Comparative Analysis of IEEE 802.1x Authentication Methods

MONIS AKHLAQ, BABER ASLAM, MUZAMMIL A KHAN, M NOMAN JAFRI
Information Security Department, College of Signals
National University of Sciences & Technology
Tamizuddin Road, Rawalpindi
PAKISTAN

Abstract: - The IEEE Standard 802.11 is one of the most widely adopted mechanisms for WLANs, it provides comprehensive guidelines for their operational smoothness. 802.11 suffered from limited data confidentiality and cumbersome procedure for exchange of security parameters. In response to the security limitations in 802.11, IEEE introduced 802.1x for authentication and key management. The 802.1x is a port based network access control protocol that uses Extensible Authentication Protocol (EAP) at the transport layer. The 802.1x only defines authentication mechanism and does not recommend any appropriate authentication method. Consequently wireless vendors implemented their own 802.1x adaptations such as MD5 (Message Digest 5), TLS (Transport Layer Security), TTLS (Tunneled TLS), PEAP (Protected Extensible Authentication Protocol), LEAP (Lightweight Extensible Authentication Protocol) etc.

The paper analyses the performance of 802.1x authentication with respect to different solutions i.e, EAP TLS, PEAP and EAP TTLS. The network performance is gauged with respect to throughput, round time trip (RTT)/response time and packet error in different configurations.

Key-Words: - Authentication, EAP, Packet Error, Round Trip Time, Security, Throughput, Wireless LANs, 802.1x.

1 Introduction

The IEEE standard 802.11 is one of the most widely adopted standard for WLANs. The standard had defined two security mechanisms, Entity Authentication (open system authentication and shared key authentication) and WEP (wired access privacy) [1].

These mechanisms had inherent flaws and vulnerabilities which had led to the creation of 802.11i [2]. The 802.11i addresses the security issues concerning confidentiality and integrity of data in wireless LANs through Temporal Key Integrity Protocol (TKIP) and Counter Mode with CBC-MAC Protocol (CCMP) while IEEE 802.1x ensures authentication [3]. TKIP is designed for legacy devices and hardware that can only support WEP, while CCMP is a more advanced, robust protocol designed for all new devices. Either of these can be combined with 802.1x authentication mechanism as Wi Fi Protected Access (WPA) and Wi Fi Protected Access 2 (WPA2) [4].

The 802.1x uses the Extensible Authentication Protocol EAP [5] at the transport layer for authentication and do not specify any authentication method to identify the credibility of users. The EAP also does not select a specific authentication mechanism at link control phase and postpones it till the authentication phase. 802.1x only defines authentication process and not the authentication method, thus allowing developers to design their own algorithms. This has led to the development of various 802.11 adaptations.

This paper is organized in sections. Section 2 gives the overview of Extensible Authentication Protocol (EAP) with special emphasis on EAP Transport Layer Security (EAP TLS), EAP TTLS and PEAP [6], [7], [8]. Section 3 describes the related work in relation to WLANs and impact of security on network performance. Section 4 gives experimental evaluation of the research work and includes test bed setup, network configuration, performance metrics and security levels. Section 5 shows the results and analyzes the experiment conducted.

2 Extensible Authentication Protocol (EAP)

The Extensible Authentication Protocol (EAP) is an Internet Engineering Task Force (IETF) standard [5] that provides an infrastructure for network access. There are different EAP authentication mechanisms and IEEE 802.1x can implement any of these depending on the choice of users. In this paper we

shall restrict our discussion with EAP TLS, EAP TTLS and PEAP.

2.1 EAP Transport Layer Security (TLS)

EAP Transport Layer Security (EAP TLS) is the type that is used in certificate based security environments. The EAP TLS exchange of messages provides mutual authentication, negotiation of the encryption method, and encrypted key determination between the remote access client and the authenticator. EAP TLS provides the strongest authentication and key determination method. It is supported on servers like RADIUS [9].

2.2 EAP-TTLS

The EAP-TTLS extends EAP-TLS to exchange additional information between client and server by using the secure tunnel established by TLS negotiation. An EAP-TTLS negotiation comprises of two phases: the TLS handshake phase and the TLS tunnel phase. The messages are protected by the TLS tunnel established in first phase. The authentication of supplicant in second phase can use any non EAP protocols such as PPP Authentication Protocols (PAP), PPP Challenge Handshake Authentication Protocol CHAP, Microsoft PPP CHAP Extensions (MS CHAP) or Microsoft PPP CHAP Extensions, Version 2 (MS CHAP V2) [10], [11], [12]. Since only the authentication server needs to have a valid certificate therefore EAP TTLS is more manageable than EAP TLS.

2.3 PEAP

Although EAP provides authentication flexibility through the use of EAP methods, the entire EAP conversation might be sent as clear text (unencrypted). PEAP is an EAP method that addresses this security issue by first creating a secure channel that is both encrypted and integrity protected with TLS. Then, a new EAP negotiation with another EAP method occurs within the secure channel thus authenticating the network access attempt of the access client. Because the TLS channel protects EAP negotiation and authentication for the network access attempt, password-based authentication protocols such as MS-CHAP v2 (susceptible to dictionary attack in an open environment) can be used for wireless LAN authentication.

3 Related Work

WLANs network performance was comprehensively evaluated in [13], [14], [15], [16] however, these efforts did not focused on the impact of security mechanisms on network performance.

Wong investigated the affect of Virtual Private Network (VPN) and IEEE 802.1x security frame work on network performance [17]. The results obtained identified that stronger the security level, lower the network performance. The research was limited to one client sending to one client only. However, Baghaei extended this research work by adding more clients [18]. It also evaluated the affects of packet length on the network. The study of Baghaei showed the network performance is reduced as the number of clients in the network increases (in all security levels).

Andrew Gin analyzed the affects of extending the work to 802.11i (WPA and WPA2) specifications on network performance [19].

No previous research has comprehensively evaluated affects of different 802.1x authentication methods and security levels (EAP TLS, WPA EAP TLS, WPA PEAP, WPA2 PEAP, WPA EAP TTLS and WPA2 EAP TTLS) on network performance in a single work. This work includes the impact of re authentication mechanism, increase in packet length (8000 byte) and increase in number of clients on network performance.

4 Experimental Evaluation

4.1 Test bed

The test bed configuration was based upon the traditional client/server architecture using wireless connections. The hardware used to perform the experiments is shown under respective configuration. The technical specifications of the equipment used in the test bed are shown in Table 1.

TABLE 1
Technical Specifications of Equipment used in the Test bed

Equipment / Connection Used	Specifications/ Details
Server 1*	DNS/DHCP Server.
Server 2*	RADIUS Server (via Microsoft Internet Authentication Service). Funk Odyssey Server Software for EAP TTLS.
Access Point (AP)	D Link 2100 and 3 Com APs were used. Operated in the 80.2.11g, 5 GHz, 5 Mbps mode. The APs have hardware acceleration for both AES and TKIP.
Connection	AP connected to servers via 100 Mbps Ethernet connections.
Client 1, 2, 3 & 4	Pentium IV, 2.4 GHz with 256 MB RAM using Microsoft Windows XP Professional (Service Pack 2).Funk Odyssey Client Software.
Wireless Adaptors for each Client	802.11a, 802.11b, 802.11g using USB 2.0 adopter (DWL – G122).

* The Servers have specification of Pentium IV, 2.4 GHz with 256 MB RAM, using Microsoft Windows Server 2003 Enterprise Edition (Service Pack 1).

4.2 Network Configurations

Two network configurations were used to examine the effect of various authentication schemes:

4.2.1 Multiple Users on a Single Link (Configuration 1)

In the similar scenario as in configuration1, multiple clients' exchange of data was tested. Initially two and later three clients as shown in figure 1 generated the traffic for a single client. The traffic was of variable packet size and inter packet delays.

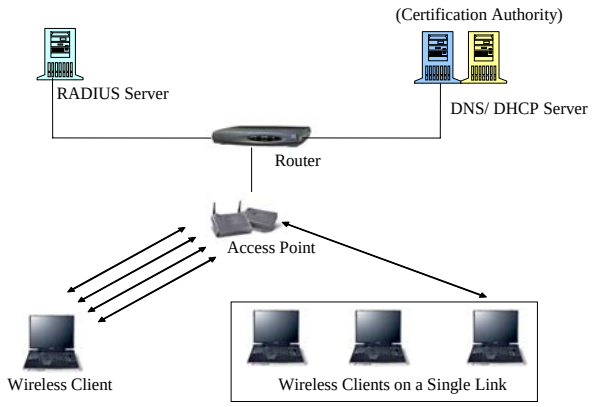

Figure 1: Multiple Users on a Single Link

4.2.2 Re authentication on a Single Link (Configuration 2)

The test bed was placed in the same lab with three clients sending data to one client as shown in Figure 2. In this arrangement each client was setup to reauthenticate itself with RADIUS server in different time intervals. Re authentication function is not available at all access points therefore wireless Access Point 3 Com was used to perform this test.

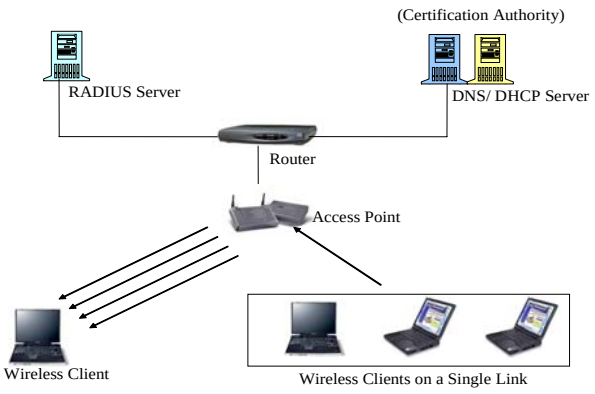

Figure 2: Re authentication on a Single Link

4.3 Performance Metrics

This comparative analysis has been carried out by experimentally analyzing the performance of each network configuration with respect to Throughput, Latency/ Round Trip Time (RTT) and Packet Errors (sum of lost and out of sequence packets).

4.4 Security Level

Various security options available in Wireless LANs are included in this work for a comprehensive evaluation, it ranges from No Security to CCMP/ WPA2 alongwith IEEE 802.1x authentication protocol methods (EAP TLS, PEAP and EAP TTLS). IEEE 802.11 networks currently have three encryption protocols (WEP, Temporal Key Integrity Protocol (TKIP), and Counter Mode/CBCMAC Protocol (CCMP)) and these form the base line for this comparative study. A total of eleven security combinations were selected for the study.

- No Security.
- WEP 64 - Shared Key Authentication
- WEP 128 - Shared Key Authentication
- WPA (TKIP) - PSK Authentication
- WPA2 (CCMP) - PSK Authentication
- WPA (TKIP) - EAP-TLS Authentication
- WPA 2 (CCMP) - EAP-TLS Authentication
- WPA (TKIP) - PEAP Authentication
- WPA2 (CCMP) - PEAP Authentication
- WPA (TKIP) - EAP- TTLS Authentication
- WPA2 (CCMP) - EAP TTLS Authentication

5 Results and Analysis

5.1 Results

5.1.1 Multiple Users on a Single Link

To evaluate the performance of the network in a secure multi client environment, the experiments were conducted with more clients (three clients sending to one). The overall reductions in throughput across all security levels were observed. The WEP 128 and EAP TLS security level has the largest decrease in throughput as a result of multiple clients, comparing with the other security levels.

5.1.1.1 TCP Throughput

The IP Traffic generators in all three clients were configured for TCP protocol at different ports. Packet contents for TCP traffic and inter packet delay were kept as of configuration 1. Initially the packet size was set to 1000 byte but it did showed a major affect on the throughput. The packet size was changed from 1000 bytes to 8000 bytes for better

evaluation. Figure 3 and 4 show the selected results obtained in the test conducted.

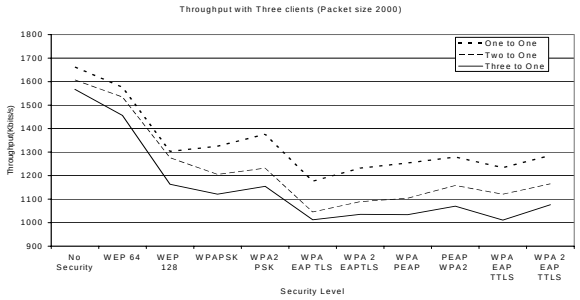

Figure 3: TCP Throughput – 2000 Byte Packet

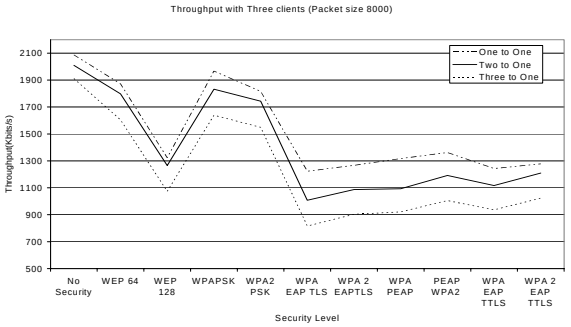

Figure 4: TCP Throughput – 8000 Byte Packet

5.1.1.2 Round Trip Time

Clients 2, 3 and 4 were configured to send time coded packets to Client 1. The packet sizes were again varied from 1000 bytes to 8000 bytes. Figure 5 and 6 show the result for 2000 and 8000 bytes packets respectively.

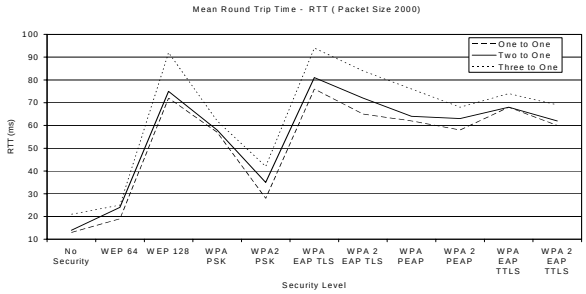

Figure 5: Round Trip Time–2000 Byte Packet

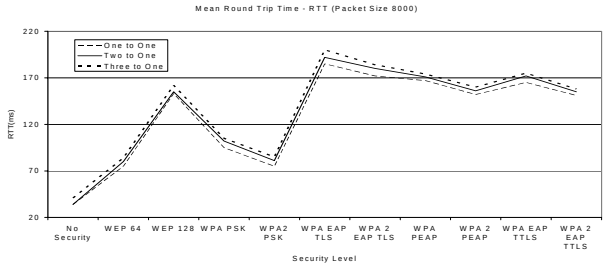

Figure 6: Round Trip Time– 8000 Byte Packet

5.1.1.3 Packet Errors

Clients 2, 3 and 4 were configured to send time coded packets to Client 1. Packet error during TCP traffic were measured and are shown in Figure 7 and 8.

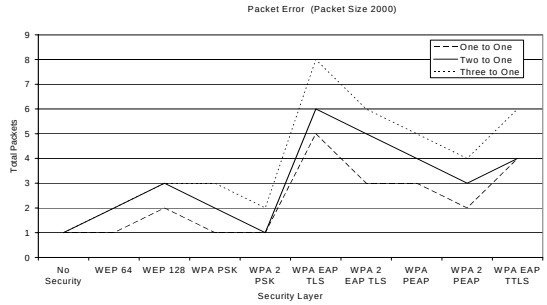

Figure 7: Packet Errors– 2000 Byte Packet

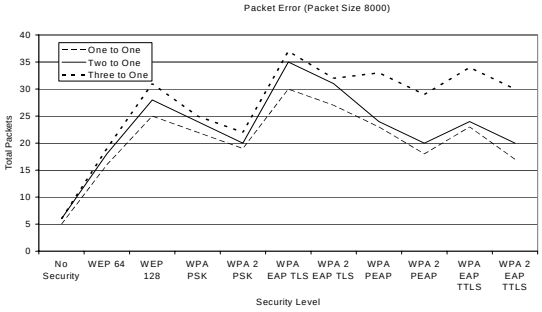

Figure 8: Packet Errors– 8000 Byte Packet

5.1.2 Re authentication on a Single Link

In this configuration test bed was placed in the same lab with three clients sending data to a single client, however in this arrangement each client was setup to re authenticate itself with RADIUS server in different time intervals. Re authentication time was set to 5 minutes in both AP and RADIUS server (Remote Access Policy).

5.1.2.1 Throughput

The IP Traffic generator was configured for TCP protocol at port 2009. Packet contents for TCP traffic were set to 5A (HEX) and inter packet delay to 20 ms, re authentication time was set to 5 minutes in Access point and remote access policy of radius server. The packet size was changed from 1000 to 8000 byte. Figure 9 shows the graphical results for throughput from the TCP test.

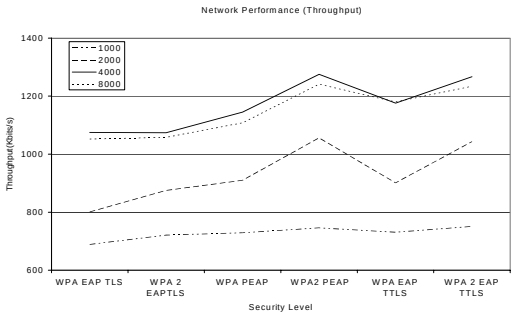

Figure 9: TCP Throughput

5.1.2.2 Round Trip Time

For the calculation of round time trip the answering parameters of IP traffic in (receiving client) was set to echo data and similarly the time code option was enabled on the IP generator side. Each echoed packet is analyzed at the Client 1 and RTT value is computed as shown in Figure 10.

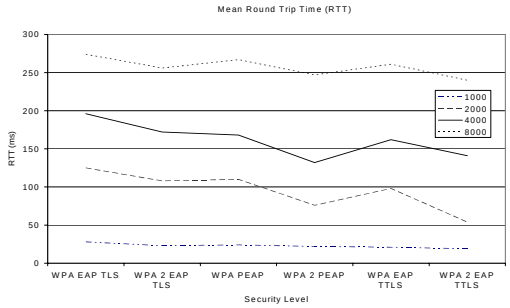

Figure 10: TCP Round Trip Time

5.1.2.3 Packet Error

TCP packet error was also measured by forcing clients to re authenticate as in previous test. Figure 11 gives the results.

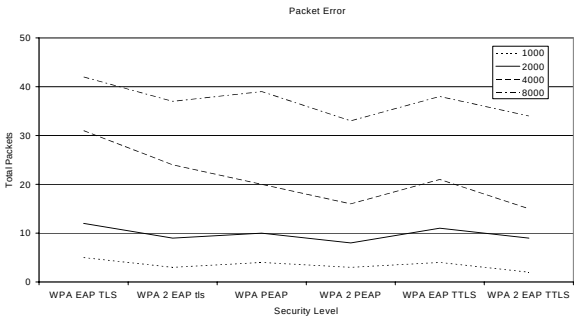

Figure 11: Packet Errors

5.2 Analysis

The results indicate that encrypting traffic causes a substantially greater burden on a network depending on the type of encryption method deployed. Further authentication introduces additional performance overheads and increases latency. Initially when no encryption was used, the network throughput was best. Within different encryption schemes the performance of WEP 128 and TKIP were worse. More importantly, CCMP encryption scheme is better than TKIP. CCMP encryption is typically implemented within the access point or client hardware while TKIP is often done within software, which could be a major cause of throughput reduction. This is further compounded by the fact that TKIP has several mixing processes operating at the same time to generate the data stream. WEP uses RC4 (a stream cipher) and encryption is done between the client and the AP. When bandwidth is not enough, the buffer at the AP fills up and it keeps dropping the packets and a single bit data loss encrypted under RC4 causes the loss of all data following the lost bit.

Two types of authentication schemes were analyzed. The results indicate that incorporation of authentication, authorization, accounting (AAA) [21] architecture into the network results in extra overhead. This is due to the fact that more authentication frames are transferred over the wireless network. These authentication frames impose significant performance degradation. A large increase in round time trip, packet error and decreased throughput is experienced when changing basic WEP authentication to more complicated authentication methods. Utilizing client and server certificates instead of only server side certificate authentication/user name and password methods also introduces another layer of performance overheads, as the EAP TLS technique requires mutual authentication.

Initially the packet size was set to 1000 byte but it did not show any major effect on throughput, therefore variable packet sizes i.e ranging from 1000 to 8000 byte were tested under different security mechanisms.

To evaluate the performance of the network in a secure congested environment, the experiment was conducted using four clients. The performance of a congested network is less then the performance of the network with single client. Moving from one sender to two senders effectively reduces the outgoing throughput and increases the round time trip/packet error from each sending client.

Re authentication is to improve the security by forcing the clients to repeat the authentication steps. This also ensures that fresh keys are established. The performance of PEAP and EAP TTLS is comparable and better then EAP TLS. This poor performance of EAP TLS is due to the fact that EAP TLS uses certificates on both side and is based on mutual authentication.

Conclusion

This work was aimed at analyzing the impact of security mechanisms on different authentication mechanisms used in WLANs. The security techniques include the 802.11 security standard using WEP protocol and the enhanced security standard 802.1x with the EAP protocol were evaluated. The analysis confirmed that security levels within each model produced different impacts on performance. The work is concluded by recommending the use of appropriate security level in relation to network performance.

References:

[1] IEEE Computer Society, "IEEE 802.11 Standard, IEEE Standard for Information Technology", 1999. *http:// standards.ieee.org/catalog/oils/lanman.html.*

[2] IEEE Computer Security," IEEE 802.11i standard, 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) specifications Amendment 6: Medium Access Control (MAC) Security Enhancements. July 2004. *http://standards.ieee.org/catalog/oils/lanman.html.*

[3] IEEE Computer Society, "IEEE Standard 802.1x-2001,IEEE Standard for Local and Metropolitan Area Networks – Port-Based Network Access Control. June, 2001. *http:// standards.ieee.org/catalog/oils/lanman.html*

[4] WPA and WPA2 Implementation White Paper, "Deploying Wi Fi Protected Access WPA) and WPA 2 in the enterprise", March 2005. http://www.wi-fi.org/white_paper/whitepaper-022705- deployingwpawpa2enterprise/.

[5] Blunk.L and Vollbrecht.j, PPP Extensible Authentication Protocol (EAP), IETF RFC 2284,March 1998.

[6] B.Aboba and D.Simon, PPP EAP-TLS Authentication Protocol (EAP-TLS), IETF RFC 2716, October 1999.

[7] Funk.P and Blake-Wilson.S, EAP Tunneled TLS Authentication Protocol (EAP-TTLS), draft-ietf-pppext-eap-tls-02.txt, Feburary 2002.

[8] H.Anderson, S. Josefsson, G. Zorn and B. Aboba, Protected Extensible Authentication Protocol (PEAP), draft-josefsson-pppext-eap-tlseap- 02.txt, Feburary 2002.

[9] Rigney.C, Willens. S, Rubens. A and Simpson. W, Remote authentication dial in user service (RADIUS), IETF Internet Request for Comments 2865, June 2000.

[10] PPP CHAP Extensible Authentication Protocol (EAP)IETF/rfcRFC 2284 March 1998.

[11] W. Simpson . PPP Challenge Handshake Authentication Protocol (CHAP), Internet Request for Comments 1994 August 1996.

[12] G. Zorn, Microsoft PPP CHAP Extensions, Version 2, Internet Request for Comments 2759, January 2000.

[13] B Bing, "Measured performance of the IEEE 802.11 wireless LAN",in Conference on Local Computer Networks,1999.LCN'99, pp. 34-42, October 1999.

[14] L.Chandran Wadia, S Mahajan, and S.Iyer, "Throughput performance of the distributed and point coordination function of an IEEE 802.11 wireless LAN", in IEEE International Conference on Computer Communications (ICCC), August 2002.

[15] A. Vasan and A.U.Shankar, "An Empirical Characterization of Instantaneous Throughput in 802.11b WLANs," Department of Computer Science, University of Maryland, September 2002.

[16] G.Xylomenos and G.C .Polyzos, "TCP and UDP Performance over Wireless LAN," in Eighteenth Annual Joint Conference of the IEEE Computer and Communication Societies. Proceedings of IEEE, vol. 2, pp 439-446, March 1999.

[17] R Hunt, J.Vargo, and J .Wong, "Impact of Security Architectures on Wireless Network Performance," in Fifth IEEE International Conference on Mobile and Wireless Communications Networks (MWCN 2003), October 2003.

[18] N.Baghaei and R. Hunt, "Security Performance of loaded IEEE 802.11b Wireless Networks," Computer Communications, Elsevier, U.K. vol. 27, no.17,pp.1746-1756,2004.

[19] Andrew Gin and R Hunt, " The Performance of the IEEE 802.11i Security Specifications on W LANs," November 2005.

[20] IP Testing Software, "TCP and UDP Traffic Generators". http://www.zti-telecom.com/pages/iptraffic-test-measure.htm.fr.

[21] C De Laat, G Gross, L Gommas, J Volbrecht and D Spence, Interlink Networks, Internet Request for Comments 2903, Aug 2000.