Design & Implementation ISP MPLS Backbone Network on IPV6 using 6PE Configuration

Dr.T.Ravichandra Babu[1], V.Kiran Kumar[2], Md.Rizwan[3], M.Mamatha[4], V.Akhil Varma[5]

[1] Professor, Department of ECE, Sreyas Institute of Engineering & Technology, Nagole, Hyderabad

[2] B.Tech Student , Department of ECE, Sreyas Institute of Engineering & Technology, Nagole, Hyderabad

[3] B.Tech Student, Department of ECE, Sreyas Institute of Engineering & Technology, Nagole, Hyderabad

[4] B.Tech Student, Department of ECE, Sreyas Institute of Engineering & Technology, Nagole, Hyderabad

[5] B.Tech Student, Department of ECE, Sreyas Institute of Engineering & Technology, Nagole, Hyderabad

Abstract—

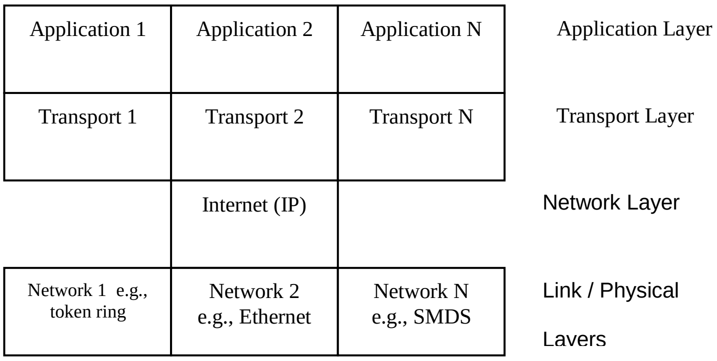
Internet is a global computer network made up of smaller computer networks; it has been called a "Network of Networks." As the Internet becomes increasingly popular with every day that passes, it is now considered as one of the best ways to do business (e- commerce), network (by email), and build partnerships (on-line collaboration).IPv6 (Internet Protocol version 6) is a revision of the Internet Protocol (IP) developed by the Internet Engineering Task Force (IETF). IPv6 is intended to succeed IPv4, which is the dominant communications protocol for most Internet traffic as of now. IPv6 was developed to deal with the long-anticipated problem of IPv4 running out of addresses. IPv6 implements a new addressing system that allows for far more addresses to be assigned than with Ipv4. IPv6 provides a platform for new Internet functionality that will be needed in the immediate future, and provide flexibility for further growth and expansion. Multiprotocol Label Switching (MPLS) is deployed by many service providers for establishing their backbone networks. Service providers want to introduce IPv6 services to their customers, but changes to their existing Ipv4 infrastructure can be expensive and the cost benefit for a small amount of IPv6 traffic does not make economic sense. To leverage an existing IPv4 MPLS infrastructure and add IPv6 services without requiring any changes to the network backbone, IPv6 over MPLS backbones enables isolated IPv6 domains to communicate with each other over an MPLS IPv4 core network. This implementation requires backbone infrastructure upgrades and no reconfiguration of core routers because forwarding is based on labels rather than the IP header itself, providing a very cost-effective strategy for the deployment of IPv6.

Keywords—MPLS;IPV4;IPV6;IETF

I. INTRODUCTION

The Internet architecture is of a layered design, which makes testing and future development of Internet protocols easy. The architecture and major protocols of the Internet are controlled by the Internet Architecture Board (IAB). Internet architecture is illustrated in Figure 1.

The Internet provides three sets of services. At the lowest level is a connectionless delivery service (network layer) called the Internet protocol (IP). The next level is the transport layer service. Multiple transport layer services use the IP service. The highest level is the application layer services. Layering of the services permits research and development on one without affecting the others.



Application 1	Application 2	Application N	Application Layer
Transport 1	Transport 2	Transport N	Transport Layer
	Internet (IP)		Network Layer
Network 1 e.g., token ring	Network 2 e.g., Ethernet	Network N e.g., SMDS	Link / Physical Lavers

Figure:1 Conceptual layering of Internet protocols.

For any two systems to communicate, they must be able to identify and locate each other. While these addresses in below Figure are not actual network addresses, they represent and show the concept of address grouping. This uses the A or B to identify the network and the number sequence to identify the individual host.

A computer may be connected to more than one network. In this situation, the system must be given more than one address. Each address will identify the connection of the computer to a different networkThis address, operating at Layer 3, allows one computer to locate another computer on a network. All computers also have a unique physical address, known as a MAC address. These are assigned by the manufacturer of the network interface card. MAC addresses operate at Layer 2 of the OSI model.

II. Literature Survey

An IP address is a 32-bit sequence of 1s and 0s. To make the IP address easier to use, the address is usually written as four decimal numbers separated by periodsThis dotted decimal notation also prevents a large number of transposition errors that would result if only the binary numbers were used. Using dotted decimal allows number patterns to be more easily understood. Both the binary and decimal numbers in the Figure represent the same values, but it is easier to see in dotted decimal notation It is easy to see the relationship between the numbers 192.168.1.8 and 192.168.1.9, where 11000000.10101000.00000001.00001000 and 11000000.10101000.00000001.00001001 are not as easy to recognize. Looking at the binary, it is almost impossible to see that they are consecutive numbers.

A. 2.1 IPv4 addressing

A router forwards packets from the originating network to the destination network using the IP protocol. The packets must include an identifier for both the source and destination networks. Using the IP address of destination network, a router can deliver a packet to the correct network. This kind of address is called a hierarchical address, because it contains different levels. An IP address combines these two identifiers into one number. This number must be a unique number, because duplicate addresses would make routing impossible.

The first part identifies the system's network address. The second part, called the host part, identifies which particular machine it is on the network. IP addresses are divided into classes to define the large, medium, and small networks. Class A addresses are assigned to larger networks. Class B addresses are used for medium-sized networks and Class C for small networks.

To accommodate different size networks and aid in classifying these networks, IP addresses are divided into groups called classes. This is known as classful addressing. Each complete 32-bit IP address is broken down into a network part and a host part. A bit or bit sequence at the start of each address determines the class of the address.

There are five IP address classes as shown in the Figure below.The Class A address was designed to support extremely large networks, with more than 16 million host addresses available. Class A IP addresses use only the first octet to indicate the network address. The remaining three octets provide for host addresses. The first bit of a Class A address is always 0. With that first bit a 0, the lowest number that can be represented is 00000000, decimal 0. The highest number that can be represented is 01111111, decimal 127. The numbers 0 and 127 are reserved and cannot be used as network addresses.

The Class B address was designed to support the needs of moderate to large-sized networks. A Class B IP address uses the first two of the four octets to indicate the network address. The other two octets specify host addresses. The first two bits of the first octet of a Class B address are always 10. The remaining six bits may be populated with either 1s or 0s. Therefore, the lowest number that can be represented with a Class B address is 10000000, decimal 128. The highest number that can be represented is 10111111, decimal 191. Any address that starts with a value in the range of 128 to 191 in the first octet is a Class B address.

The Class C address space is the most commonly used of the original address classes. This address space was intended to support small networks with a maximum of 254 hosts. A Class C address begins with binary 110. Therefore, the lowest number that can be represented is 11000000, decimal 192. The highest number that can be represented is 11011111, decimal 223. If an address contains a number in the range of 192 to 223 in the first octet, it is a Class C address.

The Class D address class was created to enable multicasting in an IP address. A multicast address is a unique network address that directs packets with that destination address to predefined groups of IP addresses. Therefore, a single station can simultaneously transmit a single stream of data to multiple recipients.

The Class D address space, much like the other address spaces, is mathematically constrained. The first four bits of a Class D address must be 1110. Therefore, the first octet range for Class D addresses is 11100000 to 11101111, or 224 to 239. An IP address that starts with a value in the range of 224 to 239 in the first octet is a Class D address.

Figure 2:Broad cast address

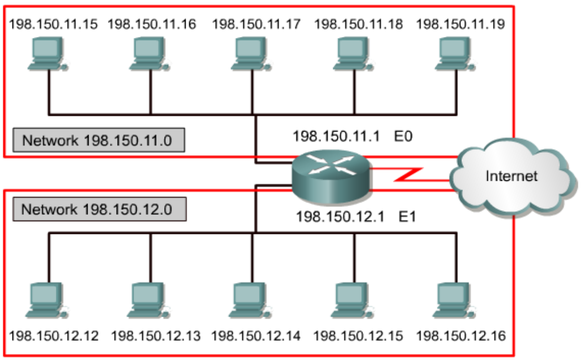


Figure 2: Broadcast address

A Class E address has been defined. However, the Internet Engineering Task Force (IETF) reserves these addresses for its own research. Therefore, no Class E addresses have been released for use in the Internet. The first four bits of a Class E address are always set to 1s. Therefore, the first octet range for Class E addresses is 11110000 to 11111111, or 240 to 255.

III. TECHNICLA REQUIREMTS

The following components are required fro the development of this work such as

- LAN components and terminology
- Networking basics and topologies
- Hub
- Switch
- Router
- Gateway

A. LAN COMPONENTS

Local Area Network is a high speed, low error data network covering a relatively small geographic area. LAN connects workstations, peripherals, terminal and other devices in a single building or other geographically limited area. LAN standard specifies cabling and signaling at the physical and data link layers of the OSI model. Ethernet, FDDI and Token ring are widely used LAN technology.

B. Ethernet Terminology

Ethernet follows a simple set of rules that govern its basic operation. To better understand these rules, it is important to understand the basics of Ethernet terminology.

Medium - Ethernet devices attach to a common medium that provides a path along which the electronic signals will travel. Historically, this medium has been coaxial copper cable, but today it is more commonly a twisted pair or fiber optic cabling.

Segment - We refer to a single shared medium as an Ethernet segment.

Node - Devices that attach to that segment are stations or nodes.

Frame - The nodes communicate in short messages called frames, which are variably sized chunks of information. The Ethernet protocol specifies a set of rules for constructing frames.

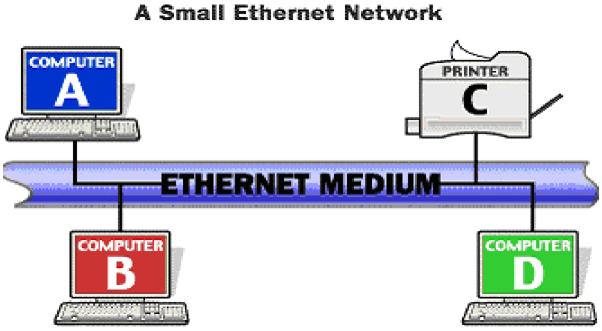


Figure 3:Ethernet Network

Since a signal on the Ethernet medium reaches every attached node, the destination address is critical to identify the intended recipient of the frame. For example, in the figure above, when computer B transmits to printer C, computers A and D will still receive and examine the frame. However, when a station first receives a frame, it checks the destination address to see if the frame is intended for itself. If it is not, the station discards the frame without even examining its contents.

C. CSMA/CD

Acronym CSMA/CD signifies carrier-sense multiple access with collision detection and describes how the Ethernet protocol regulates communication among nodes.When one Ethernet station transmits, all the stations on the medium hear the transmission. Before a station transmits, it "listens" to the medium to determine if another station is transmitting.

If the medium is quiet, the station recognizes that this is an appropriate time to transmit A single Ethernet segment is sometimes called a collision domain because no two stations on the segment can transmit at the same time without causing a collision. When stations detect a collision, they cease transmission, wait a random amount of time, and attempt to transmit when they again detect silence on the medium. The random pause and retry is an important part of the protocol. If two stations collide when transmitting once, then both will need to transmit again

D. Networking

Here are some of the fundamental parts of a network:

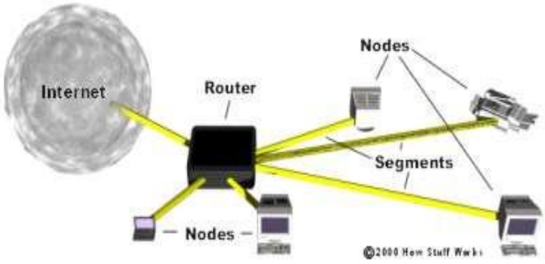


Figure : 4 Fundamental parts of Network

Network - A network is a group of computers connected together in a way that allows information to be exchanged between the computers.

Node - A node is anything that is connected to the network. While a node is typically a computer, it can also be something like a printer or CD-ROM tower.

Segment - A segment is any portion of a network that is separated, by a switch, bridge or router, from other parts of the network.

Backbone - The backbone is the main cabling of a network that all of the segments connect to. Typically, the backbone is capable of carrying more information than the individual segments. For example, each segment may have a transfer rate of 10 Mbps (megabits per second), while the backbone may operate at 100 Mbps.

Topology - Topology is the way that each node is physically connected to the network. Common topologies include:

Bus - Each node is **daisy-chained** (connected one right after the other) along the same backbone. Information sent from a node travels along the backbone until it reaches its destination node.

Each end of a bus network must be **terminated** with a resistor to keep the signal that is sent by a node across the network from bouncing back when it reaches the end of the cable.

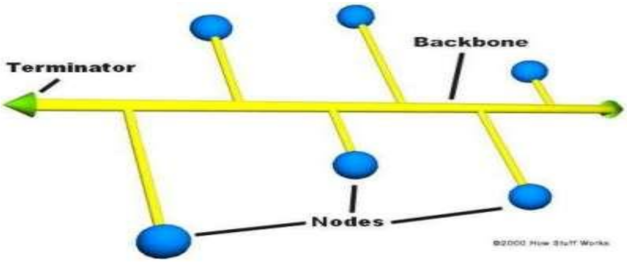


Figure:5 Bus network topology

Ring - Like a bus network, rings have the nodes daisy-chained. The difference is that the end of the network comes back around to the first node, creating a complete circuit. In a ring network, each node takes a turn sending and receiving information through the use of a **token**.

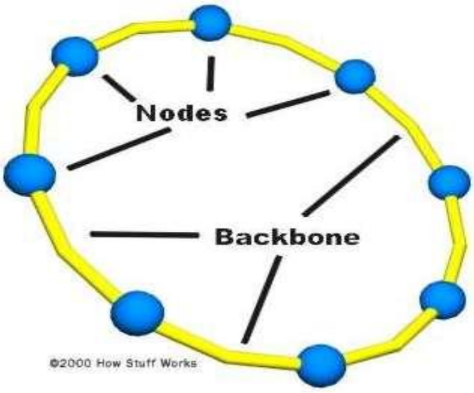


Figure: 6 Ring network topology

E. ***Star*** –

In a star network, each node is connected to a central device called a hub. The hub takes a signal that comes from any node and passes it along to all the other nodes in the network.

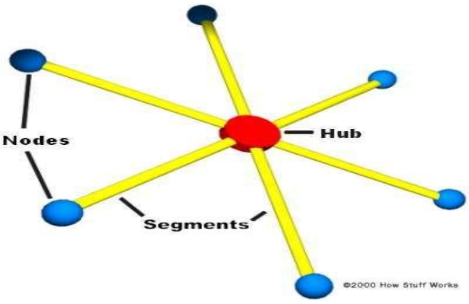


Figure:7 Star network topology

F. ***Star bus*** –

Probably the most common network topology in use today, star bus combines elements of the star and bus topologies to create a versatile network environment.Nodes in particular areas are connected to hubs (creating stars), and the hubs are connected together along the network backbone (like a bus network). Quite often, stars are nested within stars, as seen in the example below:

G. ***Local Area Network (LAN)*** –

A LAN is a network of computers that are in the same general physical location, usually within a building or a campus. If the computers are far apart (such as across town or in different cities), then a **Wide Area Network** (WAN) is typically used.

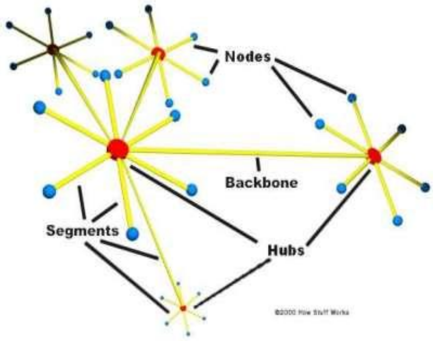


Figure: 8 A typical star bus network

IV. Implementation

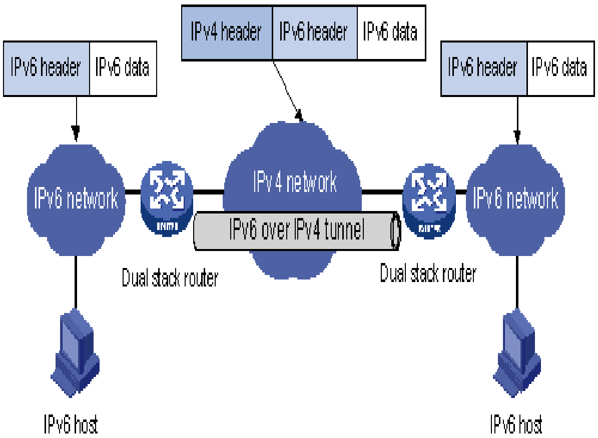


Figure.9: Tunneling Mechanism

The IPv6 protocol was established because the number of IPv4 addresses is quickly running out. The IPv6 protocol creates a 128-bit address, four times the size of the 32-bit IPv4 standard, so there will be infinitely more available IP addresses. This will accommodate all the Smartphone's, tablets and other computers on the network, but also the coming proliferation of Internet-connected devices including refrigerators, cars, and myriad sensors in homes, buildings and on IP networks.

Overlay tunneling encapsulates IPv6 packets in IPv4 packets for delivery across an IPv4 infrastructure (a core network or the Internet (see the figure below). By using overlay tunnels, you can communicate with isolated IPv6 networks without upgrading the IPv4 infrastructure between them. Overlay tunnels can be configured between border routers or between a border router and a host; however, both tunnel endpoints must support both the IPv4 and IPv6 protocol stacks. IPv6 supports the following types of overlay tunneling mechanisms

V. Results & Discussions

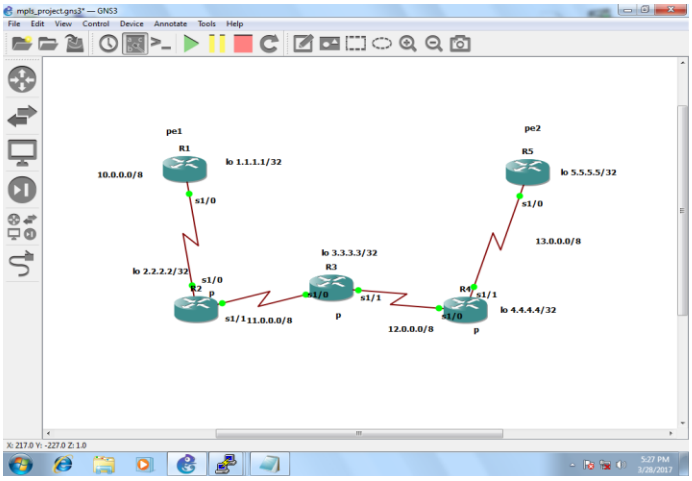
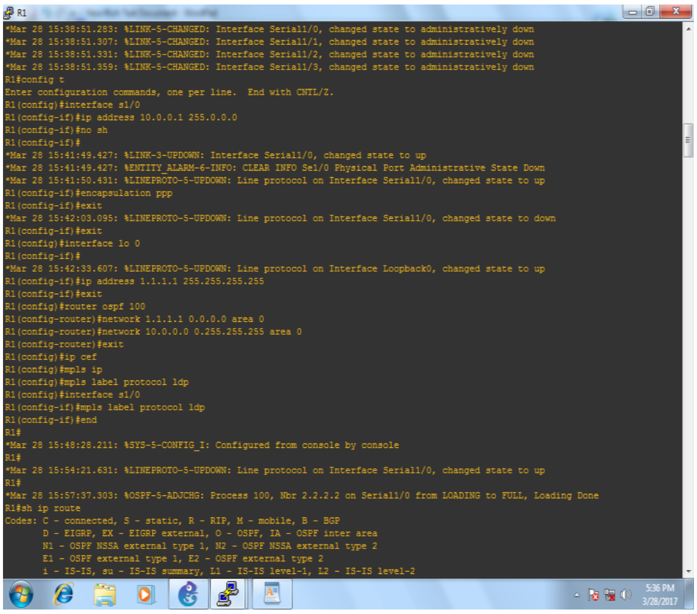


Figure.10: Implementation of IPV4 in CISCO Packet Tracer screen shot



```
*Mar 28 15:38:51.283: %LINK-5-CHANGED: Interface Serial1/0, changed state to administratively down
*Mar 28 15:38:51.307: %LINK-5-CHANGED: Interface Serial1/1, changed state to administratively down
*Mar 28 15:38:51.331: %LINK-5-CHANGED: Interface Serial1/2, changed state to administratively down
*Mar 28 15:38:51.359: %LINK-5-CHANGED: Interface Serial1/3, changed state to administratively down
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface s1/0
R1(config-if)#ip address 10.0.0.1 255.0.0.0
R1(config-if)#no sh
R1(config-if)#
*Mar 28 15:41:49.427: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up
*Mar 28 15:41:49.427: %ENTITY_ALARM-6-INFO: CLEAR INFO Se1/0 Physical Port Administrative State Down
*Mar 28 15:41:50.431: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up
R1(config-if)#encapsulation ppp
R1(config-if)#exit
*Mar 28 15:42:03.095: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to down
R1(config-if)#exit
R1(config)#interface lo 0
R1(config-if)#
*Mar 28 15:42:33.607: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
R1(config-if)#ip address 1.1.1.1 255.255.255.255
R1(config-if)#exit
R1(config)#router ospf 100
R1(config-router)#network 1.1.1.1 0.0.0.0 area 0
R1(config-router)#network 10.0.0.0 0.255.255.255 area 0
R1(config-router)#exit
R1(config)#ip cef
R1(config)#mpls ip
R1(config)#mpls label protocol ldp
R1(config)#interface s1/0
R1(config-if)#mpls label protocol ldp
R1(config-if)#end
R1#
*Mar 28 15:48:28.211: %SYS-5-CONFIG_I: Configured from console by console
R1#
*Mar 28 15:54:21.631: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up
R1#
*Mar 28 15:57:37.303: %OSPF-5-ADJCHG: Process 100, Nbr 2.2.2.2 on Serial1/0 from LOADING to FULL, Loading Done
R1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

Figure 11: Observation of IPV4 screen shot

In router implementing Open Shortest Path First (OSPF) & Multiprotocol Label Switching (MPLS) which shows the transfer of data packets from source to destination is made by using GNS3 software. The observation gives data transfer between source to destination by using MPLS

VI. Conclusion

In this project we Providing the Quality of Service (QOS) and traffic engineering capabilities in the Internet is very essential. For this purpose, the current Internet must be enhanced with new technologies such as MPLS.MPLS will play a key role in future service providers and carriers IP backbone networks. The use of MPLS in IP backbone network will facilitate the development of new service such as real-time applications in the Internet.

ACKNOWLEDGMENT

The authors would like thank to the management, Principal and the faculty members of ECE Department of Sreyas Institute of Engineering & Technology.

XX REFERENCES

[1] [IPv6_Deploy] Cisco IOS IPv6 Deployment scenario guide

[2] http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/ipv6_sol/ipv6dswp.pdf

[3] [IPv6_BGP] "Connecting IPv6 Domains across IPv4 Clouds with BGP", De Clerq et al, draft-ietf-ngtrans-bgp-tunnel-04, January 2002, Work in progress.

[4] [MPLS_BGP] Carrying Label Information in BGP-4, RFC3107, May 2001. Y. Rekhter and E. Rosen.

[5] [BGP_CAP] Capabilities Advertisement with BGP-4, RFC-2842, May 2000.

[6] [v6_ADDRESS] "IPv6 Addressing Architecture", R. Hinden and S. Deering, draft-ietf-ipngwg-addr-arch-v3-10, September 2002, Work in Progress.