International Journal of Computing and Network Technology
An International Journal

@ 2013 UOB
SPC, University of Bahrain

Traffic Offloading and Load Balancing to Enable Cloud Computing Connectivity

John Cartmell

InterDigital, Melville, New York, USA
Email Address: John.Cartmell@InterDigital.com

Received: 23 Oct. 2012, Revised: 1 Nov 2012; Accepted: 12 Nov. 2012

Abstract: In this paper we consider the connectivity of an end-user with the Cloud. We examine a method to perform traffic offloading and load balancing in a network comprised of both WiFi access points and Cellular cells to better enable this connectivity. We explain the introduction of a converged gateway (CGW) to manage both the traffic offloading from licensed to unlicensed spectrum and to perform the load balancing between the Cellular and WiFi spectrum. Furthermore, we detail the procedures that are performed by the gateway to enable these two features and conclude by providing examples of how the CGW enables the interactions between the end-user and a Cloud.

Keywords: component, IP Flow Mobility, femto-cell, WiFi AP, Converged Gateway; traffic offloading; load balancing, connectivity

I. Introduction

An essential component of Cloud Computing is Connectivity – without which the entire paradigm becomes useless. Providing constant, reliable and as-needed bandwidth is *the* critical enabler of Cloud Computing. In this paper we introduce the concept of the Converged Gateway (CGW) which enhances this enabler by collecting all available connectivity options at any given time and making the best use of them for the connectivity required to support the operations the end-user performs with the Cloud.

In addition, Cloud Computing provides a number of features such as computational services, access to data, use of software and storage of data. A main benefit of Cloud Computing is the end-user does not need to be concerned where the Cloud is located. However, heretofore, the end-user is concerned with how to connect to the cloud. Currently, the end-user must decide whether to use WiFi, Cellular, or some other access to reach the Cloud. Each of these connectivity options has its own limitations and advantages. WiFi does not have a guaranteed quality of service and suffers from uneven performance. Furthermore, a single WiFi AP not managed by a central network provider will not support user mobility outside the range of that single WiFi AP. However, WiFi typically enjoys higher data rates. Cellular technology, on the other hand, does support full user mobility to the bounds of the network operator’s coverage. It does support quality of service but can be bandwidth limited. Neither WiFi nor Cellular, alone, is a panacea with respect to connectivity.

We propose that the CGW is an essential extension of cloud computing since the CGW will hide which access is used to reach the cloud. Using a CGW, the end-user does not even have to know *how* they reached the cloud. In addition, benefits of Cloud Computing include higher reliability, less costly access, device and location independence and improved performance. The CGW managing both WiFi and Cellular accesses increases each of these benefits.

This paper describes the architecture of the CGW and the functionality within the CGW. It then describes the procedures that occur between the femto-cell and Mobile Core Network (MCN) and the CGWs role in those procedures. After this discussion, IP Flow Mobility (IFOM) [1] [2] is examined in detail and then several examples are provided.

For clarity sake, it is necessary to define femto-cell. A femto-cell is a small cellular base station, usually deployed within a home, a business, or a limited public location, such as a metro rail station. It connects to the mobile core network through a broadband connection, typically, and supports a limited number of users. It allows for the deployment of network coverage in small areas that may be underserved by existing macro-cells or areas that a business or person wants to control, such as their home or place of business.

II. CONVERGED GATEWAY

The Converged Gateway (CGW) is a device that sits at the edge of a Local Area Network (LAN) and has all the features and functions required to locally manage and control femto-cells and WiFi Access Points (APs). It is possible that the CGW software, femto-cell and WiFi AP are all separate devices. To explain the functionality performed by the CGW software and its interactions with other devices, this paper assumes the three entities as separate and distinct. This assumption assists in the explanation that is the remainder of this paper. However, the physical manifestation of a CGW for a product deployment would most likely incorporate the CGW software, femto-cell and WiFi AP in one unified appliance. For example, the unified device could be an enhanced set-top box provided by a cable operator or an enhanced femto-cell (with the CGW software and WiFi AP) provided by a cellular operator.

Despite sitting between a femto-cell and the MCN, there are no additional procedures or protocols that are encumbered onto either the femto-cell or MCN. Furthermore, the CGW has features and functions which allow for the seamless dynamic movement of an end-user’s connectivity with a Cloud from one radio access technology to another. The topology of the CGWs environment is shown in Fig. 1.

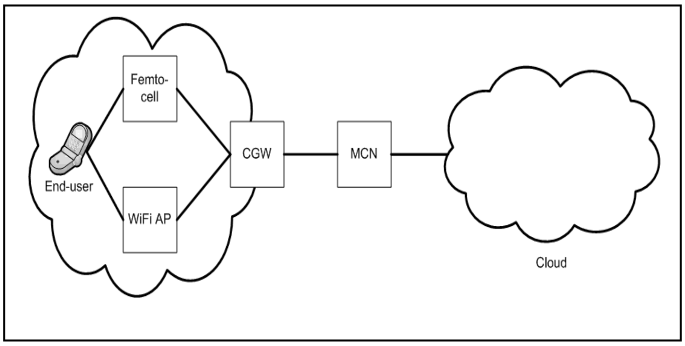

Figure 1. CGW Topology

There are three salient features of the CGW that allow it to manage the WiFi and cellular accesses and the flows that traverse these accesses. These features include:

- Transparent to both the MCN and femto-cell
- WiFi/3G association
- IFOM

A. CGW placement

The introduction of a CGW between a femto-cell and MCN, at the edge of a LAN, is transparent to both the femto-cell and MCN. No protocols or procedures require modification to allow the placement of the CGW between the femto-cell and MCN; however, it is necessary to properly provision the CGW so that it can act as an intermediary. The absence of a requirement to change any of the existing procedures and protocols is a significant advantage of the CGW solution.

To this end, the CGW will be provisioned with the security keys needed to establish a security association to both the femto-cell and the Secure Gateway (SeGW) at the edge of the MCN. The IPSec Security Associations (IPSec SA) that normally exists between the femto-cell and SeGW [3] will be split into two IPSec SAs. The first is between the femto-cell and the CGW. The second is between the CGW and the SeGW. It is expected that each interface would have unique keys. As a result of this configuration, the CGW acts as a proxy for the signaling between the femto-cell and MCN elements. When the femto-cell has a signal to send to the MCN, it sends it through the IPSec SA to the CGW. The CGW un-IPSecs the signal and then re-IPSecs the signal into the SA with the SeGW. When the SeGW receives the signal, it un-IPSecs it and forwards it into the MCN. When an element within the MCN has a signal to send to the femto-cell, it occurs in a similar fashion.

A similar mechanism occurs when data is sent between an end-user and a Cloud. As the data travels through the cellular network a GPRS Tunneling Protocol (GTP) tunnel will be used between the femto-cell and Serving GPRS Support Node (SGSN). This tunnel is used to ferry data between the femto-cell and SGSN. With the CGW in place, there are two GTP tunnels, one between the femto-cell and CGW and the other between the CGW and SGSN. Downlink data is sent from the SGSN via a GTP tunnel to the CGW. The CGW terminates the GTP protocol and places the data packet into the GTP tunnel between the femto-cell and CGW. The femto-cell receives the packet and delivers it to the end-user. Similarly, an uplink packet is sent from the femto-cell to the CGW via a GTP tunnel. The CGW terminates the GTP protocol and places the packet into the GTP tunnel that exists between the CGW and the SGSN.

The IPSec SAs and GTP tunnel configuration are shown in Fig. 2.

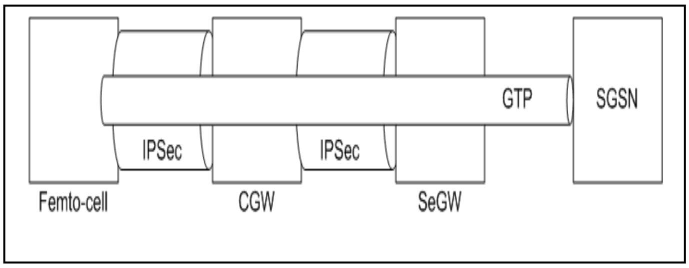

Figure 2. IPSec and GTP Tunnels

B. CGW Initialization and Provisioning

The CGW is powered on. As a result of the device being powered on, it will receive a local IP address and start the various processes that are used by the femto-cell and the WiFi AP. It is assumed that the LAN where the CGW resides has the ability to provide a LAN-based IP address.

C. Existing Femto-cell procedures in the presence of CGW

A femto-cell must perform certain procedures in order to access the Mobile Core Network (MCN) nodes. The MCN nodes that the CGW communicates with are shown in Fig. 3 as well as the functional components within the CGW.

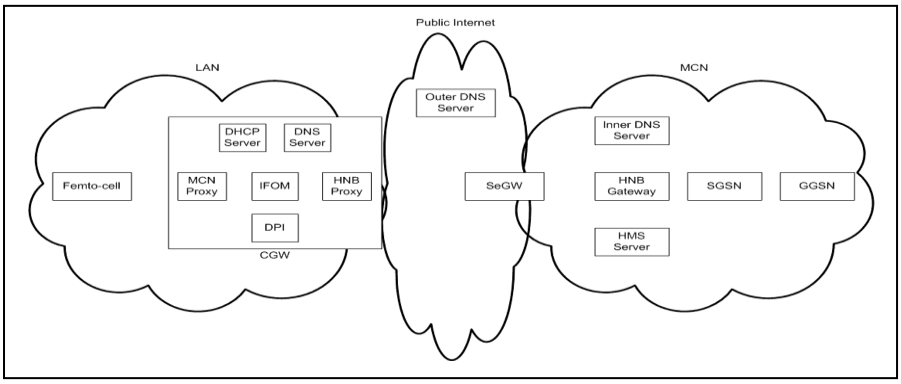

Figure 3. MCN nodes and CGW functional components

At an overview level, these procedures include the discovery of a Secure Gateway (SeGW) and establishing a secure association with the SeGW. After the establishment of this secure connection, the femto-cell communicates with nodes within the MCN. The femto-cell determines its location via a number of methods, including either using a GPS to determine its geo-location or using the cell settings of neighbor cells to determine its proximity to other known cells. After reporting its position to the Home NodeB (HNB) Management System (HMS) within the MCN, the HMS then provisions the femto-cell [4]. Once provisioned, the femto-cell begins radiating and the femto-cell is "open for business". End-user devices can then connect to the MCN via the femto-cell.

1) *Femto-cell Initialization and Provisioning*

The first step towards initializing and provisioning the femto-cell is to power it on. As a result of the device being powered on, there are several steps that must be performed as part of the bring-up on the device.

Once the device is powered on, it will require a local IP address. In order to acquire this IP address it will perform the Dynamic Host Control Protocol (DHCP) discovery procedure detailed in [5]. As a result of these steps, the femto-cell has a local IP address.

As part of the power on sequence, the femto-cell will attempt to discern information about its environment. There are several ways for the femto-cell to learn about its environment. It can listen for macro-cells and other femto-cells in the area by enabling its cellular receiver (either 2G or 3G or both). It can also determine its location by enabling its Global Positioning System (GPS) receiver. Or it can know its location based on the public IP address of the home or enterprise modem to which it is connected. Any of these are sufficient for the femto-cell to identify its location. There is no requirement that all of these must be determined, and it appears from reading the standards that determining each of these are "best effort." These steps are described in Section 6.1.2 of [6].

The femto-cell is required to communicate with the Initial SeGW after it has been energized. As part of this initial communication, the femto-cell will attempt to resolve the Fully Qualified Domain Name (FQDN) of the Initial SeGW that was pre-burnt within the femto-cell. This resolution is done with a Domain Name System (DNS) Request/Response. The CGW will act as a DNS Server (or equivalent) to the femto-cell for purposes of this step. Additionally, the CGW will resolve the Initial SeGW FQDN by sending a DNS Request to the "Outer" DNS Server on the public Internet.

In order to provide secure communications between the femto-cell and the Initial SeGW, an IPSec tunnel is established between the two entities. This process requires a pre-shared key, and agreement of security algorithms between the two entities. Since we are attempting to place the CGW between the femto-cell and Initial SeGW, two IPSec tunnels need to be established. At the conclusion of this step, there will be two IP Sec tunnels, one between the CGW and Initial SeGW and the other between the femto-cell and CGW. The establishment of these IPSec tunnels is described in detail in [7]. For the IPSec tunnel establishment between the femto-cell and CGW the same steps are followed.

After the establishment of an IPSec tunnel, the femto-cell is required to communicate with the Initial HMS. To do this, the femto-cell will attempt to resolve the FQDN of the Initial HMS with the “Inner” DNS Server located within the MCN network. In the absence of a CGW, the femto-cell would make this request to the Initial SeGW via the IPSec tunnel established previously. The Initial SeGW would un-IPSec this request and would send the packet to the “Inner” DNS Server for resolution. In the presence of a CGW, the process is the same from the point of view of the femto-cell and Initial SeGW. The CGW will un-IPSec and then re-IPSec the signaling between the femto-cell and Initial SeGW. There is no further processing required of the CGW in this section. At the conclusion of this section, the femto-cell will know the MCN IP address of the Initial HMS.

Once the IP address of the Initial HMS is known, the femto-cell will establish a TR-069 Customer Premise Equipment (CPE) Wide Area Network (WAN) Management Protocol (CWMP) session with the Initial HMS as described in Section 3.7.3 of the [8]. This session is established so the Initial HMS can provide the IP address or FQDN of some of the MCN nodes to the femto-cell. In the presence of the CGW, the signaling between the femto-cell and Initial HMS will pass through the CGW which will un-IPSec and re-IPSec each packet.

Once the above steps have been concluded, the IPSec tunnels are destroyed. Section 5.1.1 of [9] requires that even if the Serving SeGW is the same as the Initial SeGW, the tunnels are still destroyed. The order of tearing down the tunnels that traverse through the CGW is not important as long as both are removed.

2) Femto-cell Registration with mobile core network

The femto-cell is required to communicate with the Serving SeGW after the femto-cell has gone through the initialization and provisioning steps. If the Initial HMS provided the IP address of the Serving SeGW, this step is skipped. If the Initial HMS provided the FQDN of the Serving SeGW, then this step must be followed. If address resolution is required, it will be performed via a DNS Request/Response. The CGW will act as a DNS Server (or equivalent) to the femto-cell for purposes of this step. Additionally, the CGW will resolve the Serving SeGW FQDN by sending a DNS Request to the “Outer” DNS Server on the public Internet.

After this step, the femto-cell establishes an IPSec tunnel with the Serving SeGW. This is the same procedure that was followed by the femto-cell when it formed an IPSec tunnel with the Initial SeGW. In order to provide secure communications between the femto-cell and the Serving SeGW, an IPSec tunnel is established between the two entities. This process requires a pre-shared key, and agreement of security algorithms between the two entities. Since we are attempting to place the CGW between the femto-cell and Serving SeGW, two IPSec tunnels need to be established. At the conclusion of this step, there will be two IP Sec tunnels, one between the CGW and the Serving SeGW and the other between the femto-cell and CGW.

For the IPSec tunnel establishment between the femto-cell and CGW, the same steps as outlined above are followed. One requirement is that the CGW must have the MCN IP address prior to the femto-cell requesting it. The femto-cell is required to have the MCN IP address so that it can use that as the source address for IP packets that it sends to entities within the MCN. Once these tunnels are established, they will be used “forever” to provide secure communication between the femto-cell and CGW and the CGW and the Serving SeGW.

After the establishment of an IPSec tunnel, the femto-cell is required to communicate with the Serving HMS. To do this, the femto-cell will attempt to resolve the FQDN of the Serving HMS with the “Inner” DNS Server located within the MCN network. In the absence of a CGW, the femto-cell would make this request to the Serving SeGW via the IPSec tunnel established previously. The Serving SeGW would un-IPSec this request and would send the packet to the “Inner” DNS Server for resolution. In the presence of a CGW, the process is the same from the point of view of the femto-cell and Serving SeGW. The CGW will un-IPSec and then re-IPSec the signaling between the femto-cell and Serving SeGW. There is no further processing required of the CGW in this section. At the conclusion of this section, the femto-cell will know the MCN IP address of the Serving HMS.

Once the IP address of the Serving HMS is known, the femto-cell will establish a TR-069 CWMP session with the Serving HMS as described in Section 3.7.3 of [8]. This session is established so the Serving HMS can provide the operating configuration to the femto-cell and the femto-cell can transfer its location information to the Serving HMS. In the presence of a CGW, the signaling between the femto-cell and Serving HMS will pass through the CGW which will un-IPSec and re-IPSec each packet.

The same procedure will be followed to resolve the FQDN of the HNB Gateway (GW) to an IP address, if necessary, as was done for the discovery of the Serving HMS IP address.

Once the femto-cell knows the IP address of the HNB GW, it will register with the HNB GW by exchanging a series of messages. The registration message and response pass through the CGW, and the CGWs only role is to un-IPSec and re-IPSec each message as it passes through the CGW. Once the femto-cell is registered with the HNB GW, it may begin radiating and is “open for business” of allowing end-user devices to access the operator provided network.

D. WiFi AP

This configuration requires the use of a WiFi AP. It must be configured to use the DHCP Server in the CGW. This allows the CGW to provide the local IP Addresses assigned to the WiFi interface of devices connected through the WiFi AP. Using the DHCP Server located within the CGW is the key to determining that a device is reachable over both WiFi and cellular as is described below.

E. End-user Device Attachment

When an end-user device connects to a femto-cell, the femto-cell registers that device with the HNB GW and the end-user device and SGSN exchange signals to allow the end-user device to attach to the network. Once attached, the device may activate a Packet Data Protocol (PDP) context to use to exchange data with an application server on the public Internet via the MCN [10]. The exchange of data between the end-user device and SGSN is carried within a GTP tunnel that exists between the femto-cell and SGSN.

F. *Client IP Addressing*

When the end-user device associates with the WiFi AP, it requests an IP address from the WiFi AP. Since the DHCP Server in the WiFi AP is disabled, the request for an IP address is forwarded to the CGW. The DHCP Server within the CGW assigns a local IP address to the WiFi access connection of an end-user device.

The end-user device will be assigned an IP address by the Gateway GPRS Support Node (GGSN) as part of the PDP context activation procedure.

Once both these events occur, the end-user device has two IP addresses, the MCN assigned IP address and the IP address assigned by the DHCP Server within the CGW. The CGW is cognizant of both connections since both were established with its knowledge. But at this juncture, the CGW doesn't know that these two IP addresses terminate in the same end-user device. Therefore, a method is required to link these two IP addresses to the same device.

G. *WiFi/3G IP Address Association at CGW*

The process of the CGW forming an association between the WiFi and 3G interfaces is shown in Fig. 4. Once a device has requested and received an address from the DHCP Server within the CGW, the DHCP Server within the CGW knows both the locally assigned IP address and the Media Access Control (MAC) address of the WiFi interface. Further, the CGW knows that the MCN has assigned an IP address to the end-user device.

To link the WiFi parameters to the 3G IP address assigned by the MCN, the CGW issues an Address Resolution Protocol (ARP) Request using the 3G IP address assigned by the MCN. The WiFi card within the wireless device responds with its MAC address. At this point, the CGW knows that the WiFi MAC address, local WiFi IP address, and 3G IP address are all the same device.

To ensure that it is the same device, the CGW sends an Internet Control Message Protocol (ICMP) Echo Request message [11] via the WiFi AP with the destination IP address set to the 3G IP address extracted during the setup of the PDP context.

If the terminal device is connected through the WiFi AP it responds with an ICMP Echo Response message with the source and destination IP addresses reversed. From this information, the CGW infers that the end-user device has both the 3G and local WiFi connection "active".

In order to accommodate different scenarios, it may be necessary for the CGW to periodically issue the ARP Request and ICMP Echo Request messages. For example, if the 3G PDP context is activated after the WiFi has associated. It is expected that the Operating System (OS) in the CGW will take care of managing the linkage of all this information. Furthermore, the CGW still supports devices that support only WiFi connections as well as end-user devices that only support 3G connections.

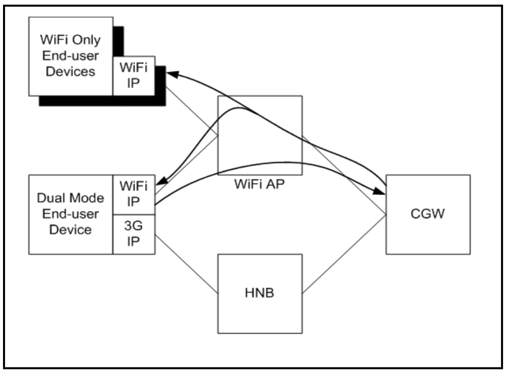

Figure 4. WiFi/3G IP Address Association at CGW

H. IP Flow Mobility (IFOM)

The CGW will have policies within it to indicate which traffic for which users to offload traffic from the cellular access to the WiFi access. It will have at least one default policy and may have policies for specific end-user devices. The default policy is used for those devices that do not have an individual policy. The policy conforms to the [12] 3GPP standards that define the criteria within a policy. The policy allows for defining which types of IP Flows are permitted (and not permitted) on which accesses. For any IP Flow, the CGW will have a routing rule that dictates one of the following:

- Cellular Only
- WiFi Only
- Cellular Preferred
- WiFi Preferred
- No Preference

So for each type of flow, such as Voice over IP (VoIP), File Transfer Protocol (FTP), or application server IP address, for each user, the operator can enforce one of the above access rules. This granularity allows the operator great flexibility in managing flows and effectuating offload to unlicensed spectrum. Additionally, the policy has a catch-all setting which is used for flows that are either unknown or just started, prior to Deep Packet Inspection (DPI) being performed. An example policy is shown below:

- IMSI = ‘12345678901234’
- Rule 1
    - Type = ‘VoIP’
    - Routing Rule = ‘No Preference’
- Rule 2
    - Type = ‘Streaming Video’
    - Routing Rule = ‘WiFi Only’
- Rule 3
    - Type = ‘Source Address = W.X.Y.Z’
    - Routing Rule = ‘WiFi Preferred’
- Rule 4
    - Type = ‘Default’
    - Routing Rule = ‘Cellular Only’

In this user-specific policy, VoIP traffic for this specific user is routed over either the cellular or WiFi access as a function of the loading on each access. Meanwhile, all streaming video is routed over the WiFi access. Furthermore, traffic from IP address W.X.Y.Z is routed with a preference for WiFi while any other traffic, regardless of its type or even if it is an unknown flow after DPI, is sent over Cellular.

III. IP FLOW MOBILITY

I. Addition of new IP Flows

When an IP Flow starts, the flow type is unknown and its packets are dispatched by the IFOM functionality within the CGW to the default access. Once DPI is performed within the CGW, the IP Flow type may be known. For example, the IP Flow type may be VoIP, FTP, or streaming video. If the DPI is not able to discern what the IP Flow is, the flow will be labeled as unknown. Once the DPI has been performed, the policy can be consulted for this specific user. As was described earlier, the policy contains the routing rule associated with this flow type. If it is the same as the default access, then no change is made. The IFOM will continue to route the data to the end-user device via the same access. Should the routing rule indicate a different access, the IFOM functionality will begin routing the data associated with this IP Flow to the end-user via the selected access. When a new flow is identified by the DPI, the IFOM routes the data associated with that IP Flow to the end-user with the selected accesses based on the following rules:

- Cellular Only and Cellular Preferred IP Flows are assigned to the cellular access
- WiFi Only and WiFi Preferred IP Flows are assigned to the WiFi access
- No Preference IP Flows are assigned to the least loaded accesses as a function of the number of existing IP Flows and of the capacity of the accesses

Using the example shown previously, if a new IP flow was detected, the CGW will place it on cellular access while DPI is performed. Let's say this new flow is streaming video, once DPI has determined the type (assume successfully), the CGW will consult the routing rule for this user, and IP Flow type and will move the flow from the cellular access to the WiFi access since it is streaming video. This behavior is shown in Fig. 5.

J. Dynamic Flow Management of existing IP Flows

Periodically, the CGW performs load balancing to ensure no access is overburdened. If an access is found to have an unfair proportion of the current IP Flows, the CGW attempts to perform load balancing without violating any of the IP Flows routing rules. When performing load balancing, the IFOM within the CGW takes into account the following factors:

- Number of IP Flows on each access
- Bandwidth capacity of each access
- The policy for each IP Flow

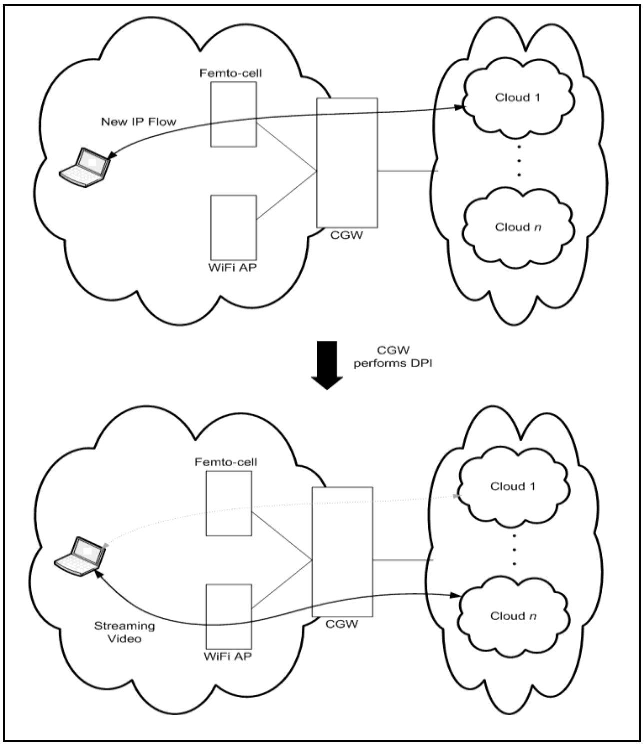

Figure 5. Example of CGW Initial IP Flow Assignment

An example helps illustrate this logic and is shown in Fig. 6. Let's assume there are many end-users all actively engaged in active sessions, performing VoIP, FTP and video streaming. Several of the users have active VoIP sessions, all using the cellular access. Another user has an active video streaming session whose data is also using the cellular access. Still another user is performing an FTP download over the WiFi access. When the dynamic flow management occurs, the CGW analyzes the IP flows on each access and the routing rules for those flows per user. Assume that the VoIP sessions all have routing rules that mandate use of the Cellular access. Further assume that the FTP session is not consuming much of the throughput and has a routing rule which mandates use of the WiFi access. Finally, assume that the streaming video session has a Cellular Preferred routing rule. For this scenario, the IFOM decides to move the streaming video flow from the cellular access to the WiFi access and leaves the remaining IP Flows as they were previously assigned. The VoIP IP flows remain on the cellular access. However, if the streaming video had a cellular only routing rule, then the CGW would leave those flows on the cellular access. In this way, the operator can have absolute control over the load balancing efforts. Fig. 6 shows the CGW moving the streaming video IP Flow from the cellular access to the WiFi access. This movement is denoted by the arrows that show the flow moving from being delivered via cellular to WiFi.

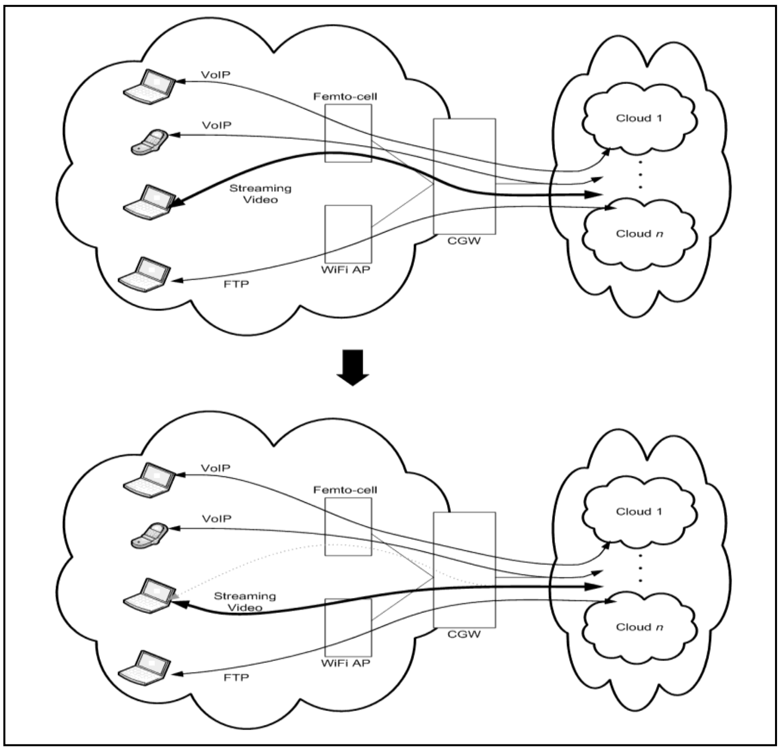

Figure 6. Example of CGW Load Balancing

K. Link-Down handling of existing IP Flows

Part of the support required to effectively manage the IP Flows will be the end-user device reporting channel metrics to the CGW. For example, the CGW will configure the end-user device to report the Received Signal Strength Indicator (RSSI) of the active accesses when they pass certain thresholds. This allows the CGW to induce the end-user device to send an alert to the CGW when the signal quality has passed through a CGW-defined limit. As the end-user device performs this monitoring, should the quality of the signal pass through this limit, the end-user device will inform the CGW. The CGW will then attempt to move as many IP Flows as possible for this user from the degraded access to the other access. There are several criteria that are used when evaluating each IP Flow for the particular user:

- Routing Rule for this IP Flow
- Quality of the non-degraded access

If an end-user reports that an access has degraded, the CGW will examine the routing rule for each IP Flow. The CGW will only move those flows away from the degraded access that have a routing rule that allows the IP Flow to move, such as WiFi-Preferred, Cellular-Preferred, or No Preference. IP Flows that have a rigid routing rule, either WiFi-Only or Cellular-Only will not be moved even in this case. Additionally, the CGW will examine the quality of the non-degraded access, if the end-user device has that access available. If the non-degraded access is also of poor-quality, the CGW will not move any IP Flows. This prevents the scenario where both accesses become degraded and the CGW attempts to mitigate this situation by moving IP Flows back-and-forth between each degraded access.

An example is usually clarifying. Assume that there is a user who is connected via both cellular and WiFi and has two flows, FTP and streaming video which are traversing the WiFi access. Further assume that the CGW has configured the end-user device to alert the CGW should the WiFi signal become degraded and that the WiFi link does become very weak. The last of the assumptions is that the FTP routing rule is WiFi-only while the streaming video routing rule is WiFi-Preferred.

The end-user device will alert the CGW that the WiFi signal has degraded. The CGW will move the streaming video session from the WiFi access to cellular access. Additionally, the CGW will not move the FTP IP Flow since its routing rule is WiFi-Only. The sequence of events as well as the movement of the streaming video IP Flow is shown in Fig. 7.

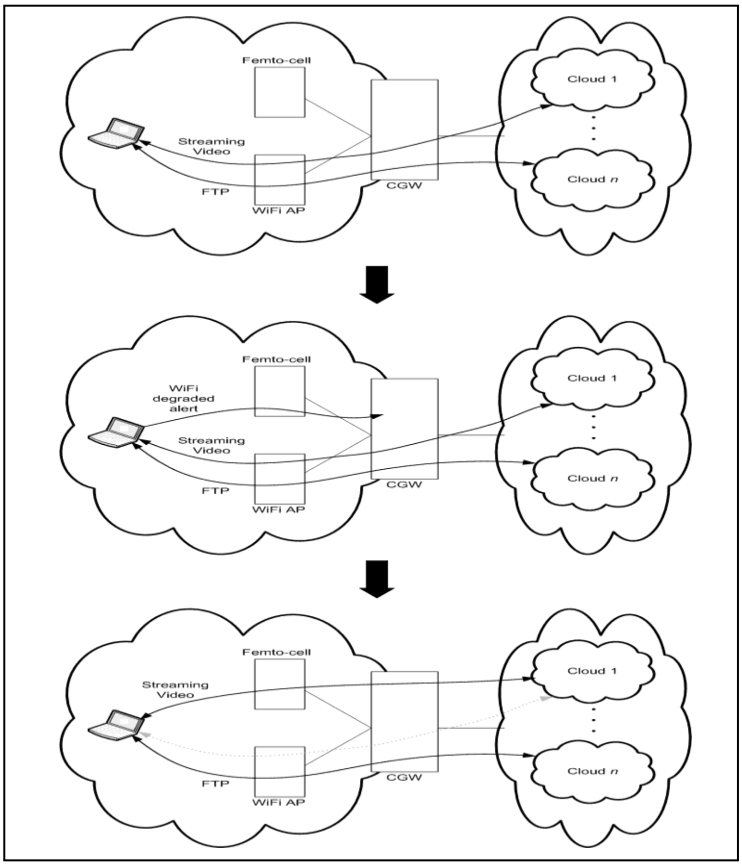

Figure 7. Example of CGW Link-Down Processing

III. CLIENT REQUIREMENTS

There are some requirements on the client. As alluded to above, but explicitly stated in this section, the end-user device must possess certain capabilities to take advantage of the capabilities provided by the CGW.

a. Reception over either Access

The end-user device must have the ability to handle the reception of downlink packets over either WiFi or Cellular. This means that both the WiFi and Cellular radios must be energized. In addition, the end-user device must accept that those packets sent over the WiFi access will use the IP address assigned by the MCN as the destination address. This is critical to allow for the flow to use both Cellular and WiFi.

b. Transmission over either Access

In addition, the client must have some algorithm relating to how it routes uplink traffic towards the Cloud through the CGW. It is sufficient that the end-user route uplink packets for the same Cloud over the same access that it received packets from that Cloud. This allows the CGW to make the routing decisions, as the end-user device will engage in uplink-follows-downlink. While not described in this paper, the end-user device can also have more sophisticated logic such as performing its own DPI and deciding the appropriate uplink path for packets based on its knowledge of its own environment. There is nothing within the CGW concept that would preclude supporting an end-user device that had this capability.

c. Measurements

To support the logic within the CGW that handles the link-down scenario, the end-user device must support measurements. It must support being configured by the CGW to perform RSSI measurements and to send these measurements to the CGW should the measurements fall below a limit (or rise above a certain value as well).

The protocol used to configure and report the measurements is not defined within this document. Any protocol will suffice, be in Open Mobile Alliance Device Management (OMA-DM) [13], Simple Object Access Protocol (SOAP) [14], or any other agreed-upon mechanism that allows the transfer of signaling between the CGW and end-user device.

V. CONCLUSION

In this paper we described the necessity of having robust connectivity when dealing with Cloud Computing. We then described the advantage of having connectivity over multiple interfaces, as it supports many of the characteristics that are desirable in Cloud Computing – namely device and location independence, reduced costs, increased reliability, and improved performance. We then walked through the architecture of the CGW and the procedures that it enables to allow connectivity to the Cloud. We concluded by showing several examples where the end-user's connectivity to the Cloud is increased by the introduction of the CGW within the architecture.

References

[1] 3GPP TS 23.261, v10.1.0, "IP flow mobility and seamless WLAN offload," September 2010.

[2] 3GPP TS 23.327, v10.0.0, "Mobility between 3GPP-WLAN interworking and 3GPP systems," March 2011.

[3] 3GPP TS 33.320, v10.3.0, "Security of Home Node B/Home evolved Node B," June 2011.

[4] 3GPP TS 32.582, v10.3.0, "Home Node B Operations, Administration, Maintenance and Provisioning Information Model for Type 1 interface Home Node B to Home Node B Management System," June 2011.

[5] R. Droms, "Dynamic Host Configuration Protocol," IETF RFC 2131, March 1997; www.rfc-editor.org/rfc/rfc2131.txt.

[6] 3GPP TS 25.467, v10.3.0, "UTRAN architecture for 3G Home Node B," June 2011.

[7] E. Kaufman, "Internet Key Exchange (IKEv2) Protocol," IETF RFC 4306, December 2005; www.rfc-editor.org/rfc/rfc4306.txt.

[8] TR-069 CPE WAN Management Protocol, v1.1, December 2007; http://www.broadband-forum.org/technical/download/TR-069_Amendment-2.pdf

[9] 3GPP TS 32.583, v10.1.0, "Home Node B Operations, Administration, Maintenance and Provisioning Procedure Flows for Type 1 interface Home Node B to Home Node B Management System," June 2011.

[10] 3GPP TS 23.060, v10.5.0, "GPRS Service description," September 2011.

[11] J. Postal, "Internet Control Message Protocol," IETF RFC 792, September 1981; www.rfc-editor.org/rfc/rfc792.txt.

[12] 3GPP TS 24.312, v10.4.0, "Access Network Discovery and Selection Function Management Object," September 2011.

[13] Open Mobile Alliance Device Management Client Provisioning, v1.1; http://www.openmobilealliance.org/Technical/release_program/cp_v1_1.aspx.

[14] Simple Object Access Protocol, v1.1, May 2000; http://www.w3.org/TR/2000/NOTE-SOAP-20000508.