

# Designing Cisco Networks

## Version 3.0.0

# Designing Cisco Networks

**Version 3.0.0**



## Abstract:

This study guide will help you to prepare for Cisco exam 640-441, Cisco Certified Design Associate (Designing Cisco Networks). Exam topics include Designing a Network to Meet a Customer's Requirements for Performance, Capacity, Security and Scalability, Assembling Cisco Product Lines in End-to-end Networking Solutions and Extended Knowledge of Your Basic Internetworking Fundamentals.

## Find even more help here:

# Contents:

# Internetworking Fundamentals

**Cisco's Fundamentals Online: Click here**
**Cisco's Internetwork Design Guide: Click here**
**OSI:**

| OSI LAYER | FUNCTIONS |
|---|---|
| *APPLICATION*<br>Message/data | • Service advertisement, service availability. Manages communications between applications. (FPDAM) File, Print, Database, Application, and Messaging services. Allows applications to use the network. Handles network access, flow control and error recovery. |
| *PRESENTATION*<br>Message/data | • Translation, compression, encryption, data conversion. Translates data into a form usable by the application layer. The redirector operates here. Responsible for protocol conversion, translating and encrypting data, and managing data compression. |
| *SESSION*<br>• Message/data<br>• RPC (Remote Procedure calls) functions here. | • Connection establishment, data transfer, connection release (Half duplex, full duplex, simplex). Allows applications on connecting systems to establish a session. Provides synchronization between communicating computers. |
| *TRANSPORT*<br>Segments (or Datagrams) | • Service addressing, segmentation and transport control, flow control, end-to-end data integrity. Responsible for packet handling. Ensures error-free delivery. Repackages messages, divides messages into smaller packets and controls error handling. |
| *NETWORK*<br>Packets (or Datagrams) | • Logical addressing, switching, routing, network control. Translates system names into addresses. Determines routes for sending data and manages network traffic problems, packet switching, routing, data congestion and reassembling data. |
| *DATA LINK*<br>Frames | • Sends data from network layer to physical layer. Manages physical layer communications between connecting systems.<br>• LLC Layer (Logical Link Control): flow control and |

| | |
|---|---|
| | timing (802.2). Manages link control and defines SAPs (Service Access Points).<br>• MAC Layer (Media Access Control): framing and physical addressing (802.3, 802.4, 802.5, 802.12). Communicates with adapter card. |
| *PHYSICAL*<br>• Bits<br>• Is concerned with definition of low level functions (voltage, media types) | • Transmits data over a physical medium. Defines cables, cards and physical aspects as well as electrical properties, transmission media, transmission devices, physical topology, data signaling, data synchronization and data bandwidth. Manages data placement on and data removal from the network media. |

## TCPIP Addressing:

IP basics Documentation by Cisco

| | |
|---|---|
| Class A | 1-127 |
| Class B | 128-191 |
| Class C | 192-223 |
| Class D | Multicast |
| Class E | Experimental |

| Decimal | Subnets | # Class A Hosts | # Class B Hosts | # Class C Hosts |
|---|---|---|---|---|
| .192 | 2 | 4,194,302 | 16,382 | 62 |
| .224 | 6 | 2,097,150 | 8,190 | 30 |
| .240 | 14 | 1,048,574 | 4,094 | 14 |
| .248 | 30 | 524,286 | 2,046 | 6 |
| .252 | 62 | 262,142 | 1,022 | 2 |
| .254 | 126 | 131,070 | 510 | NA |
| .255 | 254 | 65,534 | 254 | NA |

## Private address blocks:

| | | |
|---|---|---|
| Class A | 10.0.0.0 | 10.255.255.255 |
| Class B | 172.16.0.0 | 172.31.255.255 |
| Class C | 192.168.0.0 | 192.168.255.255 |

## Ports:

| | |
|---|---|
| Well-Known Ports | 0 - 1023 |
| Registered Ports | 1024 – 49151 |
| Dynamic or Private Ports | 49152 – 65535 |

## Ports by number:

| Type | Number |
|---|---|
| FTP - Data | 20 |
| FTP - Control | 21 |
| TFTP - **UDP** | 69 |
| SMTP | 25 |
| POP3 | 110 |
| SNMP \| Trap - **UDP** | 161 \| 162 |
| DNS – **UDP** | 53 (*TCP zone transfer*) |
| TELNET | 23 |
| TIME | 37 |
| TACACS | 49 |
| FINGER | 79 |
| HTTP | 80 |
| NNTP | 119 |
| NTP | 123 |
| NETBIOS | 137-139 |
| DHCP Server –**UDP** | 67 |
| DHCP Client -**UDP** | 68 |
| RPC - **UDP** | 111 |

## Routing and Routed Protocol Basics:

Routing basics by Cisco

- *Routed* Protocols are IP, IPX and AppleTalk (AT).
- *Routing* protocols are OSPF, RIP, RIP II, EIGRP, NLSP, RTMP, etc.
- These are Internal Routing protocols where BGP would be external.
- Distance vector protocols are RIP, RIP II, IGRP, and IPX RIP.
- Link State Protocols are OSPF, NLSP, etc
- EIGRP is considered a Hybrid Routing protocol
- Important routing Protocols based on TCPIP, NOVELL or AppleTalk:
    - IP- RIP
    - IP – OSPF
    - IP – EIGRP

  - IPX – IPX RIP
  - IPX – NLSP
  - IPX – EIGRP
  - AT – RTMP
  - AT – EIGRP
- Notice EIGRP (the Hybrid) works with them all
- Scalability restraints
  - IP – **500** Workstations
  - IPX – **300** Workstation
  - AT – **200** Workstations
  - NetBios – **200** Workstations
  - Mixed – **200** Workstations
- MTU – You should be careful and avoid changing the size of the Maximum Transmission Unit, but if you do, you can improve network performance by manipulating that size to be the largest possible.
- Ipv4 Header size: **20** Bytes W/Options
- Ipv6 Header size: **40** Bytes Fixed
- Standard administrative distances for IP routes (the *lower* the number the more preferred the route will be)

| | |
|---|---|
| Directly connected interface | **0** |
| Static route using connected interface | **0** |
| Static route using IP address | **1** |
| EIGRP summary route | **5** |
| External BGP route | **20** |
| Internal EIGRP route | **90** |
| IGRP route | **100** |
| OSPF route | **110** |
| IS-IS route | **115** |
| RIP route | **120** |
| EGP route | **140** |
| External EIGRP route | **170** |
| Internal BGP route | **200** |
| Route of unknown origin | **255** |

- Update Timers for distance vector protocols:
  - IP RIP **30** seconds
  - IP IGRP **90** seconds
  - AppleTalk RTMP **10** seconds
  - IPX RIP **60** seconds
  - IPX SAP **60** seconds (SAP is not a routing protocol)
- Other Baseline and network health facts:
  - Ethernet segments should not exceed **40%** Network Utilization

- Token Ring should not exceed **70%** Network Utilization
- WAN Links should not exceed **70%** Network Utilization
- Response time should be less than **100**ms
- Broadcasts/Multicasts should be no more than **20%** of all network traffic
- On Ethernet there should be no more than **1** CRC error per **1**million bytes of data
- Cisco Router CPU Utilization should not exceed **75%**

## Routing

**(Dynamic – Static):**

- Static Routing – manually assigned by the Admin user entering the routes
- Dynamic Routing – generated/determined by a Routing Protocol

## Dynamic:

- With Dynamic Routing, routers pass information between each other so that routing tables are regularly maintained.
- The routers then determine the correct paths packets should take to reach their destinations.

Information is passed only between routers.

- A routing domain is called an Autonomous System, as it is a portion of the Internetwork under common admin authority.
- Consists of routers that share information over the same protocol. Can be split into routing areas.

## Distance Vector:

- Used in smaller networks that are have fewer than 100 routers.
- Easy to configure and use.
- As routers increase in number, you need to consider CPU utilization, convergence time, and bandwidth utilization.
- Convergence is due to routing updates at set intervals; e.g., 90 seconds.
- When a router recognizes a change it updates the routing table and sends the whole table to all of its neighbors.
- Routing loops or counting to infinity occurs because of the delay in sending updates. This problem can be fixed with:
  - *Split Horizon* - Info cannot be sent back on the interface it was received from
  - *Route Poisoning* - When the network goes down, route gets set to 16 or unreachable until it's back up

- *Hold–Downs* - Prevents routes from changing too rapidly in order to determine if a link has really failed, or is back up

## Link-state:

- Maintains Topology Database.
- Routers have formal neighbor relationship.
- Exchanges LSA (Link State Advertisement) or hello packets with directly connected interfaces.
- These are exchanged at short intervals (typically 10 sec).
- Only new info is exchanged.
- Scales well: only downside is that link–state protocols are more complex.

## Appletalk:

Cisco's Documentation on AT

| | |
|---|---|
| Application | AFP |
| Presentation | |
| Session | ADSP, ZIP, ASP, PAP |
| Transport | RTMP, *AURP*, NBP, ATP, AEP |
| Network | DDP, *AARP* |
| Datalink | ELAP, LLAP, TLAP, FLAP |
| Physical | Localtalk |

- RTMP – Routing Table Maintenance Protocol – a Distance vector protocol that has a default update timer of 10 seconds. Updates only when changes occur.
- AURP – AT Update-based Routing Protocol that allows the creation of a tunnel to interconnect two AT based networks through TCPIP to form an AT WAN. AURP uses UDP. It does not send periodic updates through the link.
- With AT, your client devices will automatically select a network address and will then broadcast a probe to ensure that it is unique.

Also, with AT – your workstations have the ability to remember the router address that sent the last RTMP packet

## EIGRP:

Cisco's Documentation on EIGRP

- Enhanced Interior Gateway Routing Protocol
- A hybrid Routing protocol
- Proprietary to Cisco
- Uses metrics: *BAN-DEL-REL-LO-MAX* (How I remember it)
  - **BAN**DWIDTH
  - **DEL**AY
  - **REL**IABILITY

- **LO**AD
- MTU (**Max**imum Transmission Unit) Notes on MTU

Note: Documentation for IGRP

## WAN and LAN protocols

## Ethernet:

Cisco documentation on Ethernet, Fast Ethernet and Gigabit.

You must know this-

| | | |
|---|---|---|
| 10base2 | Meters –185 | Cable -Thinnet |
| 10base5 | Meters –500 | Cable –Thicknet |
| 10baseT | Meters –100 | Cable -UTP |
| 100baseTX | Meters –100 | Cable -UTP |
| 100baseFX | Meters –400 | Cable -Fiber |
| 100baseT4 | Meters –100 | Cable -UTP |
| 100VG-AnyLAN | Varies | Varies |

Make sure you visit the hyperlinks of each one and do extra research.

## ATM:

Cisco's Documentation on ATM

- Asynchronous Transfer Mode
- FIXED length, 53 byte cells (48 payload +5 header).
- ATM Layers are at layer 2 while the Adaptation Layer is Layer 3.
- AAL's have the responsibility of isolating the upper layer protocols from the ATM process details.
- Frame types (or better to be called *Adaptation* layers)
  - AAL1 – will take a continues bit stream and will place it within the ATM cells, between source and destination – ATM will Require timing synchronization.
  - AAL3/4 – supports connectionless and connection-oriented data. Adds a header and a trailer whereas AAL5 does not. (Messages can be interleaved)
  - AAL5 – Also supports connectionless and connection-oriented data but also supports LANE. (LAN Emulation) AAL5 can also be referred to as SEAL (Simple and Efficient adaptation layer)
- A knowledge of ATM and its framing should be reviewed.

## PPP:

Cisco's Documentation on PPP

- Point to point protocol.
- Major benefit is the use of more protocols then just TCPIP.
- There are other protocols used
  - *LCP* – Will establish, then configure (and test) the connection
  - *NCP* – (A family of NCP's) will establish and configure the upper layer protocols.
- PPP uses HDLC as a basis to have encapsulation of Datagrams over Point-to-point links.
- HCLC –High level data link control.
- Make sure you are comfortable with the whole PPP process.

## X.25:

**Cisco's Documentation on X.25**

- A WAN protocol that operates at Layers 1-3 of the OSI
- Offers Error checking but becomes slower due to that extra checking
- X.25 Protocol suite
  - Layer 3 – *PLP* (Packet Layer Protocol) will manage the packet exchange between the DTE devices across a virtual link
  - Layer 2 – *LAPB* (Link Access Procedure B) Data Link Layer Protocol that will deal with the packet framing between the DTE and DCE devices. Operates at Layer 2. Integrated into X25. Router can be DTE or DCE. HDLC confined to ABM transmission. Job is to make sure that frames are error free. There are three different frame types: Information frames - flow control, error detection; S Frames - requesting and suspending communications; and U Frames - link setup, disconnecting, error reporting. Has high overhead, but good error checking
  - Layer 1 – (*X.21bis*) X-21bis will handle the Layer 1 aspects of activation / deactivation at speeds of up to 19.2 Kbps.
- X.25 uses other physical layer serial interfaces: EIA-TIA 232, EIA-TIA 449, EIA-530 and G.703.

## SDLC

(Synchronous Data Link Control) Cisco's Documentation on SDLC

- Main SNA link layer protocol. PTP, half, full duplex. Two node types: Primary Stations control other stations, setup and manage links. Secondary stations can only transmit to the primary and only after permission.

## HDLC

(High-Level Data Link Control) Cisco's Documentation on HDLC

- Link layer protocol for Serial links. Cisco Default. Supports the following modes: Normal Response Mode – as per Secondary under SDLC; Asynchronous Response Mode allows secondary to communicate without permission; Asynchronous Balanced mode combines the two stations. Has lower overhead than LAPB but less error checking.

## ISDN

**Cisco's Documentation on ISDN**
Cisco's Documentation on Designing ISDN networks: Click here
Supports data, text, voice, music. BRI 2 B and 1 D Channel. PRI 23B + 1D or in Europe 30 B + 1D.
ISDN Terminals – TE1 – Terminals that understand ISDN Standards; TE2 precedes ISDN standard have to use a terminal adapter. ISDN has four reference points to define logical interfaces R = TE2 to TA, S = Terminal and NT2; T= NT1 to NT2; U = NT1 and line termination equipment

## ISDN Protocols:

- **E** = Existing network
- **Q** = Switching and signaling
- **I** = Concepts, terminology and service

## Frame Relay

Cisco's Documentation on Frame Relay

- Establishes a Frame relay Virtual Circuit that is a connection between two DTE devices.
- Two circuit types: Permanent (PVC) and switched (SVC) identified by DLCI.
- Multi–protocol support: IP, DECnet, Appletalk, IPX, XNS, ISO.
- More efficient and faster than X.25 because of less error checking.
- Default encapsulation on CISCO is CISCO or can be IETF. Use IETF if connecting to non–Cisco devices with frame relay.
- DLCI – Data Link Connection Identifier – IP addresses need to be mapped to DLCI's to communicate over a virtual circuit. Can be done dynamically with IARP or manually though the map command.

- LMI - Local Management Interface – gives DLCI global rather than local significance. Makes entire frame relay network appear as typical LAN. Manages status-providing info on keep–alives, multicasting, addressing and status of virtual circuit. With version 11.2 of IOS, auto–sensed.
- Three LMI types Cisco (default) ANSI and q933a.
- Subinterfaces allow you to route IP on one virtual circuit and IPX on the other.
- Some routers have limits - 2500 can handle max of 255. Two types of sub interface *Point–to–point and multipoint*.

*Frame Relay Congestion Control*

- **DE** – Discard Eligibility used to identify traffic importance
- **FECN** (Forward Explicit Congestion Notification) – To tell others the path is congested
- **BECN** (Backward Explicit Congestion Notification) – Goes back to sending router to tell it to slow down
- **CIR** (Committed Information Rate) – Minimum bandwidth guaranteed. Choose realistic level; can choose zero if retransmission is acceptable. Can be by BC or committed burst size that allows customers to exceed CIR for limited time

*IBM networks – Source Route Bridging*

For in depth explanations on Cisco's site click here: SRB | SNA | IBM

- Bridging basics: *Creates a single data–link, flat network*
    - Transparent Bridging – Connects two or more Ethernet segments. Learns MAC address of all devices and then starts filtering.
    - Integrated Routing/Bridging – Allows you to route and bridge the same protocol by using a virtual bridge–group interface
    - Source–Route Bridging – Knows the entire route to destination before it sends data. Not designed for large networks.
    - Source–Route Transparent Bridging – Use this when you have to go across bridging domains. Affects spanning tree, as packets cannot cross over domains and therefore you cannot have multiple paths between these domains.

- Source Route Bridge (also known as –SRB)

- Route descriptors – They are bridge/ ring #'s fields in a RIF. They are used to set the path that a frame should take on a SRB network.
- SRB frames contain a RIF that has routing descriptors to the destination
- SRB networks use DLSw+ to establish a TCP link so that it can reduce NetBios / broadcast traffic queries occurring between peers.
- In SRB networking, the *SOURCE* determines the route to arrive at the destination node *BEFORE* sending information frames to it.
- In SRB networking, the source node will acquire the routes to destinations using something called *EXLORER FRAMES*.
- SRB can use STP, but does not rely on it because it is usually loop free. It would use STP when sending explorer frames to reduce the traffic on the line during its route discovery process.
- SRB is locked down to a hop count of **7** bridges.

Cisco's Documentation on Designing SRB networks: **Click here**
Cisco Documentation on Designing DLSw+ network: Click here

## Router Basics

## Router Switching:

- Process Switching
  - Packet gets copied to process buffer, address is retrieved and the packet is encapsulated and forwarded on the appropriate outbound interface. Cache is updated and subsequent packets to the same address are handled on cached info. Most processor intensive.
- Silicon Switching
  - Only 7000 Series + SSP6. The SSP is a dedicated switch processor that takes over from the router processor. Fast solution.
- Optimum Switching
  - Faster than both Fast and Netflow Switching. Replaces fast switching on high-end routers.
- Fast Switching
  - Is used when no entries exist in more efficient caches; on by default in low-end routers; sometimes necessary to disable due to memory limits or to aid troubleshooting.
- Autonomous Switching
  - Compares packets against autonomous switching cache. When a packet arrives the interface checks the switching cache closest to it. Only found on 7000 and AGS+ series routers.
- Distributed Switching

    - Happens on VIP (Versatile Interface Processor), very efficient. Gets more efficient as more VIP cards added. No need to use router processor.
- Netflow Switching
    - Admin tool increases overhead; gathers stat data, port, protocol, and user info that can be sent to a management station.

**Commands:**

- ***Show interface*** *- Will show router Layer 2 errors (CRC, collisions, etc.)*
- ***Ping | traceroute*** *- Enables you to ping and perform Route Tracing functions*
- ***Show access-lists*** *- Will display your access lists and you can also specify by number*
- ***Debug*** *- Shows real time - should be used with caution - very CPU intensive*
- ***Show {***protocol***} route*** *- Will show routing table*
- ***Show processes*** *- Will show CPU usage and CPU time*
- ***Show buffers*** *- Will show usage and misses*

## Route Summarization:

- Contiguous networks are grouped together and advertised as a single entity called a supernet.
- Move network prefix to the left (i.e., borrow bits from network portion of address) to describe a single route to contiguous block of IP addresses (Classless Inter–Domain Routing or CIDR).
- This can only be done using contiguous IP addresses.

*Note: Classful routing uses Class A, B, C addresses.*

- **IOS Software:** Familiarize yourself with IOS feature sets: Click here
- Offers a rich set of features:
    - Access lists – to filter / security
    - Proxy services – see below
    - Encryption - never use if CPU is at 65% utilization
    - Compression – to compress / WAN-serial link optimization
    - Queuing – *FIFO, Weighted fair, Priority, custom*
- Proxy services:
    - IPX GNS Request
    - IPX Watchdog Spoofing
    - Proxy ARP
    - IP Helper

## Design Fundamentals

**Hierarchical Topologies (Cisco defines a three–layered approach)**

| | |
|---|---|
| CORE | • The backbone of the network.<br>• If there is a problem here everyone is likely to be affected.<br>• Key issues: Bandwidth, Fault Tolerance, no workgroup access at this level. |
| *DISTRIBUTION* | • This is where the management really takes place.<br>• At this level you would implement filtering, security policies, routing and other support functions |
| *ACCESS* | • This is where users connect to the Internetworks.<br>• Some functions of this layer are creation of collision domains, access control, and policies.<br>• Examples of technology at this layer are DDR and Ethernet switching. |

## Cisco's Small/medium Sized Business Solution Framework

**Broken into three Categories:**

| | |
|---|---|
| Media Problems<br>*-USE A SWITCH* | • High *collision* rate<br>• High utilization<br>• Segment Collision Domains |
| Protocol Problems<br>*-USE A ROUTER* | • Protocol generating high level of *broadcasts*<br>• Segment Broadcast Domains |
| Transport Problems<br>*-USE ATM OR fast / Gigabit Ethernet* | • Bandwidth requirements need to be higher<br>• Use faster switching technologies or ATM |

**Analyzing Customer Requirements falls into two areas:**

| | |
|---|---|
| Administrative Data | • What the company does, who the contacts are, who has authorization to sign off on approval, what the company growth forecast is, whether or not a solution has been attempted before. |
| Technical Data | • Analysis of information flow, shared data, locations, network traffic between segments<br>• Broken even further into: Performance Requirements, Application Requirements, Security Requirements, and Network Management Requirements. (FCAPS) |

**Network Management:** (**FCAPS**)

| | |
|---|---|
| *F* | Fault Management |
| *C* | Configuration Management |
| *A* | Accounting Management |
| *P* | Performance Management |
| *S* | Security Management |

*Network Management straight from Cisco*: Click here

**Constraints to Design:**

| | |
|---|---|
| Business / Political Constraints | • How many people will be hired next month (Current and future staffing requirements)<br>• Business goals / motivations<br>• The corporate, geographic structure<br>• Politics and policies |
| Technical assessment - constraints | • Applications assessment – information flows, shared data – how are these constraints to design?<br>• Performance assessment questions and baselining<br>• Network management and security assessments- what are the risks? |

## Twelve steps to document the customers existing network:

| | |
|---|---|
| *1. Characterize the Customer's applications* | • Applications, type, how many users use the applications, what servers hold the applications and what segment they reside on.<br>• Map and monitor application flows – very helpful. |
| *2. Characterize the network protocols* | • Protocols, types, how many users use each of the protocols, servers using protocols. |
| *3. Document the current network* | • Document the network topology, addressing schemes and your major concerns. |
| *4. Identify the potential bottlenecks* | • **20/80 rule** (No more than 20% of network traffic should cross over into another segment – or that 80% of your traffic should stay local to that segment)<br>• Use network management tools to analyze with: Netsys, Netflow, CiscoWorks, and a Protocol analyzer/Sniffer.<br>• Cisco's Network Management Home page- click here. |
| *5. Identify the business constraints / inputs into the network design* | • Identify what kinds of business-based constraints can affect your network design, like politics, people being hired and a future layoff that could affect you. |
| *6. Characterize the existing network availability* | • Which segments are critical?<br>• Concern yourself with the MTBF (Mean time between failures)<br>• What is the cost to the company for major outages. |
| *7. Characterize the network performance* | • This simply means to measure the response times that are between your hosts.<br>• Helpful for baselining. |
| *8. Characterize the existing network reliability* | • Documenting the traffic can very well be your most time consuming effort. |

| | |
|---|---|
| | • You can use a protocol analyzer for the task.<br>• You basically want to start documenting the total MB's, # of frames, CRC errors, MAC layer errors, and total broadcasts / multicasts. |
| *9. Characterize the network utilization* | • You need to determine peak network utilizations.<br>• *For example*: Ethernet should not peak for more than one minute at 40% - because this is not good network performance and utilization. |
| *10. Characterize the status of your major routers* | • This is where your command (listed above) comes into play.<br>• *Show* interfaces, process, etc. |
| *11. Characterize the existing network management tools* | • Characterize the list of tools that are available to you to use for design purposes. |
| *12. Summarize the health of the existing network* | • Use these findings to make a summarization-<br>○ Ethernet segments should not exceed **40%** Network Utilization<br>○ Token Ring should not exceed **70%** Network Utilization<br>○ WAN Links should not exceed **70%** Network Utilization<br>○ Response time should be less than **100**ms<br>○ Broadcasts/Multicasts should be no more than **20%** of all network traffic<br>○ On Ethernet there should be no more than **1** CRC error per **1**million bytes of data<br>○ Cisco Router CPU Utilization should not exceed **75%** |

## Fields for documenting the customer's existing applications: (Step 1)

| Application | Application type | # Of users | # Of hosts or servers | Segment | Comments |
|---|---|---|---|---|---|
| *Identify each application Running on the network* | *Characterize the type of application Database, Web* | *# Of users for each application* | *How many servers provide each of the applications* | *The segments the applicatio n runs on* | *Comments that could be useful at a later time* |

## Fields for documenting the customers existing Protocols: (Step 2)

| Protocol | Protocol type | # Of users | # Of hosts or servers | Comments |
|---|---|---|---|---|
| *Identify each Protocol Running on the network* | *Characterize the type of Protocol – routing, routed, LAN* | *# Of users for each Protocol* | *How many use each of the Protocols* | *Comments that could be useful at a later time* |

## Three Part Firewall:

| External: | DMZ (De-Militarized Zone): (Isolation LAN) | Internal: |
|---|---|---|
| *On the outside of the isolation LAN is a router that will implement access lists to filter traffic usually from the Internet.* | • *In the isolation LAN, hosts are installed to provide WWW, FTP, mail relay and DNS services to name a few.*<br>• *These isolated hosts are named **bastion hosts**.* | *An internal filtering router permits access to the internal LAN from the isolation LAN or to filter it.* |

Note: A PIX Firewall is Cisco's Firewall based product, but remember that the IOS has a Firewall / NAT based feature set.

## Design Document Components:

Responding to an RFP (Request for Proposal)

| | |
|---|---|
| Executive Summary | • Directed to decision makers.<br>• Provides an explanation of the purpose of the project, a list of strategic recommendations and a description of how the solution meets the customers requirements. |
| *Design Requirements* | • Shows current topology, current applications and current network health.<br>• Lists performance and scalability requirements, business requirements and constraints and expected performance. |
| *Design Solution* | • Shows the proposed network topology, selected hardware and media, suggested routing protocols and proposed network management tools. |
| *Summary* | • Provides a concise summary of the solution and a description of how the solution meets the requirements. |
| *Appendixes* | • Lists contacts and provides additional information about products, circuit information and prototype results. |
| *Cost (Optional)* | • Provides an itemized and detailed cost listing of equipment to be purchased. |

## Network Management:

Cisco documentation on SNMP and RMON

| | |
|---|---|
| Managed device | Is a router or switch with agent software. |
| NMS | Runs network management applications. Polls devices for SNMP information and configuration. |
| Agent | Gather statistics. |

## More Products:

| | |
|---|---|
| CiscoWorks for Windows | • Suite of integrated network management tools designed to simplify the administration and maintenance of small-to-medium sized business networks or workgroups.<br>• Runs on NT. |
| CiscoWorks Blue | • Suite of products designed to simplify management of a consolidated SNA and IP network. |
| CiscoWorks2000 | • A family of products based on Internet standards for managing Cisco enterprise networks and devices.<br>• It includes Resource Manager Essentials and |

| | |
|---|---|
| | CWSI Campus.<br>• It runs on UNIX or Windows NT. |
| CiscoView | • GUI-based device management software application that provides dynamic status, statistics and comprehensive configuration information for Cisco systems internetworking products.<br>• Displays a graphical real-time physical view of Cisco devices. |
| Cisco ConfigMaker | • An easy-to-use Microsoft Windows application used to configure a small network of Cisco routers, switches, hubs and other network devices from a single PC, without requiring knowledge of Cisco IOS. |
| Netsys Baseliner | • Tool that displays, debugs and validates your network configuration.<br>• Tests configurations and changes offline before committing them to the live network. |
| RMON<br><br>Cisco Site | • Used to provide more information and can work offline in continuous manner.<br>• Mainly used to monitor packet and traffic patterns on LAN Segments. |
| Traffic Director | • Has the RMON features of monitoring traffic, user definable thresholds, multidomain view. |

For a detailed list of most of Cisco's Network Management tools: Click here

## Routers and Switches:

Make yourself familiar with the Product lines: Click here
Click here for a Switches index: click here
Core High-end routers: Click here
Routers: Click here | Switches: Click here

## Test your design:

(Determining the Appropriate Testing Plan)

- Pilot – Very small implementation, used to get your point across
- Prototype – A *larger* scale and costly test of your design.

## Notes for study and test:

- Make sure you have studied thoroughly; you will be asked in depth questions from every corner of your study guides.
- Make sure you have enough practice with case studies. This is not a test for you to just memorize all these facts. You need to know how to implement them. Therefore, practice the case studies. Click here
- Make sure you are comfortable with the Cisco Product line. You will be expected (like any good designer) too offer your advice on what products to implement for the best price.
- Use the Cisco Site – you can look at most of your information right from the Documentation provided to you. Click here