

Personal Computer Footprints

Each personal computer (PC) leaves electronic evidence of its existence. This evidence is called a footprint. The type of the footprint varies by what the user is doing and where he/she is located at the time. Included below are some of the various tools that we use to track PCs.

On the Wire – Connected to the Internet

PCs can be in one of six operational states, from powered off (but connected to a power source) to fully functional (machine in use), and phases in between. Each state holds a unique property.

When a PC is connected to a power source and connected to a working ethernet environment managed by CiscoWorks or Campus Manager, our management tool has the ability to communicate with the PC's Network Interface Card (NIC). Each NIC holds a unique number or identifier. That unique number is called a MAC address. Whether the PC is powered up, sleeping or powered off, the NIC has the ability to communicate to the Ethernet connection. Cisco provides a tool that can identify the machine, its name, the MAC address and the Internet protocol (IP) address whether it is powered on or not. We use these characteristics to identify the machine's existence on the domain.

IP Address Ranges

The IP address in the COV environment provides the agency identification and the physical street address for that agency's site. Please note, however, that there can be multiple agencies at the same or neighboring sites. In these cases, the IP address can determine the location but not the specific agency. Additionally, when a user connects via virtual private network (VPN) from alternate locations outside the COV domain, we cannot determine the physical address based on the IP address.

User Authentication on the COV Domain

Footprints are generated when a user authenticates to a COV domain resource. The domain controller records information such as user name, date, time, machine name and IP address each time a person logs on.

Asset Survey

Every 90 days users are asked to respond to a pop-up survey to collect information for their specific PC. The data received from the user is analyzed for accuracy, but if the user enters incorrect information or doesn't validate the information provided, this could result in incorrect information being uploaded to the asset management database. Having employees provide and/or validate information is crucial since it is this information that is used to bill agencies.

McAfee Virus Scan

Each McAfee agent on a PC calls into the server daily at 10 a.m. and 2 p.m. for virus and rule definition updates. Machines that check in leave information in a database regarding network connectivity.

Verification and Validation (V&V) Process

Over the past year, the asset management team has continued to refine the asset validation process. On a monthly basis we use the tools above to validate assets, make corrections to data and update data fields within asset center, the asset database of record where billing is generated. The V&V process is continually evaluated, and changes are made as needed when process improvement is identified.