OSI Model for Wireless Communication

Rishipal Bangarh

Astt. Prof., DAV College, Sadhaura –Yamunnagar (India), Pin. No. -133204

Abstract – The WAP stack is an entity of protocols which cover the wireless data transfer. The diagram above shows the order of the different stacks and their protocols. This includes the stacks responsible for the layout as well as the stacks resposible for the actual data transfer. The highest level or stack is the one which deals with the layout. A lower stack is responsible for the transfer and the security through WTLS (Wireless Transport Layer Security). All stacks lower than this one are being called network stack.

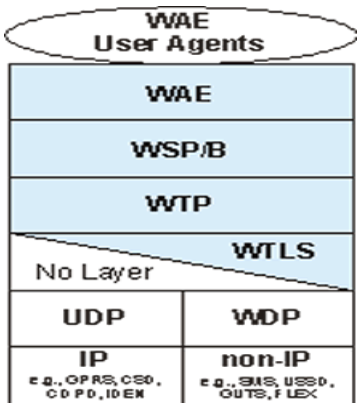
----------♦----------

INTRODUCTION

WAP, Wireless Application Protocol aims to provide Internet content and advanced telephony services to digital mobile phones, pagers and other wireless terminals. The protocol family works across different wireless network environments and makes web pages visible on low-resolution and low-bandwidth devices. WAP phones are "smart phones" allowing their users to respond to e-mail, access computer databases and to empower the phone to interact with Internet-based content and e-mail.

WAP specifies a Wireless application Environment and Wireless Protocols. The Wireless application environment (WAE) is based on WSP (Wireless Session Protocol) and WTP (Wireless Transaction Protocol).

The OSI Model for Wireless Communication



WAP STACK

The basic construction of WAP architecture can be explained using the following model. The order of the independent levels – which are a hierarchy - has the advantage that the system is very flexible and can be scaled up or down. Because of the different levels – or stacks - this is called the "WAP Stack", which is divided into 5 different levels.

- Application Layer: Wireless Application Environment (WAE).
- Session Layer: Wireless Session Protocol (WSP).
- Transaction Layer: Wireless Transaction Protocol (WTP).
- Security Layer: Wireless Transport Layer Security (WTLS).
- Transport Layer: Wireless Datagram Protocol (WDP).

Each stack overlaps with the stack below. This stack architecture makes it possible for software manufacturers to develop applications and services for certain stacks. They may even develop services for stacks which are not specified yet.

The WAP stack is an entity of protocols which cover the wireless data transfer. The diagram above shows the order of the different stacks and their protocols. This includes the stacks responsible for the layout as well as the stacks resposible for the actual data transfer. The highest level or stack is the one which deals with the layout. A lower stack is responsible for the transfer and the security through WTLS (Wireless Transport Layer Security). All stacks lower than this one are being called network stack. Due to this hierarchy of stacks any changes made in the network stacks will have no influence over the stacks above

APPLICATION LAYER (WAE AND WTA)

The environment for wireless applications (Wireless Application Environment WAE) and the application for wireless phones (Wireless Telephony Application WTA) are the highest layer in the hierarchy of WAP architechture. These two are the main interface to the client device, which gives and controls the description language, the script language of any application and the specifics of the telephony. WAE and WTA have only a few easy functions on the client device, like the maintenance of a history list, for example.

SESSION LAYER (WIRELESS SESSION PROTOCOL WSP)

The Wireless Session Protocol (WSP) has all the specifications for a session. It is the interface between the application layer and the transfer layer and delivers all functions that are needed for wireless connections. A session mainly consists of 3 phases: start of the session, transfering information back and forth and the end of the session. Additionally, a session can be interrupted and started again (from the point where it was interrupted.)

TRANSACTION LAYER (WIRELESS TRANSACTION PROTOCOL WTP)

The specifications for the transfer layer are in the Wireless Transaction Protocol (WTP). Like the User Datagramm Protocol (UDP), the WTP runs at the head of the datagramm service. Both the UDP and the WTP are a part of the standard application from the TCP/IP to make the simplified protocol compatible to mobile terminals. WTP supports chaining together protocol data and the delayed response to reduce the number of transmissions. The protocol tries to optimize user interaction in order that information can be received when needed.

WIRELESS TRANSPORT LAYER SECURITY WTLS

The Wireless Transport Layer Security (WTLS) is a optional layer or stack which consists of description devices. A secure transmission is crucial for certain applications such as e-commerce or WAP-banking and is a standard in these days. Furthermore WTLS contains a check for data integrity, user authentication and gateway security.

TRANSPORT LAYER (WIRELESS DATAGRAM PROTOCOL WDP)

The Wireless Datagram Protocol (WDP) represents the transfer or transmission layer and is also the interface of the network layer to all the above stacks/layers. With the help of WDP the transmission layer can be assimilated to the specifications of a network operator. This means that WAP is completely independent from any network operator. The transmission of SMS, USSD, CSD, CDPD, IS-136 packet data and GPRS is supported. The Wireless Control Message Protocol (WCMP) is an optional addition to WAP, which will inform users about occurred errors.

WAP APPLICATIONS

A typical corporate use involves attaching several WAPs to a wired network and then providing wireless access to the office LAN. The wireless access points are managed by a WLAN Controller which handles automatic adjustments to RF power, channels, authentication, and security. Further, controllers can be combined to form a wireless mobility group to allow inter-controller roaming. The controllers can be part of a mobility domain to allow clients access throughout large or regional office locations. This saves the clients time and administrators overhead because it can automatically re-associate or re-authenticate.

A hotspot is a common public application of WAPs, where wireless clients can connect to the Internet without regard for the particular networks to which they have attached for the moment. The concept has become common in large cities, where a combination of coffeehouses, libraries, as well as privately owned open access points, allow clients to stay more or less continuously connected to the Internet, while moving around. A collection of connected hotspots can be referred to as a lily-pad network.

A WAP may also act as the network's arbitrator, negotiating when each nearby client device can transmit. However, the vast majority of currently installed IEEE 802.11 networks do not implement this, using a distributed pseudo-random algorithm called CSMA/CA instead.

WIRELESS ACCESS POINT VS. AD HOC NETWORK

There is a confusion of Wireless Access Points with Wireless Ad Hoc networks. An Ad Hoc network uses a connection between two or more devices without using a wireless access point: the devices communicate directly when in range. An Ad Hoc network is used in situations such as a quick data exchange or a multiplayer LAN game because setup is easy and does not require an access point. Due to its peer-to-peer layout, Ad Hoc connections are similar to Bluetooth ones and are generally not recommended for a permanent installation.

LIMITATIONS

One IEEE 802.11 WAP can typically communicate with 30 client systems located within a radius of 100 m. However, the actual range of communication can vary significantly, depending on such variables as indoor or outdoor placement, height above ground, nearby obstructions, other electronic devices that might actively interfere with the signal by broadcasting on the same frequency, type of antenna, the current weather, operating radio frequency, and the power output of devices. Network designers can extend the range of WAPs through the use of repeaters and reflectors, which can bounce or amplify radio signals that ordinarily would go un-received. In experimental conditions, wireless networking has operated over distances of several hundred kilometers.

Wireless networking lags behind wired networking in terms of increasing bandwidth and throughput. While typical wireless devices for the consumer market can reach speeds of 300 Mbit/s (megabits per second) (IEEE 802.11n) or 54 Mbit/s (IEEE 802.11g), wired hardware of similar cost reaches 1000 Mbit/s (Gigabit Ethernet). One impediment to increasing the speed of wireless communications comes from Wi-Fi's use of a shared communications medium, so a WAP is only able to use somewhat less than half the actual over-the-air rate for data throughput. Thus a typical 54 MBit/s wireless connection actually carries TCP/IP data at 20 to 25 Mbit/s. Users of legacy wired networks expect faster speeds, and people using wireless connections keenly want to see the wireless networks catch up.

SECURITY

WIRELESS LAN SECURITY

Wireless access has special security considerations. Many wired networks base the security on physical access control, trusting all the users on the local network, but if wireless access points are connected to the network, anyone on the street or in the neighboring office could connect.

The most common solution is wireless traffic encryption. Modern access points come with built-in encryption. The first generation encryption scheme WEP proved easy to crack; the second and third generation schemes, WPA and WPA2, are considered secure if a strong enough password or passphrase is used.

REFERENCES

1. The HCI blog: A brief History of WAP

2. OMA: Frequently Asked Questions

3. MX Telecom: WAP Push

4. Openwave: WAP Push Technology Overview[*dead link*]

5. Will Wap's call go unanswered?

6. Silicon.com: BT Cellnet rapped over 'misleading' WAP ads

7. http://press.nokia.com/PR/199902/777256_5.html

8. http://www.filibeto.org/mobile/firmware.html

9. The Globe and Mail: "Survivor's guide to wireless wonkery",

10. IT Web: "A RIVR runs through it"

11. Builder.au 2004/08/10: UK WAP usage doubles in 12 months

12. IMCR: NTT DoCoMo Inc.: Leadership Position in Japanese Mobile Market under Threat?

13. "FCC Revises 700 MHz Rules To Advance Interoperable Public Safety Communications And Promote Wireless Broadband Deployment",

14. "FCC Revises 700 MHz Rules To Advance Interoperable Public Safety Communications And Promote Wireless Broadband Deployment"

15. Wired News: Gopher: Underground Technology