Cisco Networking Academy Program – Semesters III and IV

Instructor: Chris Widmer

The Threaded Case Study

OBJECTIVE

The purpose of the Threaded Case Study is to allow you to apply the knowledge that you have gained during your Cisco Studies to a real life example.

OVERVIEW OF THREADED CASE STUDY (TCS):

The TCS is a performance assessment that was introduced to you in the first semester, although the actual project work will not be done until semesters 3 and 4. As concepts are introduced, you will learn to apply them.

Your Engineering Journal (notebook) and the online curriculum will contain content, concepts, and examples from the first two semesters that will assist in building the prerequisite knowledge for the TCS. A large school district nominally located in Phoenix, Arizona will be the field model that is included in the TCS. You will be divided into teams, and each team of students will be given architectural drawings (electronically) of the various schools along with the actual wiring drawings (electronic format). The teams of students will each submit a final design document, and make an oral presentation of their project near the end of semester 4. Criteria for the project will be a series of learning outcomes in the broad areas of Networking, Science, Mathematics, Design, Reading, Writing, and SCANS.

Technology Implementation Requirements

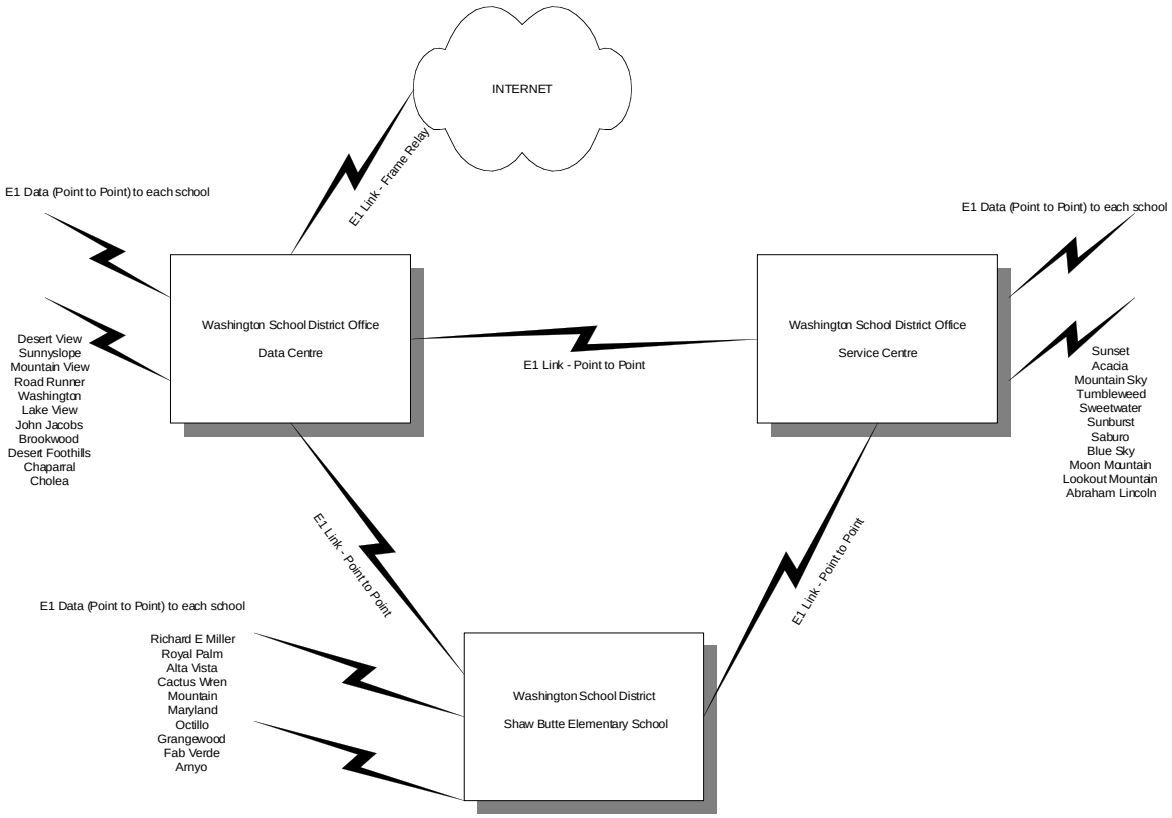
General Requirements

The nominated School District is in the process of implementing a enterprise wide network which will include Local Area Networks (LANs) at each site and a Wide Area Network (WAN) to provide data connectivity between all school sites. Access to the "Internet" from any site in the school district is also an integral part of this implementation. Once the network is in place the school district will implement a series of servers to facilitate online automation of all of the district's administrative and many of the curricular functions. Since this network implementation will have to continue to be functional for a minimum of 7-10 years all design considerations should include 1000% growth in the LAN's and 100% growth in the WAN. The minimum requirements for initial implementation design will be 1.0 Mb/s to any host computer in the network and 100 Mb/s to any server host in the network. Only two OSI layer 3&4 protocols - TCP/IP and Novel's IPX - will be allowed in this network.

TABLE OF CONTENTS

SECTION 1 - WIDE AREA NETWORK

The Washington School District Wide Area Network (WAN) will connect all school and administrative offices with the district office for the purpose of delivering data. The WAN will be based on a two layer hierarchical model. Three (3) Regional Hubs will be established at the District Office, Service Center and Shaw Butte Elementary School for the purpose of forming a fast WAN core network. School locations will be connected into the WAN core hub locations based on their proximity to each hub.

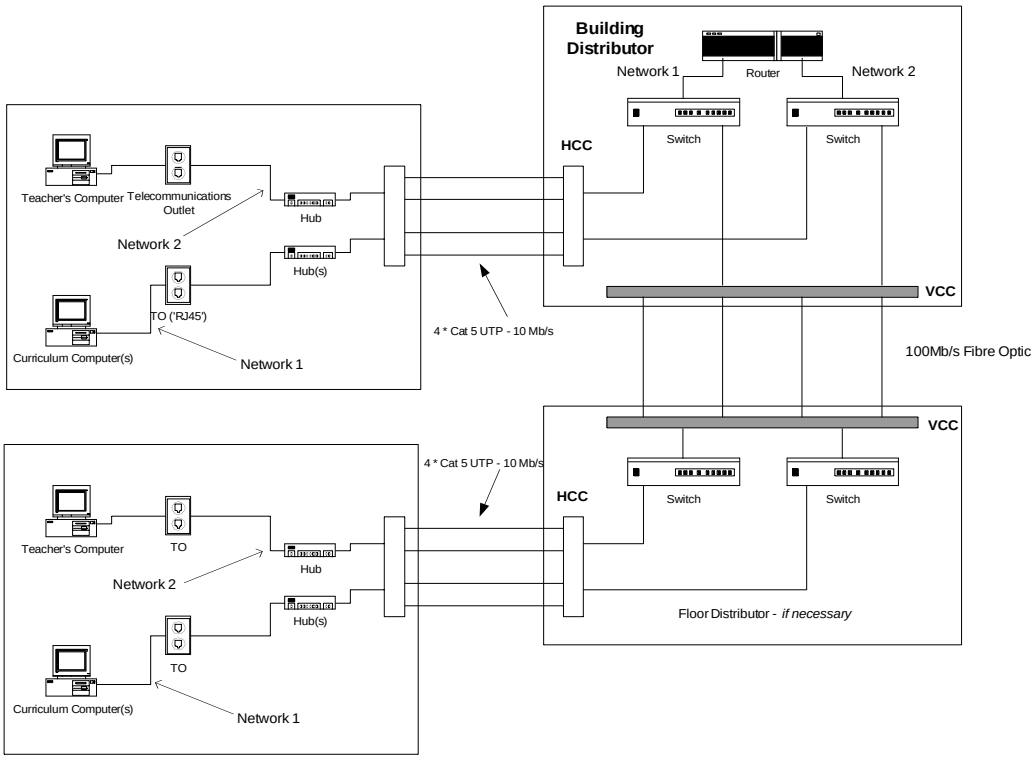


TCP/IP and Novel IPX will be the only networking protocols that will be acceptable to traverse the district WAN. All other protocols will be filtered at the individual school sites using routers. Routers will also be installed at each WAN core location. Access to the "Internet" or any other outside network connections will be provided via the District Office through a frame relay WAN link. For security purposes, no other connections will be permitted.

SECTION 2 - LOCAL AREA NETWORK & WIRING SCHEME

Two Local Area Networks (LAN) segments will be implemented in each school and the District office. The transport speeds will be Ethernet 10BaseT, 100BaseTX and 100BaseFX. Horizontal cabling shall be Category 5 Unshielded Twisted Pair (CAT5 UTP) and will have the capacity to accommodate 100Mb/s. Vertical (Backbone) cabling shall be CAT5 UTP or fiber-optic multimode cable. The cabling infrastructure shall comply with EIA/TIA 568 standards. One LAN will be designated for student / curriculum usage and the other will be designated for administration usage
(see Section 5 - SECURITY SECTION).

The LAN infrastructure will be based on Ethernet LAN switching which will allow for a migration to faster speeds (more bandwidth) to the individual computers and between Building Distributors [BD/MDF] and Floor Distributors [FD/IDF] without revamping the physical wiring scheme to accommodate future applications. In each school location, a Telecommunications Closet (also called a MDF Room) will be established as the central point to which all LAN cabling will be terminated and will also be the point of presence for the Wide Area Network connection. All major electronic components for the network, such as the routers and LAN switches will be housed in this location. In some cases a Floor Distributor room (also called an IDF room) will be established, where horizontal cabling lengths EIA/TIA 568 recommended distances or where site conditions dictate. In such cases, the IDF will service its geographical area and the IDF will be connected directly to the MDF in a STAR or EXTENDED STAR topology. Each room requiring connections to network will be able to support 26 workstations and be supplied with four (4) CAT 5 UTP runs for data, with one run terminated at the teachers workstation. These cable runs will be terminated in the closest MDF or IDF. All CAT 5 UTP cable run will be tested end-to-end for 100Mb/s bandwidth capacity. A single location in each room will be designated as the wiring point of presence (POP) for that room. It will consist of a lockable cabinet containing all cable terminations and electronic components; i.e. hubs or switches. From this location data services will be distributed within the room via decorative wire molding. Network 1 will be allocated for general curriculum usage and Network 2 will be allocated for administrative usage.



SECTION 3 - DISTRICT SUPPLIED SERVERS AND FUNCTIONS

All file servers will be categorized as Enterprise or Workgroup type services then placed on the network topology according to function and anticipated traffic patterns of users.

Domain Names and e-mail Services

Domain Name Services (DNS) and e-mail delivery will be implemented in a hierarchical fashion with all services located on the master server at the district office. Each Hub location will contain a DNS server to support the individual schools serviced out of that location. Each school will also contain a host for DNS and e-mail services (local post-office) that will maintain a complete directory of all staff personnel and student population for that location. The school host will be the local post office box and will store all e-mail messages. The update DNS process will flow from the individual school server to the Hub server and to the district server. All regional servers will have the capability to communicate between themselves thus building redundancy in the system in the event that the District master server is unavailable. Should the District master server require a partial or complete restore of data, the ability to query any or all of the regional servers to acquire the needed information would be provided.

Administrative Server

The school district is moving towards a totally automated server based administration system. Each school location will contain an Administration server, which will house the student tracking, attendance, grading and other administration functions. This server will be running TCP/IP as its OSI layer 3&4 protocols and will only be made available to teachers and staff.

Library Server

The school district is implementing an automated library information and retrieval system, which will house an online library for curricular research purposes. This server will be running TCP/IP protocols and will be made available to anyone at any school site.

Application Server

All computer applications will be housed in a central server at each school location. As applications such as word processing, spreadsheets, presentation packages, etc are requested by users, these applications will be retrieved from the application server. This will provide district support staff with an easy and efficient method for upgrading applications without having to reload new software on each computer in the district network. This server will use TCP/IP protocols and will be made available to anyone at any school site.

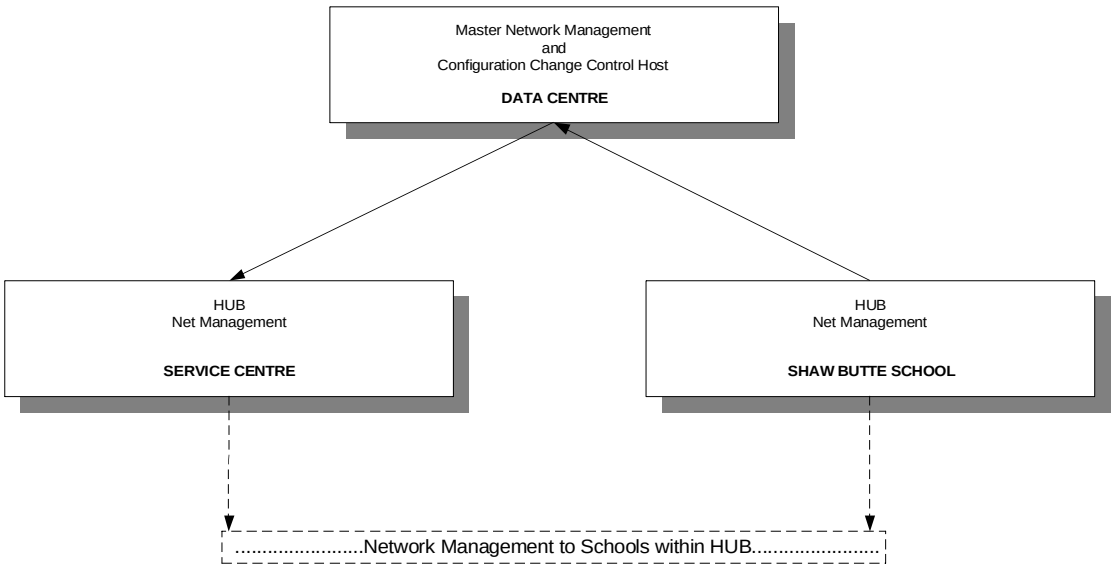
Other Servers

Any other servers implemented at the school sites will be considered departmental (workgroup) servers and will be placed according to user group access needs. Prior to implementation of other servers, a requirement analysis must be submitted for the purpose of determining placement of the server on the district network.

SECTION 4 - ADDRESSING AND NETWORK MANAGEMENT

A complete TCP/IP addressing and naming convention scheme for all host, servers and network interconnect devices will be developed and administered by the District Office. The implementation of unauthorized addresses will be prohibited. All computers located on the administrative networks will have static addresses; curriculum computers will obtain addresses by utilizing Dynamic Host Configuration Protocol (DHCP). A master network management host will be established at the District Office and will have total

management rights over all devices in the network. This host will also serve as the router configuration host and maintain the current configurations of all routers in the network. Each region location will house a regional network management host to support its area. The management scheme for the data portion of the network will be based on the Simple Network Management Protocol (SNMP) standards. All routers will be pointed to the master Network Management host for the purpose of downloading new or existing configurations. The District Office will maintain the 'super user' passwords for all network devices and configuration changes on these devices will be authorized from the District Office: i.e. Routers and LAN Switches.



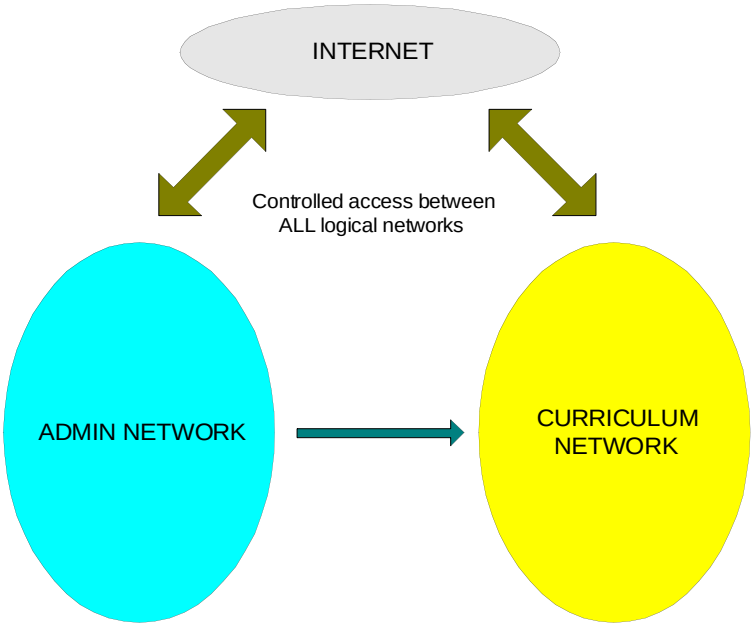
SECTION 5 – SECURITY

External Threats

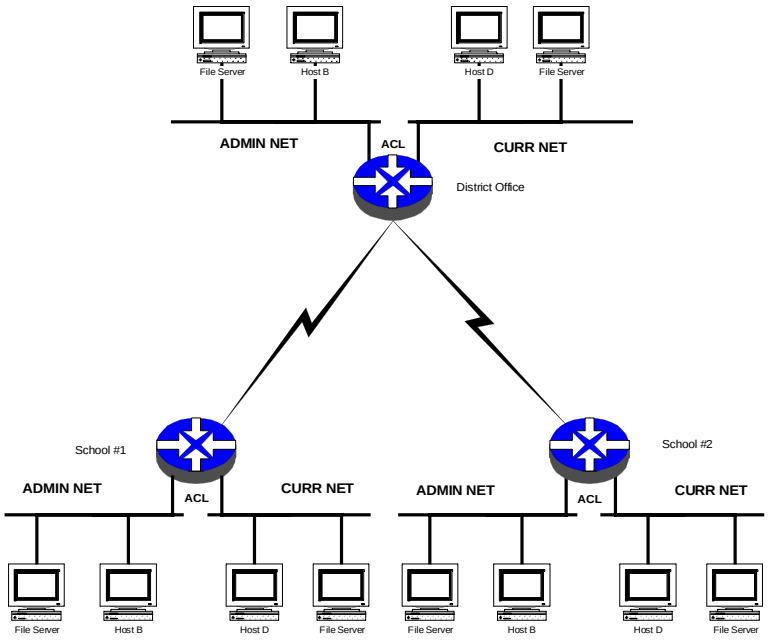
Internet Connectivity shall utilize a double firewall implementation with all Internet exposed applications residing on a public backbone network. In this implementation all connections initiated from the Internet into the schools private network will be refused. In the district security model the network will be divided into three (3) logical network classifications:

1. administrative,
2. curriculum, and
3. external

With secured interconnections between them.



This model will dictate that two physical LAN infrastructures are installed at all schools and the District Office, with one designated administrative and the other curriculum. Every computer and file server will be categorized according to its function and placed on the appropriate LAN segment at the schools each LAN segment will have a file server. All applications will be categorized and placed on the appropriate server. By utilizing Access Control Lists (ACL's) on the routers, all traffic from the curriculum LANs will be prohibited on the administration LAN. Exceptions to this ACL can be made on an individual basis. Applications such as e-mail and Directory services will be allowed to pass freely since they pose no risk. A user ID and Password Policy will be published and strictly enforced on all computers attached to the administration LAN. All computers in the District network will have full access to the Internet. All ACLs will be controlled at the district office and exceptions to the ACLs will be reviewed prior to implementation.



SECTION 6 - INTERNET CONNECTIVITY

All Internet connectivity will be supplied through the District Office with the District Office being the single point of contact for all schools and organizations within the district. This connection will be highly controlled and capacity (bandwidth) upgraded as usage dictates. The Internet connection will utilize double firewall implementation with a public network (Ethernet backbone) established for services that will be exposed to the Internet such as master e-mail, Domain Name Services (DNS) and a World Wide Web (WWW) server. All connectivity that is initiated from the Internet to the internal District network will be protected via Access Control Lists (ACLs) on the routers that make up the double firewall architecture. Any connectivity initiated from the District to the Internet will be permitted to communicate freely. E-mail and DNS services will communicate freely in both directions, since these applications poses no security threat. A Web server will be located on the public backbone and partitioned to allow any school to install a Web home page on the Internet. Individual Web servers that need total exposure to the Internet will not be permitted on the internal District network. If schools require an independent web server host, this host will be placed on the public network backbone.