CSET 150

NETWORK DESIGN AND MANAGEMENT

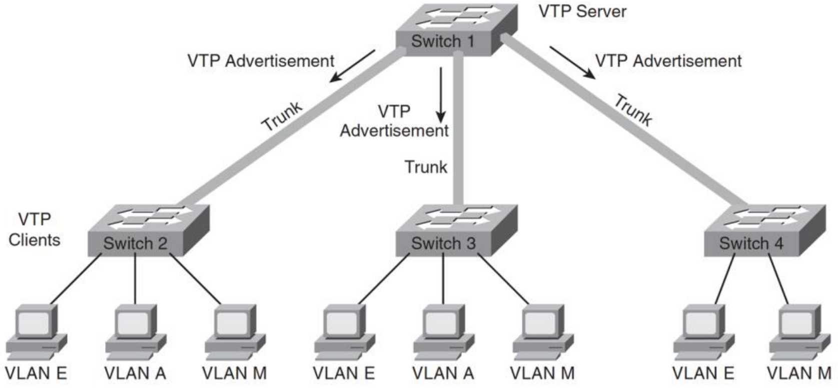
EVENING MASTERS EDITION

DR. MAHBOOB QAOSAR

ASSOCIATE PROFESSOR, CSE, RU

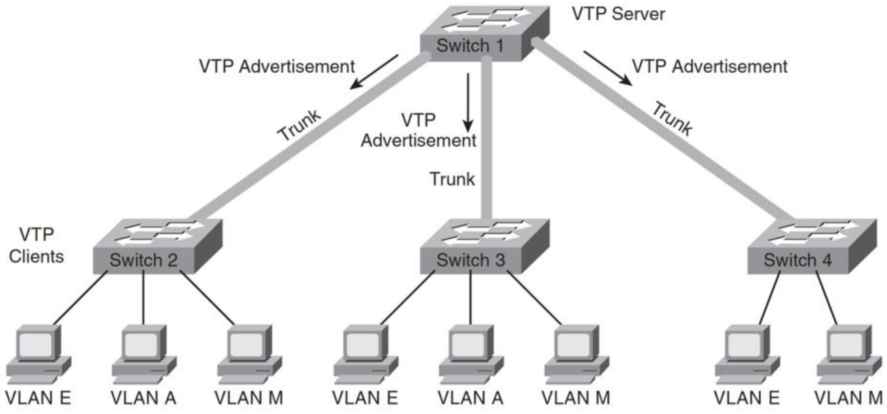
Week # 2

VLAN Trunking Protocol (VTP)



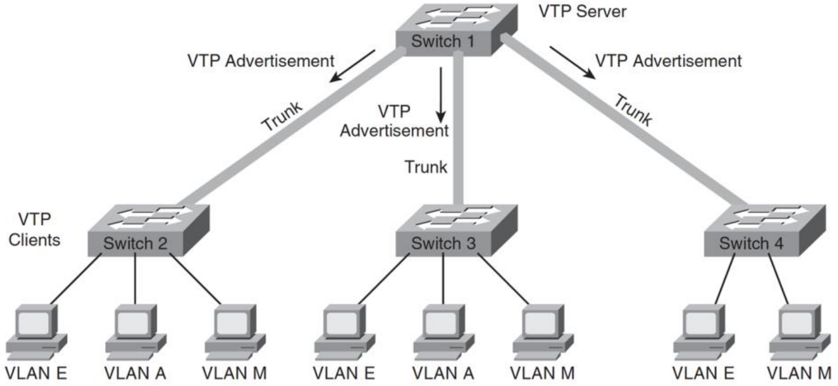
- The VLAN Trunking Protocol (VTP) is a Cisco-proprietary Layer 2 protocol that allows easier configuration of VLANs on multiple switches
- A switch in a VTP domain (a group of switches communicating with VTP) can be in one of three modes:
  1. server (which is the default mode),
  2. client,
  3. or transparent mode

VLAN Trunking Protocol (VTP)



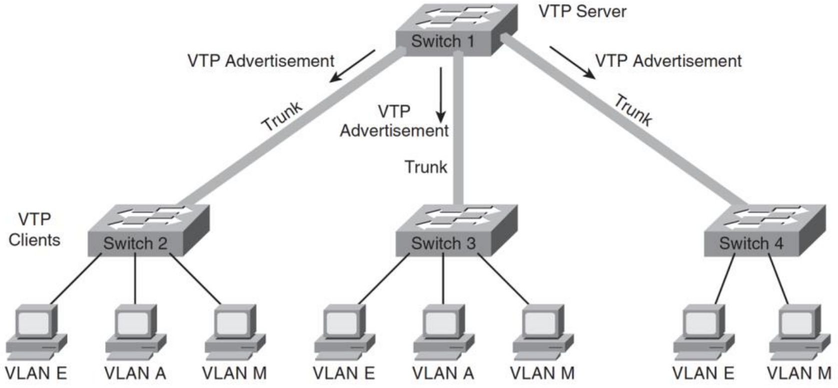
- The VTP server is the one on which you **configure** the VLANs;
- It sends VTP advertisements, containing VLAN configuration information, to VTP clients in the same VTP domain,
- VTP advertisements are only sent on trunks.

VLAN Trunking Protocol (VTP)



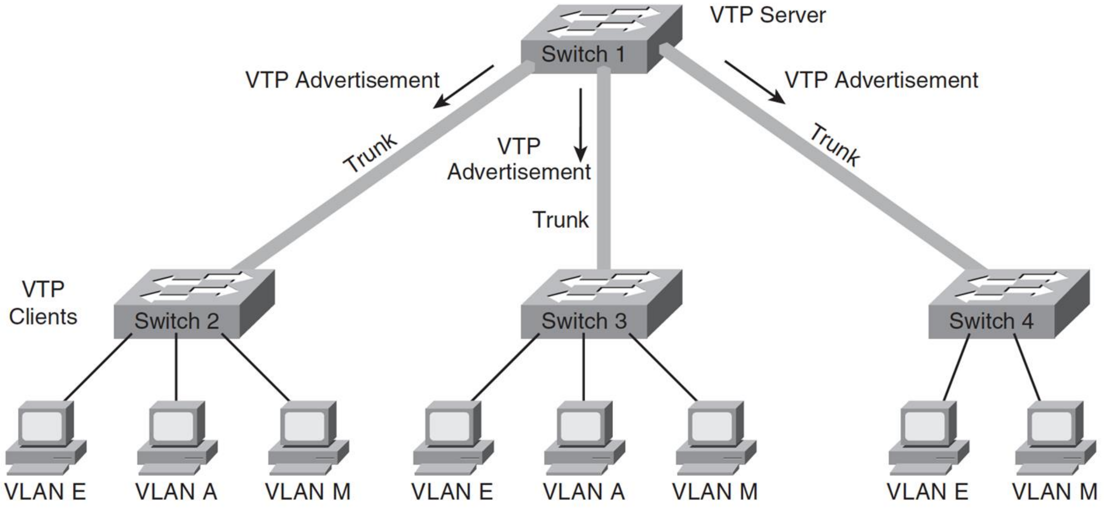
- You **cannot** create, modify, or delete VLANs on **a VTP client**;
- a VTP client only accepts VLAN configuration information from a VTP server.
- A VTP client also forwards the VTP advertisements to other switches.

VLAN Trunking Protocol (VTP)



- You can create, modify, or delete VLANs on a switch that is in VTP **transparent mode**;
- This information is **not sent to other** switches, and the transparent-mode switch ignores advertisements from VTP servers
- But does pass them on to other switches.

VTP Pruning



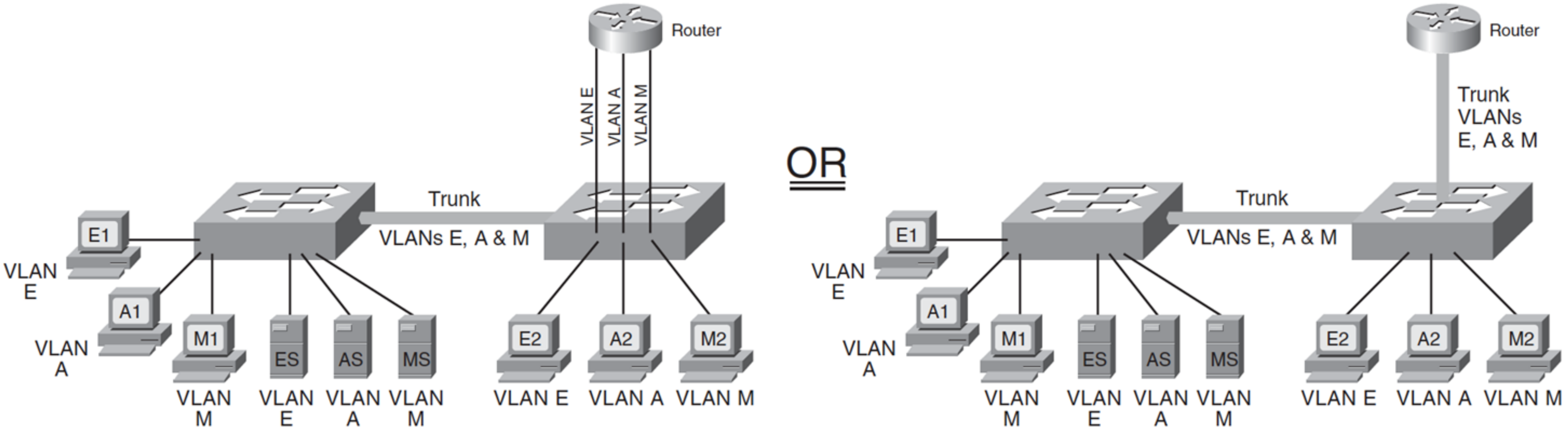
- VTP pruning (trim/ reducing) is a VTP feature that helps reduce the amount of flooded traffic that is sent on the network.
- …, the switches communicate with each other to find out which switches have ports in which VLANs;
- switches that have no ports in a particular VLAN (and have no downstream switches with ports in that VLAN) do not receive that VLAN's traffic

Inter-VLAN Routing

- But how do networked devices on different VLANs communicate with each other?
- Just like devices on different LANs, those on different VLANs require a Layer 3 mechanism (a router or a Layer 3 switch) to communicate with each other.

Inter-VLAN Routing

- A Layer 3 device can be connected to a switched network in two ways:
  - by using multiple physical interfaces or
  - through a single interface configured as a trunk.
- The diagram on the left in this figure illustrates a router with three physical connections to the switch; each physical connection carries traffic from only one VLAN.

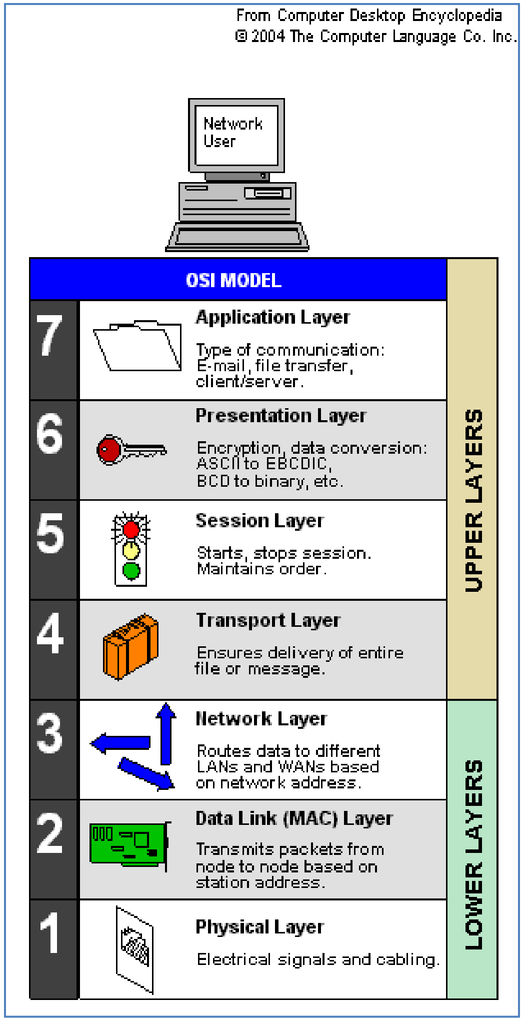


Multilayer Switching

- The 2 different ways that **Layer 3 switching is implemented** within Cisco switches:
  1. Multilayer switching and
  2. Cisco Express Forwarding

Multilayer switching

- Multilayer switching… **MLS**
  - allows switching to take place at different protocol layers.
  - Switching can be performed only on Layers 2 and 3,
  - or it can also include Layer 4.
  - MLS is based on network flows.
    - A network flow is a unidirectional sequence of packets between a source and a destination.



From Computer Desktop Encyclopedia
© 2004 The Computer Language Co. Inc.

OSI MODEL

7	Application Layer	Type of communication: E-mail, file transfer, client/server.	UPPER LAYERS
6	Presentation Layer	Encryption, data conversion: ASCII to EBCDIC, BCD to binary, etc.	
5	Session Layer	Starts, stops session. Maintains order.	
4	Transport Layer	Ensures delivery of entire file or message.	
3	Network Layer	Routes data to different LANs and WANs based on network address.	LOWER LAYERS
2	Data Link (MAC) Layer	Transmits packets from node to node based on station address.	
1	Physical Layer	Electrical signals and cabling.	

MULTILAYER SWITCHING

- The three **major components** of MLS are as follows:

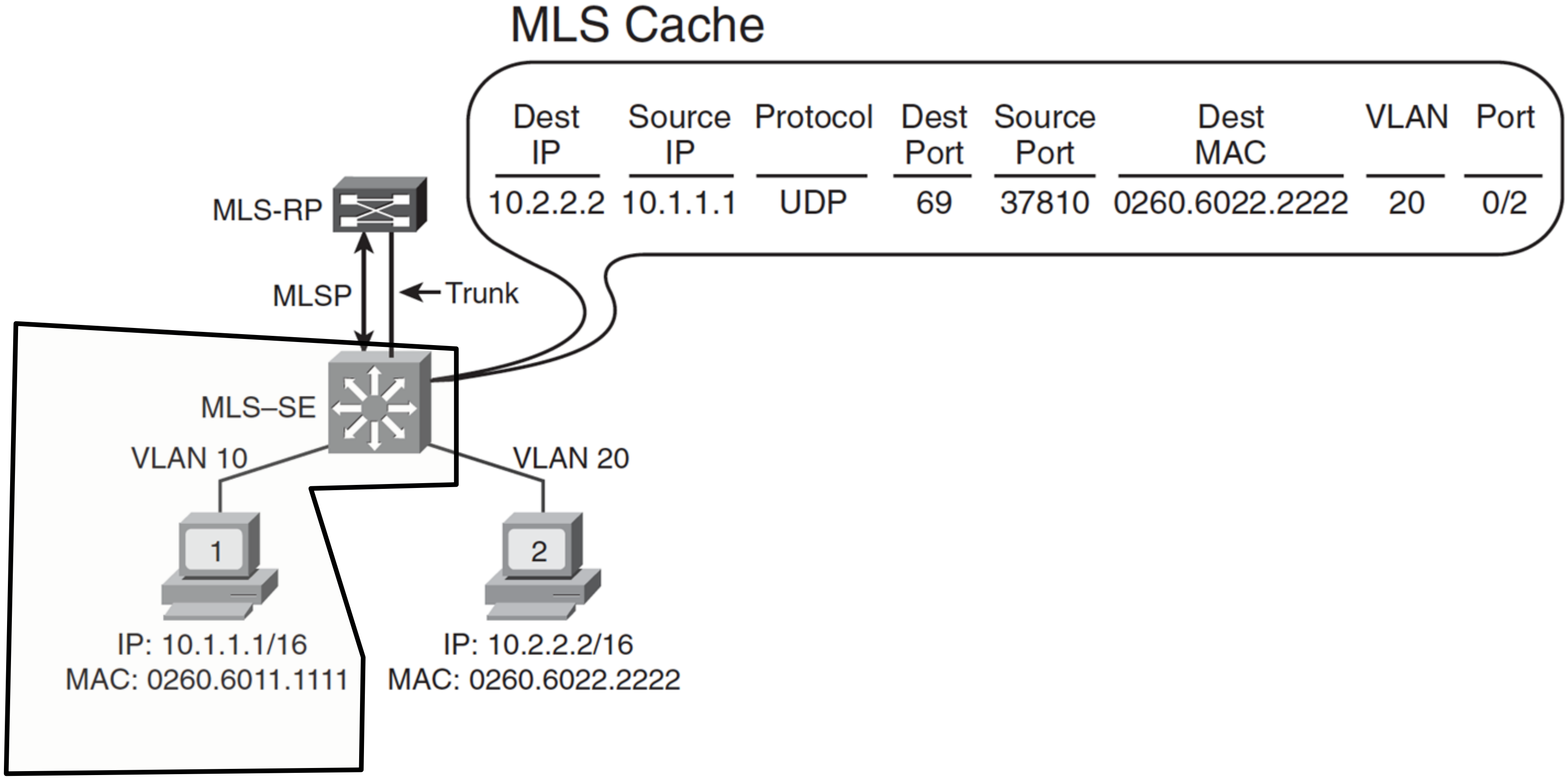
1. **MLS Route Processor (MLS-RP)**
    - The MLS-enabled router that performs the traditional function of routing between subnets
2. **MLS Switching Engine (MLS-SE)**
    - The MLS-enabled switch that can offload some of the packet-switching functionality from the MLS-RP
3. **Multilayer Switching Protocol (MLSP)**
    - Used by the MLS-RP and the MLS-SE to communicate with each other

MULTILAYER SWITCHING

- MLS can be implemented in the following two ways:
  - **Within a Catalyst switch**
    - Here both the MLS-RP and the MLS-SE are resident in the same chassis.
    - An example of an internal MLS-RP is a Route Switch Module (RSM) installed in a slot of a Catalyst 5500 Series switch.
  - **Using a combination of a Catalyst switch and an external router**
    - An example of a router that can be an external MLS-RP router is a Cisco 3600 Series router with the appropriate IOS software release and with MLS enabled.

MULTILAYER SWITCHING

Figure 2-10 *The MLS-SE Offloads Work from the MLS-RP*



MLS Cache

Dest IP	Source IP	Protocol	Dest Port	Source Port	Dest MAC	VLAN	Port
10.2.2.2	10.1.1.1	UDP	69	37810	0260.6022.2222	20	0/2

Cisco Express Forwarding

- **Cisco Express Forwarding (CEF)**
- Aims to speed the data routing and forwarding process in a network.
- However, the two methods use different approaches.

- CEF uses two components to optimize the lookup of the information required to route packets:
  1. Forwarding Information Base (FIB) for the Layer 3 information and
  2. Adjacency table for the Layer 2 information

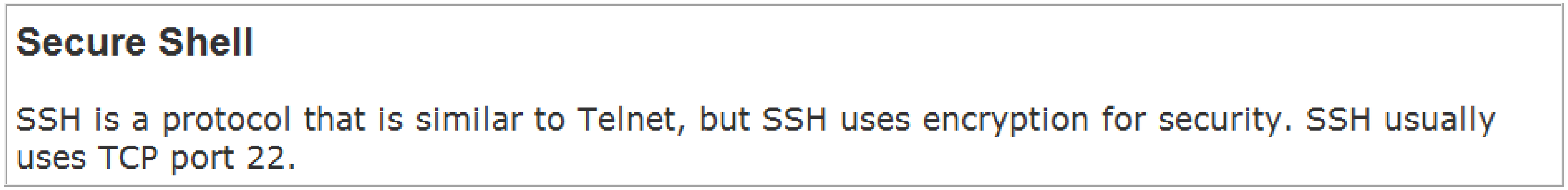
Switching Security

- Two types of switch security as follows:
  1. **Catalyst native security**
     ⍰ Those features built into the switch itself
  2. **Catalyst hardware security**
     ⍰ Features of hardware that can be installed in the switch

Catalyst Native Security

- Cisco switches have many native attributes that can be used to secure a network.

- Some attributes are related to the secure management of the switch itself.
  - One example is the use of secure shell (SSH), rather than Telnet, when remotely managing the switch.
  - Another example is disabling unused switch ports so that the network cannot be accessed through them.

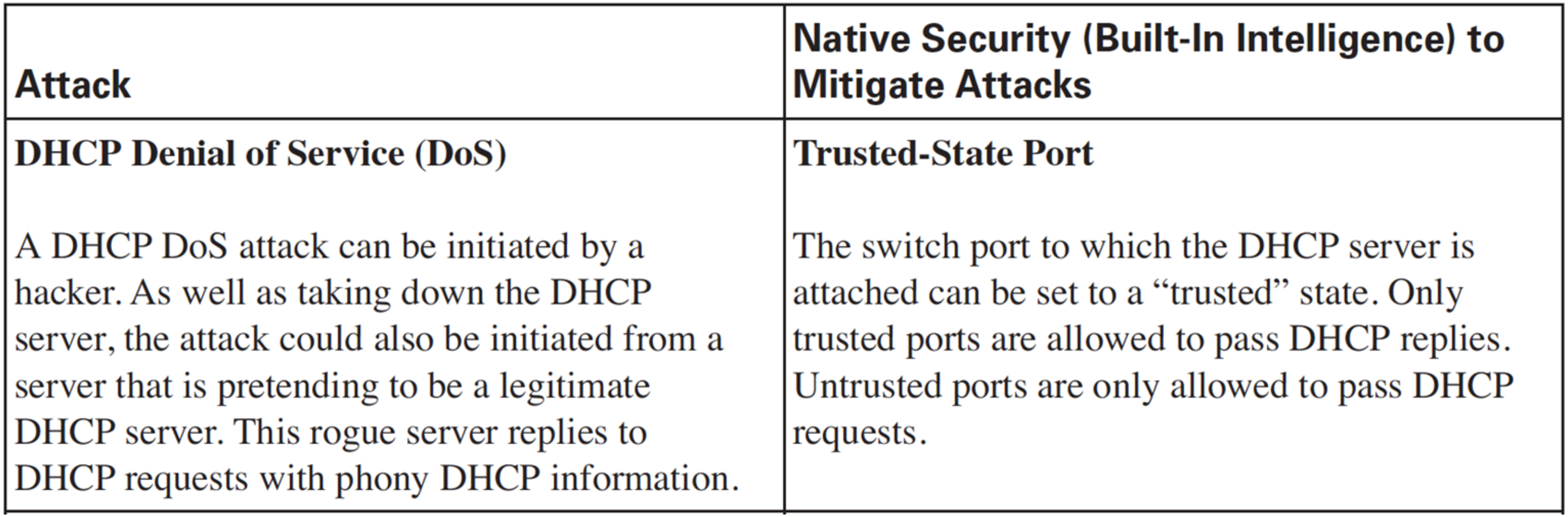


Secure Shell

SSH is a protocol that is similar to Telnet, but SSH uses encryption for security. SSH usually uses TCP port 22.

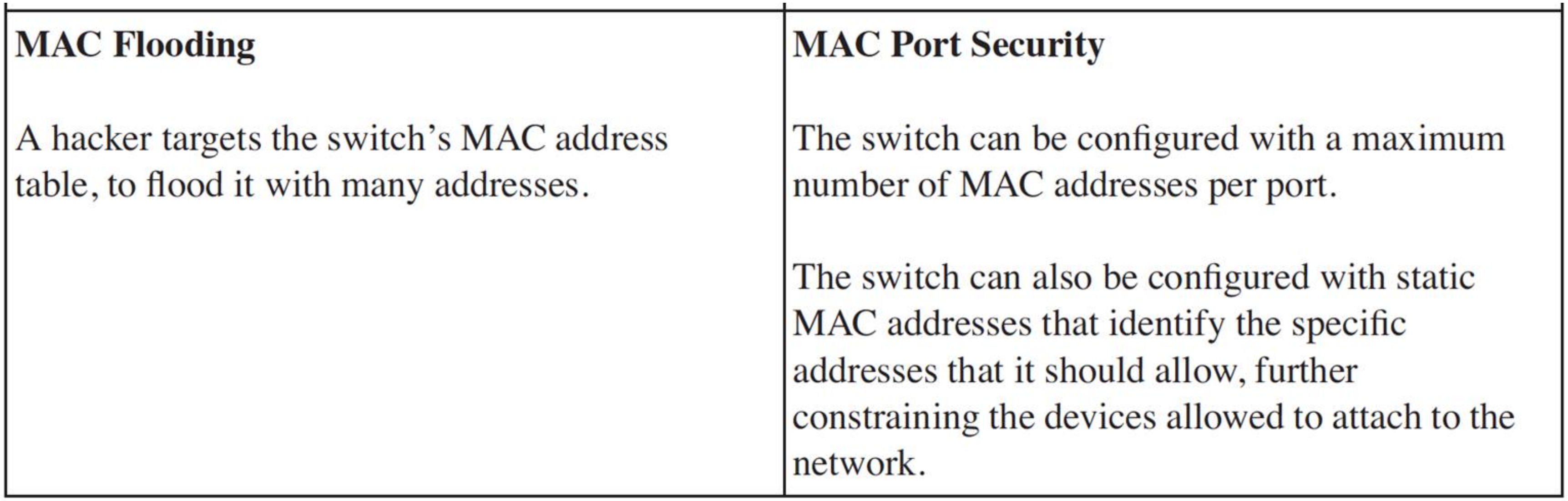
Catalyst Native Security

- **Examples of Built-In Intelligence to Mitigate Attacks**



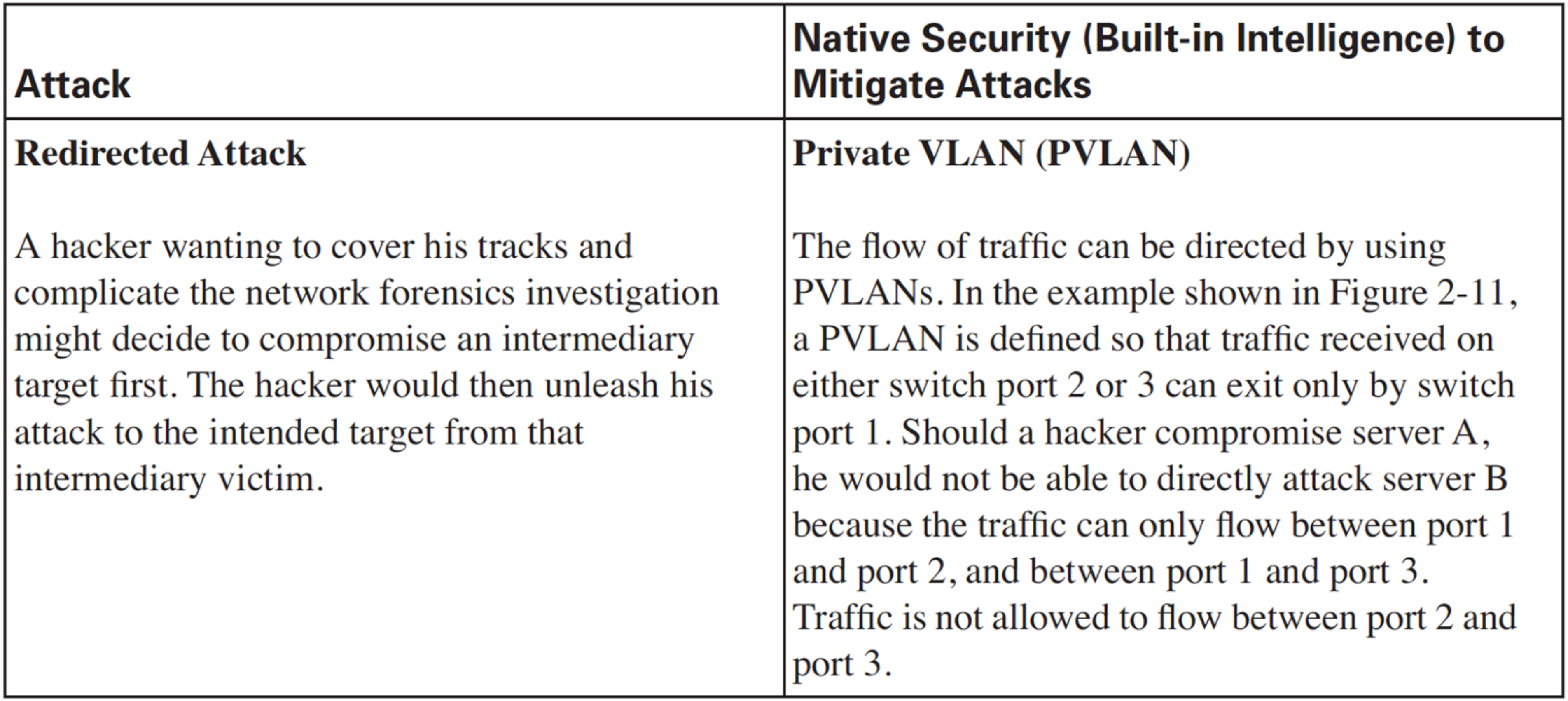
Attack	Native Security (Built-In Intelligence) to Mitigate Attacks
DHCP Denial of Service (DoS) A DHCP DoS attack can be initiated by a hacker. As well as taking down the DHCP server, the attack could also be initiated from a server that is pretending to be a legitimate DHCP server. This rogue server replies to DHCP requests with phony DHCP information.	**Trusted-State Port** The switch port to which the DHCP server is attached can be set to a "trusted" state. Only trusted ports are allowed to pass DHCP replies. Untrusted ports are only allowed to pass DHCP requests.

Catalyst Native Security



MAC Flooding	MAC Port Security
A hacker targets the switch's MAC address table, to flood it with many addresses.	The switch can be configured with a maximum number of MAC addresses per port. The switch can also be configured with static MAC addresses that identify the specific addresses that it should allow, further constraining the devices allowed to attach to the network.

Catalyst Native Security

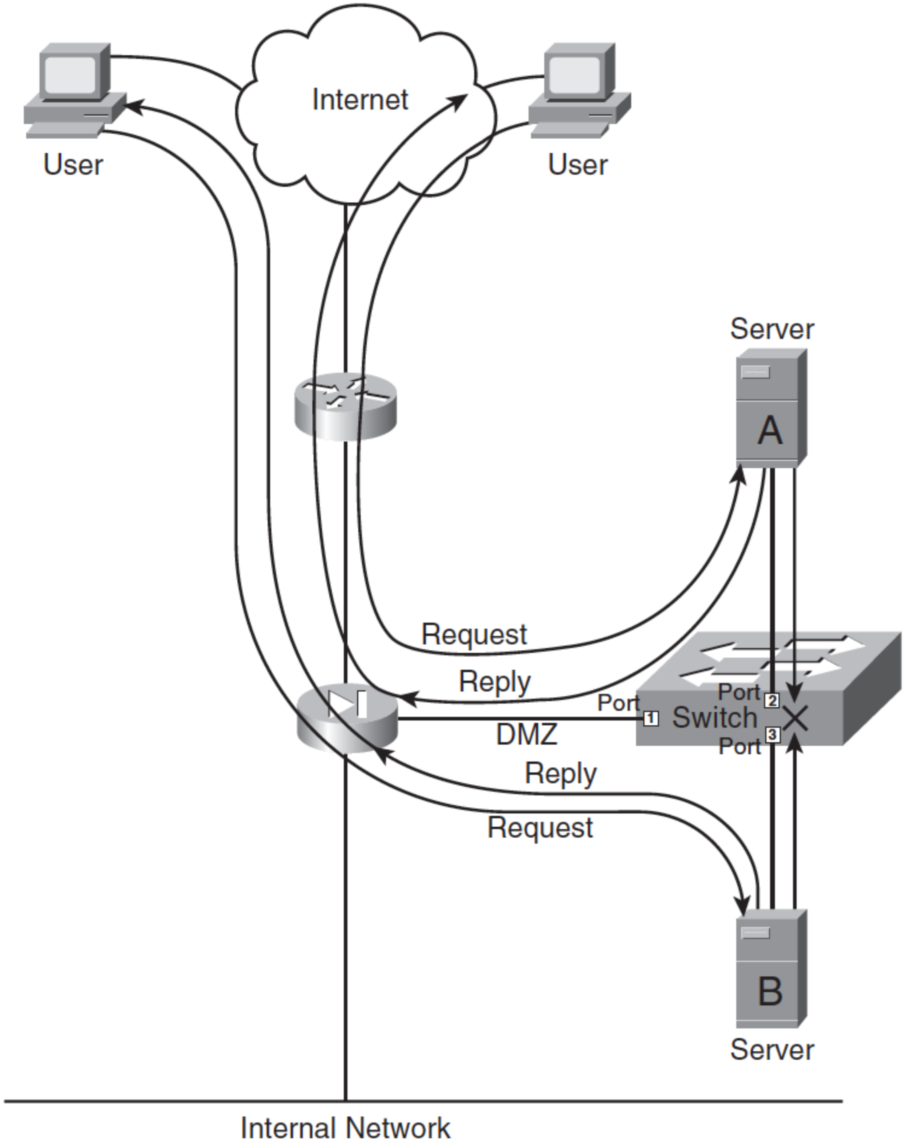


Attack	Native Security (Built-in Intelligence) to Mitigate Attacks
Redirected Attack A hacker wanting to cover his tracks and complicate the network forensics investigation might decide to compromise an intermediary target first. The hacker would then unleash his attack to the intended target from that intermediary victim.	**Private VLAN (PVLAN)** The flow of traffic can be directed by using PVLANs. In the example shown in Figure 2-11, a PVLAN is defined so that traffic received on either switch port 2 or 3 can exit only by switch port 1. Should a hacker compromise server A, he would not be able to directly attack server B because the traffic can only flow between port 1 and port 2, and between port 1 and port 3. Traffic is not allowed to flow between port 2 and port 3.

Native Security (Built-in Intelligence) to Mitigate Attacks

Private VLAN (PVLAN)

The flow of traffic can be directed by using PVLANs. In the example shown in Figure 2-11, a PVLAN is defined so that traffic received on either switch port 2 or 3 can exit only by switch port 1. Should a hacker compromise server A, he would not be able to directly attack server B because the traffic can only flow between port 1 and port 2, and between port 1 and port 3. Traffic is not allowed to flow between port 2 and port 3.



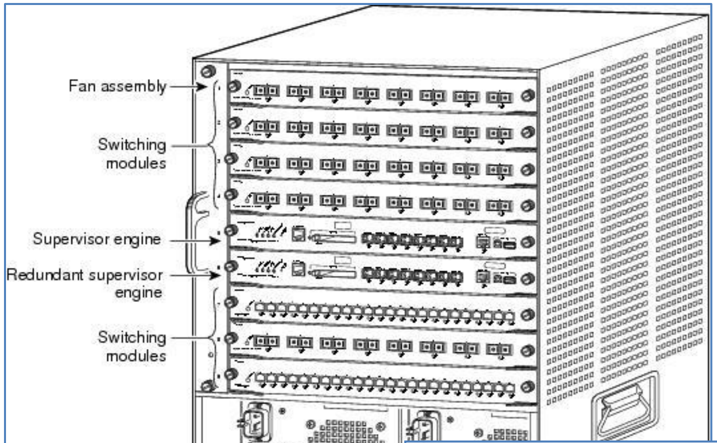
Traffic can not flow between Server A and Server B

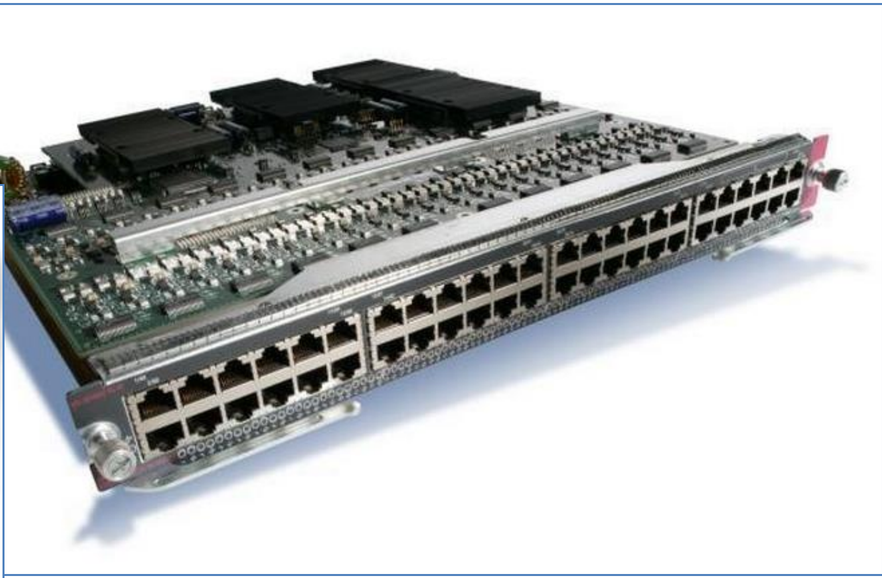
Catalyst Hardware Security

- As an example, the **Catalyst 6500 Series** switches **can be equipped** with modules that are full-fledged security devices themselves.
- Some example security modules are as follows:
  - Cisco Firewall service module
  - Cisco Internet Protocol security (IPsec) virtual private network (VPN) service module
  - Cisco Intrusion Detection System (IDS)
  - Cisco Secure Socket Layer (SSL)

Catalyst Hardware Security

- **As an example** of the flexibility provided by these modules, consider that when using a **Cisco Firewall service module**, *any port on a Catalyst 6500* switch can operate as a firewall.
- An example of the expandability of the modules is the use of the IPsec VPN module.
  - This module can terminate up to 8000 VPN connections (known as VPN tunnels) simultaneously and can create 60 new tunnels per second; up to 10 of these modules can be installed in a Catalyst 6500 switch.


Fan assembly
Switching modules
Supervisor engine
Redundant supervisor engine
Switching modules
Power supply 1
ESD groun
connec

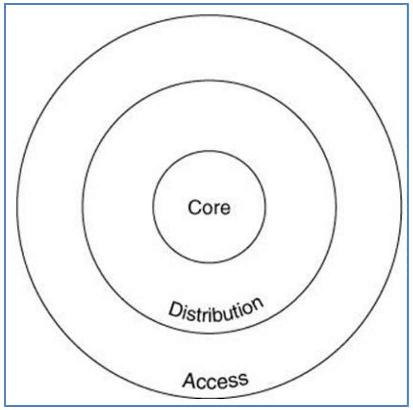


Switching Design Considerations

- We Know:
  - the hierarchical network design model and
  - the Enterprise Composite Network Design model
- **Hierarchical ..:** the access layer, the distribution layer, and the core layer
- **Enterprise Composite Network** ..: Enterprise Campus, Enterprise Edge, and Service Provider Edge.
  - Each of these functional areas contains network modules, which in turn can include the hierarchical layers.

FOR THE ACCESS LAYER

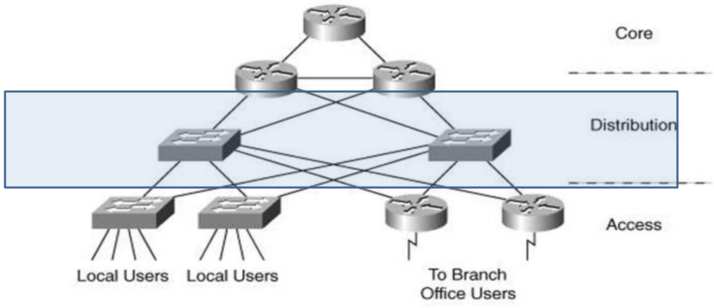
- For the access layer, design considerations include the following:
  - The **number of end-user devices** to be supported
  - The **applications** that are being used this defines some of the features required in the switches, as well as the performance and bandwidth needed
  - The **use of VLANs**, including whether trunks are required between switches
  - **Redundancy** requirements



FOR THE DISTRIBUTION LAYER

- For the distribution layer, design factors include the following:
  - The **number of access switches** to be aggregated
  - **Redundancy** requirements
  - **Features** required for **specific applications** to be supported
  - Required **interfaces** to the **core** layer
  - For **Layer 3 switches**, the **routing protocols** to be supported and whether sharing of information among **multiple routing protocols** is required

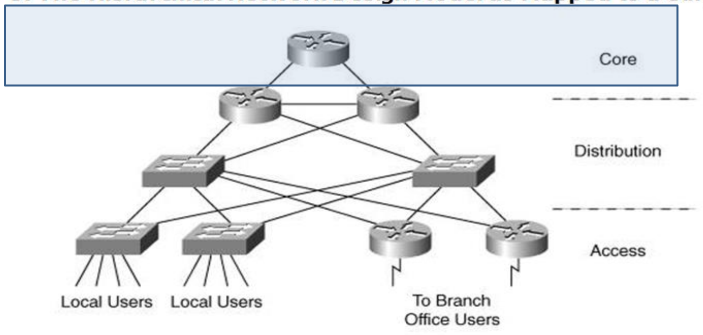
Figure 1-5. The Hierarchical Network Design Model as Mapped to a Simple Network



FOR THE CORE LAYER

- The role of the core layer is to provide a high-speed backbone.
- Thus, the **key requirement** is the **performance** needed to support all the access and distribution data.
- The number of ports to the distribution layer, and the protocols (for example, routing protocols) that need to be supported on those ports, are also important considerations.
- Redundancy in the core is a typical requirement, to meet the availability needs of the network

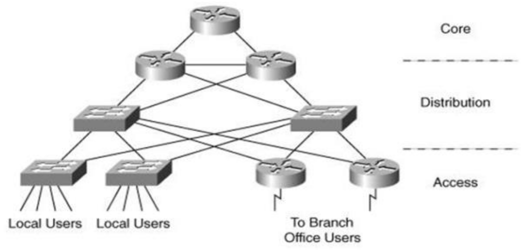
Figure 1-5. The Hierarchical Network Design Model as Mapped to a Simple Network



CISCO RECOMMENDATIONS

- Cisco current campus design recommendations include the followin:
  - **Layer 2** switches can be used at the **access layer**, with **Layer 3** switches at the **distribution and core layers.**
  - **VLANs** should **not** spread across the campus, because this can slow network convergence.
  - The **core and distribution** layers can be combined into one layer (called a **collapsed backbone**) for smaller networks.
  - **Larger** campuses should have a **separate** distribution layer to allow the network to grow easily.
  - **Redundancy** in the core, between the core and distribution layers, and between the distribution and access layers is also recommended.

Figure 1-5. The Hierarchical Network Design Model as Mapped to a Simple Network


Core
Distribution
Access
Local Users
Local Users
To Branch Office Users