Lan topology

WAN Layout There is considerable planning required when connecting multiple geographically distant sites to create a WAN topology with security at the top of the list. The existing LANA topology, legacy equipment, incorporating new equipment, budget restraints, ND security concerns help dictate the network structure. Circuit-switched or Packet- Switched connection technologies are cost-effective options. Internet Service Providers (Sips) used shared routes with other companies to distribute data.

A secure (and expensive) method of inter-connecting locations are leased and dedicated lines. For example, an MILS (T 1) circuit is a secure, scalable choice for connecting two sites with diverse protocols and legacy equipment, but expensive because it is available only to the organization leasing the equipment and path lines. Access Control Lists Deciding how to implement system Calls is determined by organizational needs. Calls allow or prevent specified IP addresses, subnet masks, TCP, and JODI protocols to travel through a network interface.

Only one configuration per CAL, interface, direction, and protocol is possible. CAL configurations come in standard or extended versions, with either a number (1-99 standard) or (100-199 extended) or a name that helps identify the purpose of the CAL (e. G. Block Backbone). Implementation requires proper interface placement for maximum effectiveness and increased system performance. For example; limiting access to a sensitive data-store, protected by a strict CAL for authorized agents only is a common scenario.

Permissive Calls can be configured internally to allow employees use of organizational assets and external interfaces can use strict Calls to deny

users from accessing the internet or blocking incoming traffic from non-work related sites. To configure Calls on a Cisco device verify there are no other active Calls already filtering intended traffic. Unless applied to the correct interface and direction, the CAL will not function correctly. Show Calls; Show Calls- Routers#show access-lists" command in global configuration mode.

Create CAL; RI into Ethernet 0/0 Rl(Congo-if)# IP access-group 101 out RI (Congo)# access-list 101 deny TCP any host www. Backbone. Com CEQ www RI (confining)# access-list 101 permit TCP any any CEQ www RI (Congo-if)#end Name an CAL; IP access-group Deny_Backbone out command creates an names the CAL named " Deny Backbone" Remove unwanted Calls: Routers(Congo)#no access-list X" (X representing the number of the list). Troubleshooting Calls requires close attention to detail; View existing Calls- Routers#show IP access-list

Use Terminal Monitor to view debug output Use debug IP packet or debug packet detail to generate debug information No debug all to end debug session Using the same naming convention for Calls across multiple devices in the network, as well as providing comments describing the purpose each CAL is encouraged to allow for efficient troubleshooting at a future date. Virtual Private Networks VPN allow information to travel securely over long physical distances; typically over a WAN. VPN are important for companies (with multiple locations) that require synchronous communication.

Multiple protocols are available to facilitate VPN implementation (SSL, PPTP, LOTT, and Pipes). Secure Socket Layer (SSL) is a transport protocol used over a standard TCP port. SSL VPN create secure environments using browsers as

a client. It is easy to implement, requires no specialized software, provides access to decentralized resources, and is cost effective for many businesses. Microsoft's Point-to-Point Tunneling Protocol (PPTP) is accepted and widely supported. Microsoft incorporates into most operating systems, it is available for Apple and Linux and has low overhead.

The flexibility PPTP provides an advantageous security solution. Layer 2 Protocol Tunneling (LAP) is the amalgamation of PPTP and Layer 2 Forwarding (ELF); it works with non-lap networks, X. 25, ATM, and Frame Relay. It functions on the data link layer and works in tandem with a majority of firewalls. Internet Protocol Security (Pipes) comprises of various protocols that provide secure IP communications. Considered the De facto standard for site-to-site IP connections, Pipes requires a client, involves key exchanges, and tunnel encryption. A variety of security options to implement an Pipes VPN are available.

Pipes provides a strong defensive posture against Denial of Service (DOS), replay, and " man-in-the-middle" attacks" (Shinier, 2004). IPPP/NAT/PAT/live Routers connect to other devices through interfaces. Each device requires a unique IP address to communicate with other devices. Until recently IPPP addresses were the only way anyone could connect to the Internet via their ISP. The depletion of Pop address sparked the need to develop different strategies to preserve dwindling IPPP address. The advent of subnets, NAT/PAT and Variable Length Subnet Masks (EVILS),

IP addressing can be customized to cope with IPPP depletion. Subnets are used to divide IPPP addresses into three useable classes for the general use

(A, B, C). There are public and private IP addresses. Public IP addresses are required to establish connection to the Internet. Private Pips are distributed within a home or businesses with multiple users and devices. NAT/PAT is a process of translating a private IP to a public IP or vise-versa, on a router, depending on the direction of traffic. The need for NAT/PAT stems from the cost of connecting multiple users to the Internet.

NAT intercepts the private IP address assigned to each device, cloaks it with a unique public IP assigned to that user, creates a routing table for that device and presents it to the world. When data reaches its destination and returned, the process is reversed. The router references the routing table and directs the traffic back to the host device. If the translated IP address in not located on the routing table the packets are dropped. PAT is similar to NAT but includes the use of port assignments with the IP information. When a request it made the router creates a session for that quest.

It captures the host IP and port address. The translating router records the IP and port assignment translates the private IP to a public IP and records the session on its routing table. The routing table is cleared once a connection has completed and a new session is established. IPPP is the answer to dwindling IPPP address concerns. There is no need to worry about exhausting the available range of Pop addresses. Now each device can have a different IPPP address and not burden a router with NAT/PAT translation or subnets. There are enough IPPP addresses to give ACH person alive, thousands of individual addresses.

Enhanced Interior Gateway Protocol Routing protocols like EIGRP require knowledge of the available equipment and network topology. EIGRP is a Cisco proprietary distance vector protocol; it dynamically learns routes to other devices that are directly attached to them. It sends/receives hello packets to recognize when neighbor devices are unreachable and updates its routing table. Sharing distance vectors within the network, it builds a routing table with " hops" then selects the best path to send/forward packets. Useful EIGRP nomads include: Network Setup- Router(Congo-router)#network 10. X. X. " command in order to setup the network that is to be advertised. Bandwidth- Router(Congo-if)#bandwidth x" (x representing the bandwidth speed) (Meson, 2013). Frame-Relay Frame-Relay fast packet technology transfer's data between LANA and WAN devices in packets called " frames. " It requires a dedicated connection to communicate, operates on the Data Link Layer of the OSI model, and it is often used to couple Lana with WANTS. Host devices accelerate data delivery by providing error correction. PVC routes o/from devices can fluctuate depending on network congestion, but end-users are not affected.

When connection issues develop there are troubleshooting measures that help in the recovery of a Frame-Relay configured network. " In general, debug commands are used on a Cisco router only for diagnostic and troubleshooting purposes (Chin, 2004). " Some debug commands that aid in troubleshooting Frame-relay networks are: RI #debug frame-relay events- " Displays Frame Relay Inverse ARP packets exchanged between the local router and the Frame Relay network (Chin, 2004). " RI#debug Ramee-relay MIM " Used to determine whether the router and the Frame Relay switch are

sending and receiving LIMIT packets properly (Chin, 2004). Rl#debug frame-relay packet - " Used to analyze packets sent on a Frame Relay interface (Chin, 2004). " Point- to-Point Protocol Point-to-Point Protocol (APP) is commonly used by companies with locations linked via leased-line or serial connection. APP offers security via the Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP). APP can be configured on Synchronous serial (leased-line or Cable/DSL broadband) or Asynchronous serial (phone lines). APP employs the use of Coco's proprietary Link Control Protocol (LCP).

LCP automatically configures interfaces on both sides of the connection and takes responsibility for establishing, configuring, and testing the connection. APP encapsulation requires proper configuration in order to establish a working router connection. Primary uses for CHAP include authentication and security. Cisco provides a proprietary encapsulation method (HEAD) although APP is common because it supports Non-Cisco equipment. Hosannas-Router(Congo)# hosannas Router X in global configuration mode. Surname/Password- Routers(Congo)# surname Router Z password al 234.