Network Design & Modelling V

Washington School District Wide Area Network

Cisco Threaded Case Study Report

Khayam Asghar

Michael Clarke

Contents

Project Overview……3

Requirements Analysis……...3

Design Considerations……5

Two-Layer Hierarchical Model……..…..5

Hardware Specifications for Regional Hubs……..…..6

Extra Redundancy……..…...7

Internet Connection Specifications……..7

WAN Connection Specifications for Individual School locations…. 7

Physical Security……8

Logical Security……...8

Summary……..….9

Appendix A – Washington School District WAN Logical Plan… ..10

Appendix B – Detail View of Data Centre Hub……..…...11

Appendix C – Detail View of Shaw Butte Hub……..…..12

Appendix D – Detail View of Service Centre Hub……...…13

Appendix E – LAN/WAN Integration Logical Plan ……14

Appendix F – Washington School District Addressing……15

Appendix G – Washington School District Access Lists……..……16

Appendix H – Router Configurations……17

Appendix I – Access Lists……19

Appendix J – PPP, IPX and TCP/IP Protocols..……20

Appendix K –Frame Relay and ISDN……..22

Bibliography……24

Disc containing PowerPoint Presentation……

Project Overview

The Washington School District is seeking to implement a Wide Area network (WAN) that will provide data connectivity to all of its school sites. The School District seeks to provide Internet connectivity to each site while limiting the types of security problems that might go along with such access. Upon implementation of the WAN, the school district will begin to automate its administrative and curricular processes through the installation of a series of LAN-based servers.

The School District expects that all solutions for their WAN implementation will remain viable and operative for seven (7) to ten (10) years. To that effect all network designs must account for a minimum of 2x (times) growth in the WAN core throughput and 10x (times) growth in the District Internet Connect throughput. Upon initial implementation, any host computer in the network must be able to accomplish 1.0 Mbps throughput while any server host must be able to accomplish a throughput of 100 Mbps. Additionally, all network designs are constrained to the use of OSI layer 3&4 protocols TCP/IP and Novell IPX.

Requirements Analysis

1. Network implementation to remain viable for 7 to 10 years.
2. Support minimum of 2x growth in WAN throughput.
3. Support minimum of 10x growth in District Internet Connection throughput.
4. Implement standardisation and management solutions for WAN.
5. WAN will connect all school and administrative offices with the district office.
6. WAN allows for redundant paths.
7. Only TCP/IP and Novell IPX will be allowed to traverse the district WAN.
8. Core WAN between three regional hub locations through 4 1.544Mbps T1 lines.
9. Internet connectivity achieved via Frame Relay WAN link out of District Office/Data Centre provided by an Internet Service Provider.
10. Schools connected to WAN by one 1.544Mbps T1 line connection to nearest Hub.
11. A series of servers implemented enterprise-wide to accommodate district services.
12. Domain Name Services (DNS) and e-mail delivery provided via the master server at District Office, Secondary DNS services located at each district Hub.

13. District is implementing an automated library and information and retrieval system housed at District Office and available to all school locations.

14. Complete TCP/IP addressing and naming convention for all hosts, servers, and network devices developed and administered by the District Office.

15. Unauthorised addresses will be prohibited.

16. District Office will maintain the super user passwords on all network devices and authorise any configuration changes.

17. A class B address will utilised and may include Private Network Numbers.

18. All administrative hosts on administrative networks will have static IP addresses.

19. All curriculum network computers will have their addresses assigned via DHCP.

20. All network devices will be managed from a master network management host established at the District Office.

21. Each regional Hub will have a regional network management host.

22. Appropriate security measures applied to WAN implementation to guard against external threats.

23. Internet connectivity shell utilise a double firewall implementation.

24. Internet-exposed applications will reside on a public backbone network.

25. Security model divided into 3 logical groups with secured interconnections between Administrative, Curriculum and External networks.

26. Access Control Lists on all routers.

27. E-mail and DNS will be allowed to pass freely due to low risk.

28. All Internet connectivity will be supplied through the District Office.

29. Connection is of highly controlled capacity that is upgraded as usage dictates.

30. A Web server will be located on the publicly accessible backbone. It will be partitioned so any school can install a Web home page on the Internet.

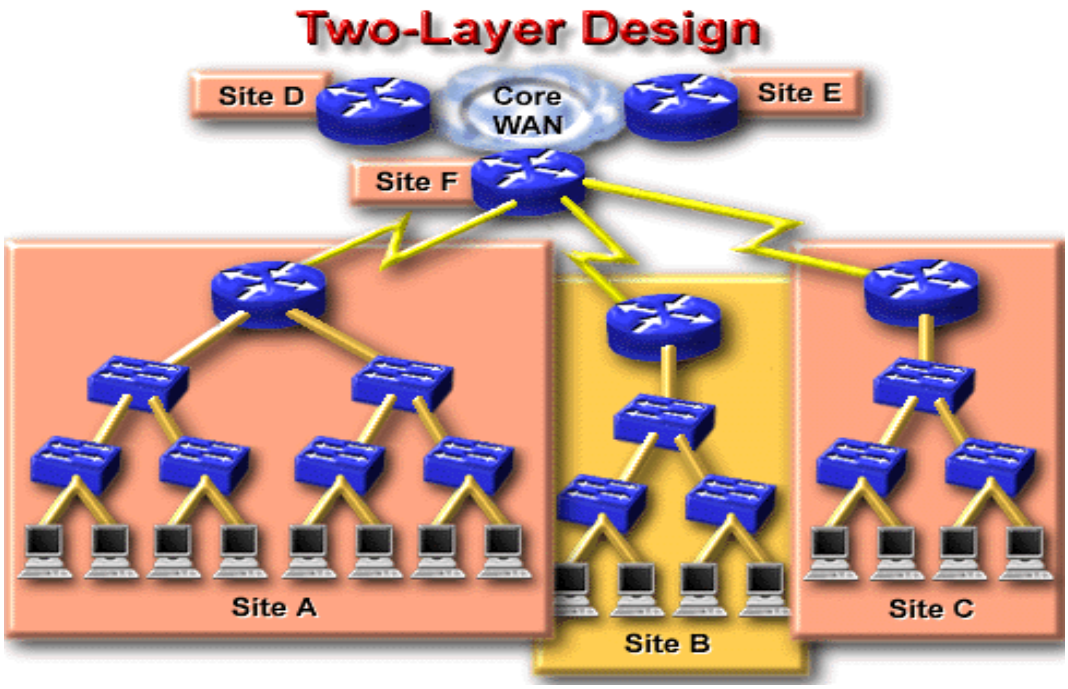
Design Considerations

The design of the WAN will comprise of the following areas:

- **Basic Hardware**
- **Extra Redundancy**
- **Physical Security**
- **Logical Security**
- **IP Addressing**
- **Router Configuration**

Two-Layer Hierarchical Model

The WAN will be based on a two-layer hierarchical model. By using a hierarchical model we gain advantages such as scalability, ease of implementation, ease of troubleshooting, predictability, protocol support, and manageability.



These layers are split from each other in regard to their function. The core layer provides a fast, redundant connection between the core WAN Hubs. The distribution layer gives individual local school locations access to the WAN district core services, and the local schools access to school location LANs.

The WAN will connect all school and administrative offices with the district office. It will consist of 3 regional hubs established at the District Office, the service centre, and at Shaw Butte Elementary School. These locations will form the core of the Washington School District WAN and will be connected to each other through 4 1.544 Mbps T1 lines using Point to Point Protocol. The use of one IS DN PRI link between each of the hubs will be used in case of connection failure in any of the T1 lines.

Each of the 33 schools in the Washington School District will then be connected into the WAN core through a single 1.544 Mbps T1 link to the core hub depending on its locality to the hub. One ISDN BRI link will be put in place in case the T1 link between the hub and the school fails.

Internet connectivity will occur through only the data centre by using Frame Relay Permanent Virtual circuit T1 link, which will connect to an ISP. A backup T1 connection will be in place connected to a separate ISP if there is connection failure in the first T1 link. The 2 ISPs' will be in contact with one another to monitor any problems that may occur.

Hardware Specifications for Regional Hubs

Each of the regional hubs will be equipped with a powerful Cisco 7513 router. The router has eleven extension slots, providing a lot of room for future growth. The router will contain two 8-port T1 cards with integrated CSU/DSU's. This set-up will provide enough T1 ports for connecting the eleven schools. To ensure reliability, each school will have a backup Integrated Services Digital Network (ISDN) Basic Rate Interface (BRI) connection to the appropriate regional hub. For this reason, the Cisco 7513 will be equipped with two 8-port ISDN BRI cards.

Connections between regional hubs will be ensured through 4 T1 connections in between each pair of hub locations (four between the District Office/Data Centre and the Service Centre, four between Service Centre and Shaw Butte and four between Shaw Butte and the District Office). In order to provide reliability, route differentiation will be required for the first two and the second two of the four T1's.

At the District office there will be 3 enterprise servers connected to a Cisco 3512 XL FastEth switch with a 1000BaseSX uplink to the Cisco 7513 router. The servers will comprise of a Master/Primary DNS/e-mail server, secondary DNS/e-mail server and a library and information retrieval server. The servers will be connected via Fast Ethernet UTP cabling.

In order to enable access to 75 administration personnel, a Cisco Catalyst 4006 switch will be connected to the above Cisco 3512 XL. The 4006 modular six-slot switch will have 48-port 10/100 interface cards, providing ample room for future expansion. Workgroup servers will be attached to this switch to meet server requirements for the administration network.

Extra Redundancy

Redundancy and backup will be provided through three ISDN Primary Rate Interface (PRI) interfaces. The three of them will be used to connect each of the regional hubs. In order to ensure reliable backup, the ISDN PRI connection will require route differentiation from the four T1 links i.e. they'll be connected at a separate point of presence (POP) when connected to the buildings (hubs). Each school will have an ISDN BRI backup path. Each of the ISDN links will also be linked at separate Point of Presence (POP) when connected to each of the schools.

ISDN provides great flexibility to the network designer because of its ability to use each of the B channels for separate voice or data applications; for example, a long document can be downloaded from the corporate network over one ISDN 64-kbps B channel while the other B channel is being used to connect to browse a World Wide Web page. Care should be taken in the design phase to ensure that the equipment selected has the feature set that takes advantage of ISDN's flexibility.

Internet connection Specifications

Access to the Internet at the Data Centre will occur via a firewall and a filtering router. The Cisco 520 firewall will be connected to the 7513 router on one end and the Cisco 3662 filtering router on the other end through a FastEthernet port. The firewall will be equipped with three 10/100 Ethernet interfaces. One interface will connect to the 7513 router, the second will go to the filtering 3662 router, and the third will be used to connect the enterprise web server.

The filtering router providing connection to the Internet will be a Cisco 3662. The router will be equipped with a one-port T1 connection with an integrated DSU/CSU. For connectivity to the firewall, the router will also contain two 10/100 Ethernet ports. In case of future expansion, enough empty slots (6 in total) are available for more cards.

One enterprise class server will be placed on the public access backbone and serve as the Washington School District's Web Server. It will be protected by PIX firewall that will only allow outside access to its web services. A second enterprise class server will be placed at the District Office to serve as the district's library retrieval system. It will be accessible through the district WAN to all school locations via TCP/IP. Finally, three servers will be individually placed in each WAN district hub location. These will serve as secondary DNS and e-mail servers for the school locations directly connected to each District Hub.

WAN Connection Specifications for Individual school Locations

Each school will be fitted out with a Cisco 3662 router to ensure connection to the regional hub. The router will contain a one-port T1 card with an integrated DSU/CSU. The router will also contain a one-port ISDN BRI card for backup in case the T1 connection fails. To ensure connectivity to the LAN, the router will use it's built in two port 10/100 copper ports plus an additional Fast Ethernet port card for the Domain Name Service (DNS), e-mail message store, and Dynamic Host Configuration

Protocol (DHCP) server. The community school will be connected to the Shaw Butte regional hub through an ISDN BRI link.

Physical Security

There are numerous ways to physically secure the network. The most obvious one is keeping doors locked that lead to areas such as the MDF or IDF rooms, and allowing only staff that have reason to access the area permission to enter and leave by allocating them keys. Another security measure that will be utilised is the Swipe card system. Which again will only be allocated to staff that need access to the secured areas. By using this system, information regarding the person's name, the room they entered and the time they left will all be logged on the system.

Logical Security

There are numerous ways to logically secure the network below is a list of techniques that will be implemented.

- Allocating passwords to every one using the network and changing them on a regular basis.

- Setting access control lists on routers to specify what is or isn't allowed across the network

  Access lists filter network traffic by controlling whether routed packets are forwarded or blocked at the router's interfaces. Your router examines each packet to determine whether to forward or drop the packet, based on the criteria you specified within the access lists. Access list criteria could be the source address of the traffic, the destination address of the traffic, the upper-layer protocol, or other information.

  You can also use access lists to decide which types of traffic are forwarded or blocked at the router interfaces. For example, you can permit e-mail traffic to be routed, but at the same time block all Telnet traffic.

- Establish a protective net of filters to detect and eradicate viruses - covering workstations (PCs), servers, and gateways. Ensuring that virus signatures are kept up-to-date.

- Make sure that back-ups are run regularly, that files can be restored from those backups.

- Enable logging for important system level events and for services and proxies, and set up a log archiving facility.

- Install a double firewall and enhance the firewall rule sets to block most sources of malicious traffic.

  Taking into account the external threats therefore the 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, Administrative, curriculum and external with secured interconnections between them.

- Separate Administrative and Student networks via a VLAN network set-up

- Limit FTP and Telnet access into district and within schools

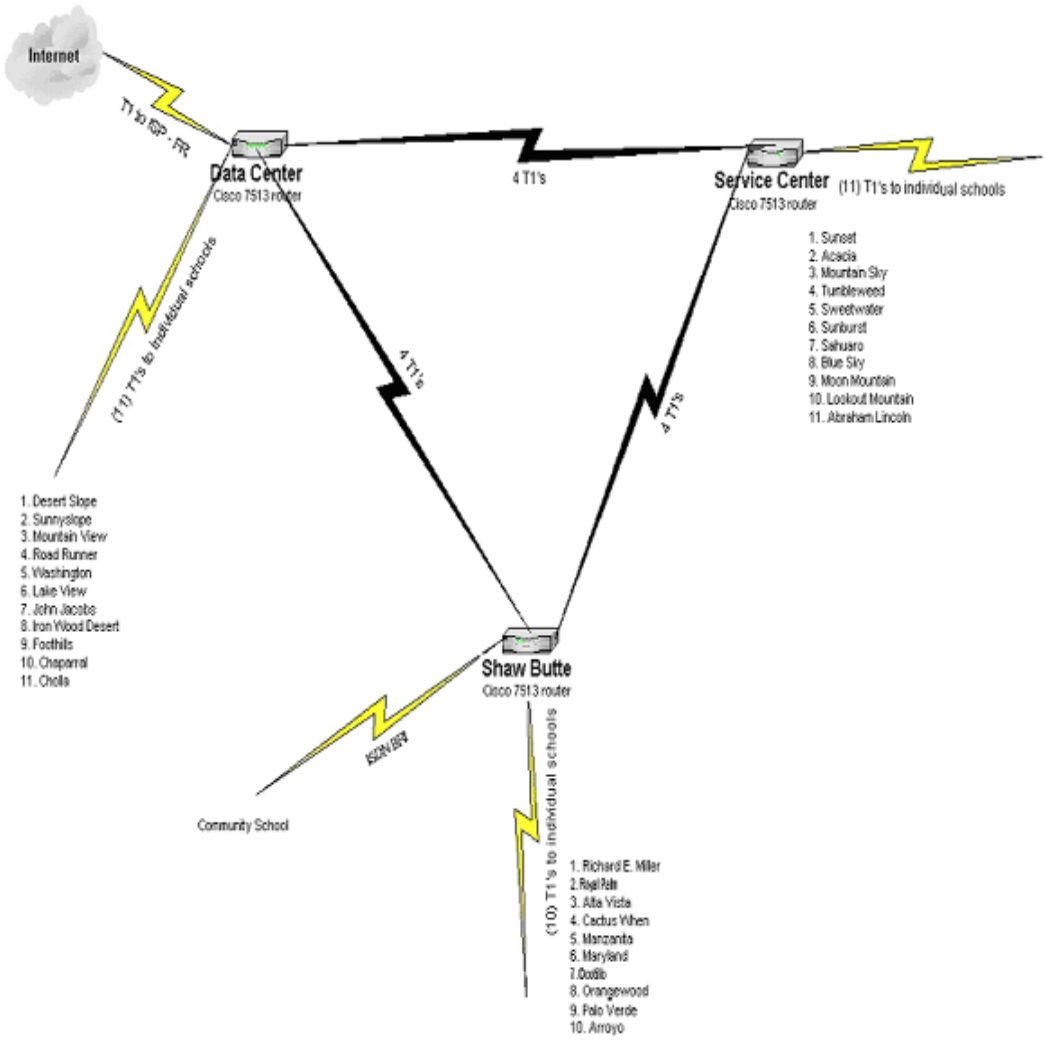
Summary

The WAN proposal makes use of a hierarchical approach to networking and divides the WAN into 3 layers- Core, Distribution, and access layers. These layers are split from each other in regard to their functions. The core provides for a fast, redundant, connection between the core WAN hubs. The distribution layer gives individual local school locations access to the WAN district core services, and the local schools access to school location LANs. Using this tiered design allows many advantages such as easier implementation of services, scalability, predictability and manageability. Such an approach also allows for a wider range of protocol support while making it easier to isolate and troubleshoot problems within the network.

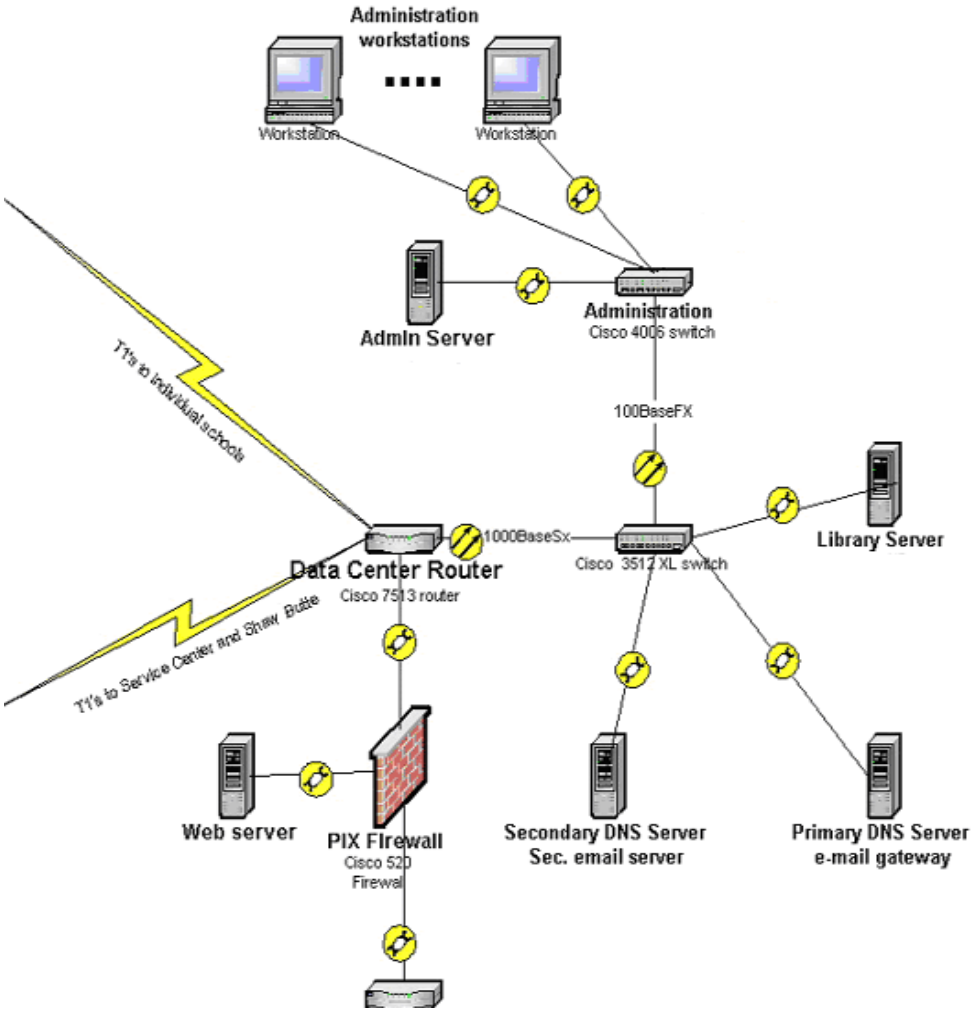
All mission critical servers within the network will be established at the District Office of the School District. This allows for centralised management, upgrades and troubleshooting should there be problems with the servers. Additionally, all network equipment and servers will be managed remotely from this centralised location. This allows for consistency in administration and for the consistent application of security and addressing procedures across the network and the regulation of unauthorised network accesses.

The WAN can remain viable through multiple upgrades in carrying capacity as the need arises. The use of chassis based servers and routers allows the School District to upgrade only the needed components as they are deemed necessary without having to completely throw away previous investments in hardware and infrastructure. Similarly, the T1 lines at the core and distribution layers can be upgraded to T3 lines allowing faster throughput as need and financing allows.

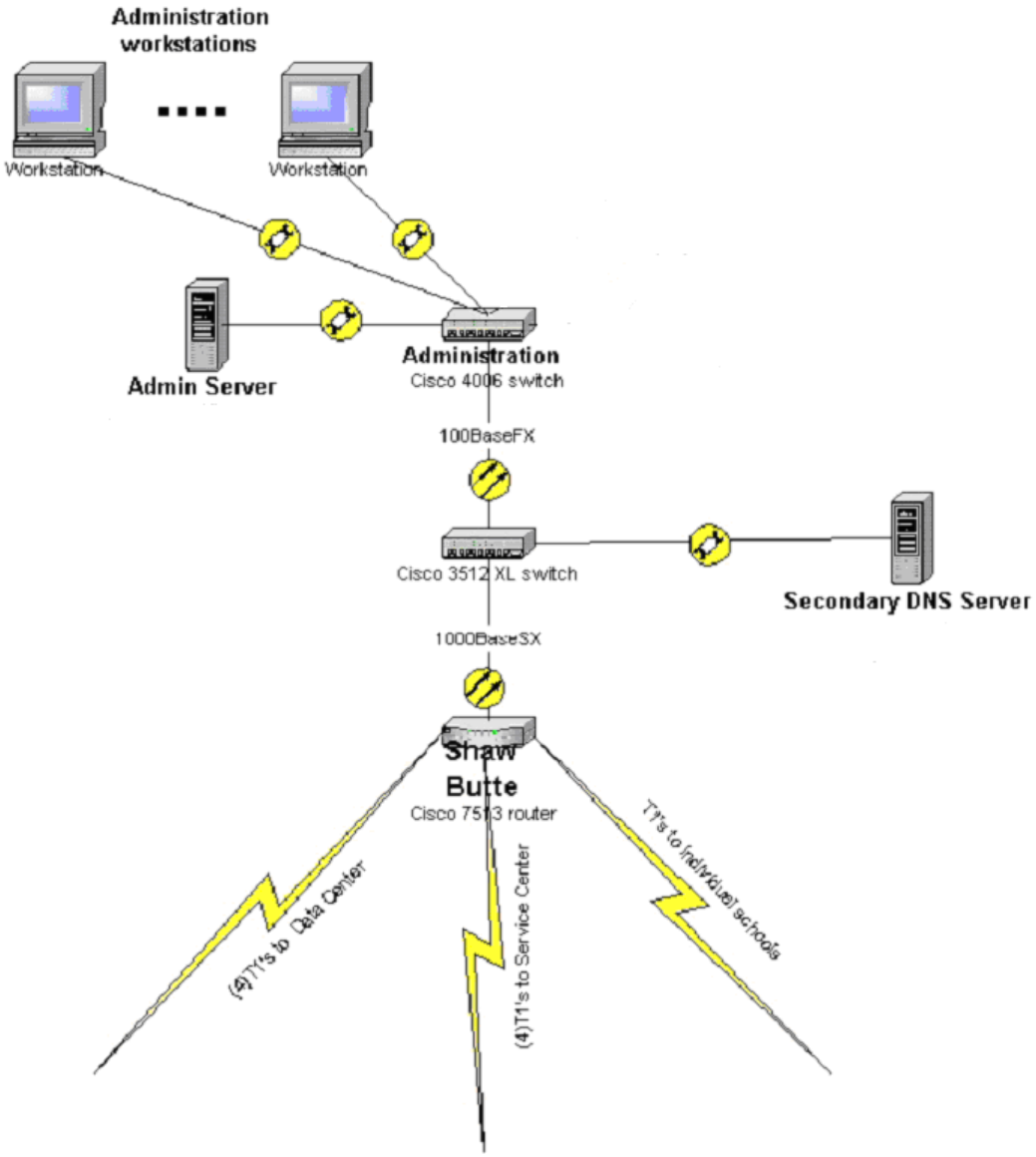
Appendix A – Washington School District WAN Logical Plan



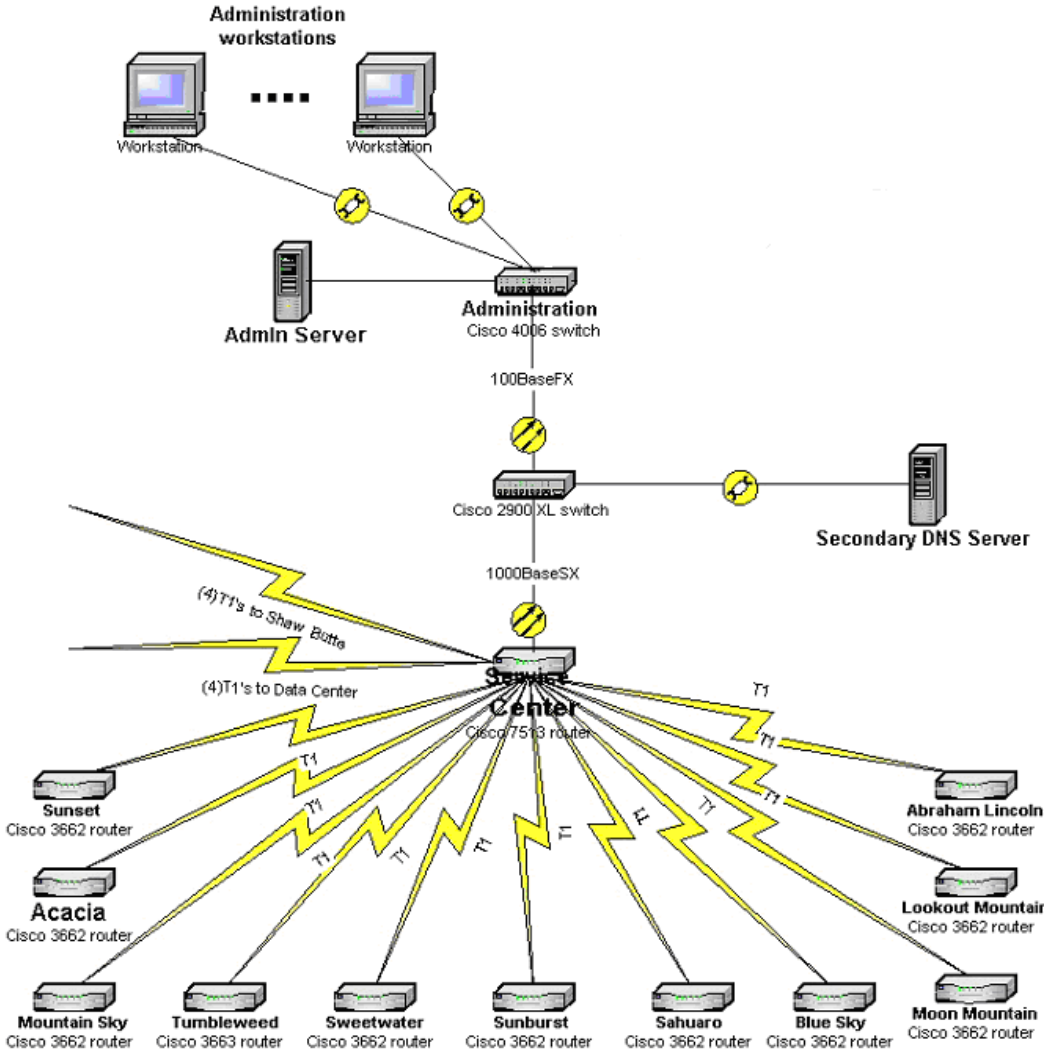
Appendix B – Detail View of Data Centre Hub



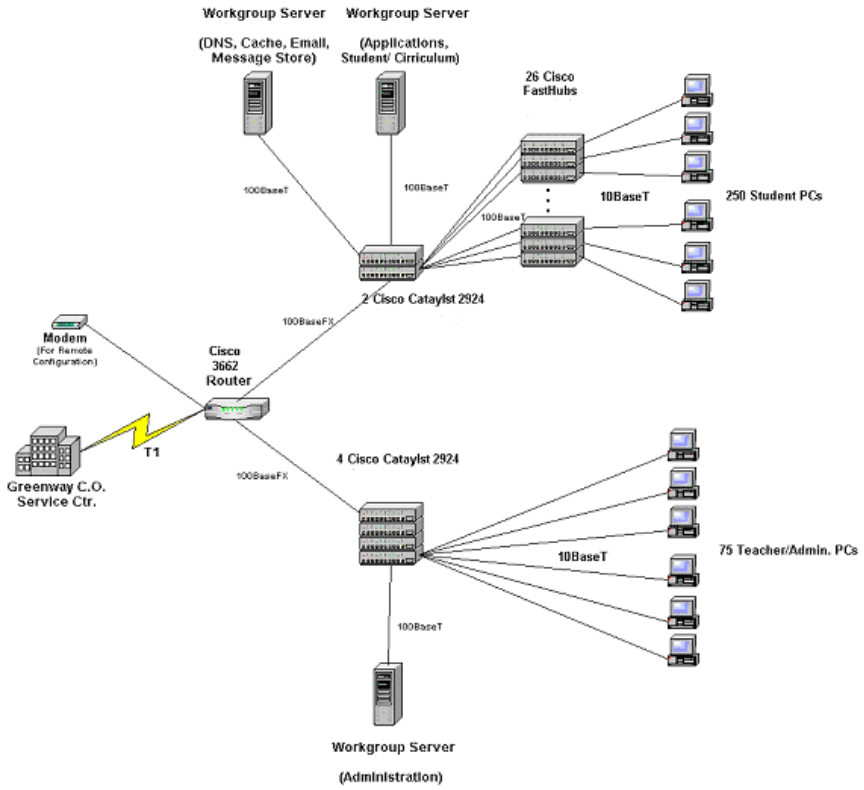
Appendix C - Detail View of Shaw Butte Hub



Appendix D - Detail View of Service Centre Hub



Appendix E – LAN/WAN Integration Logical Plan (example: Accacia School)



Appendix F - Washington School District Addressing

Subnetting

Class B IP address **150.100.0.0** for 3 regional hubs.

- Borrowing 7 bits produces 126 subnets (about 42 subnets for each hub) and 510 hosts per subnet.
- Subnet mask 255.255.254.0/23

Subnet 1	10010110.01100100. **0000001**0.00000000	150.100.2.0
Subnet 2	10010110.01100100. **0000010**0.00000000	150.100.4.0
Subnet 3	10010110.01100100. **0000011**0.00000000	150.100.6.0
.		
.		
.		
Subnet 126	10010110.01100100. **1111110**0.00000000	150.100.252.0

Hub 1 assigned subnet addresses from 150.100.2.0 to 150.100.84.0 **Service Centre**
Hub 2 assigned subnet addresses from 150.100.86.0 to 150.100.168.0 **Data Centre**
Hub 3 assigned subnet addresses from 150.100.170.0 to 150.100.252.0 **Shaw Butte**

Acacia IP addressing

Serial 0 router port (to Greenway Service Centre) is unnumbered to save on subnet addresses.

Serial 1 router port (for Remote Configuration via Modem) is unnumbered to save on subnet addresses.

Ethernet 0 router port (to Teacher/Administration Network): 150.100.2.1

Teacher Network Switch:	150.100.2.2
Administrative Server:	150.100.6.2
Teacher/Admin. Workstations:	Assigned statically within network 150.100.20.0

Ethernet 1 router port (To Student Network): 150.100.4.1

Student/Administration Switch:	150.100.4.2
DNS Server:	150.100.10.2
Curriculum Server:	150.100.12.2
Student Workstations:	Assigned dynamically via DHCP (Dynamic Host Configuration Protocol) within network 150.100.18.0

Appendix G - Washington School District Access Lists

District Office Access

The following commands only allow DNS, SMNP and Internet access from the District Office:

access-list 100 permit tcp 150.100.0.0 0.0.255.255 any eq 53
access-list 100 permit tcp 150.100.0.0 0.0.255.255 any eq 25
access-list 100 permit tcp 150.100.0.0 0.0.255.255 any eq 80
access-list 100 deny ip any any

int s0
ip access-group 100 out

Acacia LAN Access

1) **Student Network** - 150.100.18.0
   The following commands restrict student access to the teacher/administrative network:
   access-list 1 deny 150.100.18.0 0.0.0.255
   access-list 1 permit any
   int e0
   ip access-group 1 out

2) **Teacher/Administrative Network** – 150.100.20.0
   The following command allows teacher/admin. access:
   access-list 2 permit 150.100.20.0 0.0.0.255
   int e1
   ip access-group 2 out

3) **Applications Server** – 150.100.12.2
   The following command allows access to any host:
   access-list 3 permit any
   int e1
   ip access -group 3 out

4) **DNS/Email Server** – 150.100.10.2
   The following command allows access to any host:
   access-list 4 permit any
   Int e1
   ip access -group 4 out

5) **Administrative Server** – 150.100.6.2
   The following command only allows access from the Teacher/Admin. network:
   access-list 5 deny 150.100.18.0 0.0.0.255
   access-list 5 permit 150.100.86.0 0.0.0.255 (Data Centre)
   access-list 5 permit 150.100.170.0 0.0.0.255 (Shaw Butte)
   access-list 5 deny ip any any
   int e0
   ip access-group 5 out

Appendix H – Router Configurations
Commands Necessary to Implement IPX on a school router
IPX Router Configuration

Configuration of a router for IPX requires global and interface configurations.

```
Acacia(config)# ipx routing
Acacia(config)# int s0
Acacia(config-if)# novell-ether
Acacia(config-if)# ipx network 1b1a
Acacia(config-if)# exit
Acacia(config)# int e0
Acacia(config-if)# novell-ether
Acacia(config-if)# ipx network b5a
Acacia(config-if)# exit
Acacia(config)# int e1
Acacia(config-if)# novell-ether
Acacia(config-if)# ipx network b5c
Acacia(config-if)# exit
Acacia(config)# exit
```

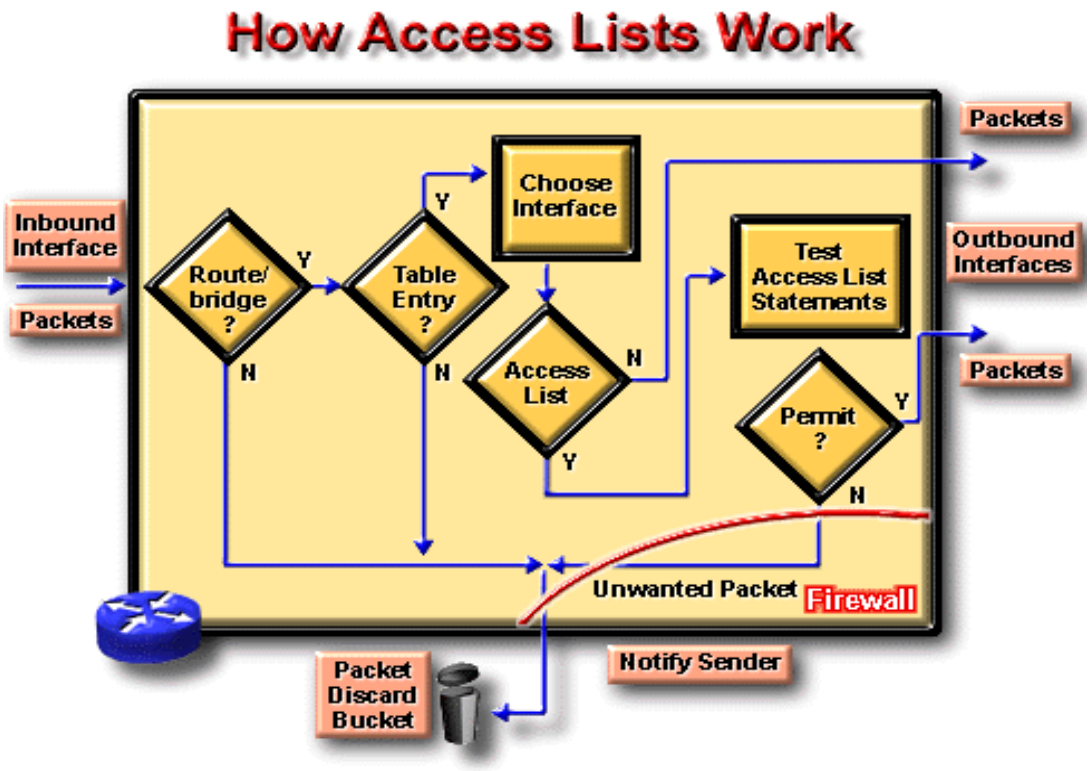
Router Commands to Implement ISDN on Access Layer Router
ISDN Router Commands

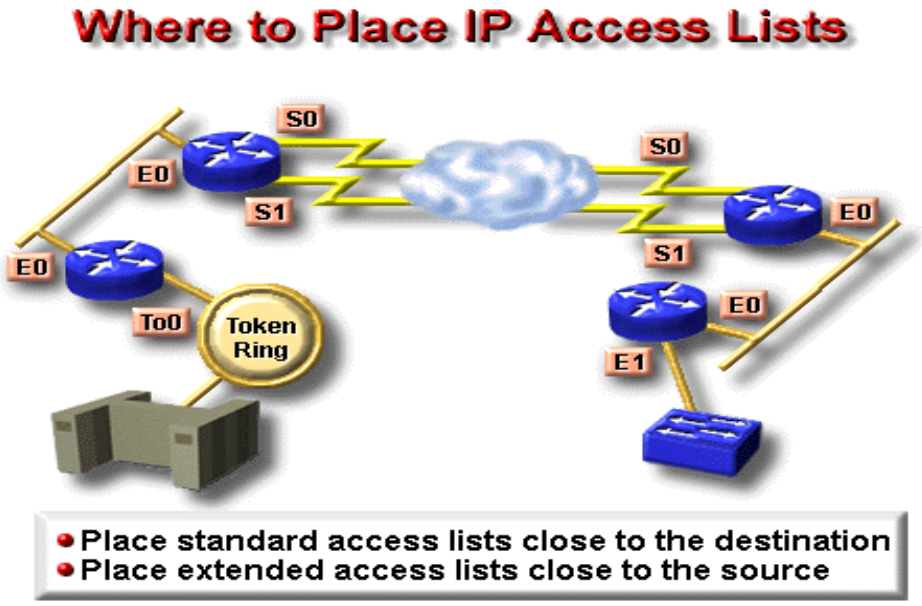
```
Acacia(config)# isdn switch-type basic-5ess
Acacia(config)# interface bri 1/0
Acacia(config-if)# no shutdown
Acacia(config-if)# encapsulation ppp
Acacia(config-if)# dialer pool-member 1
Acacia(config-if)# dialer pool-member 2
Acacia(config-if)# exit
Acacia(config)# interface bri 1/1
Acacia(config-if)# no shutdown
Acacia(config-if)# encapsulation ppp
Acacia(config-if)# dialer pool-member 1
Acacia(config-if)# dialer pool-member 2
Acacia(config-if)# exit

Acacia(config)# interface Dialer 1
Acacia(config-if)# description connected to SunnySlope
Acacia(config-if)# encapsulation ppp
Acacia(config-if)# dialer in-band
Acacia(config-if)# dialer idle-timeout 120
Acacia(config-if)# dialer string 1001
Acacia(config-if)# dialer hold-queue 10
Acacia(config-if)# dialer remote-name SunnySlope
Acacia(config-if)# dialer snapshot 1
Acacia(config-if)# dialer-group 1
Acacia(config-if)# dialer pool 1
Acacia(config-if)# ppp authentication chap
Acacia(config-if)# no ppp multilink
Acacia(config-if)# snapshot client 15 360 suppress-statechange-update dialer
```

```
Acacia(config-if)# no cdp enable
Acacia(config-if)# exit
Acacia(config)# interface Dialer 2
Acacia(config-if)# description connected to Acacia
Acacia(config-if)# no ip address
Acacia(config-if)# no ip split-horizon
Acacia(config-if)# encapsulation ppp
Acacia(config-if)# dialer in-band
Acacia(config-if)# dialer idle-timeout 120
Acacia(config-if)# dialer string 1003
Acacia(config-if)# dialer hold-queue 10
Acacia(config-if)# dialer remote-name Acacia
Acacia(config-if)# dialer-group 1
Acacia(config-if)# dialer pool 2
Acacia(config-if)# ppp authentication chap
Acacia (config-if)# no ppp multilink snapshot server 15 dialer
Acacia(config-if)# no cdp enable
Acacia(config-if)# exit
Acacia(config)# exit
Router Commands to Implement PPP on an interface
Router(config)# username District password Secret
Router(config)# int s0
Router(config-if)# encapsulation ppp
Router(config-if)# ppp authentication chap
Router(config-if)# ppp chap hostname District
Router(config-if)# ppp chap password Secret
Router(config-if)# ctrl z
Router#
Router Commands to Implement Frame Relay
router> enable
password:
router#config term
router (config)# int s0
router (config-if)#ip address 150.100.10.10 255.255.0.0
router (config-if)#encapsulation frame-relay ietf
router (config-if)#bandwidth 1544 kilobits
router (config-if)# ctrl z
```

Appendix I – Access Lists





Appendix J – PPP, IPX and TCP/IP Protocols

PPP is the most widely used and most popular WAN protocol because it offers the following features:

1. Control of Data Link set-up.
2. Assignment and management of IP addresses.
3. Network protocol multiplexing.
4. Link configuration and link quality testing.
5. Error detection.
6. Option negotiation for capabilities such as network-layer address negotiation and data compression negotiation.

PPP is designed to allow the simultaneous use of multiple network-layer protocols. PPP supports other protocols besides IP, including IPX and DECnet.

CHAP is used at the start-up of a link, and periodically, to verify the identity of the remote node using a three-way handshake. CHAP is done upon initial link establishment and can be repeated any time after the link has been established.

After the PPP link establishment phase is complete, the local router sends a "challenge" message to the remote node. The remote node responds with a value calculated using a one-way hash function (typically MD5). The local router checks the response against its own calculation of the expected hash value. If the values match, the authentication is acknowledged. Otherwise, the connection is terminated immediately.

CHAP provides protection against playback attack through the use of a variable challenge value that is unique and unpredictable. The use of repeated challenges is intended to limit the time of exposure to any single attack. The local router (or a third-party authentication server such as TACACS) is in control of the frequency and timing of the challenges.

Implementing IPX can have a serious effect on your network. Because IPX uses lots of broadcasts in order for users of the network to be able to perform certain tasks such as printing, using IPX can have a big impact on your bandwidth.
One of the reasons that IPX uses so many broadcasts is because it is a client/server-based protocol. When a user wants to perform a certain task, the machine must first send out a broadcast to locate the nearest server that can handle this task. These broadcasts are called GNS (Get Nearest Server.) Once the machine locates a server it can then begin performing its desired task.

Another type of broadcast used in IPX routing is called a SAP (Service Advertisement Protocol.) These are broadcasts that are sent out by the Netware servers that tell everyone on the network what services it can perform. Adding, finding, and removing services on the internetwork are dynamic because of SAP advertisements. Each SAP service is an object type identified by a hexadecimal number. For example, a Netware file server is the number 4, a print server is number 7, and a router is number 24.

When Novell IPX is implemented on the schools network it will have a decent impact on the bandwidth. Because of all the broadcasts that it uses, there will be an increase in traffic overall across the network. There will be even more traffic in the areas that are close to the Netware servers. The traffic will be mostly SAP's and GNS's as far as the IPX goes. There will still be other traffic on the network because multiple routing protocols (IP and IPX) are being run.
Although implementation of IPX on a network could be an efficient way to do things, it will have a negative impact on the network because with all of the broadcasts from the IPX combined with all of the ARP & RARP of the IP, which would still be running, it would just completely reduce/slow the bandwidth.

A complete TCP/IP addressing and naming convention scheme for all hosts, servers, and network interconnection devices will be developed and administered by the District Office. The implementation of unauthorized addresses will be prohibited. The District Addressing Scheme can be implemented in a number of ways. Class B, Addresses with appropriate subnetting, Network Address Translation (NAT), and Private Network Numbers.

All computers located on the administrative networks will have static addresses; curriculum computers will obtain addresses by utilizing Dynamic Host Configuration Protocol (DHCP). Each site should have a server running DHCP and use only addresses consistent with the overall District Addressing Scheme. A master network management host will be established at the District Office and will have total management rights over all devices in the network.

- The TCP/IP protocol of the OSI model Layer 4 (transport layer) has two protocols - *TCP* and *UDP*.
- *TCP* supplies a virtual circuit between end-user applications. These are its characteristics:
    - Connection-oriented
    - Reliable
    - Divides outgoing messages into segments
    - Reassembles messages at the destination station
    - Re-sends anything not received
    - Reassembles messages from incoming segments.
- *UDP* transports data unreliably between hosts. These are the characteristics:
    - Connectionless
    - Unreliable
    - Transmit messages (called user datagrams)
    - Provides no software checking for message delivery (unreliable)
    - Does not reassemble incoming messages
    - Uses no acknowledgments
    - Provides no flow control

Appendix K – Frame Relay and ISDN

Frame Relay is a Packet-Switched connection in which network devices share a single point-to-point link to transport packets from a source to a destination across a carrier network. Frame Relay was designed to provide high-speed, reliable links. As a result, Frame Relay does not offer much error checking or reliability, but expects upper-layer protocols to attend to these issues. Frame Relay is called a non-broadcast multi-access technology because it has no broadcast channel. Broadcasts are transmitted through Frame Relay by sending packets to all network destinations.
Frame Relay is a cost-effective alternative to point-to-point WAN designs. Each site can be connected to every other by a virtual circuit

The router needs only one physical interface to the carrier. Frame Relay service is offered through a permanent virtual circuit (PVC). A data-link connection identifier (DLCI) identifies the PVC. The DLCI number is a local identifier between the DTE and DCE that identifies the logical circuit between the source and destination devices.

There are really only two things required to implement ISDN to a site, an ISDN capable router and the remote user software. The router will usually be on the service provider's side and the remote user software will be on the users side.

There are five major devices in the implementation of ISDN:

1. Terminal Equipment 1 (TE1) - Designates a device that is compatible with the ISDN network. A TE1 connects to a Network Termination or either Type 1 or Type 2.
2. Terminal Equipment 2 (TE2) - Designates a device that is not compatible with ISDN and requires a Terminal Adapter.
3. Terminal Adapter (TA) - Converts standard electrical signals into the form used by ISDN so that non-ISDN devices can connect to the ISDN network.
4. Network Termination Type 1 (NT1) - Connects 4-wire ISDN subscriber wiring to the conventional 2-wire local loop facility.
5. Network Termination Type 2 (NT2) - Directs traffic to and from different subscribe devices and the NT1. The NT2 is an intelligent device that performs switching and concentrating.

As well as four major reference points:

R - References the point (connection) that is a non-ISDN compatible device and a Terminal Adapter.
S - References the points that connect into the NT2, or customer-switching device. It is the interface that enables calls between the various customer premises equipment.
T - Electrically identical to the S interface, it references the outbound connection from the NT2 to the ISDN network.

U - References the connection between the NT1 and the ISDN network owned by the phone company.

An ISDN link should be installed at the distribution layer of a hierarchical WAN model. The reason for this is that the ISDN link should be considered part of the backbone between the remote user and the central WAN switch or router. Backbone cabling is by definition located at the distribution.

Bibliography

Books:

CCNA Second-Year Companion Guide 2nd Edition ISBN 1 -58713-029-7

CCNA Lab Companion 2nd Edition ISBN 1 -58713-030-0

Internetworking Technologies 3rd Edition ISBN 1 -58705-001-3

Internet sources:

CCNA online curriculum Semester 4 Chapters 1-4

http://www.cisco.com/univercd/home/home.htm

http://www.cisco.com/univercd/home/search.htm

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/introwan.htm

http://www.rackspace.com/index.php?supbid=google210

http://www.pgp.com/

http://netsecurity.about.com/mbody.htm

http://www.netsurf.com/nsf/v01/01/nsf.01.01.html