College of Computer Science
Northeastern University
Wireless Networks CS G250

Lecture 11
October 20th 2008
Lecturer: R. Sundaram

802.11 (cont'd.), Mobile IP, WAP

1 802.11

1.1 The OSI and IEEE models

Any networking protocol can be analyzed in terms of the seven layers of the OSI model. The model was developed by Open Systems Interconnection as part of the effort for standarizing computer networks. Conceptually, the layers are stacked one on top of each other, and every layer provides a certain subset of services. Layers above can use the services provided by the layer beneath it, and conversely, the layer below is said to provide services to the above layers (see Figure 1).

In particular, some of the services provided by the layers are:

Transport Provides an End-to-End connection

Network Provides Addressing and Routing on network

Link Provides a concept of link between two nodes, Medium Access Control, Logical Link, retransmission, error control

Physical Voltages, light, modulation

Similar to the OSI model, the IEEE model attempts to standarize network implementations, and upper layers use the services of the lower ones. In contrast however, the Link and Physical counterparts of the IEEE model are further divided as follows:

Link **Logical Link control** Handles retransmissions

Medium Access control Error control and framing

Physical **Physical Convergence Procedure** Translates frames into bits

Medium Dependency layer Operations tied to the physical medium

The IEEE 802.11 protocol falls under the Link and Physical layers and specifies its behavior for those portions of the model. The protocol has been amended several times, and each one is referred to by a letter suffix. Hence, the a, b, g, i, or n versions of the protocol:

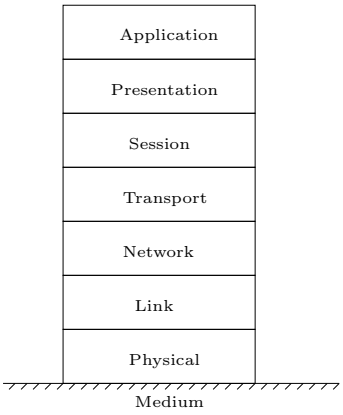

Figure 1: The OSI model's seven layers

802.11a Operating frequency of 5GHz, uses OFDM modulation and supports data rates up to 54Mbps

802.11b/g 2.4GHZ, DSSS, up to 54Mbps

The standard describes two modes of operation (shown in):

Ad-hoc Nodes talk 1 to 1 in a mesh network (Figure 2

Managed mode A distribution system (typically wired) contains wireless Access Points (AP) to which the client nodes can associate. Every AP has a zone of influence under which it can be seen (related to its radio range). Communication is done exclusively with the AP, even when under the same zone of influence (Figure 3).

Association with an access point consists of the following steps:

1. Send a probe frame from node
2. Probe response from AP
3. Select AP, send association request
4. AP replies with association response

In addition, APs can send periodic beacons (which contain the SSID), which the nodes can use later to associate.

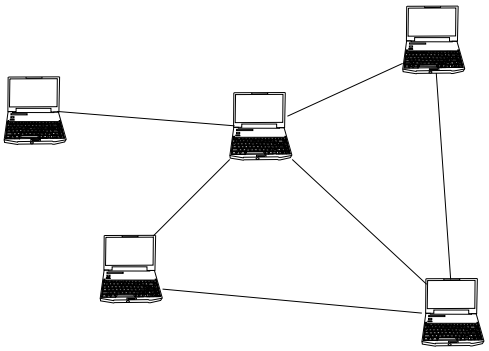

Figure 2: Adhoc mode

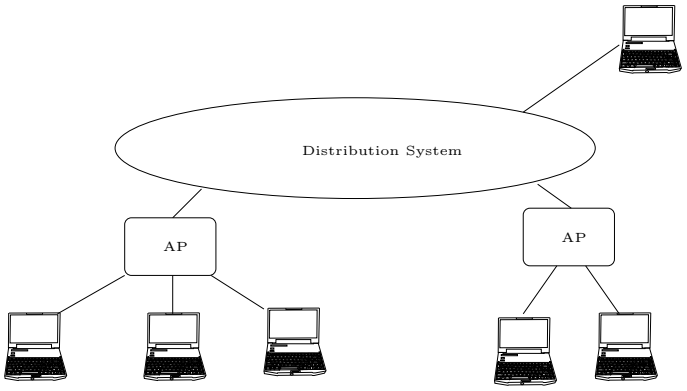

Figure 3: Managed/AP mode

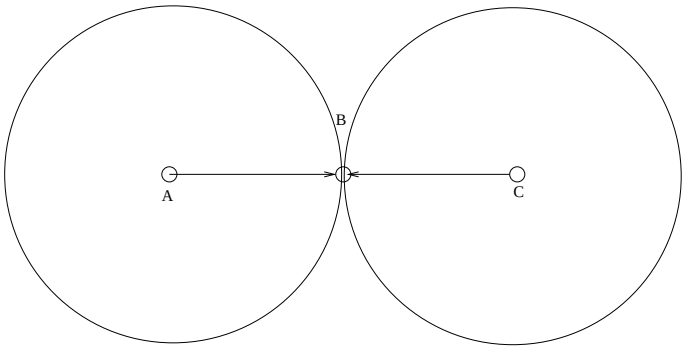

Figure 4: Hidden terminal problem

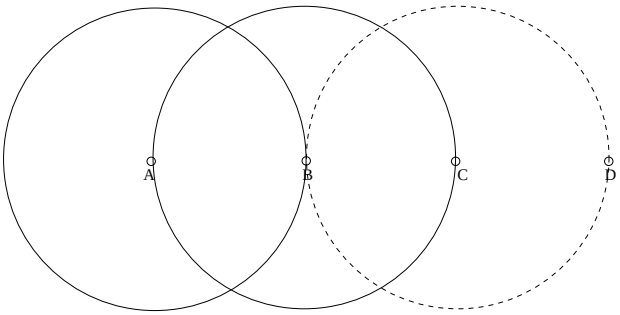

Figure 5: Exposed terminal problem

1.2 MAC Layer

When in a wired network context, medium contention consists of listening for silence on the medium and detecting collisions (i.e. checking if the voltage in the wire is high when one speaks). In the case of a collision, nodes simply back off for a time and retry. In a wireless network however, sensing the medium is does not guarantee being able to detect collisions. Take for instance the hidden and exposed terminal problems depicted in Figures 4 and 5.

In the hidden terminal case, A is sending data to B. C is out of A's range, therefore just sensing the medium is not enough to avoid a collision between A and C at B. In the exposed terminal, C is within range of B. However, neither A nor D are, but just sensing the medium, C decides not to send to D. This would cause no collisions, but the capacity from C to D to communicate is wasted.

Because of this, 802.11 uses Multiple Access Collision Avoidance (MACA)

which introduces Request to Send (RTS), Clear To Send (CTS) packets, in conjunction with Inter-Frame Spacing (IFS) to solve the above types of problems.

Roughly, for A to send data to B under MACA, the following things happen:

1. Wait for IFS
2. Send RTS
3. Wait for timeout or CTS
4. If CTS is received, start sending.
   If timeout, random exponential backoff + IFS and return to step 2

Inter-frame spacing is introduced to give certain types of communication a higher priority and to avoid collisions. There are 3 types of IFS by increasing order of their duration:

SIFS Short IFS – For the highest priority communications: ACKs, CTS

PIFS Point Coordination IFS – For AP managed mode, polling notifications (who talks next), for taking control of transmission

DIFS Distribute Coordination IFS – For Ad-hoc mode.

2 Mobile IP

Mobile IP extends IP to allow nomadic connections. When a device sends data and moves to other networks, it is necessary to make the returning packets reach the moving device. A schematic of this is shown in Figure 6.

A device that tipically connects to a given network (called the Home Network) registers itself with a device called the Home Agent. After the device leaves the home network and enters a different network (Foreign Network), it will discover its original home agent is gone, and will see a Foreign Agent. The nomad then will register with both the FA and let the Home Agent know its IP address on the foreign network.

If the mobile node was engaged in a connection with some external server (which only knows the nomad's address in its home network), the HA and FA will set up an IP-in-IP tunnel. Any packet addressed to the nomad's home address will be forwarded to the foreign agent which in turn will pass it over to the nomad. Packets sent from the nomad can be sent without tunneling, but it is possible to tunnel them as well.

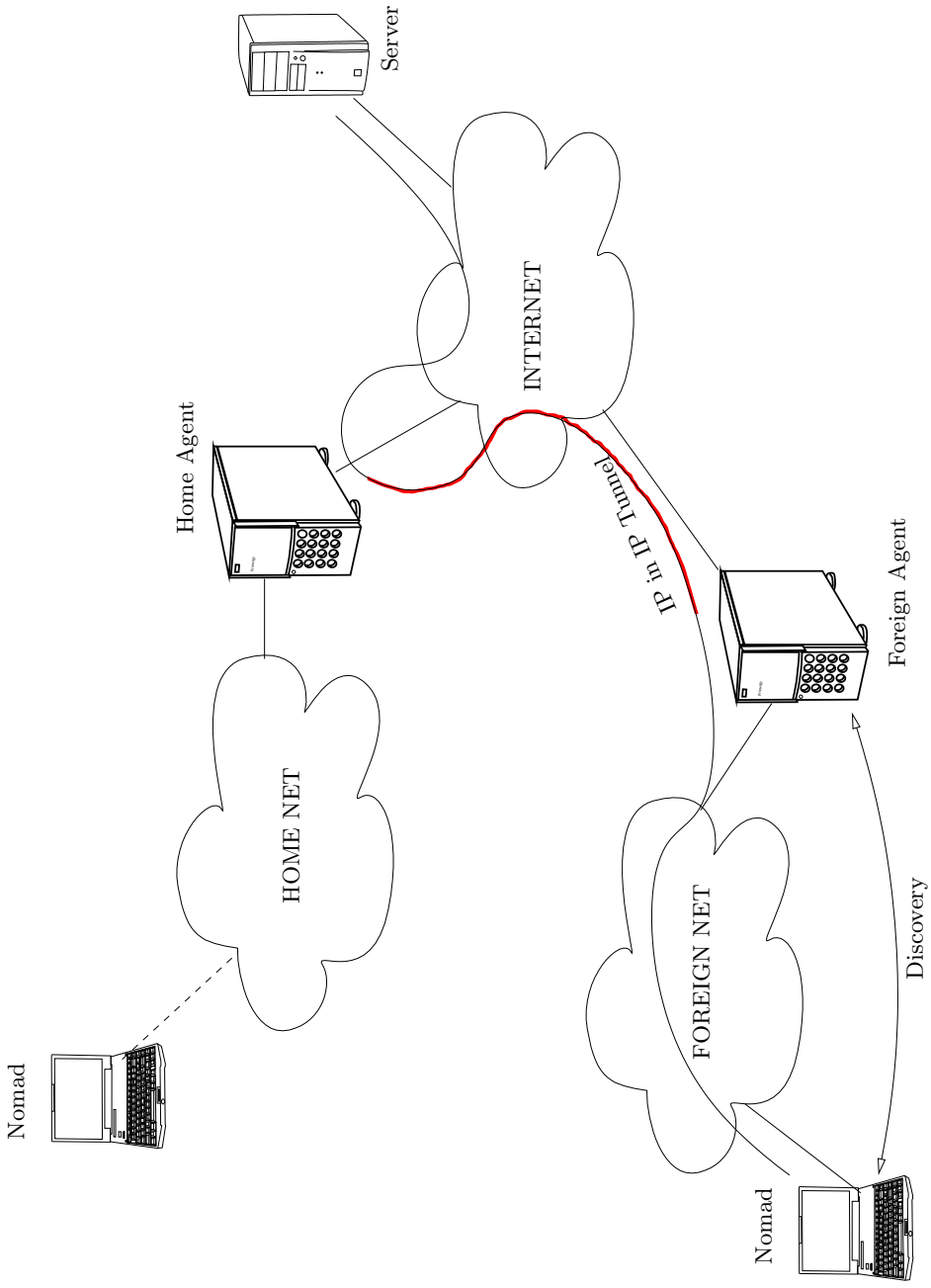

Figure 6: Mobile IP

The main operations taking place in mobile IP are

Discovery Every mobile node sends broadcasts to discover agents in whatever network it is in.

Registration The nomad node needs to inform its home agent what address it has in the foreign network

Tunneling This is used to forward packets addressed to the home address to the foreign address.

3 Wireless Application Protocol (WAP)

WAP is an standard that attempts to bring access to the internet to wireless phones and other mobile devices, independent of wireless technology and using existing Internet standards. Given that small wireless devices are very limited in terms of display area and processing power, the idea is to offload the main processing capabilities to a special nodes called the WAP proxy. This server then becomes the central point where translation to and from HTTP and the wireless specific communication scheme is done. In addition, the proxy translates HTML content into a more suitable set of instructions for the devices to display content in their screens.