Alcatel·Lucent

TECHNOLOGY WHITE PAPER

Alcatel-Lucent 9900 Wireless Network Guardian

Powerful solution to classify wireless data traffic, understand wireless resource usage and improve network performance

Today's wireless networks now offer subscribers a true mobile broadband experience. As expected, increased penetration has caused increased traffic loads in the wireless operator's radio network. However, a significant portion of the increase results from the fact that identical packets can consume widely varying network resources, simply based on how the host applications transmit the packets. As a result, network inefficiencies, unexpected congestion, and outages are becoming commonplace and more difficult to resolve. Addressing the need to confidently deliver data over wireless networks, the Alcatel-Lucent 9900 Wireless Network Guardian integrates wireless-intelligent behavior-based traffic classification and end-to-end network performance monitoring in one system, resulting in simplified network management, design and operation.

Table of contents

Introduction — the wireless data challenge

Wireless networks are quickly evolving to become more like IP networks. Evidenced by market penetration, one might argue that wireless networks have transformed into IP networks overnight. Most mobile devices in the market today are not only IP-enabled, but are actually used by subscribers to gain access to the Internet and run data-intensive applications. Revenue generated from data transmitted over wireless networks has recently exceeded 20 percent of total revenue in some operator networks, and continues to grow quarterly and globally. The rapid evolution of the network and how subscribers use it — from simple traffic (such as voice) to delivering rich content (such as data/voice/video/location) — has introduced new challenges to operators, requiring the delivery of a high-performance wireless broadband experience while keeping infrastructure and management costs to a minimum.

The good news is that wireless operators can leverage vast industry knowledge and experience about building, operating and optimizing wired IP networks to efficiently build and operate wireless IP networks. Moreover, many IP-network-, event-, policy- and traffic-management tools are readily available and can be used immediately in wireless IP networks.

The not-so-good news is that wireless IP networks do not behave like IP networks without wires — at least not yet. When wires between devices and networks are removed, a tremendous number of physical and architectural issues arise, and the wireless last mile — enabled by the use of air spectrum — becomes highly shared, with the expectation that any one subscriber uses the network infrequently. Accordingly, wireless operators have traditionally been concerned with managing the number of voice calls and minute usage that can be supported by the Radio Access Network (RAN). The addition of data to wireless networks now requires operators to simultaneously manage and optimize RAN usage (such as minutes) and traffic volume (such as bytes).

Common data applications in use today were not designed with the architectural constraints of the wireless last-mile in mind. As a result, they can consume far beyond the expected share of RAN resources, even though only small amounts of volume are sent. In the limit of a deployed RAN with infinite capacity, this does not present a problem. However, as this whitepaper illustrates, very innocent-looking IP applications can cause sufficient load that can easily overload the volume-sensitive and/or the minute-sensitive portions of the deployed networks. Today, data traffic has a direct and widely varying impact on network performance, a dramatic departure from the “good old days” of supporting very predictable wireless voice applications. New solutions and tools to comprehensively address wireless IP networking are therefore required.

This paper summarizes basic wireless network concepts and describes the resulting impact of anomalous signaling, airtime and bandwidth usage introduced by the delivery of data applications over wireless 2.5G, Third Generation (3G) and Fourth Generation (4G) networks. Common types of IP applications are outlined — mobile e-mail, virtual private networks (VPNs), peer-to-peer (P2P), location-based services, worms and video — with a focus on the range of impacts they are likely to have on the network. The paper explains how Radio Network Controllers (RNCs), backhaul links and base stations can be congested, along with the causes and impacts of each type. The discussion then focuses on the limitations of current isolated tools and technologies that address wireless IP–usage traffic classification and traffic-volume network performance issues. Introduced as a comprehensive new solution for identifying resource usage and managing performance in wireless IP networks, the Alcatel-Lucent 9900 Wireless Network Guardian (WNG) is described in detail, including:

- Alcatel-Lucent 9900 Detector and Alcatel-Lucent 9900 Central components
- Generation of anomaly events, analyzing signaling and bearer traffic to extract wireless-specific information
- Mobile Flow records, with wireless-specific resource-usage information and the relation of traffic to individual subscriptions and devices
- Comprehensive reports, showing network-element usage and traffic-source contributions to the wireless network load
- Value and benefits for operators and service providers, specific to operations, planning, security, engineering and marketing sectors

How common IP applications can impact wireless networks

Maximizing device-specific battery life and managing usage of finite air spectrum are key to the efficient operation of wireless networks. The introduction of data applications, with their differing needs for active radio-frequency (RF) connections, produces wide non-correlated variations in traffic volume, airtime minute usage, and signaling events.

Wireless fundamentals

To send and receive data, mobile devices must actively connect to the radio access network. Most mobile devices, however, do not maintain an active RF connection to the network, even though these devices do have an active IP address. The reason is simple. If the device continuously supports an active RF connection to the network, the mobile's battery will last for hours, whereas, if connected infrequently, it will last for days. To preserve battery power, the device connects to the RF network only when sending or receiving packets; otherwise, it transitions to an idle (sleep) state. Every assigned RF connection consumes resources throughout the network, whether it is a slice of air spectrum to transmit packets between the network and mobile devices or power at a base station or processor resources at a Radio Network Controller, independent of how much data is actually being sent or received. These multiple constraints are limited and must be carefully managed to avoid interference and congestion in the last mile. In order to preserve battery life and manage network resources, mobile devices secure an active RF connection to the network only when it is necessary to send or receive packets.

When an idle device needs to send or receive packets, it obtains an active RF connection to the network using a series of approximately 50 mobile-network messages, collectively referred to in this paper as a signaling event. After the last data packet is transmitted, the network will retire the connection and the device will transition to an idle state after a dormancy time expires, typically set by an operator in a range from 5 to 30 seconds. If an additional packet requires delivery to a dormant device, a new connection is required, and the signaling process starts again.

In the context of simple voice, this approach is straightforward. When a phone call is initiated, the device establishes a connection, and when the phone call is over, the connection is terminated until the next call is initiated or received. A similar approach is used for activating a data connection, initiated when data is sent or received. However, applications transmit data in ways that are different than voice, as follows:

- Continuously, as in the case of a file transfer
- At regular intervals, as in the case of a security or location-based heartbeat
- At irregular intervals, as in the case of a subscriber fetching and reading multiple web pages

The varied transmission behavior a data application uses to transfer packets to and from a mobile device can have a profound impact on radio access resources, as shown in the following examples.

Anomalous signaling usage

Assume that the wireless network dormancy timer is set at ten seconds and that a data application server is designed to send a session keep-alive heartbeat — assume a single packet — to a mobile device every 11 seconds. An RF connection must be established to deliver the heartbeat packet, resulting in one signaling event. Ten seconds later, because no other packets have been sent, the RF connection is terminated and the device goes dormant. However, the keep-alive is sent every 11 seconds, so one second after the device goes dormant, the network must renew the RF connection with the device to deliver the next single-packet heartbeat. The application will force the network and device to reinitiate RF connections every 11 seconds for the duration of the activity.

Over a one-hour period, such an application could deliver 330 packets — at least 13 kB in one hour, consume at least 54 minutes of device battery life and RF airtime, and generate approximately 330 signaling events.

Anomalous airtime usage

Assume the same application for the signaling usage example, except that the heartbeat is sent more frequently, at an interval less than the dormancy timer — for example, every five seconds. In this case, one packet delivered every five seconds ensures that the device never transitions to an idle state, and the RF resources remain constantly active and permanently assigned to the mobile device. Over a one-hour period, the application delivers 720 packets — 28.8 kB in one hour, consumes 60 minutes of device battery life and RF airtime, and generates only one signaling event.

Anomalous bandwidth usage

The wireless network is intended to support a broadband mobile experience where devices upload and download data. However, some applications require tremendous bandwidth; for example, a video download can easily exceed 1 GB. At 1.5 Mb/s sustained download rates, such a download would consume at least 1.5 hours of continuous RF resources.

The above examples illustrate the extreme variation in traffic volume and signaling events. Depending on the network dormancy timer, loading conditions and maximum download speeds, during the consumption of one hour of actual RF airtime the network may encounter the transmission of loads anywhere between 15 kB to 675,000 kB and 1 to 330 signaling events.

Classifying common IP applications

It is useful to classify and evaluate a few of the more common data applications that are operating in today's wireless data networks, and to characterize what their impacts will most likely be to the variable consumption of wireless network resources as discussed previously. The list of applications running on wireless networks is evolving rapidly, as is the associated impact on the network. The list below is intended to illustrate the range of possible loads, but is not intended to be exhaustive.

Mobile e-mail

Mobile e-mail is arguably one of the most popular data applications in today's wireless networks, and is available for business professionals and casual users using push- and pull-based interfaces. Push and pull approaches to e-mail delivery have very different impacts on the wireless network. With push applications, an external server immediately pushes an e-mail to the mobile device when it arrives in the email server's queue. The network establishes an RF connection with the device and then terminates the connection after the email is delivered and the dormancy timer expires. Pull-based e-mail, however, will transmit e-mails in the queue less frequently and only at the request of the device.

Mobile e-mail generally contributes very little volume to the network but consistently consumes more than 30 percent of airtime and approximately 50 percent of the signaling load caused by wireless-data traffic. This disparate use of wireless resources arises because only milliseconds of RF time are required to send an actual e-mail, but for roughly every new e-mail, a new RF connection must be established, and wireless airtime is used while the dormancy time of approximately ten seconds expires, during which no data is sent.

Virtual private networks

VPNs are often used by mobile professionals who connect to their enterprises remotely using a laptop and a cellular modem, such as a 3G/4G aircard or USB dongle. To maintain a secure tunnel, heartbeats are exchanged between the host VPN gateway and the remote computer. These continuous low-volume heartbeats require active RF connections to be delivered. Depending on VPN heartbeat settings, the application can consume high amounts of RF airtime, equal to the length of the VPN session, and/or high signaling — all while sending very little data.

Peer-to-peer

P2P is a common application used for sharing content files such as video, audio and data. P2P receives significant attention because it transmits disproportionately large files and, in some networks, has been identified as contributing to significant network congestion. In wireless networks, P2P is predominantly used by only a fraction of wireless IP subscribers who have aircards or use their mobile phones as data modems, and connect them to laptops or devices with large hard drives. Because of the modest download rates currently available in wireless networks, P2P sessions that transfer gigabytes of data can last for many continuous hours, consuming significant backhaul and air resources. However, P2P sessions are arguably one of the most efficient uses of wireless radio resources because almost the entire session is used for actual data transmission. When RF resources are allocated to a device sending P2P, the resources are mostly supporting the delivery of packets instead of being allocated to dormancy-related “dead airtime”.

Location-based services

These services rely on network knowledge of the geographical presence of a device. Location can be determined by the network or (increasingly) by the device, and communicated to the network. Location-based services allow wireless operators to tailor content relevant to the mobile device’s proximity, or to use devices for tracking purposes such as inventory tracking. Continuous communication of proximity and content will result in traffic loads that resemble push-based mobile e-mail, and will likely scale to the entire subscriber base that decides to opt for such services.

Worms

Worms are ubiquitous threats in wireline networks and are becoming an increasing concern for wireless operators. Worms can be introduced to the mobile network easily when an infected laptop accesses the network with an aircard or mobile phone as a tethered modem. The worm then attempts to propagate and potentially target other mobile devices in the same mobile IP-address range. When a worm attempts to exploit a new victim, it sends packets to the victim device, requiring at least one signaling event and ten seconds of dormancy for each new attempt.

Worms target a large range of victims at once, magnifying instantaneous signaling and connection load in the RAN, causing both network-impacting spikes in signaling events at the RNC and local-connection denial of service (DoS). This congestion occurs even when the worm attempts to spread, but is unsuccessful in infecting the victim’s mobile device. The impact of a mobile-to-mobile worm may have disastrous effects to the performance of a wireless network.

Video

Video transmissions over mobile networks are a new and growing phenomenon. Subscribers have started to deploy video cameras with 3G backhaul as a way of remote monitoring, including traffic, home-security and even baby monitoring. This video traffic relies heavily on the uplink data path into the network. Subscribers have also begun to download video content available from service providers and from the Internet. Increasingly, subscribers are also accessing their personal video content by connecting back to their home-based digital video recorders and downloading those files to their mobile device over the wireless network. The traffic creates significant volume in the network on both uplink and downlink paths, with extended connection durations and backhaul congestion because video files are typically very large. Video also places additional constraints on the network, in that the applications require low latency, and very low packet-loss end-to-end.

Types and causes of wireless network congestion

The above examples demonstrate that data applications can have an important impact on the usage of the wireless data network and in certain cases, can result in impairments and outages in the network. The following sections outline different types of congestion, their causes and impacts.

Radio Network Controller congestion

Applications such as push e-mail, VPNs, mobile port scanning, Hypertext Transfer Protocol (HTTP) over Secure Socket Layer (HTTPS), Secure Shell (SSH), location-based services, push-to-talk, wireless-specific signaling attacks and worms introduce anomalously high amounts of signaling in the network. Such applications can contribute individually or as an aggregate to signaling congestion and even overloads in RNCs, resulting in DoS conditions, whereby new subscribers cannot establish an active connection with the network to legitimately send and receive packets. These impairments and outage conditions — RNC overloads — can exist despite the fact that the bearer path is not loaded with high-traffic volumes.

Backhaul congestion

High-volume applications such as video download, video upload, P2P, File Transfer Protocol (FTP), single-source flood attacks, and distributed source flood attacks all typically send large amounts of volume that, in aggregate, can contribute to the congestion of backhaul links between the base station, the RNC and network elements in the path. Subscriber use of volume-intensive applications results in traffic composition that differs greatly from typical design points and expected usage models, and can overload backhaul links which were not generally engineered for this type of intense subscriber usage.

Base station congestion (high airtime usage)

Devices that are “always-on” or that use an anomalously high amount of airtime relative to the amount of data they transmit can strongly influence how efficiently the radio resources are used. Airtime consumption can vary between one packet per dormancy time (~32 bits per second) to maximum download rates on the order of a few Mb/s, a range extending over five orders of magnitude. Certainly, base-station packet-delivery scheduling is designed with variable bandwidth allocation for subscribers to adjust to the needs of low- and high-bandwidth applications, such as VPN and video respectively. However, often overlooked is that the base station can typically handle only a finite number of active, concurrent data subscribers, independent of how much data any one or multiple subscribers are sending. In this way, low-volume/high-airtime subscribers can consume base station resources in a way that is equivalent to high-volume/high-airtime subscribers. For any new subscriber who is trying to connect to the network to actively send and receive data, the connection probability relies on the availability of an open slot in the total number of instantaneously supported subscribers at the base station, which can be consumed far beyond expected usage and availability models simply by the application’s transmission behavior.

The number of instantaneously supported subscribers is often highly oversubscribed based on the assumption of infrequent usage by all other subscribers. Always-on, "high airtime" users erode the validity of this assumption because each subscriber consumes resources at the base station for much longer periods than typically expected, with data rates as low as 32 bits per second (one 40 byte packet sent every ten seconds). Assuming that a base station can support 50 instantaneous subscriber connections, the base station can soon be completely exhausted, resulting in DoS connection conditions while transmitting an instantaneous load of 1.5 kb/s. Examples of high-airtime applications with widely varying airtime efficiencies are VPNs, P2P and battery-drain attacks.

Types and limitations of wireless management tools

The above congestion and impairment issues are well known to service providers who manage and operate wireless broadband networks. Today, wireless service providers have access to many tools they can use to start troubleshooting and addressing problems:

- Radio-network fault management
- Network-element monitoring and management
- IP traffic management
- Deep packet inspection
- Billing systems
- Security
- Event management

When new IP applications or a new device loaded with a broad set of new applications introduces new stress and congestion to the wireless data network, operators must maintain, support and correlate across all of these tools to discern why an impairment has occurred. For example, RNC management tools will report that the RNC is overloaded, but they will not elucidate root cause, such as identifying that a new enterprise gateway in the Internet is sending traffic to the enterprise's mobile devices for location-based inventory tracking (in total, a very low volume) but forces thousands of mobile devices to continuously transition in and out of dormancy and focus their excessive signaling requests into the RNC signaling processors.

Root cause analysis of situations using the current tool set (such as the previous example) is sufficient when wireless broadband penetration is low and events are singular in nature. However, root cause analysis is slow, complex, expensive, and unscalable for operators who have experienced high penetration of wireless broadband services and who introduce new devices and applications with high frequency. Automatic and simple forensic and proactive analysis will become more important as the numbers of wireless broadband users and applications increase in the network. Moreover, the traffic generated by each of the tools discussed herein above is highly invasive to the network by nature of the number of locations across the network from which each tool needs to tap traffic, and requires a sizable management network simply to collect all of the generated data.

> To manage and use these isolated tools, operators ultimately need to build, pay for and maintain custom intelligence tools to correlate all the data. New wireless-specific behavioral technologies developed at the Alcatel-Lucent Bell Laboratories can radically simplify this situation: one tool — the Alcatel-Lucent 9900 Wireless Network Guardian —crosses the IP-RAN boundary, providing operational simplification, real-time visibility and correlation, and wireless intelligence.

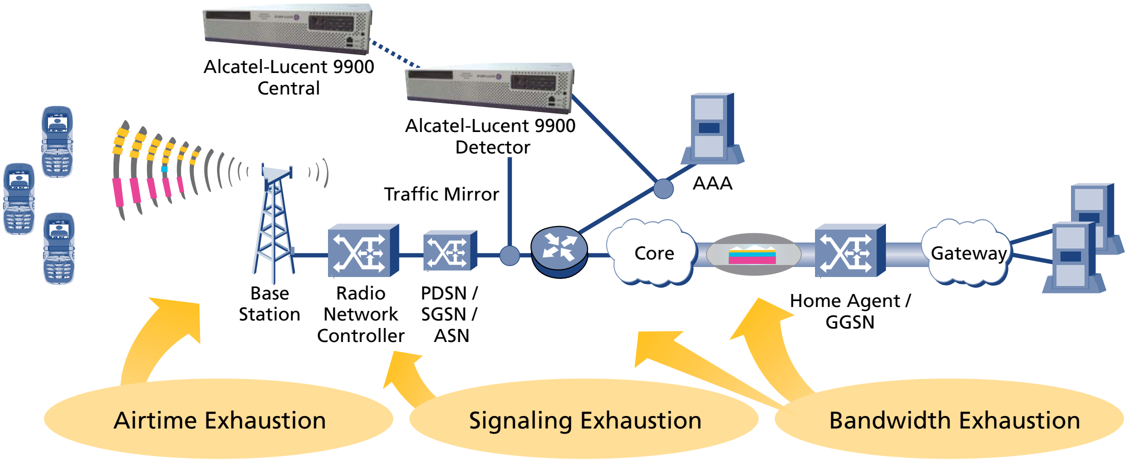
Alcatel-Lucent 9900 Wireless Network Guardian

The Alcatel-Lucent 9900 Wireless Network Guardian (WNG) was developed to provide wireless operators with a management solution that integrates and correlates traffic analysis, network performance monitoring and network behavioral anomaly detection in one system. It understands how every packet, flow, subscriber, device, realm, Access Point Name (APN), Internet server and application manifest as load on the limited resources in a wireless data network in real time. The solution is generally applicable to all wireless data protocols, including Enhanced Data for Global Systems for Mobile Communications Evolution (EDGE)/Universal Mobile Telecommunications System (UMTS), Code Division Multiple Access (CDMA)/Third Generation Partnership Project 2 (3GPP2)/IS835 and Worldwide Interoperability for Microwave Access (WiMAX) networks.

The Alcatel-Lucent 9900 WNG monitors every packet exchanged between mobile-to-mobile, mobile-to-Internet and Internet-to-mobile sources and destinations, and from this real-time traffic it builds a representative "state engine" for how that traffic manifests as load on every network element in the packet's path. The IP traffic is reduced to Mobile Flow records which provide a concise description of the traffic on the network. The Alcatel-Lucent 9900 WNG provides real-time dashboard visibility into how traffic manifests as load on the network, provides on-demand and periodic reporting and trends, and is used as a forensic tool to investigate faults, billing errors, and to explore how to increase the efficient use of the network. The Alcatel-Lucent 9900 WNG also generates anomaly events to identify, in real time, when subscribers or servers are consuming excessive network resources — for example, airtime, signaling, volume or peers — or when a network element is being overloaded. It has the resolution to identify events as subtle as a single mobile-to-single mobile battery-drain attack and Mobile Internet Protocol (MIP) anomaly attacks, as well as events such as a distributed flood of data traffic or signaling that would cause the overload of a network element or a subscriber. In all cases, Mobile Flow records and anomaly events are resolved to the individual devices, identified by their unique device credentials instead of by IP address only, in real time.

The Alcatel-Lucent 9900 WNG product has two components, the Alcatel-Lucent 9900 Detector and the Alcatel-Lucent 9900 Central, as shown in Figure 1. The Alcatel-Lucent 9900 Detector deploys in the packet core, and the Alcatel-Lucent 9900 Central deploys in the Network Operations Center (NOC).

Figure 1. Alcatel-Lucent 9900 WNG components — Alcatel-Lucent 9900 Detector and Alcatel-Lucent 9900 Central



Alcatel-Lucent 9900 Detector

The Alcatel-Lucent 9900 Detector monitors every packet on the Gn interface between the Gateway GPRS Support Node (GGSN) and Serving GPRS Support Node (SGSN) in General Packet Radio Service (GPRS), EDGE, UMTS, and Wideband CDMA (W-CDMA) networks. In CDMA-based networks, the Alcatel-Lucent 9900 Detector monitors data traffic between the Packet Data Serving Node (PDSN) and Home Agent or Foreign Agent. In WiMAX networks, the Alcatel-Lucent 9900 Detector monitors traffic between the ASN Gateway and the Home Agent (HA) and Foreign Agent. The Alcatel-Lucent 9900 Detector also monitors accounting messages that are transmitted to the Charging Gateway Function (CGF) if Authentication, Authorization and Accounting (AAA)/ Remote Authentication Dial-In User Service (RADIUS) are used. Each Alcatel-Lucent 9900 Detector currently supports data rates and mobile active session quantities that exceed today's deployed networks.

The Alcatel-Lucent 9900 Detector has embedded algorithmic intelligence of the end-to-end wireless network. Accordingly, as each packet transmits through the packet core, the Alcatel-Lucent 9900 WNG infers what the corresponding loads will be across the network. By watching this traffic, the Alcatel-Lucent 9900 WNG:

- Tracks how every mobile device transitions in and out of dormancy
- Determines uplink-packet data rates and attempted downlink-packet data rates
- Determines the total RF connection time using logic that identifies how devices transition in and out of dormancy

The Alcatel-Lucent 9900 Detector auto-discovers the network, and maps the path of each packet through the network. With this data, the Alcatel-Lucent 9900 Detector creates a network "state engine" that relates loads across the network, resolved to devices, subscribers, applications and servers on a per-network-element basis. The Alcatel-Lucent 9900 Detector generates Mobile Flow records to describe the traffic patterns and state engine for reporting and forensics analysis. In addition, the Alcatel-Lucent 9900 Detector applies wireless-specific anomaly behavioral algorithms to the state engine to determine when a traffic source is causing anomalous and harmful loads in the network. Each deployed Alcatel-Lucent 9900 Detector communicates Mobile Flow records and anomaly events northbound to an Alcatel-Lucent 9900 Central.

Alcatel-Lucent 9900 Central

The Alcatel-Lucent 9900 Central communicates with the deployed Alcatel-Lucent 9900 Detectors. Operators can access the user-customized dashboard and anomaly event manager using an intuitive graphical user interface, generate on-demand and periodic reports to understand immediate and long-term trends, and manage the entire Alcatel-Lucent 9900 WNG solution through the Alcatel-Lucent 9900 Central.

Anomaly events

The Alcatel-Lucent 9900 WNG currently supports a continuously growing number of wireless behavioral anomaly events, based on key behavioral characteristics in the traffic and network state engine. The anomaly events analyze both signaling and bearer traffic to extract wireless-specific information. A few examples of wireless behavioral anomalies include:

- Wireless-specific congestion and overload traffic
    1. Excessive signaling from single source
    2. Battery-drain traffic from single (multiple) source(s)

3. RNC signaling overload
4. Maliciously crafted routing message

- Port scans and unwanted traffic
  5. Mobile-to-mobile (or internet) port scans
  6. Flooded mobile from single (multiple) source(s)
  7. Unwanted source of traffic

- "Abusive" subscribers
  8. High-usage subscriber
  9. Always-active airtime subscriber
  10. High-signaling subscriber
  11. P2P mobile

The Alcatel-Lucent 9900 WNG does not depend on or require Layer-7 deep packet inspection, a common technique used to analyze traffic by matching content in the packet to known signature databases, principally because nothing inside a single packet will describe how that packet will impart load on the network. To relate traffic to network performance, it is necessary to analyze the traffic behaviors, not the packet content.

Mobile Flow record

In addition to generating anomaly events, the Alcatel-Lucent 9900 WNG provides network diagnostic and forensic tools using a newly developed "Mobile Flow" record to better understand network-impacting behaviors. This new record appends industry-standard Netflow records with attributes that are unique to wireless data networks. Starting from a network-level impairment, it takes three mouse clicks to identify every real-time flow, source/destination pair by IP and/or International Mobile Station Equipment Identification (IMEI)/International Mobile Subscriber Identification (IMSI) or Network Access Identifier (NAI)/Electronic Serial Number (ESN)/Mobile Station Identifier (MSID), application(s) and wireless network resources that were consumed. Currently, Mobile Flow records are used internally in the Alcatel-Lucent 9900 WNG system.

Mobile Flow is a bidirectional flow record with the following key fields:

- 5-tuple — orig_ip, orig_port, resp_ip, resp_port, proto
- Mobiles' identifiers — NAI/ESN/MSID/Mobile Equipment Identifier (MEID)/IMEI/IMSI
- Wireless network elements to which the mobiles are attached
- Arrival time of the first packet/last packet in each direction
- Packet/byte counts in each direction
- Airtime usage
- Connection setup counts

Alcatel-Lucent 9900 WNG reports

The Alcatel-Lucent 9900 WNG provides reporting capabilities to summarize the usage of every network element — Gateway GPRS Support Node (GGSN), Serving GPRS Support Node (SGSN), Home Agent, PDSN, ASN, and RNC — by attributes such as volume, connections, handoffs and number of subscribers. The Alcatel-Lucent 9900 WNG also reports how sources of traffic in the network — subscriber, device, realm, APN, servers and applications — contribute to the complete wireless network load. A partial list of reports is summarized in Figure 2.

Figure 2. Alcatel-Lucent 9900 WNG reports

Active subscribers and roaming partners
- Active mobiles (detector)
- Subscriber count by service provider
- Traffic by service provider

Overall network cost of unwanted/ malicious activity (aggregate and per hour)
- Airlink resources wasted
- Bandwidth wasted
- Signaling resources wasted
- Event breakdown
- Incident breakdown

Per network element view (ASN, HA, PDSN, GGSN, SGSN, RNC)
- MIP handoffs (..)
- Active mobiles (..)
- Mobile flows (..)
- Mobile volume (..)
- Signaling load (rnc)

General network/realm statistics
- Overall network statistics:
  - Total mobile flows (detector)
  - Total mobile volume (detector)
  - Traffic distribution by protocol (Mb/s)
- Protocol usage per realm
  - By airtime
  - By external hosts
  - By signaling cost
  - By subscribers
  - By traffic type
  - By volume

Top (applications / servers) exchanging traffic with mobiles per realm
- By air-time
- By signaling cost
- By subscribers
- By volume

Security and top attackers
- Top attacks by duration, intensity
- Top wireless DoS attacks
  - Battery attack sources
  - Signaling attack sources
- Top scanning activity
  - Top internet scanners by scans/victims
  - Top mobile scanners by scans/victims
  - Top ports by scanners / scans/victims

Abusive/heavy usage subscribers
- Top mobiles by wireless network resource (per realm):
  - By airtime
  - By bandwidth
  - By signaling cost
- Network abusive subscribers:
  - Top high usage mobiles
  - Top always active mobiles
  - Top mobiles by peers (per realm)
  - Top P2P mobiles by airtime
  - Top P2P mobiles by peers
  - Top P2P mobiles by volume

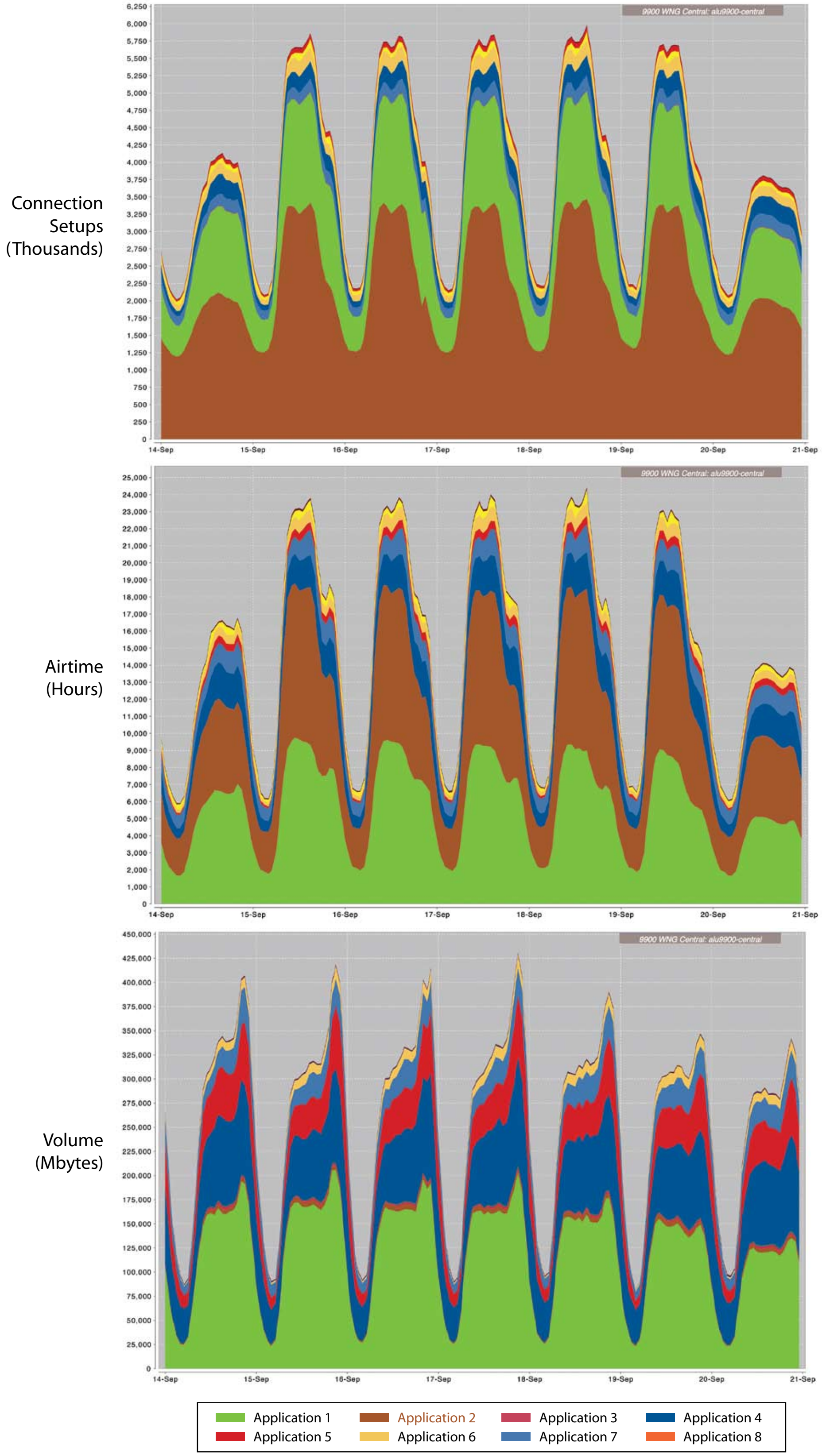
Figure 3 and Figure 4 show sample Alcatel-Lucent 9900 WNG reports, all of which can be viewed individually through a web-based interface, or collated in a complete daily, weekly and monthly report. Figure 3 shows a sample report summarizing key applications, by realm or APN, as they relate to network traffic load.

Figure 3. Alcatel-Lucent 9900 WNG report — sample of top applications using network resources by realm/APN

Application	Number of servers	Volume (MB)	Airtime (hrs.)	Connection setups	Number of subscribers
I	58954	137648.25	3534.68	705974	15702
II	8591	22629.54	4656.52	1435150	14794
III	320	12189.748	1163.08	297210	1479
IIII	1151	6834.41	754.68	235164	584
IV	2186	5914.94	914.20	251987	7522
V	53	5472.17	623.98	145838	388
VI	688	3671.20	375.24	84174	2843
VII	525	3283.52	606.20	244342	977
VIII	134	2737.26	299.14	70552	227
IX	66	2736.61	202.61	60501	179

Figure 4 shows a sample report that describes how all of the IP traffic, resolved to applications and anomalies, relate to network-wide signaling load, airtime usage and volume.

Figure 4. Alcatel-Lucent 9900 WNG report —Top applications as they relate to signaling, airtime, and volume load in the wireless network



Alcatel-Lucent 9900 WNG value proposition

The Alcatel-Lucent 9900 WNG provides new, differentiated value to operators and service providers in a number of areas.

Operations

Operators can determine which subscribers, servers and applications are the most significant contributors of non-value-added traffic, load and cost to the network, so individual sources of exceptional load — bandwidth, airtime and signaling — can be appropriately managed to enable fair but utilitarian use for all subscribers. A pre-scripted list of applications is not required because the Alcatel-Lucent 9900 WNG is application agnostic, and easily adapts to the constant introduction of new applications and devices to the network. The product offers tremendous cross-layer network diagnostic capabilities that have proven invaluable for identifying network problems related to quickly resolving application-induced network outages, addressing device provisioning and network configuration errors, and understanding the full-stream cost to support hosted and over-the-top applications and services. Operations organizations benefit from more efficient use of the installed base, and greatly reduced time and effort required to diagnose network challenges.

Planning

Wireless service providers can establish a baseline measurement of network use at the individual subscriber level, allowing more accurate predictions of network-capacity trends based on application-specific trends and subscriber usage patterns in various locations in the network. These trends and patterns are known to vary significantly across the network. The benefits are better capacity planning and network architectures, along with savings in network build-out strategies.

Security

Service providers can detect a new class of wireless-specific DoS attacks targeted at the signaling layer and exhausting RF channels. It identifies mobile devices that are maliciously or surreptitiously participating in attacks on the wireless network, often as a consequence of the device or wireless-enabled laptop being infected with worms. The Alcatel-Lucent 9900 WNG also identifies sources of fraud. The benefit is reduced network outages and down time.

Engineering

Service providers can ensure that packet transmissions from devices and networks are consistent with design and are not being sent fraudulently or as a result of device malfunction. The benefit is more predictable network and device performance, per design and specification.

Marketing

With the Alcatel-Lucent 9900 WNG, service providers can better determine the network cost associated with supporting a given application, thereby enabling application-level return on investment (ROI) calculations. The benefit is increased awareness of the overall cost of delivering specific applications and services.

Revenue Assurance

Accurate accounting of a subscriber's data usage, as well as forensic analysis of the subscriber's activity as it relates to a bill, is consistently presented as a challenge to the industry. The Alcatel-Lucent 9900 WNG, through analysis of the Mobile Flow records, allows quick and complete auditing of subscriber activity. The benefit is improved customer satisfaction for billing dispute resolution and improved wireless data billing.

Acronyms

3G	Third Generation
3GPP2	Third Generation Partnership Project 2
4G	Fourth Generation
AAA	Authentication, Authorization and Accounting
APN	Access Point Name
CDMA	Code Division Multiple Access
CGF	Charging Gateway Function
DoS	denial of service
EDGE	Enhanced Data for GSM Evolution
ESN	Electronic Serial Number
FTP	File Transfer Protocol
GB	gigabyte
GE	Gigabit Ethernet
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GTP-c	GPRS Tunneling Protocol – core
GTP-u	GPRS Tunneling Protocol – user data
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
IMEI	International Mobile Station Equipment Identification
IMSI	International Mobile Subscriber Identification
IP	Internet Protocol
kB	kilobyte
MEID	Mobile Equipment Identifier
MIP	Mobile Internet Protocol
MSID	Mobile Station Identifier
NAI	Network Access Identifier
NOC	Network Operations Center
P2P	peer to peer
PDSN	Packet Data Serving Node
RADIUS	Remote Authentication Dial-In User Service
RAN	Radio Access Network
RF	radio frequency
RNC	Radio Network Controller
ROI	return on investment
SGSN	Serving GPRS Support Node
SSH	Secure Shell
UMTS	Universal Mobile Telecommunications System
VPN	virtual private network
WiMAX	Worldwide Interoperability for Microwave Access
WNG	Alcatel-Lucent 9900 Wireless Network Guardian

Contacts

Mike Schabel
schabel@alcatel-lucent.com
+1 908 582 4354

Jessica Azzi
azzi@alcatel-lucent.com
+1 978 952 1008

Eric Schnell
ericschnell@alcatel-lucent.com
+1 908 582 2432

www.alcatel-lucent.com Alcatel, Lucent, Alcatel-Lucent and the Alcatel-Lucent logo are trademarks of Alcatel-Lucent. All other trademarks are the property of their respective owners. The information presented is subject to change without notice. Alcatel-Lucent assumes no responsibility for inaccuracies contained herein. Copyright © 2008 Alcatel-Lucent. All rights reserved.
CMO2888080707 (10)

Alcatel·Lucent