Setting up of a Wireless Distribution System (WDS) - a user’s perspective

Sudipto Das

Co-worker: Rajesh Roy

Department of Computer Science & Engineering
Jadavpur University
Kolkata – 32
{sudipto.das,rajesh.roy}@rediffmail.com

Under the Guidance of

Dr. Pradip K. Das

Professor
Department of Computer Science & Engineering &
Coordinator
Centre for Mobile Computing & Communication
Jadavpur University
Kolkata – 32
We would like to take the opportunity to thank all those people who had directly or indirectly helped us through our project titled “Setting up of a Wireless Distribution System (WDS) – a user’s perspective” during the academic year 2004-05.

To be precise, we would like to thank our esteemed professor Dr. P. K. Das for his wise lectures that enabled us to comprehend various aspects of the topic and examine our work thoroughly & with great patience and give valuable advices whenever required to upgrade our skills. We also thank him for providing us the opportunity and the necessary resources required to carry out the work.

And last, but by no means the least, we are proud to declare that we are fortunate enough to thank everybody associated with The Centre for Mobile Computing and Communication, Jadavpur University, for extending their co-operation during the project and without mention of whom our efforts would have been incomplete; again thanks to all concerned.
Contents

1. WDS – an overview

1.1. An Introduction
1.2. How does it work?
1.3. Pros and Cons
   1.3.1. Advantages
   1.3.2. Disadvantages

2. Notes on Hardware Selection

2.1. DWL 7100 AP
2.2. Asus WL 330 Wireless Access Point
2.3. TwinMos Wireless Router
2.4. Avaya Access Point AP-6

3. Deployment at Jadavpur University Campus

3.1. Features of the Avaya Access Point:
3.2. Requirements:
3.3. Important Notes
3.4. Set-up Procedure

4. Looking ahead: Possible enhancements

4.1. Star Configuration
4.2. Chain Configuration
1. WDS - an Overview

1.1 An Introduction:

With the arrival of the Access Points, WDS operation as defined by the IEEE802.11 standard has been made available. Using WDS it is possible to wirelessly connect Access Points, and in doing so extend a wired infrastructure to locations where cabling is not possible or inefficient to implement.

In IEEE 802.11 terminology a “Distribution System” is a system that interconnects so-called Basic Service Sets (BSS). A BSS is best compared to a “cell”, driven by a single Access Point (one of those circles in the diagram below). So a “Distribution System” connects cells in order to build a premise wide network which allows users of mobile equipment to roam and stay connected to the available network resources. A distribution system can Wired (typically Ethernet), or Wireless (using the radio device inside the Access Point).

The following diagram shows a wired distribution system.

If no cable is used but the connection between the APs is established using the PC card a wireless distribution system is created as shown in the next figure:
One important aspect of WDS (this in contrast to other existing wireless AP to AP connection schemes used in for instance outdoor installations) is the fact that a single PC card in the Access Point can assume multiple roles at the same time. It can “drive” a cell (as in wired connected APs), and as such connects wireless clients to the infrastructure, and it can maintain up to six different wireless connections to other Access Points. For that to be possible the operational (frequency) channel will need to be the same for the cell that is controlled by the AP and for the wireless links to the other APs.

1.2 How does it work?

LAN devices (including wireless LAN devices) communicate with each other by using MAC addresses (which are hardware addresses uniquely assigned in the factory to each device). Each Wireless PC Card therefore has a unique MAC address that is used by the system to send data frames to it. If a LAN device transmits data, it will add its own MAC address to the frame as well in order to indicate to the recipient where the frame came from. In short all data frames transmitted over a LAN will contain a Destination and a Source MAC address as part of the frame header. If a data frame is transmitted over an Ethernet cable just those two MAC addresses are required. When data frames are to be transmitted between LAN end-stations that are not connected to the same LAN segment, an intermediate device is required to “bridge” the frame from one segment to another. An access point is such a device, also known as a bridge, that has the capability to relay traffic from one segment to another. It performs this task with the use of a “Bridge Learn Table”, where MAC addresses are stored in association with the LAN segment (or physical interface) where they reside (from the perspective of the bridge).

Traffic between wireless LAN devices that conform to the IEEE 802.11 standard require 4 MAC addresses instead of 2. When a wireless device is associated to an access point it will always direct its traffic to the access point by using the MAC address of the PC card in the access point as its direct destination address. The MAC address of the end station to which the frame was to be sent to is also included in the frame header, so that the PC card in the access point can determine where to relay the frame to. Finally the sending station’s own MAC address is in the frame as the source address. So a total of three addresses are used. When a WDS link is set up between two access points, all four available address fields in the MAC header are used:

- the MAC address of the sender,
- the MAC address of the final destination,
- the MAC address of the sending PC card in the access point,
- MAC address of the receiving PC card in the other access point.

Roaming between cells that are interconnected by a WDS link works exactly the same as for cells that are interconnected via Ethernet. The effect of a relocation of a station from one cell to the other is that the Bridge Learn Tables will be updated to reflect the new location of the station. This is done by the hand-over request messages that are part of the IAPP (Inter Access Point Protocol).

1.3 Pros and Cons:

WDS offers great flexibility at low cost and as such can be applied in many useful situations. However there are also a few considerations that may lead a user to decide not to use WDS.

1.3.1: ADVANTAGES:

- **Cost effective:** No additional expense in terms of adding a wireless link to an already installed Access Point. Adding a WDS link merely requires a reconfiguration of the Access Point, without having to pay the price for an additional PC Card
- **Flexible:** Expanding an existing wired infrastructure network by adding coverage for office space that is not adjacent to the existing office can be easily achieved, providing great flexibility.
  - WDS is also an excellent solution to create a roaming network in an area where wired connections between the APs cannot be established.
1.3.2: DISADVANTAGES (CURRENT AND/OR TEMPORARILY):

- **Encryption**: It is not possible to use encryption with dynamic assigned and rotating keys, on the WDS link. Only fixed assigned WEP keys can be used to provide encryption.
- **Performance**: Use of a single PC Card (and a single channel) results in sharing the same channel amongst the Access Points and the clients, the end-to-end throughput will be less than the maximum attainable value. Obviously using a second PC card can improve this situation but in that case the expense of a second card has to be accepted.
- **Outdoor operation**: WDS allows creation of point to point connections, which would suggest that this could be applied to outdoor installations as well. Though in principle this is true, one has to remember that the IEEE802.11 standard has been devised primarily for LAN (indoor) operations, and that for use in outdoor situations (especially long distances and point to multi-point configurations) additional provisions are to be implemented.

2. Notes on Hardware Selection:

- **DWL 7100 AP (802.11 a/g Trimode Dualband Access Point)**

  **Features:**
  Supported wireless standard 802.11g/a  
  Encryption and authentication support WEP, WPA  
  Firewall support No  
  Logging support No  
  Protocols supported TCP/IP  
  VPN support No  
  Additional LAN ports None  
  Management interfaces Web based, SNMP  
  Print server No  
  Firmware upgradeable Yes  
  Ref: [http://www.dlink.co.in/dlink/Products/wireless/dwl7100ap.htm](http://www.dlink.co.in/dlink/Products/wireless/dwl7100ap.htm)

- **Asus WL-330 Wireless Access Point**

  **Features:**
  Supported wireless standard 802.11b  
  Encryption and authentication support WEP  
  Firewall support No  
  Logging support Yes  
  Protocols supported TCP/IP  
  VPN support No  
  Additional LAN ports None  
  Management interfaces Software based  
  Print server No  
  Firmware upgradeable Yes  

- **TwinMOS Wireless Router B-AP-20**

  **Features:**
  Supported wireless standard 802.11b  
  Encryption and authentication support WEP  
  Firewall support Yes  
  Logging support No  
  Protocols supported TCP/IP, IPX/SPX, NetBEUI  
  VPN support No
Avaya Access Point AP-6

Features:

- Enterprise-class functionality at small business price: Yes
- Advanced Security features: Yes
- Future-ready: Yes
- Supports 802.3af standard: Yes
- Integrated Management: Yes
- Voice-Ready: Yes
- Management interfaces: Web based, SNMP, CLI


3. Implementation at Jadavpur University Campus

We, at Jadavpur University, have set up a WDS using the Avaya AP-6 Access Point.

3.1 Features of the Avaya Access Point:

- **Enterprise-class functionality at small business price**
  Has high-performance radio for better range and interference immunity than other products; advanced security capabilities; standards-based to integrate into multivendor networks; less costly than equivalent products from other vendors. Enterprises can deploy high performance access points at low price; making expanded wireless LAN coverage and accessibility more cost effective.

- **Advanced Security features**
  802.1x support (auto key management, user-based authentication); EAP-TLS, EAP-MD5, EAP-TTLS; Auto key rotation; Access control table and RADIUS Access Control implementation, PUPS (Per user per session) dynamic generation of encryption keys for 802.11 clients using 802.1x.
  Provides more security (dynamic key exchange, better authentication) than basic WEP – making WLAN deployment more secure.

- **Future-ready**
  Can upgrade to WPA and 802.11i security standard.
  Provides customer with investment protection.
**Supports 802.3af standard**

Power over Ethernet (PoE) Support.
Reduces implementation costs by eliminating local power distribution; support of standard for operation in multivendor environments.

**Integrated Management**

Avaya AP-6 element manager is integrated with Avaya Integrated Management via Avaya Multiservice Network Manager.
Simplifies administration and maintenance of Avaya network infrastructure through centralized management.

**Voice-Ready**

Supports Spectralink Voice Priority (SVP) protocol to prioritize voice traffic.

### 3.2 Requirements:

The following are a few essential requirements for setting up of a WDS using the Avaya AP-6 Access Point:

- A terminal in the same network as the APs to be configured.
- MAC Addresses of the APs which are to be integrated in the WDS. If the MAC Addresses of the APs are not known, knowing the IP Addresses of the APs the MAC address can be found out by using the ScanTool, or logging on to the HTTP interface.

### 3.3 Important Notes:

Each WDS link is mapped to a logical WDS port on the AP. WDS ports behave like Ethernet ports rather than like standard wireless interfaces: on a BSS port, an Access Point learns by association and from frames; on a WDS or Ethernet port, an Access Point learns from frames only. When setting up a WDS, keep in mind the following:

- The WDS link shares the communication bandwidth with the clients. Therefore, while the maximum data rate for the Access Point’s cell is still 11 Mb, client throughput will decrease when the WDS link is active.
- If there is no partner MAC address configured in the WDS table, the WDS port remains disabled.
- Each WDS port on a single AP should have a unique partner MAC address.
- Each Access Point that is a member of the WDS must have the same Channel setting to communicate with each other.
- Each Access Point that is a member of the WDS must have the same network domain.
- Each Access Point that is a member of the WDS must have the same WEP Encryption settings. WDS does not use 802.1x. Therefore, if encryption in the WDS link is required, each Access Point must be configured to use WEP encryption, and each Access Point must have the same Encryption Key(s).
- If the network does not support spanning tree, care should be taken to avoid creating network loops between APs. For example, creating a WDS link between two Access Points connected to the same Ethernet network will create a network loop (if spanning tree is disabled).

### 3.4 Set-up Procedure:

To create a WDS link the only thing that is needed, is to configure the access points at one end of the WDS link with the MAC address of the PC card in the access point at the other end of the link.
Logging into the HTTP Interface.

Open a Web browser on a network computer.

**Note:** The HTTP interface supports the following Web browser:
- Microsoft Internet Explorer 6 with Service Pack 1 or later
- Netscape 6.1 or later

If necessary, disable the Internet proxy settings. For Internet Explorer users, follow these steps:
- Select **Tools > Internet Options**....
- Click the **Connections** tab.
- Click **LAN Settings**....
- If necessary, clear the **Use a proxy server** box.
- Click **OK** twice to save your changes and return to Internet Explorer.

Enter the Access Point's IP address in the browser's **Address** field and press **Enter**.

Result: The Enter Network Password screen appears.

Enter the HTTP password in the **Password** field and click **OK**. Leave the **User Name** field blank. (By default, the HTTP password is "public").

Result: The System Status screen appears.

Click the **Configure** button located on the left-hand side of the screen.
Click **Interfaces > Wireless**.

Auto Channel Select must be disabled. Each Access Point that is a member of the WDS must have the same Channel setting to communicate with each other.

- Remove the check on the **Enable Auto Channel Selection** check box and select the Channel to be used.
- Click **OK**.
- Write down the MAC Address of the radio that you wish to include in the Wireless Distribution System.
- Scroll down to the **Wireless Distribution System** heading.

### Wireless Distribution System (WDS)

WDS can be used to establish point to point (i.e. wireless backhaul) connections with other access points. This table is used to configure WDS partner access points.

<table>
<thead>
<tr>
<th>Port Index</th>
<th>Partner MAC Address</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>00:02:2d:12:34:56</td>
<td>Disable</td>
</tr>
<tr>
<td>2</td>
<td>00:00:00:00:00:00</td>
<td>Disable</td>
</tr>
<tr>
<td>3</td>
<td>00:00:00:00:00:00</td>
<td>Disable</td>
</tr>
<tr>
<td>4</td>
<td>00:00:00:00:00:00</td>
<td>Disable</td>
</tr>
<tr>
<td>5</td>
<td>00:00:00:00:00:00</td>
<td>Disable</td>
</tr>
<tr>
<td>6</td>
<td>00:00:00:00:00:00</td>
<td>Disable</td>
</tr>
</tbody>
</table>
Click the **Edit** button to update the Wireless Distribution System (WDS) Table. The WDS Configuration screen will be displayed.

If desired, enable security by checking the **Enable WDS Security Mode** box.

If security mode is enabled, enter a value for **Encryption Key 0**.

Click **OK**.

Enter the MAC Address that you wrote down in Step 2 in one of the **Partner MAC Address** fields of the Wireless Distribution Setup window.

Set the **Status** of the device to **Enable**.

Click **OK**.

Reboot the AP.

Use the **Commands->Reboot** tab to save configuration changes (if any) and reset the AP. Entering a value of 0 (zero) seconds causes an immediate reboot.

**Notes:** The above procedure sets up the one way communication channel between the APs integrated into the WDS. The same procedure, with the same configuration settings, must be repeated for the Partner Node.

Any changes made to the configuration takes effect only after rebooting the AP.
4. Looking ahead: Possible enhancements

The flexibility that WDS offers, can yield numerous different configurations, each having significant operational benefits and limitations at the same time. A few of those configurations are shown here with some explanation on what issues to look out for:

4.1 Star Configuration:

In a star configuration WDS links are established between one AP and several others, as illustrated by the picture below. The central AP could be part of a wired infrastructure network, while the “satellite” APs are positioned to cover an area which is larger than can be covered by a single cell.

In this set-up the root AP needs three WDS ports enabled for 3 different links while the three satellites each have one WDS port enabled. It is not required that the port-index number assigned to a given WDS link is the same as the port-index number on the other side of the WDS link. In other words at the root AP, the MAC addresses for the three satellites are assigned to ports 3, 4 and 5, while in the satellite APs the MAC address of the root-AP can be entered in any port position that is available.
4.2 Chain Configuration:

Where the Star configuration can cover a more rectangular or square area, a Chain configuration allows coverage of a longer shape (for instance a long corridor). The AP's are chained together, where the first AP for example could have a connection to the existing infrastructure (with all the network resources).

In this setup the AP's at either end of the chain will need one WDS port enabled while the AP's in the middle of the chain will require two WDS ports to be configured to point upward and downward in the chain. In a local setup a chain of 3 AP’s has been created (which does not mean that 3 is the upper limit, but it indicates what possibilities exist).

Potential issues that may arise:

- The area covered by the several APs is larger than the coverage area of a single AP. This can negatively impact the defer mechanism of the radios. (i.e. the APs maybe to far away from each other so that they cannot "hear" each others transmissions, which can result in excessive collisions and retransmissions)
- If a single PC card is used for all wireless traffic and wireless clients are operational as well, end-to-end throughput may be considered too low (depending on the applications).
- In the chain configuration, if the chain becomes very long end-to-end latency issue might come into play.