Memo: USC WLAN traces format

Wei-jen Hsu
Aug. 2005

USC WLAN traces include the following files. Each type of log is separated in one-file-per-day organization. Since each trace is collected by more than one server for reliability, they may contain duplicated entries. Please be aware of such duplicated entries when processing the traces.

For details of how we obtain an "association duration trace" (i.e. Association history of each node at switch port granularity, approximately corresponds to buildings on campus) from these traces, please see another memo for trace manipulation outlines.

(1). Session traces:

These logs of sessions are collected at the VPN server for wireless users at USC. Before using the network, users must establish a VPN session to the server. The "Start" and "Stop" timestamps in the trace represents the beginning and the end of these VPN sessions.

The fields in each line of the trace are:

1. Day of the week: Sun, Mon, Tue, Wed, Thu, Fri, Sat
2. Month
3. Day
4. Time: HH:MM:SS
5. Action: "Start" or "Stop" of a session.
6. Private IP in USC network.
7. Public IP given to the host.

(2). DHCP log:

This log contains the private IP assignments to MAC addresses. The listed private IP is given to the MAC address at the indicated time. The fields are:

1. Month
2. Day
3. Time: HH:MM:SS
4. Private IP in USC network
5. MAC address

(3). Traps:

The trap log contains the (switch port, MAC address) association when the user is online. This log records the approximate location of nodes, since the switch ports correspond to buildings in USC network. However, if a node reappears repeatedly at the same switch port, a new trap entry may not be generated. Hence the trap log is mainly used as an indication of the "last seen" location of the node, and we assume it does not move unless indicated otherwise by a new trap entry.

The fields are:

1. Month
2. Day
3. Time: HH:MM:SS
4. Switch IP
5. Switch port (switch IP + switch port is used to locate the node on USC campus map, the Mapping file is also available online)
6. MAC address

For the processed trace, we have the association history for each MAC address in a separate file. The fields in these files are:

1. Start timestamp: The starting time of an association record. The timestamp is defined as the elapsed time since Apr. 1, 2005 in unit of seconds.
2. Location: the building code of the association record.
3. Duration: duration of the association record, in unit of seconds.