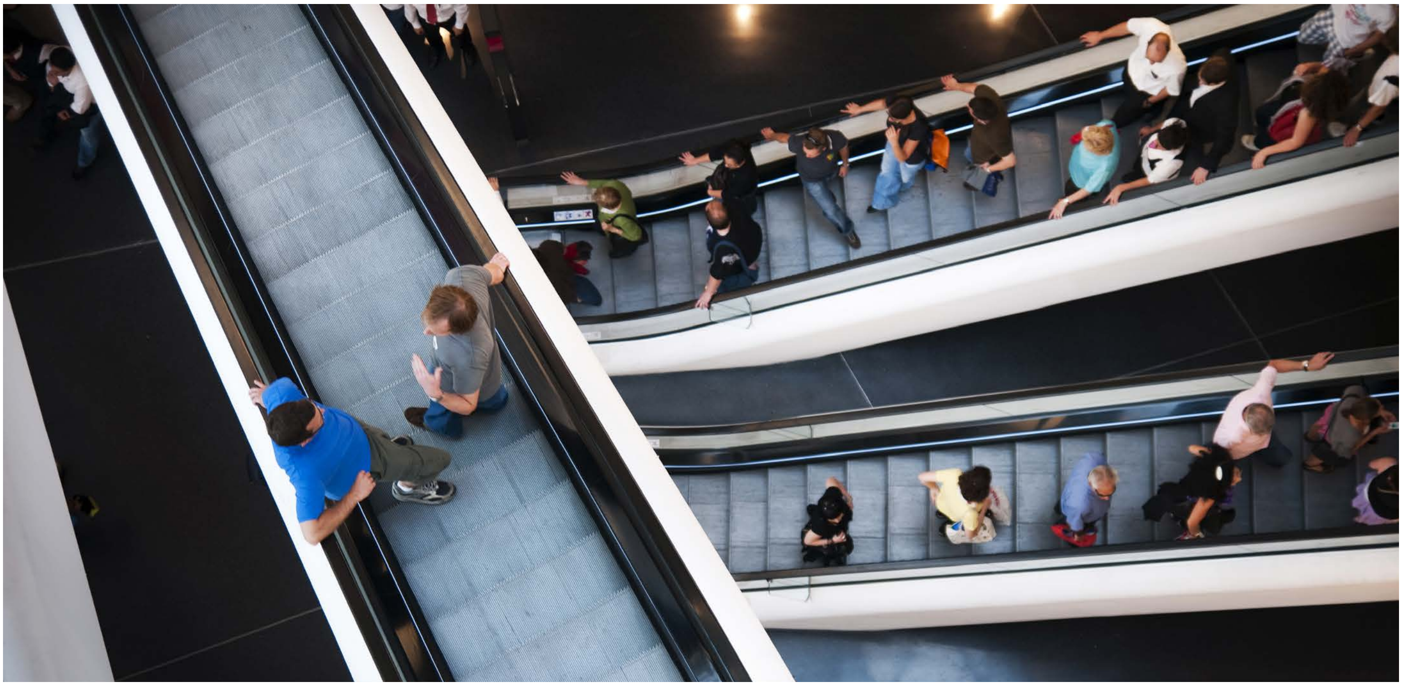


MONETIZE OVER-THE-TOP MOBILE APPLICATIONS

ALCATEL-LUCENT MOBILE APPLICATION ASSURANCE ON THE 7750 SERVICE ROUTER MOBILE GATEWAY

APPLICATION NOTE

ABSTRACT

Mobile telecommunications was a lot easier when services spanned just voice, SMS, and basic data. But with the advent of better smartphones and LTE data speeds, a deluge of over-the-top (OTT) apps like Skype, Facebook, and Netflix have changed the dynamics of the business. Today, devices tailored with user-specific apps are the norm and end users are expecting personalized services along with personalized pricing … creating service value for each individual.

As a service provider you may be struggling to stay abreast of the innovation and asking yourself: how can I turn this challenge into a new revenue opportunity? How can I change the business model? How can I avoid becoming just a fat data pipe?

This application note will discuss how Alcatel-Lucent's Application Assurance (AA) is able to dynamically manage applications by performing integrated, real-time L4-L7 inline traffic inspection and processing. This rich set of capabilities can help you personalize service offerings for your subscribers, manage the subscriber experience, and secure your network — without adding unnecessary complications or affecting your network topology.

TABLE OF CONTENTS

THE NEED FOR APPLICATION-LEVEL VISIBILITY AND CONTROL

Mobile Network Operators (MNOs) are rapidly recognizing the need to enable application-level visibility and control as a toolset that allows them to personalize and dynamically manage new mobile broadband services. In addition, the same tools can be used to efficiently protect and secure the integrity of their network.

With this application visibility, MNOs will have access to information on application-usage trends. This information will help them to better engineer their network while understanding the applications and service offerings that are most valuable to their subscribers, allowing introduction of relevant value added services and charging plans.

The following sections explain the service requirements where application-level visibility and control is needed.

Application identification and charging

The ability to identify and charge for specific traffic flows pertaining to individual service packages a subscriber has purchased opens up new revenue opportunities for the MNO while personalizing the service for the subscriber. An example would be an unlimited social media package for which the subscriber pays a monthly fee, which ensures that all packets pertaining to social media applications are zero-rated. In general the ability to identify a range of applications, or web content by HTTP URL is the basis of many mobile charging rules.

This breed of capabilities is on the upswing, and Infonetics believes that this requirement is one of the key trends in 2014:

> "… operators look to introduce new service bundles and pricing models that better correlate the price being charged with the bandwidth being consumed. [5]"

Control

Per-subscriber dynamic control of specific services is important for MNOs to manage their network resources while creating a contractually fair environment that ensures the subscriber abides by the terms of usage and allows the MNO to take measures to ensure that other subscribers do not suffer when some subscribers become heavy users, potentially unfairly impacting the service experience of other users.

An example of a control use case is enabling the MNO to be informed when a subscriber has exceeded a data usage allowance on a specific service tier and acting on this in a dynamic manner. Actions could include notifying the subscriber, rate limiting some or all applications, redirecting some web applications to a portal landing page, or proposing to the subscriber to subscribe to a different service tier.

Other examples of using application-level control include enabling network-based parental control, blacklist filtering of known malicious or offensive websites, and tethering detection and control for unlimited use plans. Regarding parental control, Heavy Reading says:

> "Parental Control is being driven especially by higher ownership among children of devices, tablets and laptops. Whitelists based on URL identification is one approach that is gaining more interest" [4].

Traffic management

Being able to dynamically identify and manage the traffic of specific applications for a given subscriber is important to both protect the network and maintain the data services of the subscriber. One classic example is managing the volume of peer-to-peer (P2P) traffic when certain subscriber or network thresholds are exceeded. Ideally, this capability should be refined by adding conditions such as time of day, day of week, subscriber profile and entitlements, and other criteria such as APN.

Another form of traffic management is the ability to proactively and temporarily manage subscriber traffic that traverses cell sites that are considered to be in a congested state. By leveraging application-level control, when subscribers are being served in a congested cell, traffic from specific usage-heavy applications could be candidates for throttling. Heavy Reading sees this as an important capability:

> "There is increasing interest in finding better ways to manage congestion in real time at the level of the individual cell and subscriber" [4].

Security

Visibility and control at the application level can be another tool in the constant fight against mobile security threats. The quantity of worldwide mobile devices is soaring and there is a significant increase in processing power and access network (3G/LTE) speeds. These are all factors that are collectively contributing to mobile devices and their applications emerging as serious security threats to the network and to other devices. In fact, the Kaspersky Security Bulletin for 2013 shows a dramatic increase in malware attacks on smart mobile devices [6].

For example, mobile devices supporting over-the-top (OTT) user-to-user video-calling applications are at risk of attack by viruses or bots that can initiate traffic flows towards other devices on the network. To protect against this, the MNO will generally need to ensure that user-to-user traffic passes through a firewall.

Using a Layer 7 application-aware stateful firewall in the mobile gateway itself avoids the costs and complexity associated with forcing all user equipment-to-user equipment (UE-to-UE) traffic to pass through the centralized Internet firewall. This reduces the firewall costs significantly, reduces traffic across the mobile core, and provides a better user experience.

Business intelligence

Application-level business intelligence is an important area that MNOs can use to understand mobile applications and how prevalent they are in their network while also understanding application trends over prescribed periods of time. Understanding bandwidth consumption trends from specific applications such as social media or determining if there is a specific new application that is exploding in popularity may be important for both network planning and also to understand new consumer trends that could lead to new service options for the MNO.

As an example, some MNOs are considering offering subscriber free WhatsApp Messenger[1] services, even if the charged quota is exhausted, and will differentiate and charge their WhatsApp Messenger sessions with rates defined by Policy and Control Charging Control (PCC) policy rules. Any such consideration starts with a detailed understanding of the application itself and how it impacts the network and its performance.

[1] WhatsApp Messenger is a cross-platform mobile messaging app that allows users to exchange messages without needing to pay for Short Message Service (SMS).

THE OPTIMAL ARCHITECTURE AND IMPLEMENTATION

This section discusses the optimal network architecture and implementation for application assurance.

Application assurance defined

To address the emerging needs for MNOs to have dynamic application-level visibility and control, Alcatel-Lucent offers Application Assurance (AA) as a feature set of the Alcatel-Lucent 7750 Service Router Mobile Gateway (SR MG). Alcatel-Lucent AA performs integrated, real-time L4-L7 inline traffic inspection and processing for managing any relevant application to the MNO from among all applications. The terms *integrated* and *inline* refer to the capability of performing these functions as a part of user (data) plane processing without additional equipment (external or internal to the Alcatel-Lucent 7750 SR MG).

Application Assurance is available as part of the 7750 SR MG [2] whether deployed as a Gateway GPRS Support Node (GGSN) or a Packet Data Network Gateway (PGW), and whether the gateway implementation is a physical node or part of a virtualized EPC.

Application Assurance identifies bearer plane applications by implementing real-time, stateful traffic inspection and identification of packets and flows. After a particular network application is identified, enforcement and charging actions can be performed in accordance with statically or dynamically configured policies as part of the PCC rules configuration of the gateway.

Web application support

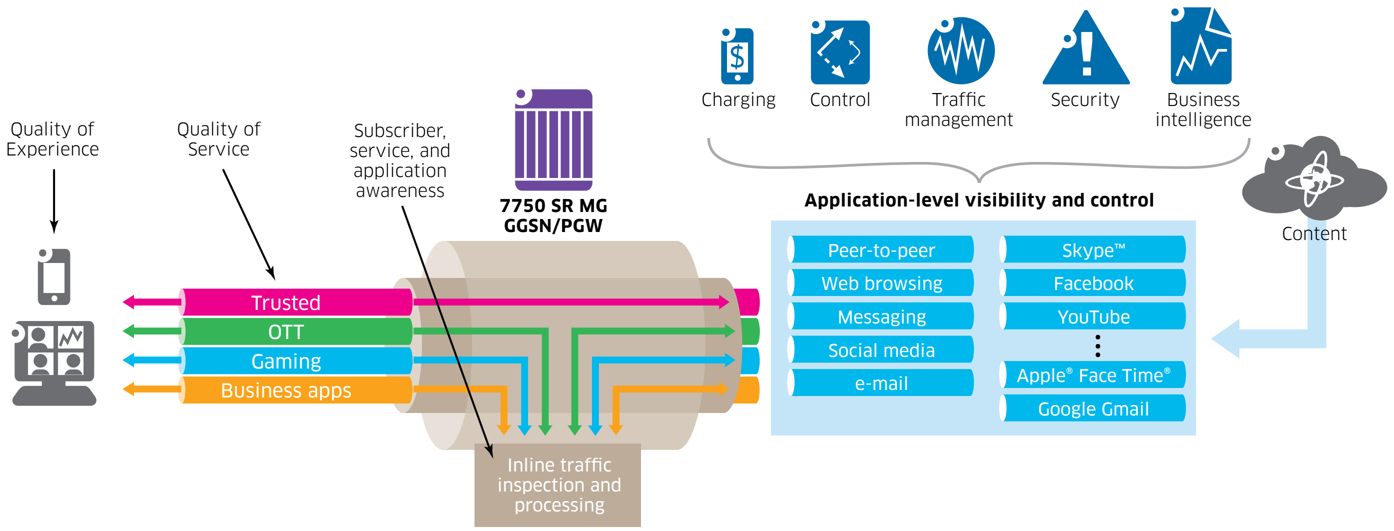
Application identification for web applications includes support for both Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS) sessions when they are used to transport the application packet flow. This is important because HTTPS use is increasing, is now used by over 30 percent of all mobile traffic. HTTPS is HTTP tunneled in a Secure Socket Layer (SSL)/Transport Layer Security (TLS) session. As such, application Identification for HTTPS traffic uses the initial setup of the SSL/TLS session, which provides the domain/application information required to identify the traffic used in that session.

AA: assuring and protecting

As can be seen with the HTTPS explanation, AA identifies applications without performing payload content inspection since the privacy of a subscriber's content is of paramount importance to Alcatel-Lucent, the MNO, and the subscriber. So while AA will identify a particular packet flow that may represent an e-mail or a video stream, the 7750 SR MG will not examine the content of the e-mail or even the title of the video. Application Assurance protects and assures the performance and the value of the applications used by the subscribers while also protecting the content.

Figure 1 shows the functional data flow of network content (right side) and various identified application flows as they traverse the mobile network through the 7750 SR MG and are identified and controlled through AA.

Figure 1. Mobile Application Assurance



7750 SR mobile gateway implementation

The 7750 SR Mobile Gateway (MG) physical implementation of AA is through its Mobile Gateway – Integrated Services Module (MG-ISM). The MG-ISM is a hot-swappable module that fits into any of the input/output (I/O) slots of the Alcatel-Lucent 7750 SR MG to provide PGW functionality for LTE networks or GGSN functionality for 2G/3G networks.

User-plane traffic — bearers in LTE or Packet Data Protocol (PDP) contexts in 2G/3G — is directed to and processed through the MG-ISM from the 7750 SR MG backplane and switching fabric. This functionality avoids the need for the MG-ISM to directly support external I/O ports, thereby maximizing its packet processing performance. The MG-ISM uses dedicated processing resources for AA and as such does not impact the performance of control plane or non-AA-treated data traffic.

Processing of user-plane traffic can include AA providing real-time L4-L7 inline traffic inspection and processing as defined by MNO-configured application-level policies. Policies and charging rules are compliant to 3GPP's PCC architecture as described in the next section.

Application Assurance also supports a virtualized deployment option where the virtualized Mobile Gateway (vMG) network function is supported on virtual machines that are allocated, sized, and maintained by the cloud infrastructure on which the vMG network function is instantiated. It is important to note that the functionality of the 7750 SR MG with AA does not change in a virtualized deployment. Specifically, AA is still an inline inherent capability for every instance of the vMG.

Policy and charging control in the 3GPP architecture

The 3GPP R11 and R12 PCC architecture define a framework to perform policy-based charging and control at both the application and bearer levels. PCC encompasses two main functions:

- Flow-based charging, including charging control and online credit control
- Policy control, including gating control, Quality of Service (QoS) control, and QoS signaling

The two essential PCC elements needed to perform these functions are the Policy and Charging Rules Function (PCRF) and the Policy and Charging Enforcement Function (PCEF). The PCRF collates subscriber and application data, authorizes QoS resources, and instructs the user (data) plane element how to further process data traffic. The PCEF is a data plane element that implements the enforcement function and typically resides on the mobile gateway (GGSN or PGW).

The PCEF uses PCC rules to classify traffic into service data flows (SDF) and apply to them the appropriate policy and charging control as instructed by the PCRF.

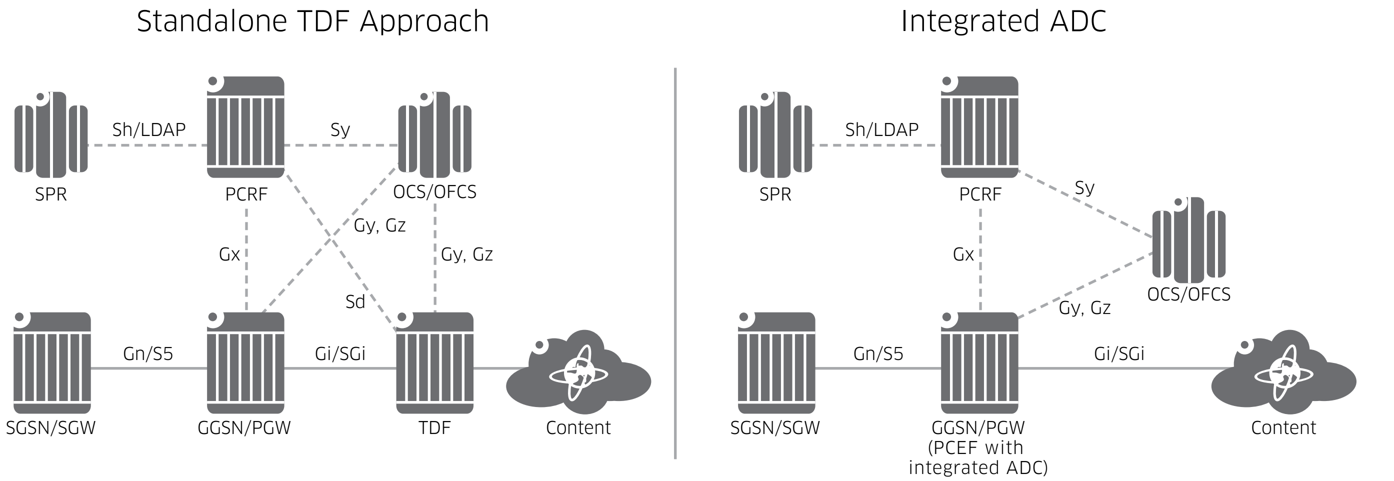
Policy and charging control through the PCC rules can be predefined (pre-provisioned) on the PCEF or instantiated dynamically to the PCEF from the PCRF. Dynamic PCC rules are derived from the PCRF, taking into consideration the subscriber profile as well as additional real-time and dynamic information such as subscriber and application usage, requested QoS, and other subscriber- or traffic flow-specific data if available.

Within the PCC framework, MNOs can extend the policy enforcement and charging rules to apply to applications as well as bearers. 3GPP prescribes two methods to provide these L4-L7 application detection and control (ADC) capabilities:

- Integrate the ADC capability in the PCEF and extend the PCC rules to include application-level control in addition to bearer-level control, all done through the Gx interface and with a single Gy/Gz interface for charging
- Deploy an external Traffic Detection Function (TDF) as a standalone appliance that uses the Sd interface to interact with the PCRF to coordinate the policy enforcement and charging between the two subscriber policy enforcement points

Figure 2 shows a side-by-side comparison of both architectural models.

Figure 2. Application Detection and Control Methods within the PCC Architecture



A standalone TDF, under Sd control, implies that two policy enforcement points will exist in the network:

- The PGW/GGSN using PCC rules via Gx for per-subscriber bearer authentication and policy control, with Gy for bearer-based charging control
- The TDF using PCC rules via Sd for per-subscriber application policy control, with Gy for application-level charging

3GPP R11 states that for application-based charging services either the PCEF or the TDF shall be used, but not both. This requirement necessitates additional integration into the Operations Support System (OSS)/Business Support System (BSS) to move charging functions from the mobile gateway to a TDF appliance.

3GPP R12 is intended to add support for billing interfaces from the TDF but work in this area is not complete and will require the MNO to implement multiple charging interfaces.

Alcatel-Lucent has adopted the integrated ADC model on the 7750 SR MG, offering a single subscriber policy enforcement and charging point for the network under a single policy interface whether the mobile gateway is physical or virtualized. The benefits of this approach include a simplification of the network topology, a seamless coupling of the PCC rules, and unified policy and charging control between both bearer and application layers.

With an integrated ADC function there is always 100 percent accuracy for charging because all packets are processed and charged from a single enforcement point. In addition, with an integrated ADC, all locally routed traffic is covered with AA, including the ability to provide an L7 firewall between UE-to-UE traffic within and between mobile gateways.

Table 1 lists some of the challenges that exist with a standalone TDF and how these challenges are addressed by deploying an integrated ADC.

Table 1. Benefits of an Integrated ADC

CHALLENGE WITH STANDALONE TDF APPROACH	SOLUTION ADDRESSED BY INTEGRATED ADC
Requires additional control interfaces (such as Sd) and additional OSSs/Network Management Systems	No new interfaces and management systems
Maintenance, provisioning, and scaling dependent on another network function and possibly another vendor	Maintenance, provisioning, and scaling all done within existing 7750 SR MG
For locally routed (UE-to-UE) traffic, the MNO will lose visibility and control provided by the TDF or will be forced to block local routing, forcing all local traffic to the internet	All traffic is visible because ADC capability is integrated within the 7750 SR MG
Possible charging discontinuity because the TDF and PCEF are not always in synch; for example, PCEF charging for uplink (UL) packets that are policed/dropped by TDF policies This also increases operational complexity cost to move all charging functions from PCEF to TDF.	No additional OPEX because there is full internal coupling among the application, the bearer, and charging; no discontinuity, leading to 100 % accuracy of charging
Use of standalone TDF can require a topology change (and therefore additional OPEX/CAPEX) because it must be placed at the private side of a Carrier Grade Network Address Translation (CG-NAT) function for subscriber visibility. If NAT is supported by the PGW/GGSN, the MNO needs to incur the additional costs of having NAT moved out to a separate appliance.	With the integrated approach the ADC function is always on the private side of the NAT function, whether NAT is implemented in the MGW or in a separate appliance.
Standalone TDF must deal with traffic asymmetry removal, which is complex and costly (links/bandwidth/topology changes)	No asymmetry at the mobile gateway point of the network
Standalone TDF deployment involves complexity to provide efficient geo-redundancy in the case of a GGSN/PGW or TDF failure.	Stateful geo-redundancy available with the integrated approach with Inter Chassis Redundancy (ICR) available on the 7750 SR MG
With standalone TDF on the Gi interface, there is no possibility to assign specific QoS with knowledge of bearer or RAN contexts.	With the integrated approach, full knowledge of bearer and RAN contexts and state is available so that hierarchical QoS can be deployed to make TM techniques much more effective.
Standalone TDF sits on the Gi between the mobile gateway and the Internet, seeing all Internet traffic for all subscribers, incurring costs in network capacity (links), processing capacity, latency, and reliability/availability by having all traffic go through it	With the integrated approach on the 7750 SR MG there is flexibility to do ADC only on traffic that benefits from the processing, by subscriber (depending on the service plan) and by bearer type/IP forwarding class.

Despite the benefits of the integrated ADC approach, there are some network deployments that use external standalone TDF appliances in cases where the mobile gateway vendor does not provide the feature set and performance required by the MNO. However, it is the Alcatel-Lucent position that, whenever possible, the mobile gateway integrated ADC capability should be used due to the significant cost savings, network simplification, and reduced OSS/BSS integration requirements.

With AA, Alcatel-Lucent delivers the scale, performance, and sophistication of leading ADC implementations but which is fully integrated as part of a single policy enforcement point in the mobile gateway.

USE CASES

Introduction

Mobile Application Assurance extends the service depth of the Alcatel-Lucent 7750 SR MG by enabling visibility and intelligent control for IP applications, including extensive per-application, per-subscriber, or per-APN policies. Mobile AA enables a range of control/action, analytics, and accounting service capabilities that are important across the range of mobile services.

In this section we describe some specific, real-world use-cases of mobile AA. Table 2 lists these use cases and provides a brief description of each.

Table 2. Mobile AA Use Cases

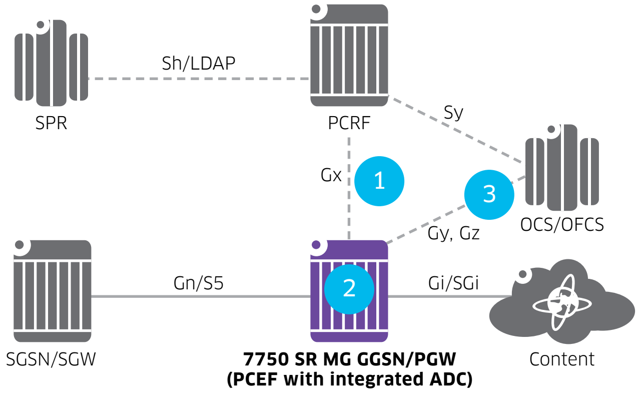
CATEGORY	USE CASE	DESCRIPTION
Application-level charging	L7 application identification and charging	Classifies on-net and Internet-based applications for charging/control
	Per-application, per-subscriber zero rating	Identifies specified free Internet-based applications and applies a zero rating charging policy
	Per-APN charging and policy	Provides application-level policies and charging options per APN as well as any other use cases listed below
Traffic management	Fair usage enforcement	Throttles and controls specific subscriber applications with unique charging and QoS profiles to enforce fair use of network resources
	Intelligent Traffic Management (ITM)	Dynamically throttles specific non-conforming applications that traverse Radio Access Network (RAN) resources in a state of congestion and releases the applications when congestion subsides
Security	Layer 7 stateful firewall	Protects subscribers against unsolicited traffic from the Internet and also from other subscribers on same PGW/GGSN
Application policy control	Per-subscriber dynamic policy control	PCRF-driven, dynamic per-subscriber, per application network control
	Authentication via HTTP enrichment	Provides enhanced, value-added web services, giving the subscriber a better customized experience based on HTTP header information used within the subscriber authentication process
	HTTP redirection and captive portal	Redirects specific subscriber HTTP requests to a dynamically activated captive portal to personalize or upsell the service
	Tethering detection and control	Detects subscriber tethering state and notifies PCRF that MNO-defined policies and enforcement models for this condition will be applied
	Parental control	Leverages Internet Content Adaptation Protocol (ICAP) client integrated within AA for large-scale HTTP/HTTPs URL filtering to determine acceptable web content with per-subscriber classification policies

CATEGORY	USE CASE	DESCRIPTION
	Network-based URL blacklisting	Mobile gateway local blacklists provide file-based URL blacklists, leveraging filter rules that are applied to all subscribers
	In-browser notification	Enables MNOs to provide notification messages to the subscriber's device web browser in the form of an overlay, banner, or full web-page messages
Business intelligence	Application-usage reporting	Offers visibility on application usage across all subscribers in the network; statistics can be exported from the mobile gateway to external analytics tools such as the Alcatel-Lucent 5670 Reporting and Analysis Manager (RAM) [1]
	Top HTTP domains and device types	Provide statistics on most popular web domains, device types, and operating systems used
	Mean opinion score (MOS) measurements and reporting for Voice over Internet protocol (VoIP) or VoLTE (Voice over Long Term Evolution)	MNO can generate reports on VoIP audio quality and CODEC used across different subscribers for different VoIP applications

Application charging

Application charging enables the delivery and monetization of enhanced personalized service bundles. This is done on a per-subscriber, per-application basis where specific packet flows can be uniquely charged or zero-rated (packets counted but not charged). A popular example of this is unlimited social networking packages where some or all applications of a prescribed group called Social Networking are not counted against the usage quota for subscribers who opt in to this service.

Figure 3. Zero-Rating Social Media Traffic



1 When Subscriber X connects to network, a social media charging policy is sent to the 7750 SR MG based on their service plan

2 When Subscriber X receives traffic from a social media site, mobile AA classifies it, enabling PCC rules to zero-rate all packets from these applications

3 7750 SR MG sends subscriber charging counts per rating group to the charging system via Gy

Another example is unlimited P2P traffic during off-hours when after a specific time P2P traffic is not charged or is charged at a much lower rate. This shifts the subscriber behavior to use the network for bandwidth-intensive applications at times where they pay less and thereby creates a smoothing effect on the network utilization.

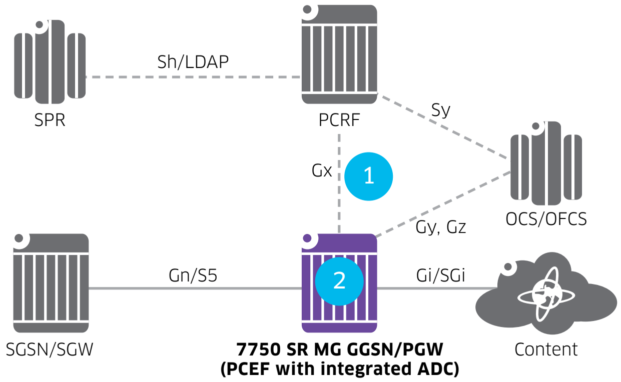
Per-Access Point Name (APN) charging and policy capability allows the MNO to create and apply any application-based charging policy for all subscribers of a given APN. For example, a corporate APN may block access for certain applications at all times or by time of day, which generally would not be the norm for a general subscriber APN.

Application traffic management

Application traffic management enables the MNO to control traffic at the subscriber and application level to implement fair-use policies. This capability can be used to prevent the disproportionate consumption of resources by some applications by limiting application volume across all subscribers or on a per-subscriber basis.

For example, a limit can be applied representing a percentage of network capacity that can be used by file-sharing applications. Or a certain usage limit can be applied to subscribers based on particular applications as specified in their contract terms of use.

Figure 4. Application Traffic Management – Fair Use



1 When a bronze subscriber connects to the network, PCRF establishes a fair use PCC ADC rule for file sharing that is instantiated on the 7750 SR MG

2 Mobile AA counts traffic for bronze subscribers from file-sharing applications; when certain contractual limits are exceeded, traffic is policed down to a prescribed level

For ITM, these policy rules can be invoked or adjusted based on dynamic network congestion observed in the RAN.

With AA, traffic management can be immediately applied to each application that has been identified, independent of needing to be bound to a specific Service Data Flow (SDF) as long as differentiated charging is not required. This option will result in improved scalability/performance.

Application security

The AA firewall capability extends application-level analysis to provide an inline integrated stateful firewall that protects subscribers from malicious security attacks. The AA stateful session filters, combined with L7 classification and control, empowers MNOs with an advanced, next-generation firewall functionality that is integrated in the 7750 SR MG.

In stateful inspection, the AA firewall not only inspects packets at Layers 3-7 but also monitors the connection’s state. If the MNO configures a “deny” action in a specific application session filter, the matching packets are dropped and no flow session state/context is created.

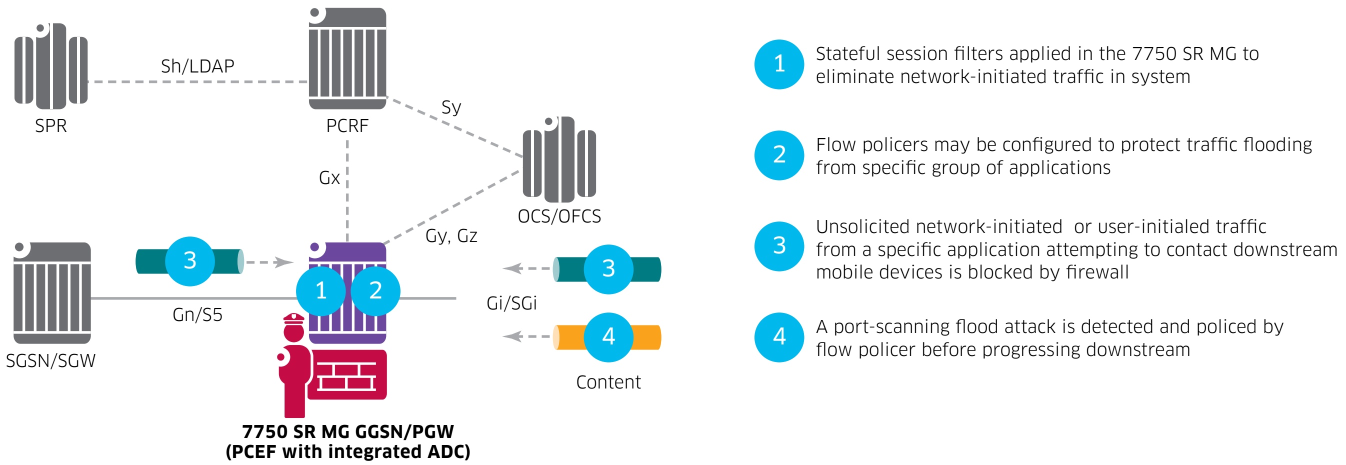
Stateful flow/session processing takes note of the originator of the session and therefore can allow traffic to be initiated from the subscriber while denying — if configured — traffic originating from the network. Packets received from the network are inspected against the session filter and only those that are part of a subscriber-initiated session are allowed.

Denial of Service (DoS) attacks work by consuming network and system resources, making them unavailable for legitimate network applications. Network flooding attacks, malformed packets, and port scans are examples of DoS attacks.

The aim of the AA firewall DoS protection is to protect subscribers and prevent any abuse of network resources. Using AA firewall stateful session filters, MNOs can protect their subscribers from any malicious port scan scheme by configuring the session filters to disallow any traffic that is initiated from the network.

In addition, an AA firewall provides configurable flow policers. Once configured, these policers prevent many types of flooding attacks (for example, Internet Control Message Protocol [ICMP] PING flooding, User Datagram Protocol [UDP] flooding, SYN flood attacks, etc.). These policers provide protection at multiple levels: per system, per subscriber, and per application/application group.

Figure 5. Application Firewall



1 Stateful session filters applied in the 7750 SR MG to eliminate network-initiated traffic in system

2 Flow policers may be configured to protect traffic flooding from specific group of applications

3 Unsolicited network-initiated or user-initialed traffic from a specific application attempting to contact downstream mobile devices is blocked by firewall

4 A port-scanning flood attack is detected and policed by flow policer before progressing downstream

Application policy control

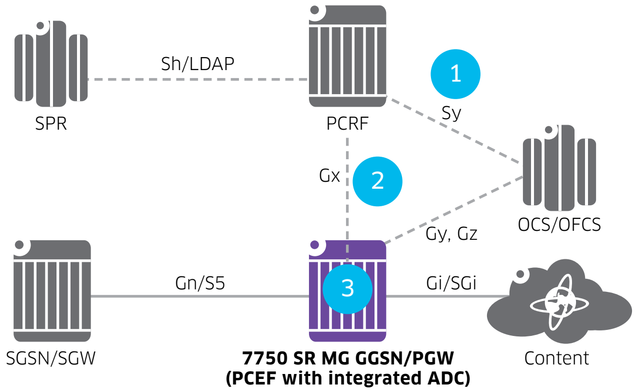
Dynamic application policy control is the ability to dynamically apply prescribed actions to different subscriber traffic flows. The per-subscriber application control via the Gx interface gives the MNO the freedom to use the different AA actions dynamically, on a specific subscriber application.

To offer flexible data plans that provide personalized subscriber policy options, the policy model of the mobile gateway must support sufficient scalability. For example, if a subscriber signs up for a social media package in addition to already purchasing the “gold” data package, and then signs up for a gaming package, there are now three different policy and charging policies applied to this subscriber.

With AA on the 7750 SR MG, a policy template and override approach is used that provides a base policy template with a la carte subscriber policy attributes called Application Service Options (ASOs) applied. This approach allows per-subscriber policy flags to be applied, ensuring a scalable approach to dynamic, flexible, per-subscriber policy under PCC rules. Some mobile gateways provide a more rigid approach to service policies that may not have sufficient scale to allow such flexible use of per-subscriber policy models.

Figure 6 is an example of an AA control use case where a dynamic policy-controlled action is instantiated based on an application that has exceeded a prescribed usage limit.

Figure 6. Per subscriber dynamic policy control in action



1 OCS informs PCRF through Sy that a specific application usage threshold has been exceeded for Subscriber X

2 PCRF sends new policy request through Gx to PCEF for that specific bearer channel or PDP context

3 PGW/GGSN leverages mobile AA to enforce new policy request by policing specific applications for that subscriber

With AA, dynamic subscriber control enables many other use cases, including:

- Per-subscriber, per-application HTTP redirect
- Per-subscriber, per-application header enrichment
- Per-subscriber tethering detection and control
- Per-subscriber, per application parental control
- Network-based URL blacklisting
- In-browser notification

HTTP redirect

Using HTTP redirect, the MNO can apply a policy that when an application's HTTP packet flow is blocked, the subscriber is directed to a web portal that displays relevant messages to indicate why the traffic is blocked, such as, "time-of-day policy to block specific content" or "top-up request." Without this capability, when HTTP packet flows are blocked, the subscriber application retries before it times out. In most cases, the subscriber is unaware of the cause of this timeout, leading to a possible reduction in goodwill and loyalty. If a non-HTTP packet flow is blocked, the Transport Control Protocol (TCP) session can also be reset (because HTTP redirect cannot be used) to improve the user visibility of the blocked session.

HTTP header enrichment

With HTTP Header enrichment, modification of the HTTP header is performed for traffic going to specific user-configured sites (URLs/IP addresses) to add a user's network-based information, such as Mobile Station-ISDN (MSISDN). An application web server site can then use this additional information to authenticate the user and/or present the user with user-specific information or services.

Tethering detection and control

Tethering detection and control allows MNOs who offer unlimited data plans to detect if and when their mobile subscribers are using tethering to access data services, which is typically defined as "not permitted" in the terms of use for unlimited usage plans. Tethering is a mechanism whereby a mobile user turns a mobile handset device into a cellular modem or cellular Wi-Fi® access point for other data devices, such as a laptop, to access the Internet.

Data traffic coming from tethered devices can be at a much higher rate than what a mobile handset generates and/or consumes, putting additional pressure on the MNO's network. With mobile AA, the MNO can identify tethering and install policies to handle tethering devices as it sees appropriate, including but not limited to: applying different charging, blocking tethered traffic, rate limiting tethered traffic, and/or redirecting the tethering mobile user to a portal that may allow opt-in to a fee-based tethering plan.

Parental control

Application Assurance delivers parental-control services (large-scale or per-subscriber URL filtering) by leveraging an ICAP client that interacts with an offline ICAP URL filtering service to deliver opt-in parental control services. This mobile gateway embedded capability dramatically reduces the costs of network-based URL filtering compared to using dedicated inline filtering appliances.

Only URLs for specific policy-defined subscribers or access points that have opted into the service are sent to the ICAP server, allowing URL filtering to have no impact on the IP network forwarding topology. This approach significantly reduces CAPEX and OPEX for the MNO by avoiding data path traffic steering to an inline web URL processing appliance and by keeping the URL classification function in an offline ICAP server.

Network-based URL blacklisting

In addition to offering parental-control URL filtering, AA also offers the ability to store local lists for tens of thousands of URLs to support use cases where 100 percent subscriber blacklist filtering is required. Examples include blacklisting URLs to guard against child sexual abuse, support sites subject to court-ordered Digital Millennium Copyright Act (DMCA), and other country-specific takedown lists.

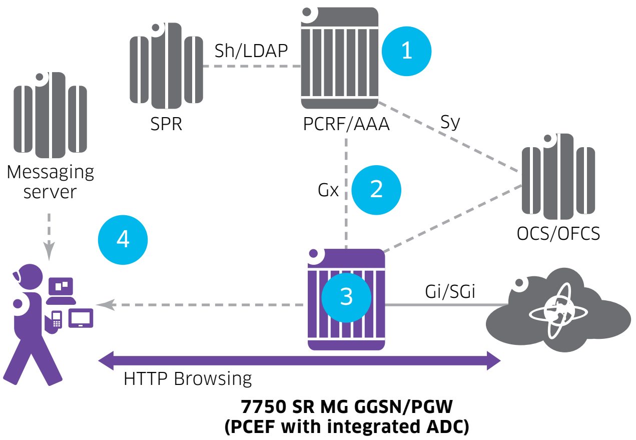
In-browser notification

Application Assurance also supports in-browser notification. This capability enables MNOs to provide notification messages to subscribers directly to their web browser in the form of an overlay, banner, or full web page when specific dynamic events occur. Examples of how this capability can be used include:

- Tethering detection notification: A message will appear on browser of the tethered device
- Welcome message (used in WLAN-Gateway when Wi-Fi is authenticated)
- Subscriber notifications: Over quota, late bill payment, network outage, and copyright infringement subscriber notification
- Advertisement embedded in select HTTP web pages

Figure 7 shows how in-browser notification works by allowing in-browser notification without the 7750 SR MG modifying the Internet web-server-provided content.

Figure 7. In-Browser Notification



1. Notification event (welcome, tethering, exceeds quota, network outage, etc.) is detected by mobile PCRF
2. Policy decision defining notification rules is provided to AA via AAA/PCRF subscriber policy
3. Mobile AA selects candidate flow for messaging, and redirects UE browser session to a messaging server
4. Message content is sent to specific subscriber's mobile device browser

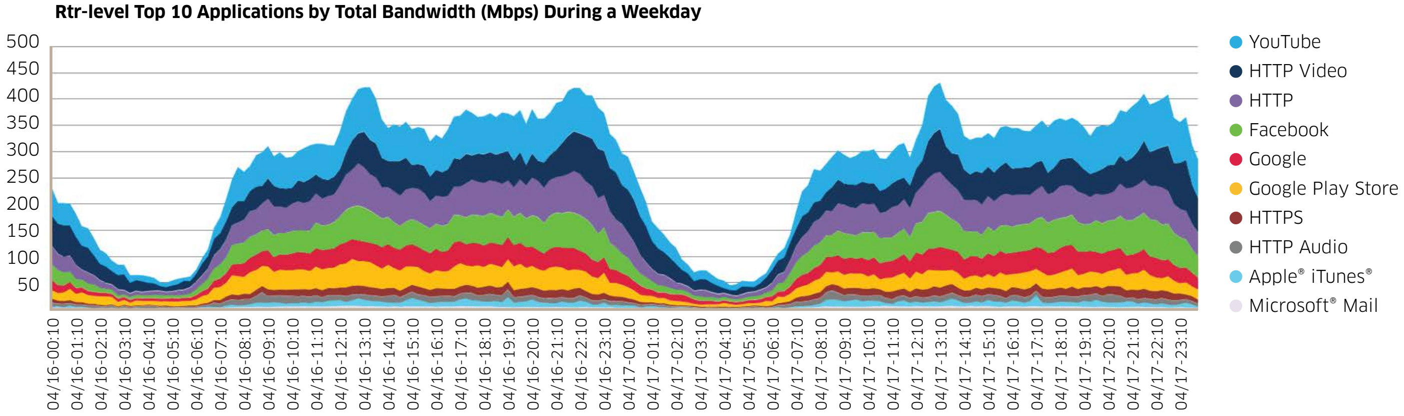
For more information about the Alcatel-Lucent in-browser notification solution, please see the Alcatel-Lucent *HTTP In-Browser Notification* application note [3].

Business intelligence

With AA, application usage reporting provides the MNO with insights to improve customer experience from an application or application-group perspective by providing visibility of the application usage by time of day and day of week as well as by device types and device operating system. In addition, MNOs can collect statistics regarding the host names and device types being used in different packet flows in the network. These per-flow statistics can be exported to a collector to enable intelligent reporting on devices and host fields.

This reporting allows insightful analysis of application traffic from the existing mobile gateway without additional probes or network taps, yielding views such as the one shown in Figure 8 from a 7750 SR MGW at a European MNO.

Figure 7. In-Browser Notification



This data shows a weekday pattern of the top ten applications, which have the following characteristics:

- Lunch-break spike from 12:00 p.m. to 2:00 p.m.
- Evening busy hours last until after 11:00 p.m. with heavy video streaming until relatively late at night
- Relatively busy from 10:00 a.m. to 11:00 p.m.

Application Assurance integrates a third-party audio/video performance measurement software stack to perform VoIP and video conferencing MOS measurements. This passive monitoring technology estimates the transmission quality of voice and video over packet technologies by considering the effects of packet loss, jitter, and delay in addition to the impairments caused by encoding/decoding technology.

A rich set of diagnostic data is provided that can be used to help network managers identify a variety of problems that could impact the quality of VoIP/VoLTE voice and video streams and/or service level agreements (SLAs).

It is important to note that business intelligence can be segmented independently and securely across specific corporate APNs or MVNOs, which can have their own flow/service definition and statistics/accounting through the use of AA policy partitions, providing per-APN NN policy and analytics.

CONCLUSION

Rapidly shifting user behavior enabled by smartphone and tablet applications makes it imperative that MNOs provide an efficient and scalable way to provide dynamic application identification and control.

Alcatel-Lucent offers a best of breed, and architecturally optimal approach to meet this imperative by using an inherent capability within the Alcatel-Lucent 7750 SR MG called Application Assurance.

Application Assurance delivers integrated and inline ADC capability, offering a broad range of use cases that simply and cost effectively enable MNOs to monetize their network and the applications that they deliver while personalizing and assuring the experience for the subscriber. AA also offers inherent application-level security features that protect the subscriber and the MNO’s network. Finally, AA capabilities are about application identification and control and not content inspection because the privacy of the subscriber is paramount.

ACRONYMS

2G/3G	Second Generation, Third Generation
3GPP	3rd Generation Partnership Program
AA	Application Assurance
ADC	application detection and control
APN	Access Point Name
BSS	Business Support System
CAPEX	capital expenditures
CODEC	coder/decoder
DoS	Denial of Service
EPC	Evolved Packet Core
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GW	gateway
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICAP	Internet Content Adaptation Protocol
ICMP	Internet Control Message Protocol
ITM	Intelligent Traffic Management
LDAP	Lightweight Directory Access Protocol
LTE	Long Term Evolution
MG-ISM	Mobile Gateway-Integrated Services Module
MNO	Mobile Network Operator
MOS	mean opinion score
OCS	Online Charging System
OFCS	Offline Charging System
OPEX	operating expenditures
OSS	Operating Support System
P2P	peer-to-peer
PCC	Policy and Charging Control
PCEF	Policy and Charging Enforcement Function
PCRF	Policy and Charging Rules Function
PDP	Packet Data Protocol
PGW	Packet Network Data Gateway
QoS	Quality of Service
RAN	Radio Access Network
SDF	Service Data Flow
SGW	Serving Gateway
SGSN	Serving GPRS Support Node
SPR	Subscriber Profile Repository
SSL	Secure Socket Layer
TDF	Traffic Detection Function
TLS	Transport Layer Security
UE-to-UE	user equipment-to-user equipment
vMG	virtualized Mobile Gateway
VoIP	Voice over Internet Protocol
VoLTE	Voice over Long Term Evolution

REFERENCES

[1] Alcatel-Lucent 5670 Reporting and Analysis Manager. http://www.alcatel-lucent.com/products/5670-reporting-and-analysis-manager

[2] Alcatel-Lucent 7750 Service Router - Mobile Gateway. http://www.alcatel-lucent.com/products/7750-service-router-mobile-gateway

[3] Alcatel-Lucent. HTTP In-Browser Notification, application note, September 2013. http://resources.alcatel-lucent.com/asset/169358

[4] Heavy Reading. Policy Control & DPI Market Tracker, April, 2014.

[5] Infonetics Research. Top 2014 Trends, January 7, 2014.

[6] Kaspersky Lab. Security Bulletin 2013. http://www.securelist.com/en/analysis/204792318/Kaspersky_Security_Bulletin_2013_Overall_statistics_for_2013

Alcatel·Lucent