End-to-end VLANs are positioned to support maximum flexibility and mobility of end devices. Users can be assigned to VLANs regardless of their physical location. As a user moves around the campus, that user's VLAN membership stays the same. End-to-end VLANs should group users according to common requirements. All users in a VLAN should have roughly the same traffic flow patterns

End-to-end VLAN follows the 80/20 rule in which 80 percent of user traffic stays within the local workgroup, whereas 20 percent is destined for a remote resource in the campus network (like Internet…).

End-to-end VLANs have the following characteristics:
Users are grouped into a VLAN based on function, not location.
The user belongs to the same VLAN no matter where he plugs his PC into the network (this requires Cisco's VMPS).
End-to-end VLANs are typically used for security reasons or for application or resource requirements.
End-to-end VLANs are difficult to implement and troubleshoot

Local VLANs
The problem with end-to-end VLANs is that they become extremely difficult to maintain as the campus network grows and changes. Because of this, most network administrators of campus environments use local VLANs.
Unlike end-to-end VLANs, local VLANs are very easy to plan and implement.
Local VLANs are based on geographic locations by demarcation at a hierarchical boundary (core, distribution, access). Therefore, a local VLAN would never span from an access layer to a core block.

Local VLAN follows the 20/80 rule: only 20 percent of traffic is local, whereas 80 percent is destined to a remote re-source across the core layer