TOP DOWN NETWORK DESIGN METHODOLOGY

PHASE 2: – LOGICAL DESIGN

During the logical network design phase, the network designer develops does the following:-

- Network topology depending on the size of the network and traffic characteristics, the topology can range from simple to complex, requiring hierarchy and modularity.
- Devises a network layer addressing model and selects switching and routing protocols.
- Logical design also includes security planning, network management design, and the initial investigation into which service providers can meet WAN and remote-access requirements.

In this phase we look at the following:-

- Design Network Topology
- Designing Models for Addressing and Naming
- Selecting Switching and Routing Protocols
- Developing Network Security Strategies
- Developing Network Management Strategies

a) Design Network Topology

Topology: - A branch of mathematics concerned with those properties of geometric configurations that are unaltered by elastic deformations such as stretching or twisting. It is also a term used in the computer networking field to describe the structure of a network.

Network Topology Design Themes

- Hierarchy
- Redundancy
- Modularity
- Well-defined entries and exits
- Protected perimeters

Hierarchy

A typical Hierarchical Design Model

- A core layer of high-speed routers and switches optimized for availability and performance
- A distribution layer of routers and switches that implement policies
- An access layer that connects users via low-end switches and wireless access points

Why Use a Hierarchical Model?

- Reduces workload on network devices i.e. Avoids devices having to communicate with too many other devices (reduces "CPU adjacencies")
- Constrains broadcast domains
- Using a hierarchical model can lead to minimization of costs: can purchase the appropriate internetworking devices for each layer of the hierarchy, and avoiding expenses on unnecessary features for a layer.
- The modular nature of the hierarchical design model enables accurate capacity planning within each layer of the hierarchy, thus reducing wasted bandwidth.
- Network management responsibility and network management systems can be distributed to the different layers of modular network architecture to control management costs.
- Modularity enables you to keep each design element simple and easy to understand.
- Testing a network design is made easy because there is clear functionality at each layer.
- Fault isolation is improved because network technicians can easily recognize the transition points in the network to help them isolate possible failure points.
- As elements in a network require change, the cost of making an upgrade is contained to a small subset of the overall network. In large flat or meshed network architectures, changes tend to impact a large number of systems. Replacing one device can affect numerous networks because of the complex interconnections.
- When scalability is a major goal, a hierarchical topology is recommended because modularity in a design enables creating design elements that can be replicated as the network grows.
  - Because each instance of a module is consistent, expansion is easy to plan and implement.
  - For example, planning a campus network for a new site might simply be a matter of replicating an existing campus network design.

Role of the Three-Layer Hierarchical Model

a) Core Layer

The core layer is the high-speed backbone of the internetwork. Because the core layer is critical for interconnectivity,

- One should design the core layer with redundant components.
- It should be highly reliable and should adapt to changes quickly.
- It should use routing features that optimize packet throughput.
- It should avoid using packet filters or other features that slow down the manipulation of packets.
- It should optimize the core for low latency and good manageability.

The core should have a limited and consistent diameter. That leads to predictable performance and ease of troubleshooting.

In case of need to connect to other enterprises via an extranet or the Internet, the core topology should include one or more links to external networks.

b) Distribution Layer

This layer has many roles, including:-

Controlling access to resources for security reasons and

- Controlling network traffic that traverses the core for performance reasons.
- The distribution layer is often the layer that delineates broadcast domains.
- In network designs that include virtual LANs (VLAN), the distribution layer can be configured to route between VLANs.
- The distribution layer allows the core layer to connect sites that run different protocols while maintaining high performance.
- To maintain good performance in the core, the distribution layer can redistribute between bandwidth-intensive access layer routing protocols and optimized core routing protocols.
- To improve routing-protocol performance, the distribution layer can summarize routes from the access layer.
- To maximize hierarchy, modularity, and performance, the distribution layer should hide detailed topology information about the access layer from core routers, and vice versa.

Access Layer

The access layer provides users on local segments with access to the internetwork.

- The access layer can include routers, switches, bridges, shared-media hubs, and wireless access points.
- Switches are often implemented at the access layer in campus networks to divide up bandwidth domains to meet the demands of applications that need a lot of bandwidth or cannot withstand the variable delay characterized by shared bandwidth

Redundancy

Redundant network designs enables meeting requirements for availability, attempts to eliminate single point of failure on network. The goal is to duplicate any required component whose failure could disable critical applications

The components used are:-

- Core router, a switch, a link between two switches,
- A channel service unit (CSU), a power supply,
- A WAN trunk, Internet connectivity,

Possible choices:

- Complete redundant, e.g., of data centers, to enable business survivability and performance benefits from load sharing.
- Less-comprehensive level of redundancy constrains network operational expenses.
- Implementing redundancy on campus networks can help meet availability goals for users accessing local services.
- Implementing redundancy on the edge of the enterprise network ensures high availability for Internet, extranet, and virtual private network (VPN) access.

Selection should be guided by:-

- Analysis the business and technical goals of customer
- Critical applications, internetworking devices, and links.
- Analysis of customer’s tolerance for risk and the consequences
- Tradeoffs of redundancy versus low cost, and simplicity versus complexity.
- Redundancy adds complexity to the network topology and to network addressing and routing.

Redundancy entails the following:-

i) Backup Paths

Purpose: maintain interconnectivity even when one or more links are down.

- Consists of routers and switches and individual backup links between them.
- Estimate of performance for a redundant network design is informed by two aspects:
- How much capacity the backup path supports
- How quickly the network will begin to use the backup path
- Backup paths must be tested:- Where backup links are also used for load sharing, there is advantage that backup path is a tested solution

ii) Load Sharing

The primary purpose of redundancy is to meet availability requirements.

- A secondary goal is to improve performance by supporting load sharing across parallel links.
- Load sharing, (load balancing), allows two or more interfaces or paths to share traffic load.

How Do You Know When You Have a Good Design?

- When you already know how to add a new building, floor, WAN link, remote site, e-commerce service, and so on
- When new additions cause only local change, to the directly-connected devices
- When your network can double or triple in size without major design changes
- When troubleshooting is easy because there are no complex protocol interactions to wrap your brain around

b) Designing Models for Addressing and Naming

Guidelines for Addressing and Naming

- Use a structured model for addressing and naming
- Assign addresses and names hierarchically
- Decide in advance if you will use
  - Central or distributed authority for addressing and naming
  - Public or private addressing
  - Static or dynamic addressing and naming

Advantages of Structured Models for Addressing & Naming

- It makes it easier to
  - Read network maps
  - Operate network management software
  - Recognize devices in protocol analyzer traces
  - Meet goals for usability
  - Design filters on firewalls and routers
  - Implement route summarization

Public IP Addresses

- Managed by the Internet Assigned Numbers Authority (IANA)
- Users are assigned IP addresses by Internet service providers (ISPs).
- ISPs obtain allocations of IP addresses from their appropriate Regional Internet Registry (RIR)

Regional Internet Registries (RIR)

- **American Registry for Internet Numbers (ARIN) serves North America and parts of the Caribbean.**
- **RIPE Network Coordination Centre (RIPE NCC) serves Europe, the Middle East, and Central Asia.**
- **Asia-Pacific Network Information Centre (APNIC) serves Asia and the Pacific region.**
- **Latin American and Caribbean Internet Addresses Registry (LACNIC) serves Latin America and parts of the Caribbean.**
- **African Network Information Centre (AfriNIC) serves Africa.**

Private Addressing

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

Criteria for Using Static Vs. Dynamic Addressing

- The number of end systems
- The likelihood of needing to renumber
- The need for high availability
- Security requirements
- The importance of tracking addresses
- Whether end systems need additional information
    - (DHCP can provide more than just an address)

Designing Networks with Subnets

- Determining subnet size
- Computing subnet mask
- Computing IP addresses

Guidelines for Assigning Names

- Names should be
    - Short
    - Meaningful
    - Unambiguous
    - Distinct
    - Case insensitive
- Avoid names with unusual characters such as asterisks

c) *Selecting Switching and Routing Protocols*

Decisions about protocols and technology should be based on information already gathered. Four factors involved in making sound decisions include:-

- Goals which must be established
- Many options should be employed
- The consequences of the decision should be investigated
- Contingency plans should be made

After decision is made, troubleshoot it:

- If this option is chosen what could go wrong
- Has this option been tried before (possibly with other customers)? If so, what problems occurred?
- How will the customer react to this decision?
- What are the contingency plans if the customer does not approve of the decision?

Selection Criteria for Switching and Routing Protocols

- Network traffic characteristics
- Bandwidth, memory, and CPU usage
- The number of peers supported
- The capability to adapt to changes quickly
- Support for authentication

Switching

- Layer 2 transparent bridging (switching)
- Multilayer switching
- Spanning Tree Protocol enhancements
- VLAN technologies

Routing

- Static or dynamic
- Distance-vector and link-state protocols
- Interior and exterior

SELECTING SWITCHING PROTOCOLS

Switches

Switches can do *store-and-forward* processing or *cut-through* processing. One disadvantage of cut-through is forwarding of illegal frames (runt) and frames with CRC errors. What is the way forward?

Adaptive cut-through switches:

- Able to automatically move from cut-through mode to store-and-forward mode when error threshold is reached

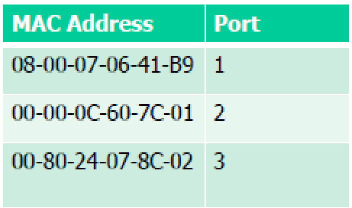
- Switches do parallel forwarding:
- Support for (numerous) simultaneous forwarding paths depending on the structure of the *switching fabric*

Transparent bridging concept

Ethernet switches and bridges use a classic technology called *transparent bridging*. A *transparent bridge* connects one or more LAN segments so that end systems on different segments can communicate with each other transparently. An end system sends a frame to a destination without knowing whether the destination is local or on the other side of a transparent bridge. Transparent bridges are so named because their presence is transparent to end systems.

To learn how to forward frames, a transparent bridge listens to all frames and determines which stations reside on which segments. The bridge learns the location of devices by looking at the source address in each frame. The bridge develops a *switching table* such as the one shown below. The switching table also sometimes goes by the names *bridging table* or *MAC address table*.

Example



MAC Address	Port
08-00-07-06-41-B9	1
00-00-0C-60-7C-01	2
00-80-24-07-8C-02	3

SWITCHING PROTOCOLS

Spanning Tree Protocol (STP)

Transparent bridges and switches implement the spanning tree protocol (STP). STP is a protocol and algorithm, for dynamically "pruning" an arbitrary topology of connected Layer 2 switches into a spanning tree. The topology that results spans the entire switched domain and is shaped like a mathematical tree, with branches that spread out from a stem without forming loops or polygons. The network designer physically connects switches in a meshed, redundant topology, but STP creates a logical tree with no redundancy.

The spanning tree has one Root Bridge and a set of ports on other bridges that forward traffic toward the root bridge. Bridges send bridge protocol data unit (BPDU) frames to each other to build and maintain the spanning tree. BPDUs identify the root bridge and help the other bridges compute their lowest-cost path to the root.

Bridges send *topology change notification BPDUs* when bridge ports change state. Bridges send *configuration BPDUs* every 2 seconds to maintain the spanning tree. BPDUs are sent to the Bridge Group Address 01:80:C2:00:00:00.

Rapid Spanning Tree Protocol

In 2004, the IEEE incorporated its 802.1w standard, "Rapid Reconfiguration of Spanning Tree," into the IEEE 802.1D standard. The goal of the 802.1w committee was to standardize an improved mode of switch operation that reduces the time STP takes to converge to a least-cost spanning tree and to restore service after link failures.

With the original 802.1D standard, networks took almost a minute to converge. In a properly configured network, the new 802.1D Rapid Spanning Tree Protocol (RSTP) can achieve convergence or re-convergence in a few hundred milliseconds.

With RSTP, bridge ports can be in one of three states:

- **Discarding:** A port that is neither learning MAC addresses nor forwarding users' frames
- **Learning:** A port that is learning MAC addresses to populate the MAC-address table but is not yet forwarding user frames
- **Forwarding:** A port that is learning MAC addresses and forwarding user frames

The original STP passively waited for the network to converge before it transitioned a port into the forwarding state. To achieve quick convergence, a network administrator had to carefully tune the conservative default values for the Maximum Age and Forward Delay timers, which put the stability of the network at stake. RSTP, on the other hand, can actively confirm that a port can safely transition to the forwarding state without having to rely on any timer configuration. There is now a synchronization mechanism that takes place between RSTP-compliant bridges so that they actively build the topology as quickly as possible.

PROTOCOLS FOR TRANSPORTING VLAN INFORMATION

VLAN Trunk Protocol

The Cisco VLAN Trunk Protocol (VTP) is a switch-to-switch and switch-to-router VLAN management protocol that exchanges VLAN configuration changes as they are made to the network.

It does the following:-

- VTP manages the addition, deletion, and renaming of VLANs on a campus network without requiring manual intervention at each switch.
- VTP also reduces manual configuration by automatically configuring a new switch or router with existing VLAN information when the new switch or router is added to the network.

In large switched networks, you should divide the network into multiple VTP domains. Dividing the network into multiple domains reduces the amount of VLAN information each switch must maintain. A switch accepts VLAN information only from switches in its domain. VTP domains are loosely analogous to autonomous systems in a routed network where a group of routers share common administrative policies.

Multiple VTP domains are recommended on large networks. On medium-size and small networks, a single VLAN domain is sufficient and minimizes potential problems.

Cisco switches can be configured in VTP server, client, or transparent mode.

- **Server mode** is the default. In VTP server mode, you can create, modify, and delete VLANs. VTP servers save their VLAN configurations when they are powered down.
- **VTP clients** exchange information with other VTP clients and servers, but you cannot create, change, or delete VLANs on a VTP client. You must do that on a VTP server.
- VTP clients do not save their VLAN configurations when powered down. Nevertheless, most switches should be clients to avoid VLAN information becoming desynchronized if updates are made on many switches.
- A **VTP transparent** switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. However, VTP-transparent switches do forward received VTP advertisements to other switches.
- Use transparent mode when a switch in the middle of the topology does not need to match other switch configurations but would cause problems for other switches if it did not forward VLAN information.

Switches need method to ensure intra-VLAN traffic goes to correct interfaces (only).

How? Tag each frame with VLAN information

Dynamic trunk protocol (DPT)

- Supports switch negotiation with remote to enable or disable 802.1QVLAN trunking protocol (VTP)
- Switch-to-switch and switch-to-router VLAN management protocol that exchanges VLAN configuration changes as they are made on the network

SELECTING ROUTING PROTOCOLS

A routing protocol

- Lets a router learn how to reach other networks
- Exchange this information with other routers or hosts
- Selecting router protocol is hard because there are so many options

Routing protocol considerations

- Send complete routing table to other routers or send specific information on status of directly connected links
- Send periodic Hello packets or not
- Share dynamic (learned) information or static configuration information
- Differ in scalability and performance characteristics
- Some perform well in static environment but has challenges in converging to a new topology when changes occur

Static and Dynamic Routing

The physical topology of an enterprise network provides the structure for forwarding data. Routing provides the mechanism that makes it work. Finding the best path to the destination becomes very difficult in an enterprise network, because a router can have many sources of information from which to build its routing table.
A ***routing table*** is a data file that exists in RAM and stores information about directly connected and remote networks. The routing table associates each network with either an exit interface or a next hop.

The ***exit interface*** is the physical path that the router uses to move the data closer to the destination. The next hop is an interface on a connected router that moves the data closer to the final destination.

The table also attaches a number to each route that represents the trustworthiness or accuracy of the source of the routing information. This value is the ***administrative distance***. (Rating of trustworthiness of a routing information source), For a Cisco router it is expressed as a numeric value of between 0 and 255. (The higher the value the lower the trustworthiness rating). Routers maintain information about directly connected, static, and dynamic routes.

A directly connected network attaches to a router interface. Configuring the interface with an IP address and subnet mask allows the interface to become a host on the attached network. The network address and subnet mask of the interface, along with the interface type and number, appear in the routing table as a directly connected network.

Static Routes

Static routes are routes that a network administrator manually configures. A static route includes the network address and subnet mask of the destination network, along with the exit interface or the IP address of the next hop router. The routing table designates static routes with an S. Static routes have the lowest administrative distance, because static routes are more stable and reliable than routes learned dynamically.

Configuring a static route

The global command for configuring most static routes is IP route, followed by the destination network, the subnet mask, and the path used to reach it. The command is:-

```
Router(config)#ip route [network-address] [subnet mask] [address of next hop OR exit interface]
```

Using the next-hop address or the exit interface forwards traffic to the proper destination. However, these two parameters behave very differently. Before a router forwards any packet, the routing table process determines which exit interface to use. Static routes configured with exit interfaces require a single routing table lookup. Static routes configured with the next-hop parameter must reference the routing table twice to determine the exit interface. In an enterprise network, static routes configured with exit interfaces are ideal for point-to-point connections like those between a border router and the ISP.

Dynamic Routes

Dynamic routing protocols also add remote networks to the routing table. Dynamic routing protocols enable routers to share information about the reachability and status of remote networks through network discovery. Each protocol sends and receives data packets while locating other routers and updating and maintaining routing tables. Routes learned through a dynamic routing protocol are identified by the protocol used. For example, R for RIP and D for EIGRP. They are assigned the administrative distance of the protocol.

Dynamic routing protocols are classified into two major categories: distance vector protocols and link-state protocols.

DISTANCE VECTOR ROUTING PROTOCOLS

Routers running distance vector routing protocols share network information with directly connected neighbors. The neighbor routers then advertise the information to their neighbors, until all routers in the enterprise learn the information.

A router running a distance vector protocol does not know the entire path to a destination; it only knows the distance to the remote network and the direction, or vector. Its knowledge comes through information from directly connected neighbors.

Like all routing protocols, distance vector protocols use a metric to determine the best route. Distance vector protocols calculate the best route based on the distance from a router to a network. An example of a metric used is ***hop count***, which is the number of routers, or hops, between the router and the destination.

Distance vector protocols usually require less complicated configurations and management than link-state protocols. They can run on older, less powerful routers and require lower amounts of memory and processing.

Routers using distance vector protocols broadcast or multicast their entire routing table to their neighbors at regular intervals. If a router learns more than one route to a destination, it calculates and advertises the route with the lowest metric.

This method of moving routing information through large networks is slow. At any given moment, some routers may not have the most current information about the network. This limits the scalability of the protocols and causes issues such as routing loops.

Examples

1. ROUTING INFORMATION PROTOCOL (RIP)

RIPv1 was the first and only IP routing protocol available in the early days of networking. RIPv1 does not send subnet mask information in its routing updates and, therefore, does not support VLSM and CIDR.
RIPv1 automatically summarizes networks at the classful boundary, treating all networks as though they were default classes A, B, and C. As long as networks are contiguous, such as 192.168.1.0, 192.168.2.0, and so on, this feature may not pose a serious problem.

By default, RIPv1 broadcasts its routing updates to all connected routers every 30 seconds.
RIP v2 has many of the features of RIPv1. It also includes important enhancements. RIPv2 is a classless routing protocol that supports VLSM and CIDR. A subnet mask field is included in v2 updates, which allows the use of discontiguous networks.

Both versions of RIP send their entire routing table out all participating interfaces in updates. RIP v1 broadcasts these updates to 255.255.255.255. This requires all devices on a broadcast network like Ethernet to process the data. RIP v2 multicasts its updates to 224.0.0.9. Multicasts take up less network bandwidth than broadcasts. Devices that are not configured for RIPv2 discard multicasts at the Data Link Layer.

Attackers often introduce invalid updates to trick a router into sending data to the wrong destination or to seriously degrade network performance. Invalid information can also end up in the routing table due to poor configuration or a malfunctioning router. Encrypting routing information hides the content of the routing table from any routers that do not possess the password or authentication data. RIPv2 has an authentication mechanism, whereas RIPv1 does not.

Common features to both RIPv1 and RIPv2

- Hop-count metric
- 15-hop maximum
- TTL equals 16 hops
- Default 30-second update interval
- Updates using UDP port 520
- Administrative distance of 120

When a router starts up, each RIP-configured interface sends out a request message. This message requests that all RIP neighbors send their complete routing tables. RIP-enabled neighbors send a response message that includes known network entries. The receiving router evaluates each route entry based on the following criteria:

- If a route entry is new, the receiving router installs the route in the routing table.
- If the route is already in the table and the entry comes from a different source, the routing table replaces the existing entry if the new entry has a better hop count.
- If the route is already in the table and the entry comes from the same source, it replaces the existing entry even if the metric is not better.

The startup router then sends a triggered update out all RIP-enabled interfaces containing its own routing table. RIP neighbors are informed of any new routes.

Problems with RIP

Various performance and security issues arise when using RIP.

- The first issue concerns routing table accuracy. Both versions of RIP automatically summarize subnets on the classful boundary. This means that RIP recognizes subnets as a single Class A, B, or C network. Enterprise networks typically use classless IP addressing and a variety of subnets, some of which are not directly connected to each other, which creates discontiguous subnets.

- Another issue to consider is the broadcast nature of RIP updates. As soon as the RIP configuration lists a network command for a given network, RIP immediately begins to send advertisements out all interfaces that belong to that network. These updates may not be needed on all portions of a network.
- The routing update could also be intercepted by any device. This makes the network less secure.
- A network running RIP needs time to converge. Some routers may contain incorrect routes in their routing tables until all routers have updated and have the same view of the network.
- Erroneous network information may cause routing updates and traffic to loop endlessly as they count to infinity. In the RIP routing protocol, infinity occurs when the hop count is 16.
- The simple hop count metric used by RIP is not an accurate way to determine the best path in complex networks. Additionally, the RIP limitation of 15 hops can mark distant networks as unreachable.
- RIP issues periodic updates of its routing table, which consumes bandwidth, even when no network changes have occurred. Routers must accept these updates and process them to see if they contain updated route information.
- Updates passed from router to router take time to reach all areas of the network. As a result, routers may not have an accurate picture of the network. Routing loops can develop due to slow convergence time, which wastes valuable bandwidth.
- These characteristics limit the usefulness of the RIP routing protocol within the enterprise environment.

2. ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL (EIGRP)

The limitations of RIP led to the development of more advanced protocols. Networking professionals required a protocol that would support VLSM and CIDR, scale easily, and provide faster convergence in complex enterprise networks.

Cisco developed EIGRP as a proprietary distance vector routing protocol. It has enhanced capabilities that address many of the limitations of other distance vector protocols. EIGRP shares some of features of RIP, while employing many advanced features.

Although configuring EIGRP is relatively simple, the underlying features and options are complex. EIGRP contains many features that are not found in any other routing protocols. All of these factors make EIGRP an excellent choice for large, multi-protocol networks that employ primarily Cisco devices.

The two main goals of EIGRP are to provide a loop-free routing environment and rapid convergence. To achieve these goals, EIGRP uses a different method than RIP for calculating the best route. The metric used is a composite metric that primarily considers bandwidth and delay. This metric is more accurate than hop count in determining the distance to a destination network.

The Diffusing Update Algorithm (DUAL) used by EIGRP guarantees loop-free operation while it calculates routes. When a change occurs in the network topology, DUAL synchronizes all affected routers simultaneously. For these reasons, the administrative distance of EIGRP is 90, whereas the administrative distance of RIP is 120. The lower number reflects the increased reliability of EIGRP and the increased accuracy of the metric. If a router learns routes to the same destination from both RIP and EIGRP, it chooses the EIGRP route over the route learned through RIP.

EIGRP tags routes learned from another routing protocol as external. Because the information used to calculate these routes is not as reliable as the metric of EIGRP, it attaches a higher administrative distance to the routes.

EIGRP is a good choice for complex enterprise networks that are composed primarily of Cisco routers. Its maximum hop count of 224 supports large networks. EIGRP can display more than one routing table because it can collect and maintain routing information for a variety of routed protocols, routing table reports routes learned both inside and outside the local system.

Unlike other distance vector protocols, EIGRP does not send complete tables in its updates. EIGRP multicasts partial updates about specific changes to only those routers that need the information, not to all routers in the area. These are called bounded updates because they reflect specific parameters. Instead of sending periodic routing updates, EIGRP sends small hello packets to maintain knowledge of its neighbors. Since they are limited in size, both bounded updates and hello packets save bandwidth while keeping network information fresh.

EIGRP Metrics and Convergence

EIGRP uses a composite metric value to determine the best path to a destination. This metric is determined from the following values:

- Bandwidth
- Delay
- Reliability
- Load

Issues and Limitations of EIGRP

Although EIGRP is a powerful and sophisticated routing protocol, several considerations limit its use:

- Does not work in a multi-vendor environment because it is a Cisco proprietary protocol
- Works best with a flat network design
- Must share the same autonomous system among routers and cannot be subdivided into groups.
- Can create very large routing tables, which requires large update packets and large amounts of bandwidth.
- Uses more memory and processor power than RIP
- Works inefficiently when left on the default settings
- Requires administrators with advanced technical knowledge of the protocol and the network

EIGRP offers the best of distance vector routing, while using additional features typically associated with link-state routing protocols, including bounded updates and neighbor adjacencies. Successful implementation of the many features of EIGRP requires careful configuration, monitoring, and troubleshooting.

LINK STATE PROTOCOLS

Enterprise networks and ISPs use link-state protocols because of their hierarchical design and ability to scale for large networks. Distance vector routing protocols are usually not the right choice for a complex enterprise network.

1. OPEN SHORTEST PATH FIRST (OSPF)

OSPF is an open standard routing protocol, developed by the Internet Engineering Task Force (IETF) to support IP traffic. OSPF is a classless interior gateway protocol (IGP). It divides the network into different sections, which are referred to as areas. This division allows for greater scalability. Working with multiple areas allows the network administrator to selectively enable route summarization and to isolate routing issues within a single area.

Link-state routing protocols, such as OSPF, do not send frequent periodic updates of the entire routing table. Instead, after the network converges, a link-state protocol sends an update only when a change in the topology occurs, such as a link going down. In addition, OSPF performs a full update every 30 minutes.

Link-state routing protocols like OSPF work well for larger hierarchical networks where fast convergence is important.

Compared with distance vector protocols, link-state routing protocols:-

- Requires more complex network planning and configuration
- Requires increased router resources
- Requires more memory for storing multiple tables
- Requires more CPU and processing power for the complex routing calculations

With the high performance of routers available today, however, these requirements are usually not a problem.

Routers running RIP receive updates from their immediate neighbors, but with no details about the network as a whole. Routers running OSPF generate a complete map of the network from their own viewpoint. This map allows them to quickly determine loop-free alternate paths in the case of a network link failure.

OSPF does not automatically summarize at major network boundaries. Additionally, Cisco's implementation of OSPF uses bandwidth to determine the cost of a link. This cost metric is used by OSPF to determine the best path. A link with higher bandwidth results in a lower cost. The lowest cost route to a destination is the most desirable path. The router trusts a metric based on bandwidth more than one based on hop count to establish the shortest path. The administrative distance of OSPF is 110, lower than RIP, because of the trustworthiness, or accuracy, of the metric.

OSPF Metrics and Convergence

OSPF bases the cost metric for an individual link on its bandwidth or speed. The metric for a particular destination network is the sum of all link costs in the path. If there are multiple paths to the network, the path with the lowest overall cost is the preferred path and is placed in the routing table.

2. INTERMEDIATE SYSTEM-TO-INTERMEDIATE SYSTEM (IS-IS)

Intermediate System-to-Intermediate System (IS-IS) is a dynamic link-state protocol developed for use Interconnection (OSI) protocol suite. Integrated IS-IS is an implementation of IS-IS for mixed OSI and limited popularity for use within large, hierarchical IP networks, especially within the core of large ISPs. It is a gateway routing protocol that is similar in operation to OSPF although somewhat more flexible, efficient, as with OSPF, IS-IS can be implemented in a hierarchical fashion. A router can play different roles:

- Level 1 routers route within an area.
- Level 2 routers route between areas.
- Level 1–2 routers participate in Level 1 intra-area routing and Level 2 inter area routing.

NOTE

From a Level 1 router's point of view, sending traffic outside the area involves finding the nearest Level router relies on the Level 2 router to reach the destination. The path taken can be suboptimal if some Level 2 routers are poorly located or have poor connectivity to the destination network. The choice based on detailed information.

CHOOSING BETWEEN DISTANCE-VECTOR AND LINK-STATE PROTOCOLS

Recommend distance vector if:

- Network uses a simple, flat topology and does not required hierarchical design
- Network uses simple hub-and-spoke topology
- Administrators do not have enough expertise to operate and troubleshoot link-state
- Worst case convergence times in the network are not a concern

Recommend Link-state if:

- Network design is hierarchical
- Administrators have the expertise required for link-state protocol
- Fast convergence of the network is crucial

Selection Criteria for Switching and Routing Protocols

- Network traffic characteristics
- Bandwidth, memory, and CPU usage
- The number of peers supported
- The capability to adapt to changes quickly
- Support for authentication

Making Decisions

- Goals must be established
- Many options should be explored
- The consequences of the decision should be investigated
- Contingency plans should be made
- A decision table can be used

Selecting Routing Protocols

- They all have the same general goal:
  - To share network reachability information among routers
- They differ in many ways:
  - Interior versus exterior
  - Metrics supported
  - Dynamic versus static and default
  - Distance-vector versus link-sate
  - Classful versus classless
  - Scalability

Interior versus Exterior Routing Protocols

- Interior routing protocols are used within an autonomous system
- Exterior routing protocols are used between autonomous systems

Autonomous system (two definitions that are often used):

- “A set of routers that presents a common routing policy to the internetwork”
- “A network or set of networks that are under the administrative control of a single entity”

Routing Protocol Metrics

- Metric: the determining factor used by a routing algorithm to decide which route to a network is better than another
- Examples of metrics:
  - Bandwidth - capacity
  - Delay - time
  - Load - amount of network traffic
  - Reliability - error rate
  - Hop count - number of routers that a packet must travel through before reaching the destination network
  - Cost - arbitrary value defined by the protocol or administrator

BORDER GATEWAY PROTOCOL (BGP)

- Allows routers in different autonomous systems to exchange routing information
  - Exterior routing protocol
  - Used on the Internet among large ISPs and major companies
- Supports route aggregation
- Main metric is the length of the list of autonomous system numbers, but BGP also supports routing based on policies
- The selection of switching and routing protocols should be based on an analysis of
  - Goals
  - Scalability and performance characteristics of the protocols
- Transparent bridging is used on modern switches
  - But other choices involve enhancements to STP and protocols for transporting VLAN information
- There are many types of routing protocols and many choices within each type

d) Developing Network Security Strategies

Developing security strategies that can protect all parts of a complicated network while having a limited effect on ease of use and performance is one of the most important and difficult tasks related to network design.

Security design is challenged by the complexity and porous nature of modern networks that include public servers for electronic commerce, extranet connections for business partners, and remote access services for users reaching the network from home, customer sites, hotel rooms, Internet cafes, and so on.

To help handle the difficulties inherent in designing network security for complex networks, this chapter teaches a systematic, top-down approach that focuses on planning and policy development before the selection of security products.

Network Security Design

To effectively plan and execute a security strategy, the security design process consists of the following steps:-

1. Identification of network assets.
2. Analysis of security risks.
3. Analysis of security requirements and tradeoffs.
4. Development of a security plan.
5. Defining a security policy.
6. Developing procedures for applying security policies.
7. Developing a technical implementation strategy.
8. Achieving buy-in from users, managers, and technical staff.
9. Training users, managers, and technical staff.
10. Implementing the technical strategy and security procedures.
11. Testing the security and update it if any problems are found.
12. Maintaining security.

IDENTIFICATION OF NETWORK ASSETS

- Network assets can include:-
- Network hosts (including the hosts’ operating systems, applications, and data),

- Internetworking devices (such as routers and switches), and
- Network data that traverses the network.
- Less obvious assets include intellectual property, trade secrets, and a company's reputation.

ANALYSIS OF SECURITY RISKS.

Risks can range from

- hostile intruders

- untrained users
- Hostile intruders can
- steal data, change data, and
- Cause service to be denied to legitimate users.

ANALYSIS OF SECURITY REQUIREMENTS AND TRADEOFFS

Security requirements boil down to the following:-

- The confidentiality of data, so that only authorized users can view sensitive information
- The integrity of data, so that only authorized users can change sensitive information
- System and data availability, so that users have uninterrupted access to important computing resources

Principle of least protection

- The cost of protecting against a threat should be less than the cost of recovering if the threat were to strike.
- Cost in this context should be remembered to include losses expressed in real currency, reputation, trustworthiness, and other less obvious measures.

Tradeoffs

Achieving security goals means making tradeoffs.

- Tradeoffs must be made between security goals and goals for affordability, usability, performance, and availability. Also, security adds to the amount of management work because user login IDs, passwords, and audit logs must be maintained.
- Security also affects network performance: consuming CPU power and memory on hosts, routers, and servers.
- Delay that packets experience while being encrypted or decrypted.

DEVELOPMENT OF A SECURITY PLAN

- One of the first steps in security design is developing a security plan.
- A security plan is a high-level document that proposes what an organization is going to do to meet security requirements.
- The plan specifies the time, people, and other resources that will be required to develop a security policy and achieve technical implementation of the policy.
- The plan should be practical and pertinent. And based on the customer's goals and the analysis of network assets and risks.

Topology, services, access, administration

The plan should reference the network topology and include a list of network services that will be provided (eg. FTP, web, email).

This list should specify who provides the services, who has access to the services, how access is provided, and who administers the services.

Minimal complexity

Complicated security strategies are hard to implement correctly without introducing unexpected security holes

Responsibility

One important aspect of the security plan is a specification of the people who must be involved in implementing network security:-

- Will specialized security administrators be hired?
- How will end users and their managers get involved?
- How will end users, managers, and technical staff be trained on security policies and procedures?
- For a security plan to be useful, it needs to have the support of all levels of employees within the organization.

Defining a security policy

Security policy: a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide.

A security policy informs users, managers, and technical staff of their obligations for protecting technology and information assets.

The policy specifies the mechanisms by which these obligations can be met.

The security policy should have buy-in from employees, managers, executives, and technical personnel. Developing a security policy is the job of senior management, with help from security and network administrators.
The administrators get input from managers, users, network designers and engineers, and possibly legal counsel.
The role of network designer is to work closely with the security administrators to understand how policies might affect the network design.
A security policy is a living document. And because organizations constantly change, security policies should be regularly updated to reflect new business directions and technological shifts. Risks change over time also and affect the security policy.

Components of a Security Policy:

- An *access policy* that defines access rights and privileges: - The access policy should provide guidelines for connecting external networks, connecting devices to a network, and adding new software to systems. An access policy might also address how data is categorized (for example, confidential, internal, and top secret).
- An *accountability policy:* - It defines the responsibilities of users, operations staff, and management. The accountability policy should specify an audit capability and provide incident-handling guidelines that specify what to do and whom to contact if a possible intrusion is detected.
- An *authentication policy:- it* establishes trust through an effective password policy and sets up guidelines for remote-location authentication.
- A *privacy policy:-* it defines reasonable expectations of privacy regarding the monitoring of electronic mail, logging of keystrokes, and access to users' files.
- Computer-*technology purchasing guidelines: - it* specifies the requirements for acquiring, configuring, and auditing computer systems and networks for compliance with the policy.

Developing procedures for applying security policies

Security procedures implement security policies. Procedures

- Define configuration, login, audit, and maintenance processes.

It is Written for:-
End users, network administrators, and security administrators.
It is Specifies
How to handle incidents (that is, what to do and who to contact if an intrusion is detected).

Maintaining Security

Security maintained by :-
Scheduling periodic independent audits,

- Reading audit logs,
- Responding to incidents,
- Reading current literature and agency alerts,
- Performing security testing,
- Training security administrators and updating the security plan and policy.

Security wheel: illustrates that implementing, monitoring, testing, and improving security is a never-ending process.

Security Mechanisms

i) Physical Security

Physical security: using physical control to protect key network resources. It can protect a network from misuse or abuse by:-

- Untrained employees and contractors (inadvertent)
- Hackers, competitors, and terrorists walking in off the street and changing equipment configurations.
- From natural disasters such as floods, fires, storms, and earthquakes should be installed to protect

Core routers, demarcation points, cabling, modems, servers, hosts, backup storage, and so on should be placed in computer rooms that have card key access and/or security guards.
Computer rooms should also be equipped with uninterruptible power supplies, fire alarms, fire-abatement mechanisms, and water removal systems.

To protect equipment from earthquakes and high winds during storms, equipment should be installed in racks that attach to the floor or wall.
Planning for physical security should start during the early phases of the top-down design process in case there are lead times to build or install security mechanisms

ii) Authentication

Authentication identifies who is requesting network services and it can refer to human users, devices or software processes. Forms of authentication include:-

Re-usable password scheme: most common
One-time (dynamic) passwords scheme:
Smartcard based implementation: - User enters a PIN, card provides a onetime password that is used to access the corporate network for a limited time. Typically used by telecommuters and mobile users.

Authentication is traditionally based on one of three proofs:

i) ***Something the user knows:*** This usually involves knowledge of a unique secret that is shared by the authenticating parties. To a user, this secret appears as a classic password, a PIN, or a private cryptographic key.

ii) ***Something the user has***: This usually involves physical possession of an item that is unique to the user. Examples include password token cards, security cards, and hardware keys.

iii) ***Something the user is:*** This involves verification of a unique physical characteristic of the user, such as a fingerprint, retina pattern, voice, or face. Many systems use two-factor authentication, which requires a user to have two proofs of identity. E.g., accesses control system that requires a security card and a password.

With two-factor authentication, a compromise of one factor does not lead to a compromise of the system. An attacker could learn a password, but the password is useless without the security card. Conversely, if the security card is stolen, it cannot be used without the password.

iii) Authorization

Authorization says what user can do after authentication. i.e. Authorization grants privileges to processes and users. Authorization lets a security administrator control parts of a network (for example, directories and files on servers).

Authorization varies from user to user, partly depending on a user's department or job function. For example, a policy might state that only Human Resources employees should see salary records for people they do not manage.

Security experts recommend use of the principle of least privilege in the implementation of authorization. It is based on the idea that each user should be given only the minimal necessary rights to perform a certain task. Therefore, an authorization mechanism should give a user only the minimum access permissions that are necessary.

iv) Accounting (Auditing)

Accounting or auditing: collecting network activity data for purposes of effectively analyze the security of a network and to respond to security incidents such as:-

- Ensure audit data include time-stamped
- Attempts to achieve authentication and authorization
- Log "anonymous" or "guest" access to public servers
- Attempts by users to change their access rights.

A further extension of auditing is security assessment

- The network is periodically examined from within by professionals, trained in the vulnerabilities exploited by network invaders.
- Output of assessment: specific plan for correcting any deficiencies

v) Data Encryption

It is the process for scrambling data to protect it from being read by an un-intended party

A router, server, end system, or dedicated device can be encryption or decryption device. Encryption should be used when a customer has analyzed security risks and identified severe consequences if data is not kept confidential and/or the identity of senders of data is not guaranteed.

On internal networks and networks that use the Internet simply for web browsing, email, and file transfer, encryption may not necessary. For connection of private sites via the Internet, using virtual private networking (VPN), encryption is recommended to protect the confidentiality authentication and integrity

vi) Packet Filters

Packet filter: forward or discard packets based on defined filtering rules. Can be set up on routers, firewalls, and servers to accept or deny packets from particular addresses or services

Broad security policies:

- Permissive: Deny specific types of packets, accept all else
- Prudent: Accept specific types of packets, deny all else

The first policy requires a thorough understanding of specific security threats and can be hard to implement. While the second policy is easier to implement and more secure because the security administrator does not have to predict future attacks for which packets should be denied.

The second policy is also easier to test because there is a finite set of accepted uses of the network. To do a good job implementing the second policy requires a good understanding of network requirements. The network designer should work with the security administrator to determine what types of packets should be accepted.

Packet filters usually use access control lists (ACL) for specifying rules. ACLs control whether network traffic is forwarded or blocked at interfaces on a router or switch. Typical criteria are: source address, destination address, or the upper-layer protocol in the packet.

vii) Firewalls

It is a device that enforces security policies at the boundary between two or more networks. It can be a router with ACLs, a dedicated hardware appliance, or software running on a PC or UNIX system. It applies a set of rules that specifies which traffic should be allowed or denied

- A static-stateless-packet-filter firewall looks at individual packets and is optimized for speed and configuration simplicity.
- A stateful firewall can track communication sessions and more intelligently allow or deny traffic

Example

Proxy firewall: It acts as an intermediary between hosts, intercepting some or all application traffic between local clients and outside servers. Proxy firewalls examine packets and support stateful tracking of sessions. These types of firewalls can block malicious traffic and content that is deemed unacceptable.

viii) Intrusion Detection and Prevention Systems

An IDS detects malicious events and notifies an administrator of the occurrence. They can also perform statistical and anomaly analysis. Some IDS devices can report to a central database that correlates information from multiple sensors to give an administrator an overall view of the realtime security of a network.

An intrusion prevention system (IPS) can dynamically block traffic by adding rules to a firewall. An IPS is an IDS that can detect and prevent attacks. There are two types of IDS devices:-

- *Host IDS*: Resides on an individual host and monitors that host.
- *Network IDS:* Monitors all network traffic watching for predefined signatures of malicious events.

A network IDS is often placed on a subnet that is directly connected to a firewall so that it can monitor the traffic that has been allowed and look for suspicious activity. A major concern with both IDS and IPS was: volume of false alarms. This problem has been ameliorated by sophisticated software and services.

Modern IPS solutions: include anomaly detection that learns about typical actual network traffic on a customer's network and alarms only upon deviation. It also supports reputation filtering and global correlation services so that an IPS can keep up-to-date on global security trends and more accurately deny traffic from flagged networks known to be currently associated with spam, and other malware.

e) Developing Network Management Strategies

Management is often overlooked during the design of a network because it is considered an operational issue rather than a design issue.
But leaving it to only be considered and added after the design is complete this likely to lead to scalability and performance problems

APPROACH

Network management design should be approached in the same way any design project

- Think about the following issues:-
  - scalability,
  - traffic patterns,
  - data formats, and
  - cost/benefit tradeoffs
- Network management systems can be expensive.
- They can also have a negative effect on network performance.

PROACTIVE MANAGEMENT:

Practice of checking the health of the network during normal operation to, e.g.

- Recognize potential problems,
- Optimize performance
- Plan upgrades

Practice of proactive network management to be encouraged

Procedure

Collect statistics and conduct tests on a routine basis such as:-
Statistics and test results used to establish network health and recognize trends.
Communicate health and trends to management and users
Network managers produce monthly or quarterly reports documenting the quality of network service delivered as compared to service goals
The service goals are defined by the network design:-

- Availability,
- Response time,
- Throughput,
- Usability,

Proactive Network Management is desirable but it requires more sophisticated network management tools and processes than reactive network management. This tradeoff can, however, be justified with less downtime.

Network Management Objective

Develop network management processes that can help

- Manage the implementation of the network
- Manage operation of the network
- Diagnose and fix problems
- Optimize performance
- Plan enhancements

NETWORK MANAGEMENT PROCESSES

ISO defines five types of network management processes referred to as FCAPS:

- Fault management
- Configuration management
- Accounting management
- Performance management
- Security management

a) Fault Management

Consists of faults

- detection
- isolation
- diagnosis
- correction

It also includes

- Reporting problems (to end users and managers)
- Tracking trends (related to problems)
- Developing workarounds (until a problem can be fixed)

Fault Management Tools

A variety of tools include:-

- monitoring tools that alert managers to problems,
- Protocol analyzers for fault resolution, and
- Help-desk software for documenting problems and alerting users of problems.

Monitoring tools often based on the standards:

- SNMP: (Simple Network Management Protocol) standard
- RMON: (Remote Monitoring) standard
- OS mechanisms: most operating systems provide a means for the system and its

Cisco devices produce syslog messages as a result of network events. A syslog message contains a *time stamp*, *leve*l, and *facility*

Syslog levels:

- Emergency (level 0, the most severe level)
- Alert (level 1)
- Critical (level 2)
- Error (level 3)
- Warning (level 4)
- Notice (level 5)
- Informational (level 6)
- Debugging (level 7)

Syslog messages can be sent to:-

- Cisco router or switch console.
- A network management station or a remote network host on which a syslog analyzer is installed.

A syslog analyzer applies filters and sends only a predefined subset of all syslog messages. This saves bandwidth and also reduces the amount of information anetwork administrator must analyze.

b) Configuration Management

This helps a network manager to:-

Keep track of network devices and maintain information on how devices are configured.

A network manager can

- define and save a default configuration for similar devices,
- modify the default configuration for specific devices,
- Load the configuration on devices.
- maintain an inventory of network asset
- Do version-logging: - *Which is keeping track of the version of operating systems, applications running on network devices.*

The inventory also includes information on the hardware configuration of devices, such as RAM size, flash memory, and the type of cabling the devices use.

CM facilitates change management.

c) Accounting Management

It facilitates usage-based billing, for charging departments, projects for network services. Even if no monetary charging, accounting can be useful to catch “abuse” in form of:-

- Un-authorized/undesirable activities which cause excessive traffic
- track unexpected traffic growth is so that the traffic can be considered during the next capacity-planning phase

d) Performance Management

The measurement of network behavior and effectiveness including

- examining network application and protocol behavior
- analyzing reachability
- measuring response time
- recording network route changes

It also facilitates the following:-

- Optimizing a network,
- Meeting service-level agreements (SLAs)
- Planning for expansion

Monitoring performance involves the following:-

- Collecting data
- Processing the data
- Displaying the data
- Archiving some or all of the data

Types of performance monitored:-

- ***End-to-end performance:*** This is performance across an internetwork. It includes availability, capacity, utilization, delay, delay variation, throughput, reachability, response time, errors, and the burstiness of traffic.
- ***Component performance***: This is performance of individual links or devices

TOOLS

- They are used for surveying remote parts of the network to test reachability and measure response times.
- Response-time: use ***ping*** and measuring the round-trip time (RTT).
- On large networks, reachability and RTT studies can be impractical. Eg, on a network with 10,000 devices polling can take hours and can cause significant network traffic.
- Use protocol analyzers or SNMP tools to record traffic loads between important sources and destinations.
- Another less reliable tool is *Traceroute*

Objective: document the mbps between pairs of autonomous systems, networks, hosts, or applications.
Source/destination traffic-load documentation is useful for capacity planning, troubleshooting, and figuring out which routing protocols to use on the routers.

e) Security Management

It involves:-

- Maintaining and distributing passwords and other authentication and authorization information.
- Processes for generating, distributing, and storing encryption keys.
- Includes tools and reports to analyze router and switch configurations for compliance with site security standards.
- Collecting, storing, and examining security audit logs. Problem with audit logs: large amount of data

Efficiency requirements (storage can be minimized by):

- keeping data for a short period of time
- Summarizing data.

Drawback to keeping less data:-

- harder to investigate security incidents
- Other solution: data compression

Tools

A variety of tools for maintaining security logs:

- *Event Viewer* on Windows systems
- *syslog* on UNIX and Cisco IOS devices

Most contemporary operating systems support audit event logging because of requirements in the Common Criteria for Information Technology Security Evaluation, an international standard for computer security certification

.