUS servers. Additional required accounting functionality

The DHCP service models have several unique aspects that impact accounting.

- accounting must be generated at the setup and takedown of a DSI.
- accounting must be tracked by Vline-Id.

### 5.4.1 Accounting AVP required by Billing

| Radius Attribute | Type | Notes |
|---|---|---|
| Acct-Session-Id | String (1-253 characters) | Generated by BNG to uniquely identify each session and make it possible to match all records for a session. |
| User-Name | String (1-253 characters) | Identifies the Vline-Id |
| NAS-Port-Id | String (1-253 characters) | Access ID |
| Date-Time | String (1-253 characters) | Date and timestamp of received accounting event. Encoded as yyyy:mm:dd:hh:mm |
| Acct-Input-Octets | Integer (4 unsigned octets) | Low order count of input traffic. |
| Acct-Output-Octets | Integer (4 unsigned octets) | Low order count of output traffic. |
| Class | String (1-253 characters) | Encoded information including service model and ISP identity. |
| Acct-Status-Type | String (1-253 characters) | Type of Accounting-Request.<br>Start<br>Stop<br>Interim |

Table 7: Accounting AVP required by billing

## 5.5 Failover and Load balancing

ISPs can choose one of the two concepts described below to interface their RADIUS servers with the Swisscom radius server.

### 5.5.1 Concept 1: Access to Redundant ISP RADIUS Servers

The radius server forwards RADIUS Access-Requests and Accounting-Requests to ISP RADIUS servers for DHCP service models. The logic table supports the configuration of both a primary RADIUS server and secondary RADIUS server for each ISP. If the RADIUS server times out a request to an ISP's primary RADIUS server it will then forward the request to the ISP's secondary RADIUS server.

– Server for Authentication and Accounting can be different.

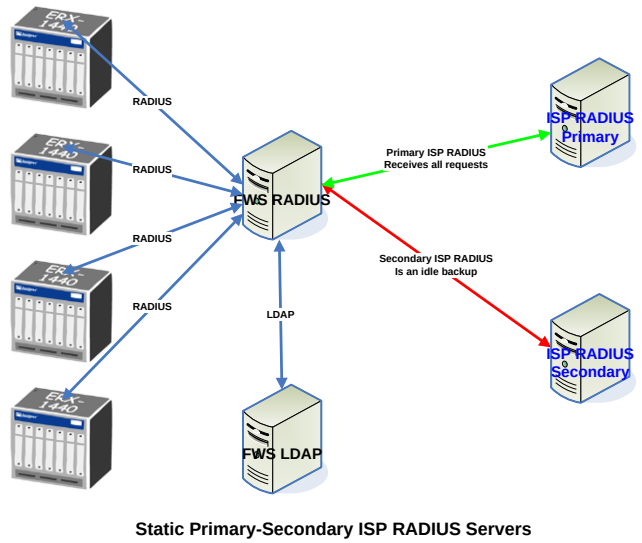



Figure 2: Access to redundant ISP RADIUS Servers

### 5.5.2 Concept 2: Dynamic Load balancing

The Swisscom RADIUS is seeking responses to its RADIUS requests to the ISP. It does not matter which of the ISP RADIUS servers responds to any given request. In the load balanced server model status on each of servers is maintained and requests are only forwarded to servers in the up state. This changes the ISP RADIUS server communication from a serial search process to a parallel communication process. The ISP RADIUS Load Balancing feature improves both the performance and the reliability of RADIUS communications with the ISP RADIUS servers. The ISP RADIUS Load Balancing feature improves scalability because the load can be shared equally among a pool of servers instead of handled by a single primary server. Server failures are detected and avoided through status checks, eliminating request timeouts in most cases.

- Limitation to 20 ISP radius servers.
- Servers for Authentication and Accounting can be different.

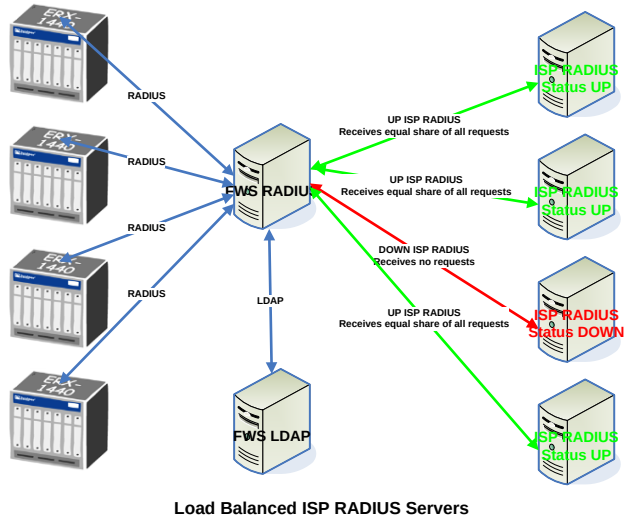



Figure 3: Dynamic Load Balancing

### 5.5.3 Fail-Safe for Inaccessible ISP RADIUS Server

If an ISP's RADIUS servers are all inaccessible and the request is recognizable as being DHCP then the user will be authorized and an Access-Accept will be returned to the BNG as configured in default values.

## 5.6 Services type identification by Class

The DHCP based Service Models will be encoded as follows.

| ISP Code | Vline-ID |
|---|---|
| e.g. 100099 | 10 digit<br>Eg:_1103312345 |

Table 8: Service type identification by Class

Example Class AVP for DHCP include100099_HBNG_BBCS_DHCP_1103312345

## 5.7 Appendices

### 5.7.1 Default DHCP Response upon ISP RADIUS Failure

The customers will be provisioned and connected like if the ISP was not sending anything back. The class attribute will have the "_FBI" string append to the normal Class.

Class = normalClass_FBI

A default "Acct-Interim-Interval= 10800" AVP will be added to the returned list to the BNG in case of a Flat user.

### 5.7.2 Common data

This lists the ports used between Swisscom RADIUS and ISP RADIUS.

| Source | Destination | Traffic Type | Port Number | Port configurable Y/N | Service Type |
|---|---|---|---|---|---|
| RADIUS | ISP | AAA/UDP | Can be defined per ISP | Y in RADIUS clients (Default Ports: 1812/1813) | Proxy RADIUS for AAA DHCP cases |
| ISP | RADIUS | AAA/UDP | Reply on random UNIX selected emitting ports | Only incoming port :Y in ISP RADIUS (Default Ports: 1812/1813) | Proxy RADIUS for AAA DHCP cases |

Table 9: Service type identification by Class

The following have to be communicated:

- shared secret agreement.
- Ip address of all the servers and ports number (default ports are preferred).

### 5.7.3 VISIO Schema

These Visio schema represent graphically the two cases:

- Radius authorization
- Radius accounting

#### 5.7.3.1 Radius authorization

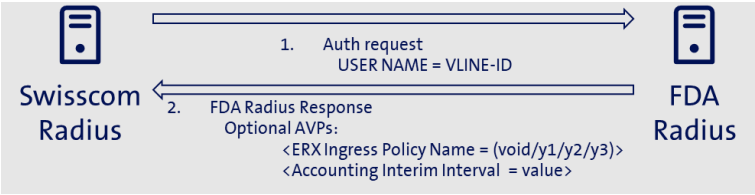



Figure 4: Radius authorization

### 5.7.3.2 Radius accounting


Figure 5: Radius accounting