sandvine®
Intelligent Broadband Networks

Contents

Executive Summary 1
Introduction to Application Zero-Rating 2
Understanding Modern Applications 2
Considerations and Best Practices 3
Choosing Appropriate Applications 4
Correctly Identifying Application Traffic 5
Accurately Enforcing Zero-Rating 7
Conclusions 14
Additional Resources 14

WHITEPAPER

Application Zero-Rating: Considerations and Best Practices for Revenue Assurance

An Industry Whitepaper

Executive Summary

Due to increased competition for Internet subscribers, it is more important than ever for communications service providers (CSPs) to launch new and differentiated services. These innovative new Internet services are critical both for building loyalty with existing customers and for enticing potential subscribers to switch providers.

One effective way that CSPs can differentiate their services and stand out from the competition is by zero-rating individual applications. Zero-rating enables unlimited usage of an application (or many applications) for a fixed price.

Before a CSP implements a zero-rated offering, they must understand the types of applications in the market, and the challenges with zero-rating them.

This whitepaper proposes a set of best practices that guide CSPs on the following:

- Selecting the best applications to zero-rate
- Identifying application traffic and correctly enforcing network policies
- Eliminating potential revenue leakage from zero-rating
- Messaging zero-rated offerings to customers

By adhering to our principles, CSPs will be able to launch profitable zero-rated offerings that minimize revenue leakage.

Introduction to Application Zero-Rating

While penetration of Internet access is extremely high in developed countries and is increasing in emerging markets, average revenue per user (ARPU) is flat or declining. According to Ovum's *Telecoms, Media & Entertainment Outlook 2015*, due to the increased competition among communications service providers (CSPs), nearly all markets will experience an ARPU decline by 2019.[1] With this fiercely competitive environment, it's imperative for CSPs to launch new and differentiated Internet services that both build loyalty with existing customers and entice potential subscribers to switch providers.

The notions of rapid and extensive service differentiation are relatively new, but the tools now exist to quickly introduce a wide variety of services that vary based on application, device, time-of-day, and a myriad of other factors—either considered alone or in combination.

One popular way that CSPs can differentiate their services and stand out from the competition is by zero-rating individual applications. Application zero-rating enables unlimited usage of an application (or many applications) for a fixed price. From the subscriber's perspective, unlimited usage of an application or class of applications is bundled into a fixed price offering, without the risk of additional charges related to usage of the application or application class. As a result, users get price certainty—a powerful psychological feeling—around usage of their favorite applications.

This approach differs from traditional Internet services where a customer simply paid (prepaid or postpaid) for a specific access speed and volume quota (i.e., an allowance of some number of megabytes, gigabytes, etc.); the quota is consumed by any and all applications, and there is always a risk of exhausting the quota (which may or may not result in overage charges or some other consequence, like reduced access speeds).

For CSPs launching zero-rated plans under net neutrality or open Internet regulations, we recommend reviewing, *Best Practices for Zero-Rating and Sponsored Data Plans under Net Neutrality*.[2]

In this paper, we will go deeper on application zero-rating by exploring a number of topics in detail:

- Understanding different types of applications
- How to select applications to zero-rate
- Identifying application traffic and enforcing network policies correctly
- Potential revenue leakage from zero-rating
- How to message zero-rated plans to customers

Understanding Modern Applications

Before discussing the applications best-suited for zero-rating, we must first clarify some terminology.

Traditionally, applications completed specific tasks like web browsing (e.g., Safari), instant messaging (e.g., Yahoo Messenger), or video chat (e.g., FaceTime). This simplicity made it very easy to differentiate between an application and a unique feature within an application platform.

However, over time, applications added new features and became much more complex. For example, WhatsApp started out as a simple instant messaging application but now also contains file sharing, voice calling, and video-chat capabilities. In the past, each of the aforementioned WhatsApp capabilities would have been stand-alone applications, but now consumers see these as features within the overall WhatsApp platform. The consumer consensus is that the overall platform (e.g., WhatsApp) is the application while each feature or service bundled inside the application platform is an application feature. It's recommended that CSPs align their offerings with the subscriber's viewpoint rather than conflict with it.

In addition to adding new features within an application, some developers also started to build what Sandvine calls *mashup applications*. Mashup applications rely on one or many external services to function. An illustrative example

1. http://info.ovum.com/uploads/files/Ovum_Telecoms_Media_and_Entertainment_Outlook_2015.pdf
2. https://www.sandvine.com/resources/whitepapers/best-practices-for-zero-rating-and-sponsored-data-plans-under-net-neutrality.html

of an mashup application is Pokémon Go. The Pokémon Go application requires data connections to the Pokémon Go server for catching and battling Pokémon, to Google services for mapping, and to Picasa for Pokéstop images. One critical aspect for mashup applications is that they don't work if the connection to the external services is severed. This reliance on external services can make zero-rating mashup applications challenging for CSPs and will be discussed in-depth in this whitepaper.

Another type of application is an *aggregator application*. This type of application is very similar to an mashup application as it relies on multiple data sources to enable 100% of its functionality. The key difference between an mashup application and aggregator application is that an aggregator application can still function (albeit fairly limited) without the data connection to the external services. The Reddit application is a good example of an aggregator application as it provides users with headlines of Reddit posts, but the links within each post (e.g., images, gifs, videos, and articles) are pulled from the Internet. If the Reddit application's data connection to the Internet was disabled, a user would still be able to see all of the content posted on Reddit (e.g., the headline post), but all of the articles, images, GIFs, and videos hosted on external websites would not appear. Web browsers (e.g., Chrome, Safari) could also be considered aggregator applications as they rely on external data sources (e.g. websites) but still technically function without a connection to external data sources.

Lastly, it's also important to clarify the difference between an application and a website. As noted above, an application is specifically designed to complete a task/service or many tasks/services whereas a website is a collection of related web pages and multimedia content. Although some websites offer features found in applications, Sandvine does not consider websites to be applications.

Table 1: Summary of Application Types

Application Type	Description	Examples
(Standard) Application	A software program designed to help users perform a specific activity (or multiple activities): e.g., browse the Internet, send instant messages, share a photo, watch a movie.	Facebook, Netflix, Spotify, Instagram, WhatsApp
Application Feature	A specific function within the overall application platform.	WhatsApp Voice Calls, WhatsApp Video Calls, WhatsApp Instant Messaging
Mashup application	An application that requires external services to operate. The application cannot function if it isn't connected to external services.	Pokémon Go, Ingress
Aggregator Application	An application that uses external services. The application has limited functionality if it isn't connected to external services.	Reddit, Flipboard

Considerations and Best Practices

When determining which applications to zero-rate, it's important to consider the following factors:

1. The popularity of the application and the data it uses
2. The ability to accurately identify the application and any associated data traffic
3. The ability to enforce a zero-rated policy
4. The potential for revenue leakage
5. The impact of regulations
6. How to best message application zero-rating

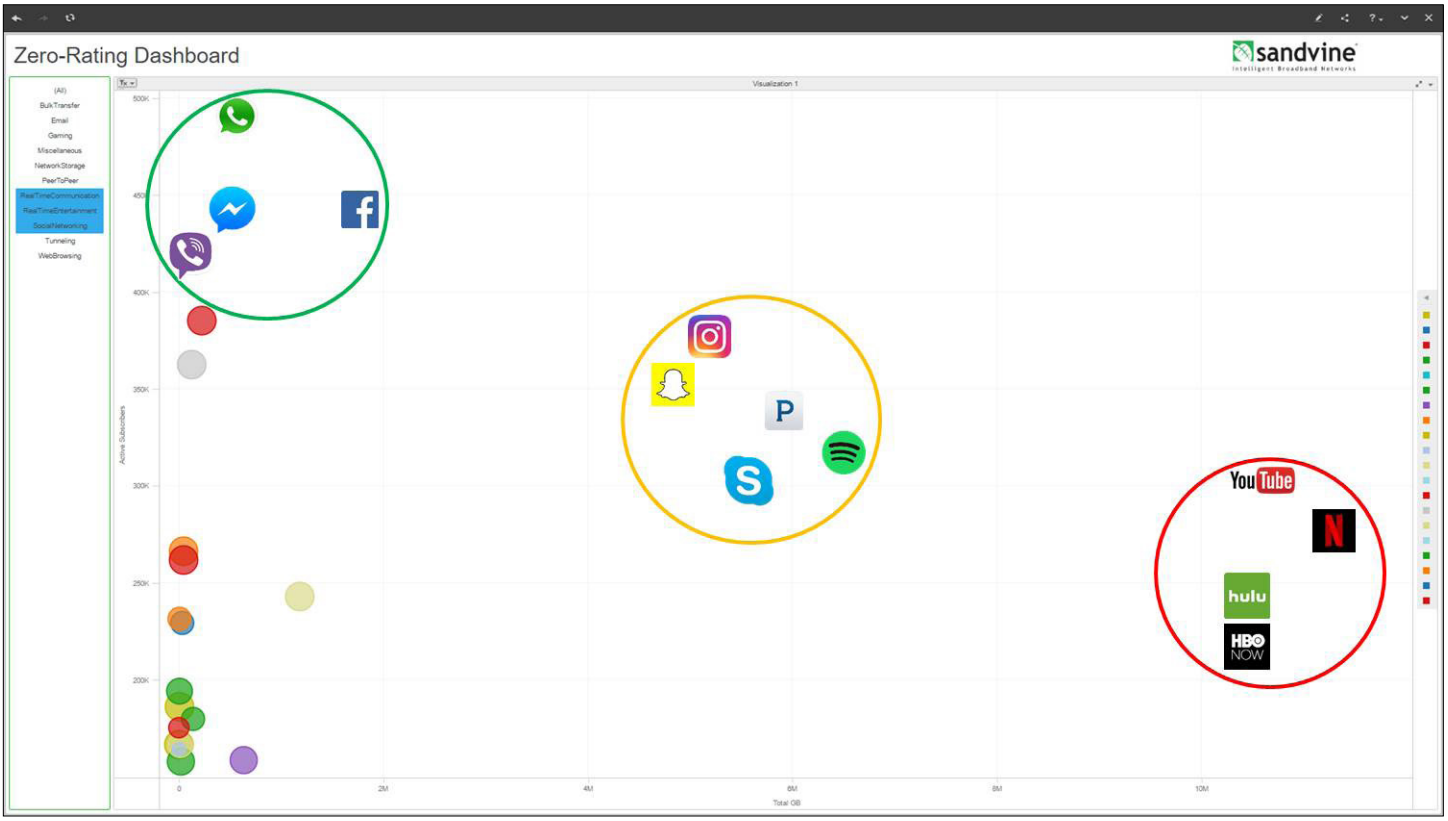
Choosing Appropriate Applications

From a business perspective, we've found that popular applications (e.g., applications actively used by large numbers of subscribers) that consume relatively little bandwidth are particularly good targets for zero-rating. These popular and low bandwidth services can be offered in an unlimited fashion for very reasonable prices to the subscriber, and they won't cause network congestion even if adopted in large numbers.

To identify ideal candidate applications, we recommend that CSPs review the top 50 applications on their network (based on the number of active users) and compare that against the total data bandwidth used by each application.

Figure 1 (see below), plots active users (Y-axis) against the total bandwidth used (X-axis) for a range of applications.

Figure 1: Choosing candidate applications for zero-rating (built in Sandvine's Network Analytics product)



The green circle in Figure 1 highlights the most ideal applications for zero-rating based on the combination of popularity and low bandwidth. Not surprisingly, instant messaging and social networking applications are typically the best candidates for zero-rated usage due to their widespread adoption and minimal data consumption. In other words, these types of applications offer the most value to the subscriber for the least cost to the CSP.

Since most subscribers don't understand how much data an application uses (e.g., per message, per photo, per video chat, etc.), they are unable to calculate how long their data balance will last. This unknown makes the value of volume data plans (e.g., 250MB or 1 GB) ambiguous to subscribers. On the other hand, subscribers easily comprehend the value of unlimited usage of an application for a specific time-period (e.g., zero-rated WhatsApp for 30 days). As a result, CSPs can leverage the customer-value relationship by providing a fixed price for popular applications that utilize low bandwidth.

Plus, by focusing on popular low-bandwidth applications, CSPs minimize revenue loss as customers still need to purchase a volume data plan for all other data activities. Many of our customers have taken this approach and offer unlimited WhatsApp and Facebook bolt-on plans that provide price certainty to customers and help differentiate from the competition (e.g., Paratus Telecom, GTT and Econet Wireless Zimbabwe)[3]. This successful zero-rating strategy contributed significantly to Econet Wireless Zimbabwe's 31% year-over-year subscriber growth and 61%

3. These examples are all explained in Success Stories available at https://www.sandvine.com/customers/

year-over-year revenue growth after the introduction of their unlimited WhatsApp offerings.[4]

Commercially speaking, zero-rating higher bandwidth services (e.g., high definition video streaming) may become unsustainable for a CSP due to the strain on the network and the high potential revenue cannibalization (e.g., no more data-cap overage fees or reduced prepaid byte usage). However, we don't recommend simply dismissing high bandwidth applications from zero-rated plans. Many users choose not to connect to high bandwidth applications on mobile networks due to a fear of rapid data exhaustion (e.g., running out of data) and/or bill shock (fear of going over data limits). As a result, zero-rating high bandwidth applications could be incredibly valuable to customers and could entice them to upgrade to a more expensive data plan. T-Mobile's (U.S.A.) Un-carrier plans (e.g., zero-rated music and video streaming) are great examples of how zero-rating high bandwidth applications can lead to both customer and revenue growth. Since the launch of T-Mobile's first Un-carrier initiative (includes both Binge On and Music Freedom), T-Mobile (at the time of this writing) has added more than 24 million customers. T-Mobile has also led the United States in year-over-year revenue percentage growth for 12 of the last 13 quarters.[5]

To alleviate potential network congestion concerns, a CSP could offset the increase in popularity of high-bandwidth applications by limiting the bitrate on those applications. In practical terms, this technique means that CSPs could shape zero-rated video streams to standard definition. This shaping method is the approach used by T-Mobile with their Binge On (unlimited streaming video) offering.

To reduce revenue cannibalization concerns, CSPs can place conditions on the zero-rated application offerings. In fact, we've seen many operators offer bolt-ons for high bandwidth applications that are only valid to subscribers that purchase a high-end device directly from the carrier (e.g., Bakcell has a combined promotion that zero-rates Instagram for customers who purchase an iPhone[6]) or who have already purchased a higher-end data plan (e.g., O2 offers unlimited music with select devices on higher-end plans).

Since no user base is the same, Sandvine strongly recommends that CSPs complete their own analysis to determine the most ideal applications to zero-rate. Once armed with this information, CSPs will have a better understanding of the revenue and network effects, and will be better prepared to launch profitable zero-rated plans.

Correctly Identifying Application Traffic

The next factor to consider before launching a zero-rated application plan is ensuring that a CSP has the ability to identify and accurately measure zero-rated application traffic. Accurate traffic identification is critical because false positives and false negatives can cause a subscriber to be overcharged, and can result in revenue leakage for the CSP (see examples in Table 2).

Due to the negative impact of false positives and false negatives, Sandvine recommends that CSPs accurately identify potential zero-rated application traffic before launching a zero-rated plan. To achieve this level of accuracy, it is highly recommend that CSPs utilize a best of breed traffic classification or deep packet inspection (DPI) solution to identify and measure zero-rated traffic. Although many GGSNs (or similar gateways) market DPI capabilities, recognition rates are not nearly as accurate as dedicated DPI vendors. This technical limitation makes sense, as DPI is not a core technology for a gateway, so identification techniques are more basic due to the limited processing power. Since identifying encrypted applications requires significant computing resources (e.g., processing power and memory) the accuracy difference between DPI and gateway vendors will become even larger as applications increasingly implement encryption techniques.[7]

4. Econet discusses their zero-rating plans and the positive business results in this webinar: https://www.sandvine.com/resources/webinars/building-a-mobile-internet-services-vending-machine.html
5. https://newsroom.t-mobile.com/news-and-blogs/2q-2016-earnings.htm
6. http://www.bakcell.com/az/free-instagram-for-iphone-users
7. For those interested, the general subject of traffic identification is explored in much greater detail in this whitepaper: https://www.sandvine.com/downloads/general/whitepapers/identifying-and-measuring-internet-traffic.pdf

Table 2: Impact of False Positives and False Negatives

Type of Inaccuracy	Impact on Charging
False Positives	False positives can cause revenue leakage for the CSP. For instance, consider a service bundle that zero-rates all Facebook traffic; when traffic is falsely identified as Facebook, it is zero-rated rather than being charged separately, and the CSP loses revenue.
False Negatives	False negatives can cause overbilling of subscribers. For instance, a subscriber purchases a service bundle that zero-rates all Facebook traffic; when Facebook traffic is not recognized, the usage is not zero-rated and is subjected to normal data charges.

For simplicity, this paper focuses on three high-level traffic detection and enforcement techniques: Deterministic, Heuristic/Machine Learning, and Policy. An overview of each of them is included in Table 3.

Table 3: Types of Traffic Identification

Method	Description
Deterministic	• This traffic identification technique reviews port numbers, server names, IP addresses, URL addresses, byte patterns, cross-packet correlation, signatures etc. associated with the application to accurately identify it. • Combining multiple techniques creates an application signature; the more techniques combined, the stronger the signature. • Deterministic methods are the most accurate type of traffic identification because they achieve the lowest rates of false positives and false negatives. • Deterministic methods are also typically the fastest at identifying traffic (i.e., within the first few packets of a flow).

Heuristic/ Machine Learning	• Heuristics are used when a deterministic match or measurement is not available directly from the inspection of traffic.
	  • By measuring the properties of traffic, conclusions can be reached that are sufficient to meet the immediate classification goals.
	• Machine learning is a type of heuristic algorithm built on mathematical models .
	  • By taking a set of known data and running it through a machine learning algorithm, correlations between the data set and the attributes associated with the traffic can be found.
	• Heuristics or machine learning techniques are often utilized as a second factor to provide more accurate traffic identification (e.g., YouTube SD vs. HD) and to identify fraud (e.g., data traffic doesn't match behavioral norms).
	• In some instances, heuristic/machine learning identification methods are not as quick to identify traffic as deterministic methods because they must examine the traffic for a short period of time (e.g., 1-3 seconds) before accurately identifying it.
	• Heuristics and machine learning techniques are required to identify specific features within an application (e.g., voice call vs. instant message in WhatsApp).

Policy	• Policy is not technically a traffic identification technique; it is the logic behind the traffic enforcement rules. • Policy is critical when zero-rating interconnected and aggregator apps, as it informs the CSP about all associated traffic that must be zero-rated in addition to the initial application. • The ability to write accurate and logical policy is integral for zero-rating mashup applications, aggregator applications, or specific application features. • Policy is also critical for protecting CSPs from revenue leakage.

Accurately Enforcing Zero-Rating

The next step in the zero-rating process is determining how to enforce the zero-rating policy.

As a prerequisite for correctly enforcing policy, CSPs must implement a solution that has robust traffic classification profiles that are kept up-to-date. Frankly, embedded DPI solutions within packet gateways just aren't suitable.

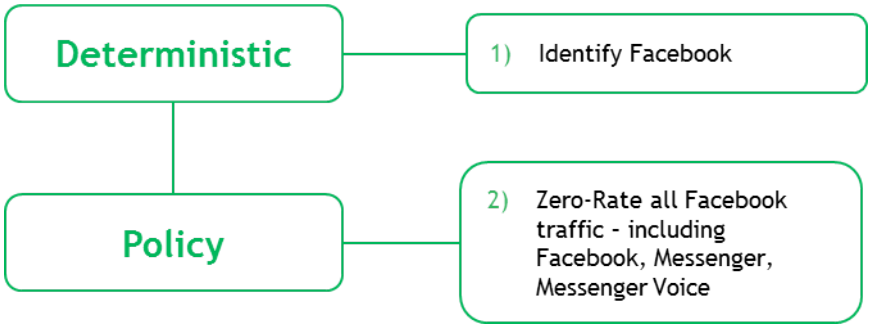
Traffic classification profiles provide CSPs with specific instructions on how to zero-rate applications. These instructions are important when developing zero-rated offerings for mashup applications. Enforcement rules for each application type are discussed in the figures below.

Since new applications are constantly being developed and existing applications are constantly adding new features, CSPs must select a vendor that issues timely updates to their traffic classification profile. These updates ensure that both zero-rating identification and policy enforcement remains accurate.

Zero-Rating a Standard Application

Figure 2, below, shows how policy is enforced on a standard application. In this example, both the traffic identification and policy enforcement are very straightforward. A deterministic signature identifies the application and a simple policy enforces the zero-rating rule. Due to the ease of both identification and enforcement, applications that fit this profile are optimal targets for zero-rating.

Figure 2: Zero-rating a (standard) application

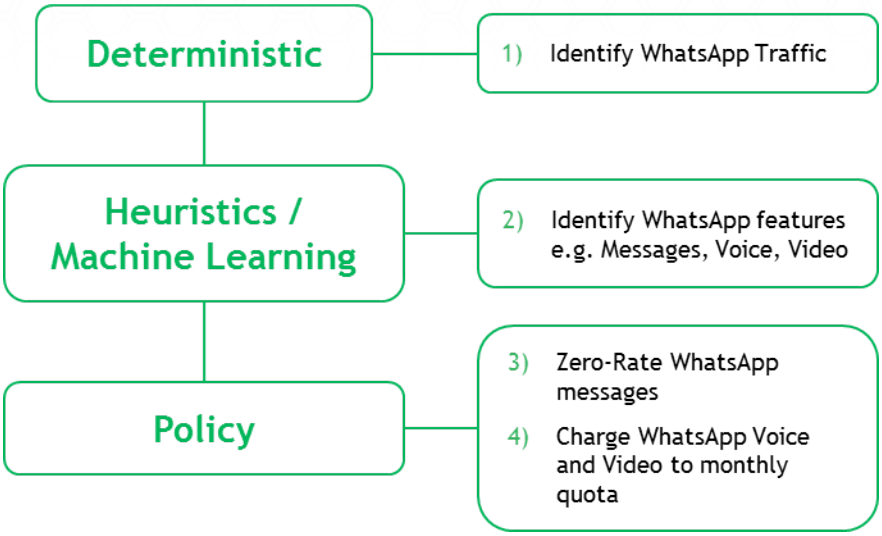


Zero-Rating an Application Feature

As previously discussed, mobile applications are much more complex and feature-rich now than they were even a few years ago. In the case where many previously standalone applications are bundled into a single platform (like WhatsApp, for example), it is technically complex to isolate individual features of that application. To isolate individual application features for zero-rating, a CSP needs to rely on advanced traffic detection capabilities like heuristics/machine learning and multiple policy enforcement rules. Figure 3, for example, shows the process for zero-rating Instant Messaging traffic on a messaging-only WhatsApp plan. As one can see, it is much more complex (for both the identification and enforcement) to zero-rate only application features than it is to zero-rate an entire application.

It's also important to note that the advanced traffic detection capabilities utilized in Figure 3 are more sophisticated than the simplistic deterministic methods relied upon by many packet gateways. As a result, it's extremely unlikely that a packet gateway could accurately isolate individual application features for zero-rating plans. That said, CSPs can work with the application providers to isolate traffic flow for individual application features. However, for this approach to be embraced, the application provider and the CSP must have aligned interests. Even in the best case scenario (i.e., full cooperation), this approach takes a long time to show benefits, severely hampering a CSP's agility.

Figure 3: Zero-rating an application feature



Challenges with Zero-Rating Interconnected and Aggregator Applications

Mashup applications and aggregator applications are the most challenging applications to zero-rate because their operation relies on at least one external service to operate. As a result, CSPs must identify all of the primary application traffic and the associated application traffic (e.g., external content) to build an accurate zero-rated offering.

Pokémon Go is a useful example of an mashup application as it cannot function without a real-time connection to Google services (for mapping data). This reliance on external services means that in order to offer a zero-rated Pokémon Go plan, a CSP must also enable a small volume quota (e.g., 1MB) for Google services before the game launches (so that a subscriber can successfully log in to Google) and a larger quota for Google services traffic (e.g., 100MB) while the game is active. Moreover, a CSP must utilize complex enforcement rules to avoid revenue leakage and abuse of the zero-rated plan (Figure 4, steps 2-5). The limits on Google services ensure that fraudulent subscribers cannot abuse the zero-rated plan to unfairly receive unlimited access to Google applications.

Unfortunately, it is technically impossible to isolate individual Google services (e.g., Gmail, Photos, Maps, Drive etc.) because they are all hosted at the same IP address. The previously mentioned traffic classification profiles should provide CSPs with detailed enforcement policy instructions for mashup applications.

Figure 4 highlights the process for zero-rating Pokémon Go. Based on this flow, one can see that identifying the application traffic and associated traffic is straightforward. However, the enforcement policy is quite complex and requires multiple steps. The key challenge is zero-rating the external services (e.g., Google services) that Pokémon Go relies on, without zero-rating the Google services (e.g., YouTube, Gmail etc.) that aren't related to Pokémon Go (see Figure 5).

Since it's technically impossible to isolate 100% of Google Maps traffic from other Google services, a CSP must create usage limits on the Google Services traffic. Due to the intricate policy required to accurately zero-rate an mashup application and avoid revenue leakage, CSPs are strongly recommended to work with a vendor that has a proven track record of accurate traffic classification and policy enforcement.

Figure 4: Zero-rating an mashup application

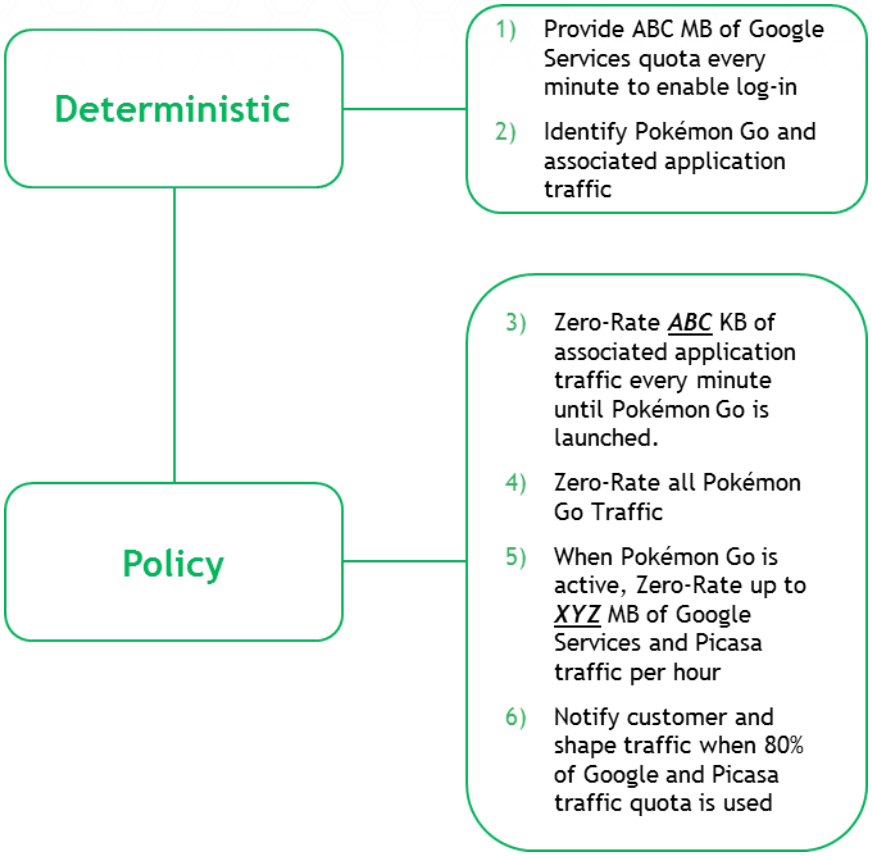
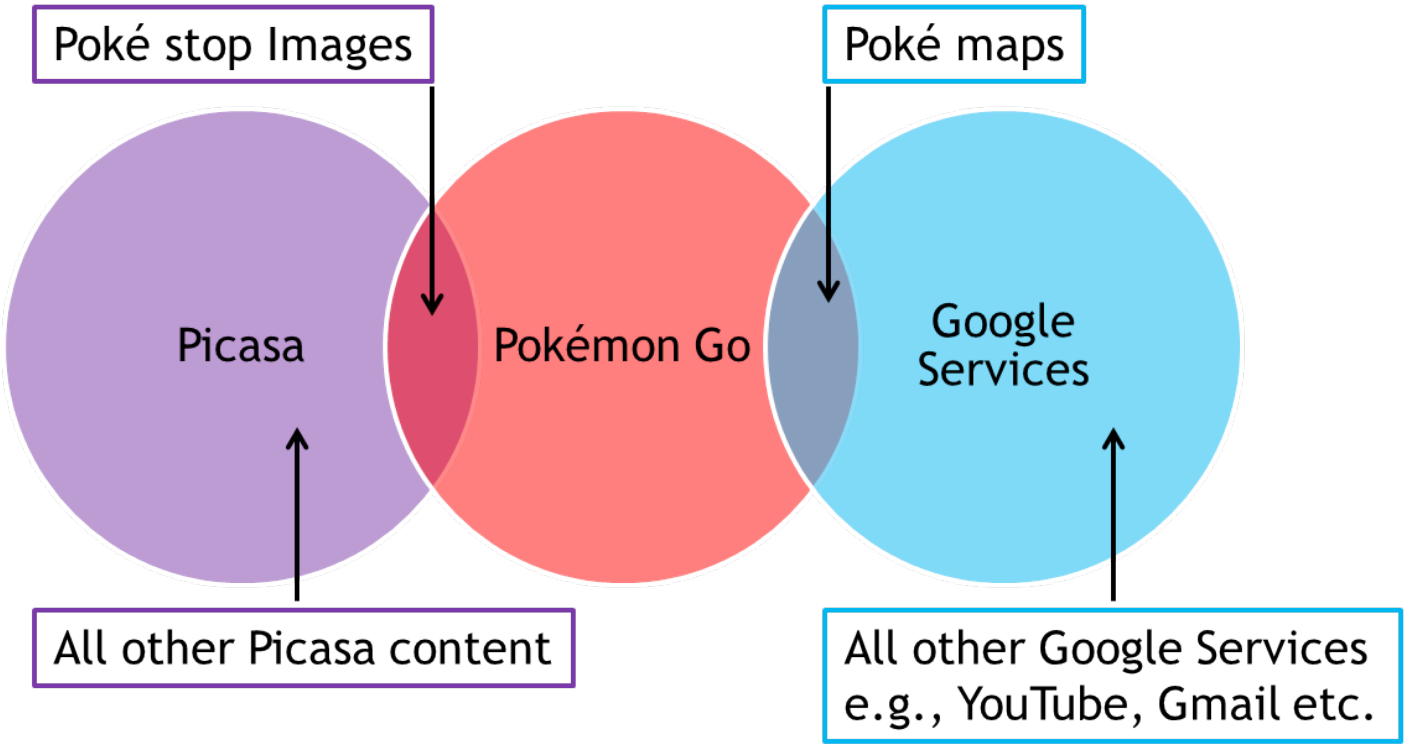


Figure 5: Isolating the correct external services related to mashup applications



Much like the previous example, applications that aggregate content from multiple sources (e.g., Flipboard, Apple News, Reddit, etc.) are also incredibly difficult to zero-rate. The problem with aggregator applications is that the bulk of the application's content is not stored in one location. The requirement to pull content from external sources means that a CSP needs to zero-rate the aggregator application (e.g., Flipboard) to enable the user to view the headlines, while also zero-rating every website from which the application pulls content (e.g., New York Times, Wall Street Journal, Globe and Mail etc.).

Essentially, CSPs are left with 2 options: building and zero-rating a list of all associated application traffic, or zero-rating all web traffic. Unfortunately, neither of these options is ideal as the list would be very difficult to assemble and it would require endless revisions. On the other hand, zero-rating all web traffic when the aggregator application is open is equivalent to offering an unlimited data plan. As a result, Sandvine does not recommend that CSPs zero-rate aggregator applications.

Avoiding Revenue Leakage

Ultimately, when determining whether to zero-rate something, each CSP must weigh the potential benefits (e.g., revenue growth, new subscribers, etc.) against the potential downsides (e.g., revenue leakage due to inaccurate traffic identification or enforcement rules, challenges of explaining the plan to subscribers, etc.). However, it should be noted that utilizing best-of-breed traffic classification technology and common sense enforcement policies can greatly reduce these downsides.

When it comes to traffic identification, it's important to note the differences between deterministic and heuristic/ machine learning detection speeds. Deterministic methods are typically the fastest methods a CSP can use to identify application traffic. As a result, zero-rated applications that can be identified through deterministic measures have almost no risk of revenue leakage (assuming the CSP is utilizing a standards compliant online charging architecture[8]).

On the other hand, heuristic and machine learning measures typically have a small detection delay as they must analyze a small amount of traffic before correctly identifying it. Due to this delay, zero-rated applications that require heuristic and machine learning identification techniques have a slightly higher risk of revenue leakage. It's important to note that the risk of revenue leakage due to heuristic or machine learning delays is negligible if a CSP is utilizing a best-of-breed traffic identification system. Table 4 provides a simple breakdown of each type of application, the detection methods required, and the risk of revenue leakage.

Table 4: Risk of revenue leakage associated with different traffic identification techniques

Zero-Rated Application Candidate	Deterministic	Heuristic/ Machine Learning	Detection Speed	Risk of Revenue Leakage	Risk of Revenue Leakage after Best Practices
Entire Application	Yes	No	Very Fast	Very Low	Very Low
Specific Application Feature	Yes	Yes	Fast	Low	Low
Mashup application	Yes	No	Fast	High	Low
Aggregator Application	Yes	No	Fast	High (zero-rating not recommended)	

As one can see (in Table 4), mashup applications pose the greatest risk of revenue leakage (ignoring aggregator applications, which we don't recommend for zero-rating). This risk is due to the fact that one or more external data sources associated with the mashup application must also be zero-rated (or enabled with reasonable limits) for the application to function.

In practical terms, if a CSP doesn't build sufficient rules into the enforcement policy for the associated application traffic, then subscribers will receive unlimited usage of the main mashup application and all of the associated services. For example, if the mashup application relied on Google services for mapping capabilities, then the

8. Online charging is discussed in detail in this whitepaper: https://www.sandvine.com/resources/whitepapers/online-charging.html

CSP could be subject to very high revenue leakage because customers could theoretically use any Google service (YouTube, Gmail, Maps, Photos etc.) for free as long as the zero-rated mashup application was open. The aforementioned free Google services are enabled because it is not technically possible to identify—with 100% certainty—what proportion of the Google service is used for the mashup application and what proportion is unrelated. Thankfully, there are multiple options that CSPs can use to reduce exposure to revenue leakage from mashup applications.

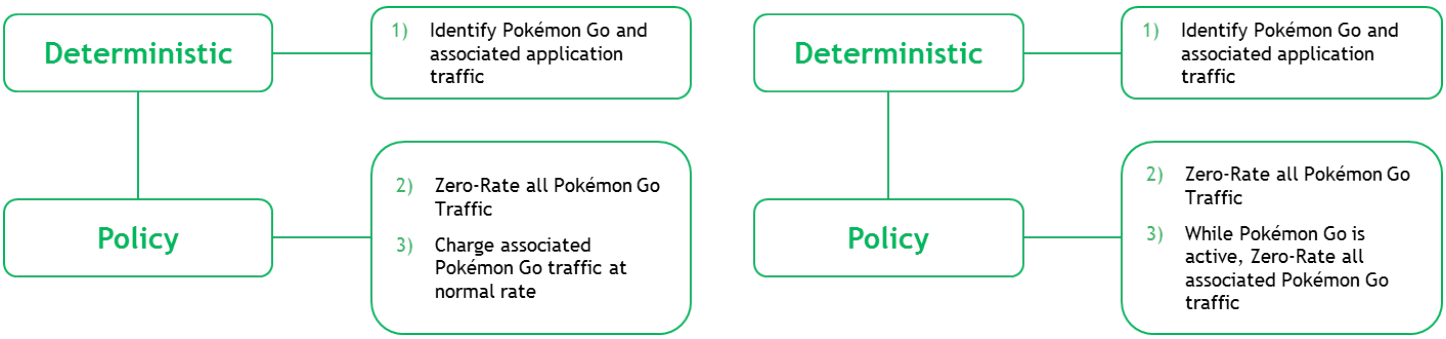
To avoid mashup application revenue leakage, we recommend that CSPs build a reasonable enforcement policy that applies data limits to the external data services utilized by the mashup application. By providing data limits on the associated application traffic, CSPs significantly reduce their exposure to revenue leakage. CSPs should also develop a clear, transparent fair use policy that explains what traffic is unlimited and what is not. These steps will make zero-rating plans for mashup applications more profitable to the CSP and more understandable to the user. As previously mentioned, the CSP should receive policy enforcement instructions from their PCEF or charging gateway vendor (e.g., traffic classification profiles).

If a PCEF or charging gateway vendor fails to provide specific enforcement instructions or fails to recommend what the upper limits of external data traffic should be, then CSPs have two less effective zero-rating options for mashup applications.

Firstly, a CSP could zero-rate the mashup application as a bolt-on and charge the associated traffic at the normal rate (Figure 6). This option is not ideal as it doesn't work without a base plan and won't be easily understood by customers.

The second option is to simply zero-rate the interconnected app and all of the associated traffic (Figure 6). As previously discussed, the lack of limits on external services leaves the CSP vulnerable to revenue leakage and abuse of the zero-rated offering. Nonetheless, the approach may be more beneficial to the CSP than ceding ground to the competition by not offering the zero-rated plan.

Figure 6: Alternate zero-rating methods for mashup applications



Regulatory Concerns

The last point to consider before zero-rating an application is the regulatory environment. Due to the wide variety of traffic identification and enforcement techniques used in zero-rated offers, it's important to review the regulatory rules related to billing accuracy. For example, Ofcom (UK communications regulator) has set incredibly strict standards on CSPs with regards to charging accuracy. Essentially, a CSP must be able to accurately identify and charge for over 99.998% of all data traffic.[9]

Due to this high standard, it wouldn't be wise to launch zero-rated plans that relied on machine learning/heuristic detection in the UK, because the small delay when identifying traffic with machine learning/heuristics is sufficient to fall short. Once again, we recommend that CSPs utilize a best-of-breed traffic identification vendor with a proven track record.

Go-To-Market Messaging

Once the decision is made regarding what applications to zero-rate, the CSP needs to consider the go-to-market messaging. Confusing and unreasonably complex experiences are responsible for a large proportion of subscriber

9. http://stakeholders.ofcom.org.uk/binaries/consultations/metering-billing-2014/statement/statement.pdf

complaints, in general. Therefore, it's imperative that zero-rated plans are transparent and easily understood by subscribers. We recommend that any zero-rated application offering is:

1. Transparent about the traffic that is or isn't included
2. Easily understood by the subscriber
3. Able to notify customers of their zero-rated activity
4. Subject to a fair use policy

Transparency

For zero-rated data offers, all significant terms must be communicated to subscribers transparently, including:

1. The commercial terms (e.g., the price of the plan)
2. A detailed description of the zero-rated application(s) and applicable content, using terms and examples understood by subscribers
3. Any requirements/limitations to participate in the offering (e.g., only on select devices, or with select data plans)

Clarity

For simplicity's sake we recommend that CSPs zero-rate an entire application (e.g., WhatsApp) as opposed to a specific application feature (e.g., only WhatsApp messages). Subscribers find this holistic offering much easier to understand than zero-rating some application traffic, but not all.

In practical terms, if a CSP advertises unlimited Instagram, then all features within Instagram should be zero-rated. However, if a CSP chooses to zero-rate an application feature and not the entire application, then they should explicitly state what data traffic is and is not included in the plan (e.g., *"Unlimited WhatsApp Messaging. Voice and Video chat is not included."*). If the messaging for the zero-rated plan is not clear, then subscribers will become confused and frustrated with the offering.

When CSPs offer zero-rated bolt-on packages (e.g., in addition to a 1GB general data plan, a subscriber purchases a zero-rated application package or 'bolt-on') they must be transparent about which data is zero-rated and which data is applied to the normal quota. For example, a bolt-on plan should explicitly state what data is zero-rated (e.g., Facebook traffic) and explicitly state what Internet traffic will be charged to the baseline data quota.

In the case of mashup applications, CSPs have additional information to explain. As you recall, mashup applications require external data sources to operate. As such, when messaging a zero-rated mashup application plan, the CSP needs to explain which data is zero-rated and which is not. Due to the potential for confusion, Sandvine recommends that CSPs position mashup applications as being unlimited, but *"subject to a fair use policy"*, and then avoid ambiguity by clearly stating what that fair use policy is.

Notifications

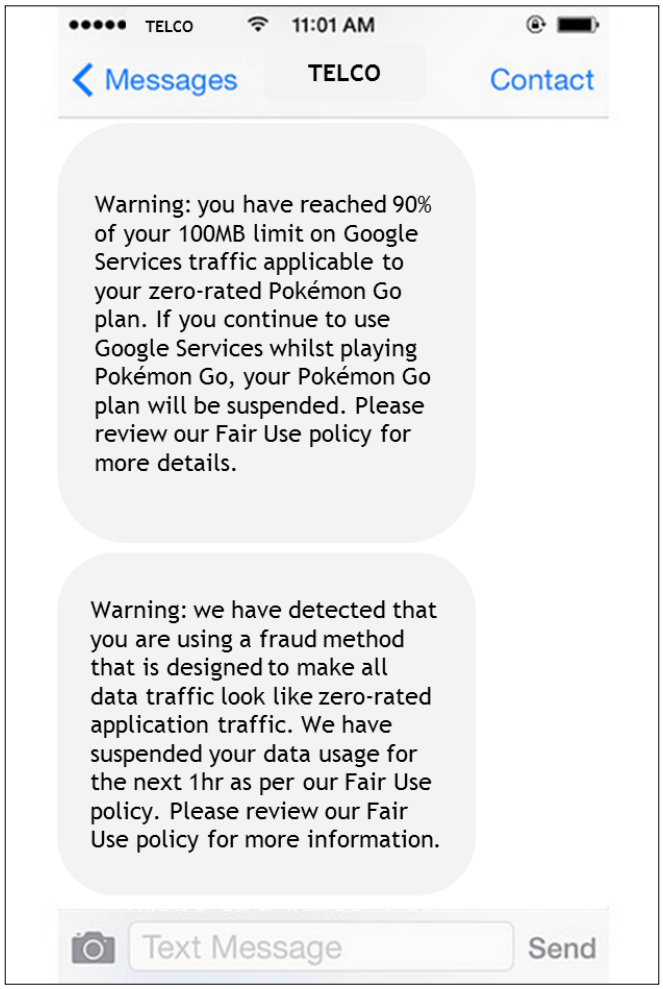
Additionally, for services (like Facebook) in which a user might click on a link and be taken to a different (i.e., not zero-rated) site, then—in accordance with the transparency principles—the CSP should alert the subscriber to that fact (e.g., a message along the lines of *"You are now accessing content that will be billed at your regular data rate of ___/GB"*).

In general, CSPs should notify subscribers when they are using zero-rated data, to provide confirmation that the data counting is operating in accordance with the plan. Similarly, CSPs could also alert customers about the benefits of a zero-rated offering when they access applications that could be zero-rated but are currently being charged at the standard rate (e.g., when a subscriber who does not have the unlimited music plan accesses a streaming music service like Spotify). Optimally, both for subscriber convenience and effective upselling and cross-selling, the notification itself would allow recipients to click a button to engage in a workflow for opting into the zero-rated plan.

When a subscriber runs afoul of the fair use policy by committing fraud (e.g., with a masquerading application) or approaching the fair limits of use (e.g., by utilizing 90% of external services associated with an mashup application),

then the CSP should notify the subscriber and educate them on the consequences of their behavior (see Figure 7). The notification should also provide a link to the fair-use policy so that the customer can better understand how to avoid breaking the terms in the future.

Figure 7: Fair Usage Policy Notification



Fair Use Policy

When CSPs enable unlimited application usage, deceitful users have a strong incentive to engage in fraudulent behavior. To minimize this risk, it's critical that CSPs develop a fair use policy for all zero-rated application plans. We recommend that a CSP's fair use policy includes language that explicitly forbids users from using masquerading agents and applications to disguise data traffic.

The fair use policy should also explain the limits that the CSP has placed on external services (e.g., Google Maps) required for mashup applications (e.g., Pokémon Go). To better inform customers, CSPs should explain why there are limits on the external services and what the ramifications are for exceeding the limits (e.g., three-strike rule before traffic is blocked).

Conclusions

Application zero-rating is a fantastic way for CSPs to offer additional value to their customers and differentiate from the competition. However, the success of zero-rated subscriber plans depends on a CSP's careful consideration of a number of factors:

1. Selecting the ideal application for zero-rating: The most ideal applications for zero-rating have a high active user base, utilize low bandwidth, and are accurately identified. High bandwidth applications can also be great zero-rating candidates, but should be offered in combination with a premium data plan or device to offset the cost.
2. The ability to accurately identify the application: To identify all types of applications or application features, a CSP requires a solution that utilizes a combination of deterministic and heuristic/machine learning technology. Applications that only require deterministic measures for identification are the easiest to zero-rate.
3. The ability to enforce a zero-rated policy: CSPs should rely on their PCEF or gateway charging vendor for specific instructions on how to zero-rate applications. Enforcement rules are incredibly important when zero-rating complex mashup applications or isolating specific application features.
4. Revenue Leakage: To minimize revenue leakage, CSPs need a combination of fast detection and well thought-out enforcement policies. As such, we recommend that CSPs utilize best-of-breed traffic identification solutions.
5. Regulatory Concerns: Before launching a zero-rated plan, ensure that you are not violating net neutrality or charging/billing standards.
6. Consumer Messaging: Make sure that all zero-rated plans are transparently communicated and can be easily identified by the subscriber. When zero-rating applications that rely on external sources, CSPs should develop a fair use policy. We also recommend that CSPs notify users when they are using zero-rated data and when they are being charged at a normal rate.

Additional Resources

Thank you for taking the time to read this whitepaper. We hope that you found it useful, and that it contributed to a greater understanding of application zero-rating, and the challenges and benefits such offerings bring to communications service providers.

In addition to the resources cited in this document, please consider reading these documents related to zero-rating, all of which are available on our website:

- *Standards-Compliant Online Charging*[10]
- *Traffic Classification: Identifying and Measuring Internet Traffic*[11]
- *Best Practices for Zero-Rating and Sponsored Data Plans under Net Neutrality*[12]

If you have any feedback at all, then please get in touch with us at **whitepapers@sandvine.com**.

10. https://www.sandvine.com/downloads/general/sandvine-technology-showcases/standards-compliant-online-charging.pdf
11. https://www.sandvine.com/downloads/general/whitepapers/identifying-and-measuring-internet-traffic.pdf
12. https://www.sandvine.com/resources/whitepapers/best-practices-for-zero-rating-and-sponsored-data-plans-under-net-neutrality.html

This whitepaper is published by Sandvine Incorporated ULC©. All rights reserved. No part of this publication may be reproduced, copied or transmitted in any form or by any means, or stored in a retrieval system of any nature, without the prior permission of Sandvine Incorporated ULC. Although the greatest care has been taken in the preparation and compilation of this whitepaper, no liability or responsibility of any kind, including responsibility for negligence is accepted by Sandvine Incorporated ULC.

© Copyright: Sandvine Incorporated ULC 2016

sandvine®

Intelligent Broadband Networks

408 Albert St. Waterloo, Ontario Canada N2L 3V3

www.sandvine.com