# Link recovery in IEEE 802.11 WLAN using WDS

Marc Portolés, Jose Luis Valenzuela, David Pérez, Oriol Sallent
Departament Teoria Senyal i Comunicacions
Universitat Politècnica de Catalunya
Barcelona, Spain
e-mail: m.portoles@eic.ictnet.es, valens@tsc.upc.es, dperez@tsc.upc.es, sallent@tsc.upc.es

*Abstract*— **This paper presents a new application scenario for the wireless distribution system (WDS) defined in the IEEE 802.11 Standard. The WDS is here used to ensure connectivity of stations associated with an access point (AP) that at a certain moment loses its connection (wired or wireless) with the network. We study the performance of using the combination of 802.1D and WDS to recover connectivity through alternative links when one fails and analyze the convenience of using such a solution for highly mutable scenes where link changes are required often. The paper also proposes a solution as an extension to current deployed solutions in the form of signaling packets that enhance the performance of the system.**

***Keywords: WLAN; 802.11; link recovery;WDS***

## I. INTRODUCTION

The IEEE 802.11 standard [1] has raised a dominant position out of a set of emerging technologies competing for broadband indoor wireless communications. The wide use of the standard implies the appearance of many practical applications with IEEE 802.11 compliant products. A good example for this is the proliferation of wireless communities [5] establishing point-to-point links and providing coverage in public places.

This work proposes and studies a new use for the concept of Wireless Distribution System (WDS) defined in the standard. Here, the WDS is used to ensure the connectivity of mobile stations when the access point (AP) where they are associated loses its connection with the service provider network, redirecting the traffic flow through another AP which still keeps its link. This idea can also be extended to an scenario where multiple mobile AP (also called wireless AP) are used in a layer-2 ad-hoc mobile scenario to ensure connectivity between mobile users and towards a possible backbone support network. A practical study in a test-bed is conducted, which analyses the behavior and convenience of the routing protocols used at MAC level of current networks based on the IEEE 802 family.

The study reflects that the IEEE 802.1D protocol [3] used for link layer routing has enough capacity to manage the route change that implies the lost of a link and thus guarantee the connectivity between the AP and the network. However, the system presents highly variable route switching times which prevent the continuity of applications running at the moment the link fails. The study proposes, as a solution, a signaling strategy between the system elements to optimize the packet routing change process.

The rest of this paper is organized as follows: Section II introduces the new scenario proposal and describes the particular case used for the practical study in a test-bed. Section III describes the test-bed used and presents the study of the performance of the 802.1D protocol and WDS when applied combined in the test-bed. Section IV introduces a solution for the performance flaws detected in the study and analyzes its performance. Finally section V concludes the paper.

## II. A NEW APPLICATION SCENARIO FOR THE WDS

The WDS concept was originally meant to support the functionality of a wireless AP. That is a STA, associated with an AP that also acts as an AP for other STAs. The WDS then serves to extend the area of coverage of an 802.11 network, substituting the most common wired infrastructure, e.g. Ethernet, to interconnect APs and connect them to a supporting backbone. From this original concept, multiple applications have come up into the market, the most popular of which may be the point to point and point to multipoint links used by the widespread wireless communities [5]. Here we propose a new application for the WDS concept extending even more possibilities of usage.

The application scenario studied is similar to those used in ad-hoc networks performance studies (e.g. the one found in [6]). Different stations establish connections when they detect that in the near proximities there are other stations capable of establishing such a connection. Routes are then updated on runtime when links between stations or towards a wired backbone fall and when new optimal links become available. The scenario studied works with stations running as wireless APs and establishing dynamic connections with other stations using WDS links. Stations running in such a mode can make use then of the layer-2 routing protocols to establish routes between hosts and update these routes when connection links fall.

Fig. 1 shows a first case of application for the WDS within the scenario described in this section. Two APs are connected to a backbone support network via wired connections. At a certain instant, an AP (AP2 in the figure) losses its connectivity to the wired support backbone (e.g. a cable failure). From that moment any STA associated with AP2 would lose its connectivity to the network. However if AP2 detects the presence of AP1 within its range of coverage a WDS link can

0-7803-8256-0/04/$20.00 (C) 2004 IEEE

be established between both APs and the traffic intended for the BSS controlled by AP2 can be redirected through AP1.

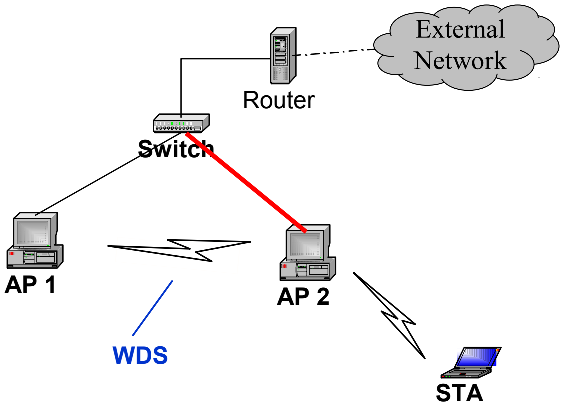

Figure 1. WDS used to maintain connectivity of a fallen wired link

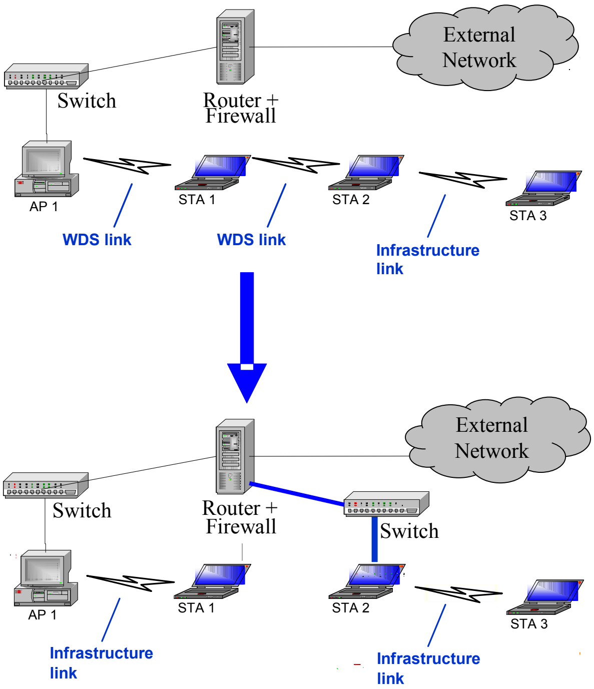

Figure 2. Multiple station scenario with a change in the routing path towards a wired backbone

This first application case can be extended to a more complex situation like the one in Fig. 2 where more stations are involved creating and disabling dynamically WDS links to accommodate the routing paths of all the mobile stations to a changing situation. One can imagine multiple new application cases such as a situation where links fall because of a high mobility of the stations but these two examples illustrate perfectly the idea.

Following sections study the capacity of a combination of 802.1D and WDS to accommodate such an application scenario. The example in Fig. 1 is used in a test-bed to conduct the performance test and evaluate possible causes and solutions to the problems detected.

## III. Study of the Performance of Combined 802.1D and WDS to Save Fallen Links

### A. *Test-bed description*

A test-bed, as depicted in Fig. 3, is used to study the capacity of an AP to redirect the traffic through a WDS link (automatically created) when the link with the distribution network (in this case wired) falls unexpectedly.

The test-bed is formed by two APs connected to the distribution service network (containing two servers) using a central switch. We obtain the APs connecting a WLAN PCMCIA card with the Intersil Prism chipset and an Ethernet card (3COM) to a computer running the Linux operating system. On one hand the computer runs a bridge software allowing the interaction between both cards, and on the other hand runs a specific driver for the WLAN card named *hostap* [2] This driver controls the service functions associated with an AP and allows the establishment of WDS connections. The Linux open source policy allows the change of packets and drivers for experimentation.

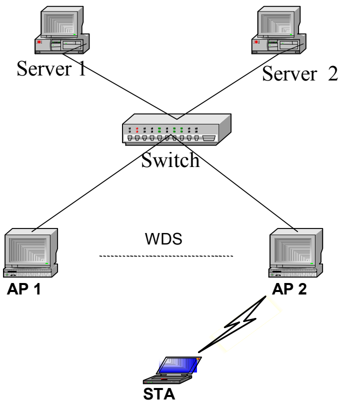

Figure 3. Structure of the Test-bed elements

Fig. 4 depicts the software structure of the system as described above. All the modules in this figure can be studied separately in order to understand their contribution to the performance results obtained in the study.

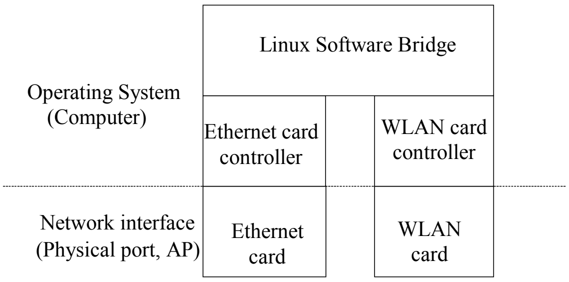

Figure 4. Software scheme of the AP

### B. *Performance study of combined 802.1D and WDS to redirect fallen links*

Fig. 5 represents the downlink throughput available between the two servers and the two APs of the system throughout the time using the topology showed in Fig. 3 where the APs detect each other and establish dynamically a WDS link. This link remains inactive while the wired connections are present. The figure shows how passed 72 seconds the Ethernet link of AP2 is disconnected and it remains disconnected until 54 seconds after. At this moment the AP uses the WDS link as an alternative route. It is possible to distinguish between one link and the other looking at the available throughput between the server and the AP2 which changes from 93 Mbps when using the Ethernet link to 4Mbps in the case of the WDS link.

Experimentally we found that the latency to establish the new route between the AP2 and the rest of the network is very variable from one test to another (between 10 and 400 seconds). There are three main parameters that affect and explain these results: (1) the detection delay by AP2 that the link has fallen, (2) the activation time of the WDS link (activation time of the ports in the bridges of the APs according to 802.1D) and (3) the delay in the detection by the system of the new route to the AP. We analyze these three parameters separately in our test-bed to determine their contribution to the total amount of time.

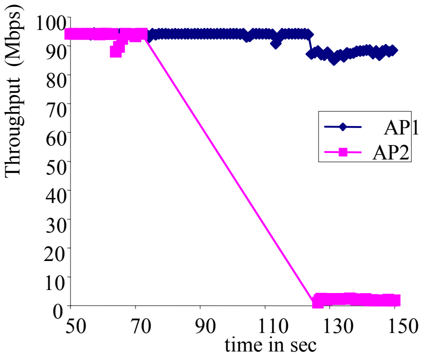

Figure 5. Downlink throughput between the server and the two APs

#### 1) *Detection delay of a fallen link in the AP*

The time that the AP takes to detect the link failure depends both on the time lost by the operating system in order to detect the failure and the time the bridge takes to “decide” that a link is lost according to the configuration parameters. This time highly depends on the configuration and source coding of the AP.

We have detected that our test-bed does not have cross-layer mechanisms that inform the operating system (and thus the bridge module in Fig. 4) that the physical link of the Ethernet card has fallen. In this case then, the detection of a fallen link fully depends on the functionality of the bridge protocol and its configuration. The 802.1D protocol defines two configuration parameters that have a direct impact in the time spent till the fallen link is detected: (1) the *hello time*, time between the emission of consecutive hello messages used for the configuration of the STP mechanism and the (2) *max age*, maximum time without receiving a hello message from the root bridge to decide the route has fallen. The configuration of these 2 values has a direct impact in the decision delay that a route has failed. By default Linux sets these values to 2 seconds for the hello time and 20 seconds for the max age time. Reducing these values should be done carefully to avoid transmission loops. However, if there is no mechanism to inform the bridge of a link failure in a cross-layer fashion, establishing lower values will reduce the delay in the detection of a fallen link.

Windows operating system seems to detect faster the failure of a link through proprietary signaling between the driver and the operating system. Such a mechanism should be considered to be defined in a standard manner to improve interaction between devices of different companies.

#### 2) *WDS link activation time*

The time spent to activate the WDS link depends on the activation time of a disabled port in a bridge, according to the 802.1D Standard. This time mainly depends on the *forward delay* parameter, defined also in the Standard and that refers to the interval the bridge takes between state transitions of the ports. The states are listening, learning, forwarding and blocking. Activating a port means bringing it to the forwarding state (after passing listening and learning states). The linux bridge by default sets the value for *forward delay* to 15 seconds, thus a full activation interval takes a minimum of 45 seconds.

Reducing this value, again, can lead to a higher loop risk when establishing routes. However it may decrease considerably the route switching delay in the AP. Again, signaling from lower levels would help accelerating the switching time. Some commercial Ethernet switches show lower commutation time (in the order of a second) when the reason of a lost link is that one of their ports has lost connectivity.

#### 3) *System detection of a route change*

It is well known that routing tables in layer-2 devices are maintained upon reception of packets using the source address in those packets and associating it to a bridge port. The 802.1D Standard defines the *ageing time* parameter that sets a maximum time an address is kept in the routing table before removing it. This parameter is set, by default in Linux, to 300 seconds. And this explains the great time delays that sometimes the route change experiments. Devices, other than the ones involved in the link failure, have no way of detecting that the route to a station is no longer through a specific port unless a packet from that station is received through another port.

In order to reduce the delay that link failure detection by the system means to the overall performance, a packet from affected stations should be sent to the system in order to update routing paths. However, in order to control the overhead that this would represent in a large system (i.e. with a lot of stations) only those stations that are active (i.e. sending or receiving frames) at the moment of the link failure should send this update frames. This will be discussed further in the next section, obtaining performance results of this proposal.

From this study, and in order to reduce and stabilize the system latency used to switch the routes one may infer that we need to: (1) speed up, at the bridge, the detection that one of its ports (Ethernet link) has fallen and the change of routing port and (2) reduce the time the system takes to detect the changes on the route path. A solution for the former, as has been discussed, needs of standardized cross-layer signalling that enhance the communication between network devices and bridge controllers. Network signaling packets are needed to solve the later. Next section proposes an implemented solution, in our test-bed, for both.

## IV. A SOLUTION AGAINST HIGH LATENCY IN SYSTEM DETECTION: SIGNALING PACKETS.

The solution to reduce the time spent on establishing a new route at system level lies in two points, as seen before: (1) accelerate the detection of fallen ports and establishment of new ports at the bridge of the AP and (2) reduce the time spent on recognizing the new route.

In order to accelerate the detection of fallen ports we look at the drivers of the cards in the system. When the voltage goes down in the physical interface of the Ethernet card (link failure) this is notified to the card driver. Then the driver generates a packet which is sent to upper layers and received by the bridge module that recognizes it and starts the redirection process. In the case we were using wireless APs, this message would be generated in the case the WDS falls, that is, in the case a certain amount of beacons are lost.

To accelerate the new route detection by the system we need to send packets with the source address of the stations affected by the route change. When the bridge module detects the link failure and once the alternative WDS link is activated it generates a packet with type Layer-2 update frame (as recommended in IEEE 802.11f [4]) for each mobile station associated with the AP, and currently active at the failure instant, and another from the AP itself. Then this packet is sent to the network to notify the route change. Thus all layer 2 elements update their routing tables according to 802.1D.

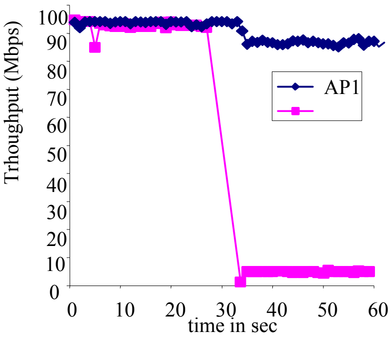

Figure 6. Downlink throughput with route change signalling

Fig. 6 shows the effect of applying the proposed scheme. In this case, after disconnecting the Ethernet link of AP2 at the 27th second the communication is restored 6 seconds after. Empirically we found that now the latency varies slightly from one test to another (from 3 to 7 seconds) the possibility of offering continuity to active applications at the moment of the link failure is improved. These results are comparable to the routing update delays obtained in the now popular ad-hoc networks [6]. These results serve on the purpose of analyzing the convenience of a layer-2 based ad-hoc scheme, using and enhancing present market widespread protocols instead of the new but not sufficiently introduced in the market layer-3 solutions.

The proposed scheme can be easily implemented and is extensible to any scene where the 802.1D protocol is used for routing at layer 2. Moreover, it adds just a little overhead to the system. The adaptation process of traditional fixed network systems to this more dynamical scenario lies in accelerating efficiently the adaptation process of the network interfaces to the continuous changes of topology due to the mobility of the users.

## V. CONCLUSIONS

This document has presented and analyzed a new application scenario for the WDS included in the IEEE 802.11 spec. This new scenario extends the usage of the WDS to dynamically changing scenarios in order to ensure continuity on the connectivity of wireless stations.

The paper shows, using a test-bed, how current layer-2 routing protocols (802.1D) together with WDS are capable of guaranteeing the connectivity of stations when a link falls but fail in maintaining connectivity due to the high and variable latency of changing the system to the new routing path.

A solution based on two level signaling is proposed to solve this situation. The analysis shows that to solve the latency problem there is need for a: (1) standard cross-layer signaling between network interfaces and bridge controllers and (2) standard network signaling to update the system routing path.

The solution proposed is implemented in the test-bed to show similar performance on updating routing paths to the performance of layer-3 ad-hoc routing schemes, arising the question again of the convenience of moving the ad-hoc routing efforts to a layer-2 based solution.

## VI. ACKNOWLEDGEMENTS

This work has been partly funded by the Spanish Research Council under the grant TIC2001-2222.

## VII. REFERENCES

[1] IEEE Std. 802.11-1999, *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications*

[2] Jouni Malinen, Host AP driver for Intersil Prism2/2.5/3, http://hostap.epitest.fi

[3] ISO/IEC 15802-3: 1998, ANSI/IEEE Std 802.1D: Information technology - telecommunications and information exchange between systems - local and metropolitan area networks - common specifications. Part 3: Media Access Control (MAC) bridges, 1998 Edition, Dec 1998

[4] IEEE 802.11f/D5.0, Draft Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution System Supporting IEEE 802.11 Operation, January 2003.

[5] List of wireless communities in the personal telco webpage, “http://www.personaltelco.net/index.cgi/WirelessCommunities”

[6] Marcel Odena, *Assessment of Ad hoc Routing Protocols for Systems Beyond 3G,* Master’sThesis, July 2002, UPC.