WIRELESS BANDWIDTH MANAGEMENT AUTHENTICATION IMPROVING QUALITY OF SERVICE

Amanda PEART & Alice GOOD

ABSTRACT: With the popularity of distributed applications such as BitTorrent and Peer 2 Peer (P2P) networks, coupled with the increase in mobility of end user devices, there is a requirement for dynamic bandwidth management. Mobile users require access to the internet at varying times and for various reasons. Generally this access is via public hotspots in places such as airports, hotels and coffee shops. Therefore it is paramount that user access is managed as some users will utilize an unfair amount of the bandwidth denying access to others. This paper proposes a dynamic wireless bandwidth management system that allocates bandwidth dynamically to users as they authenticate with a wireless access point (AP). In addition, the implementation test results illustrate how the bandwidth dynamically changes when new users are accepted and authenticated to access the bandwidth.
KEY WORDS: Quality of Service; dynamic bandwidth management; wireless networks

1 INTRODUCTION

Most wireless network access points have a finite amount of bandwidth to distribute between nodes requesting a connection. On the whole the connection policy is poorly managed, not from an administrative point of view but rather that of software design and configuration implementation. This mainly applies to hot spot public access points such as those in coffee shops and airport departure lounges. In both cases, there is a unique requirement to allow the general public to access network resources as part of the core business process.

Figure 1 – Wireless Connectivity

University of Portsmouth, Portsmouth, Hampshire, PO1 3HE, UK Email
Amanda.peart@port.ac.uk;alice.good@port.ac.uk

Abuse of the resource on public networks is common, taking only one user to consume all of the available bandwidth, spoiling the user experience for others trying to access legitimate resources. Enabling accounting and an admissions control mechanism which will restrict or limit this abuse is critical.

Currently there are existing solutions that manage this requirement. These are invoked on at the point of the user's admissions request. However these solutions are static, with preset bandwidth limits. This approach hinders access to the network and is based on historical data rather than current violations of bandwidth usage. This in turn limits the user experience and the correct distribution of bandwidth access.

Jha and Hassan (2002) highlights the dramatic increase demand in high-speed bandwidth networks driven by user requirements of real-time applications, such as multimedia and VoIP, that have specific performance requirements. With the popularity of distributed applications such as BitTorrent and Peer 2 Peer (P2P) networks, coupled with the increase in processing power of the average desktop, there is a requirement for bandwidth management.

This paper proposes a wireless bandwidth management system that allocates bandwidth dynamically to users as they authenticate with wireless access points (AP). Furthermore the implementation test results illustrate how the bandwidth dynamically changes when new users are accepted and authenticated to access the bandwidth. Wireless standards are highlighted, given their relevance to today's connectivity needs. They need to provide adequate quality of service in a challenging environment.

2 IEEE 802.11

Since the initial inception of the IEEE 802.11 standard of WiFi in 1997 the standard continues to evolve, each version standardizes the PHY and MAC layer features for wireless communication**,** as detailed in figure 1. (IEEE, 1997)**,** (IEEE, 2003) (IEEE WG802.11 - Wireless LAN Working Group, 2005).

These have evolved from the past standards of low bandwidth wireless communication systems capabilities to the emergence of a higher bandwidth infrastructure that is now capable of transmitting bandwidth hungry, time sensitive multimedia applications. Within the family of IEEE 802.11 standards, QoS had not been a consideration until the IEEE 802.11e version was ratified in 2005 (IEEE WG802.11 - Wireless LAN Working Group, 2005).

	802.11a	802.11b	802.11g	802.11n
Standard approved by IEEE	January 2000	December 1999	June 2003	Expected in 2007
Maximum data rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps
Different data rate configurations	8	4	12	576
Typical range	75 feet	100 feet	150 feet	150 feet
Modulation technologies (1)	OFDM	DSSS, CCK	DSSS, CCK, OFDM	DSSS, CCK, OFDM+
RF band	5 GHz	2.4 GHz	2.4 GHz	2.4 GHz and 5 GHz
Number of spatial streams and antennas	1	1	1	Up to 4
Channel width	20 MHz	20 MHz	20 MHz	20 MHz or 40 MHz
Number of channels	23	3	3	26

Figure 2 - IEEE WG802.11 - Wireless LAN Working Group, 2005).

This version of the standard provisioned the ability to configure the network to cope with the demands of multimedia applications. This encompassed prioritization of data, voice and video transmission which is achieved by utilizing the MAC layer, along with Time Division Multiple Access (TDMA) and an error correcting mechanisms for delay sensitive applications. Though data types can be identified to be proiritized is does not necessarily provide the mechanism for a user to gain a quality experience of connectivity. Therefore there is still a need to manage the bandwidth allocation of the available network per user.

3 QUALITY OF SERVICE

Today's, wireless networks need to support the demands of variable traffic types over converging network infrastructures. Each application requires a differentiated service to ensure that it is received in a functional state. The demand for a reliable network infrastructure instigated the need for Quality of Service (QoS) in commercial networks, thereby promoting the development of a standard with the aim to deliver an adequate quality performance to the end user (ITU, 2004).

In the ITU-T recommendation E.800, QoS is "*the collective effect of service performances, which determine the degree of satisfaction of a user*" (ITU-T Recommendation E.800, 2008). From the commercial perspective Microsoft (2011) defines QoS as "*...as set of technologies for managing network traffic in a cost effective manner to enhance the user experience of the service in home and enterprise environments*"

Microsoft goes on to define QoS still further from the technological view "*...QoS technologies allow you to measure bandwidth, detect changing network conditions (such as congestion or availability of bandwidth) and prioritize or throttle traffic....*" (Microsoft, 2011).

The mechanisms defined in these standards provide a means to manage the efficient distribution of the resources utilizing the defined parameters but also maintaining the importance of the user experience.

Traditionally best effort was the service mode for networks where network traffic is treated fairly with no guarantees of performance (Floyd & Allman, 2008). The constraint of this model is, when the network is running a bandwidth hungry application, such as streaming multimedia, VoIP, IP-TV and online games, all other applications can suffer by not receiving adequate bandwidth to transmit.

To accommodate this situation if an application is mission-critical in a commercial environment certain traffic, may then need preferential or priority treatment within the whole network to fulfil those mission-critical requirements. Therefore the aim of QoS is to balance the network resources with the network delivery requirements, thus providing a preferential delivery service. In achieving this bandwidth, latency, latency variation commonly known as jitter

and data throughput need to be managed efficiently (Microsoft, 2011).

QoS mechanisms can also be used to manage protocols such as the User Datagram Protocol (UDP) which are inherently unreliable as they do not deploy acknowledgements and therefore cannot detect network congestion (Tanenbaum & Wetherall, 2010; Stallings, W., 2004).

Therefore, QoS mechanisms can allow the mission critical application priority access to the required resources, while still allowing other applications access to their required network resources.

The admission control mechanism decides how, when, and who will be allocated available network resources. The traffic control mechanism manages the data flows by classifying scheduling and marking packets based on priorities by shaping traffic. Together they can categorize traffic into service classes and control delivery to the network based on these service classes.

4 MANAGING THE BANDWIDTH

As in the coffee shop scenario previously stated, multiple users within range of an AP hotspot attempt to connect to the internet wirelessly. In many public wireless hotspot connection sessions, users are commonly restricted by connection duration not by bandwidth capacity. It is not uncommon to gain a connection but finding the transmission rate is so slow that it is unusable even for simple tasks such as checking email.

This paper presents an implementation of dynamic bandwidth management that provides user authentication bandwidth connections, which have been implemented in open source software. As multiple users request an internet connection the bandwidth is shared equally between them. If a user disconnects then the bandwidth capacity is dynamically redistributed between the remaining connected users.

Therefore the total bandwidth B_t is divided by the number of users U_1, U_2, ….U_n, to give the allocated bandwidth B_a. The bandwidth is continued to be divide equally among users until the allocated bandwidth is reduced to 350kps as a minimum bandwidth constraint :

$$Ba \geq 350kps$$

350kbs is significant as it is required to stream Mpeg2 at a satisfactory rate.

5 EXISTING BANDWIDTH MANAGEMENT TOOLS

The purpose of this section is to evaluate existing comparative technology. There are currently many existing solutions that offer user authenticated wireless access to network resources. The most pertinent solutions are discussed in this section.

5.1 Linksys

Linksys a cisco® component offers a variety of wireless network access points and routers. These devices have preinstalled firmware that supports basic wireless access. The Linksys firmware does support authentication via a RADIUS server, which allows a central directory or database to store usernames and passwords for authentication. However it does not utilize the RADIUS attributes required to shape user bandwidth (Linksys Wrt54GL User Guide, n.d., p.10). Additionally it does not incorporate captive portal functionality, it only requests a username and password in order to authenticate.

A captive portal is a web page that the user of a public-access network is obliged to view and interact with before access is granted (Captive Portal, 2005). The Linksys user guide does support quality of service (QoS); however this form of QoS is too simplistic as it is based on Device Priority, Ethernet Port Priority, and Application Priority (Linksys Wrt54GL User Guide, n.d., p.17).

There is no functionality within this type of QoS to support centralized authentication using the current Linksys firmware.

5.2 Patronsoft

Patronsoft provides a solution called FirstSpot. FirstSpot is a Windows based product that allows access to network resources once a user has been authenticated via an AP. Additionally FirstSpot supports a captive portal login interface. Firstspots' support for RADIUS extends its abilities beyond just authentication that limits the above mentioned Linksys firmware. Firstspot supports bandwidth shaping on a per user bases by means of employing specific RADIUS attributes (FirstSpot v5, n.d.). As it is developed for the Microsoft Windows platform, this limited the amount of configuration changes to only what the operating system would allow, due to it being a proprietary product. Secondly, although it throttled bandwidth on a per user basis there was no provision for active session updates once a user had logged onto the AP.

5.3 CoovaAP and OpenWRT

CoovaAP and OpenWRT are both open source firmware projects for the Linksys WRT54GL AP, with most code contributions being from the community. This usually has the advantage of consistent updates to security enhancements, patches and functionality.

Kamikaze, a release of OpenWRT, has been updated as recently as February 2009 (Index of Kamikaze 8.09, 2009). Both have the advantages of being free, open source and support the CoovaChilli NAS software (CoovaChilli, n.d.). OpenWRT is supported by CoovaChilli NAS software open source software community. CoovaChilli NAS software addition is the only NAS software that supports Change of Authorization (CoA) updates (CoovaChilli RADIUS Attributes, 2007). This support, although generally used for Packet of Disconnect (PoD) requests will be used for dynamic session updates without disconnecting the users session.

6 CONNECTIVITY

As a user authenticates with the AP via LDAP, their attributes stored in a MySQL database will be sent back to them with an access-accept packet from the RADIUS server. The flow of authentication is represented in Figure 3.

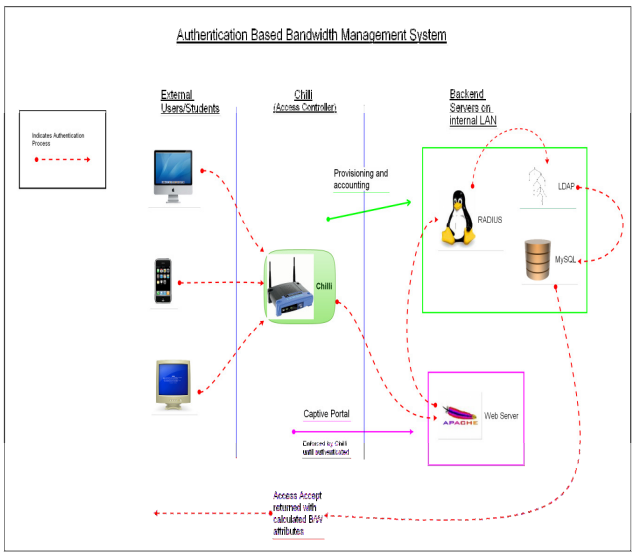

Figure 3: Authentication Process

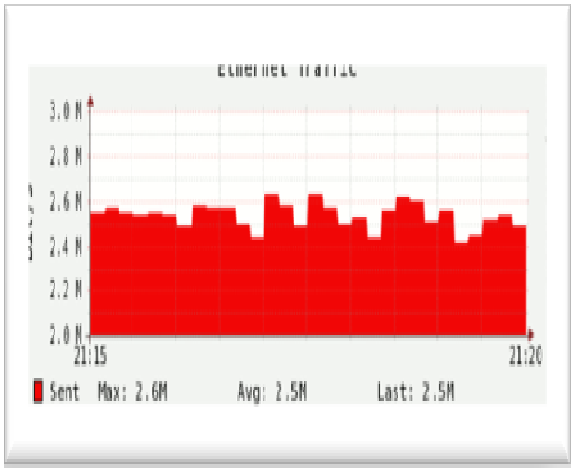

Figure 4: Full Access

The first node connects to the system which authenticates the user, then allocates the bandwidth before downloading a large file utilizing all of the available bandwidth.

The database then keeps track of each user by capturing their username as they login. The download limitations in bits per second (bps) for each user group is defined within the table, shown in Table 1.

Table 1: Download Capacity in bps

d	Groupname	Attribute	P	Value in bps
0	APgroup	WISPr-Bandwidth-Max-Down	=	2450000
5	APgroup	WISPr-Bandwidth-Max-Up	=	2450000

Node 2 will then authenticate. Before the attributes are sent back to the user with the access-accept packet, the group attributes are modified in the MySQL database, seen in table 2. The modified attributes are then sent back to existing users first then the current user with the access-accept packet.

As can be seem in this simple scenario the bandwidth attribute the bandwidth is halved now that two users are both utilizing the access point at the same time (see table 2).

Table 2 – Modified Bandwidth capacity in Bps

d	groupname	attribute	p	Value in bps
0	APgroup	WISPr-Bandwidth-Max-Down	=	1225000
5	APgroup	WISPr-Bandwidth-Max-Up	=	1225000

As can be seen in figure 5 once the second user has been admitted on to the connection the bandwidth allocated for node1 is reduced and redistributed to the new node.

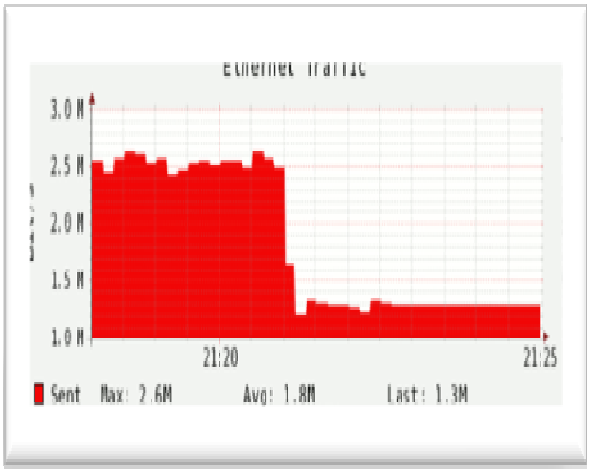

Figure 5: Bandwidth with 2 nodes

This would be a typical scenario in a public connection, but regular customers may become priority users. Therefore this redistribution can then be based on more complex criteria for instance a user labeled a priority user could be allocated a higher bandwidth than a second user.

If one of the users should then log off then the redistribution of bandwidth will happen dynamically giving all of the available bandwidth to the only user left utilizing the AP or equally amongst the remaining users. This will continue as users access and logoff the connection, as can be seen in figure 6 with three users logging in and out of the network.

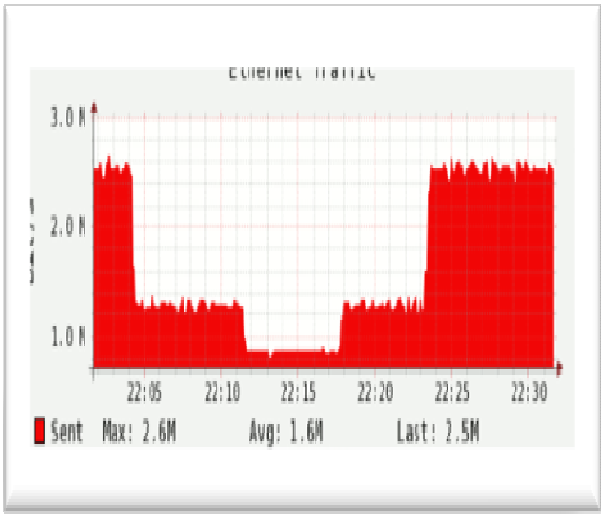

Figure 6 – 3 nodes logging on and off the network

The RADIUS server includes the functionality to execute the two external scripts necessary to modify the database attributes as displayed above and send attribute updates to currently connected users modifying their download bandwidth. The first script needs to be executed before a user logs in, but after they have authenticated. It is essential to authenticate the user before manipulating the bandwidth, otherwise if a user logs in with incorrect details, the database attributes would be redistributed unnecessarily throttling the bandwidth as if an additional user was logged onto the AP.

Existing users which have logged in before, within this scenario, need their bandwidth attributes modified so that every user currently logged in has the available bandwidth shared equally between them. Using a scripting language within the configuration file that the RADIUS server understands called unlang (unlang, 2008) solves this problem, see figure 7.

```
Authorize {
  ldap
        if(ok) {exec auth_script}
}
```

Figure 7 – unlang control structure in FreeRADIUS configuration file

7 CONCLUSION

This report discusses current solutions for managing central, authentication based wireless access to networks, specifically for networks where public users are granted access and the level of trust cannot be guaranteed.

This paper also discusses why network access for these users needs to be controlled in order to mitigate abuse. Additionally current solutions used to limit user's bandwidth by utilizing RADIUS attributes stored in a database, analysing the flaws within these proposed solutions the most prominent being that of the techniques used for bandwidth allocation.

Additionally bandwidth allocation was static even if there were a limited number of users using an AP they would only be permitted a specific amount. This would effectively waste bandwidth, which could potentially be given to users making use of these AP's. This proposed solution dynamically allocates bandwidth based on the number of users utilizing the AP. Future work can be made on grouping specific users into priority groups where they would be permitted more bandwidth, and then the remaining bandwidth would then be divided amongst the less priority users.

8 REFERENCES

► *Captive Portal*. (2005, Aug 25). http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci1117395,00.html.Accessed: 2009-4-09

►*CoovaAP Firmware*. (n.d.). http://coova.org/wiki/index.php/CoovaAP.Accessed: 2008-05-25

►*CoovaChilli*. (n.d.). http://coova.org/wiki/index.php/CoovaChilli. Accessed: 2008-11-25

►*CoovaChilli RADIUS Attributes.* (2007). Retrieved November 25, 2008, from http://coova.org/wiki/index.php/CoovaChilli/RADIUS/AttributesTable.

►*Firstspot v5*. (n.d.). http://www.patronsoft.com/firstspot/ Accessed 2008-12-15

►Jha, S., Hassan, M. (2002). Introduction. n/a (Ed.),*Engineering Internet QoS* (pp. 1-26). Norwood, MA, USA: Artech House, Incorporated.

►*Index of Kamikaze 8.09*. (2009). http://downloads.openwrt.org/kamikaze/8.09/ Accessed 2008-11-25

►Floyd, S., & Allman, M. (2008, July). *RFC 5290 Simple Best-Effort Traffic.* From IETF Network Working Group: http://tools.ietf.org/html/rfc5290 Accessed 2011-06-10

►IEEE WG802.11 - Wireless LAN Working Group. (2005). IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Spec. Retrieved from http://standards.ieee.org/findstds/standard/802.11e-2005.html- 25.6KB - IEEE SA

►IEEE. (1997). 802.11-1997 IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. IEEE.

IEEE. (2003). *Part 11: Wireless LAN Medium Access Control (MAC) and Physical layer (PHY) specifications.* IEEE.

►ITU. (2004). *Handbook Quality of Service and Network Performance Edition 2004.* Geneva: International Telecommunications Union.

►ITU-T Recommendation E.800. (2008). *Terms and definitions related to quality of service and network performance including dependability.* Retrieved from http://www.itu.int/rec/T-REC-E.800

►*Linksys Wrt54GL User Guide*. (n.d.). http://www.linksysbycisco.com/UK/en/products/WRT54GL

►Microsoft. (2011, March 31). *Networking and Access Technologies.* http://technet.microsoft.com/en-us/network/bb530836 Accessed 2011-11-06

►*OpenWRT Wireless Freedom.* (n.d.). from http://openwrt.org/ Accessed 2008-11-25

►Stallings, W. (2004). Wireless Communications & Networks (2nd Edition) Prentice-Hall, Inc. Upper Saddle River, NJ, USA ©2004 ISBN:0131918354

►Tanenbaum, A. S., & Wetherall, D. J. (2010). *Computer Networks 5th edition.* USA.

►*Unlang. (2008).* http://freeradius.org/radiusd/man/unlang.html Accessed 2008-11-25