Network Analysis and Design

Dr/Mai Ramadan Ibraheem

Lecturer at Information Technology Dept.,

Faculty of Computers and Information – KFS University

Outline

- Network Design Methodology
- Network Structure Models.
- Enterprise LAN Design.
- Data Center Design.

Network Design Methodology

- Cisco Architectures for the Enterprise
- PPDIOO life cycle
- Identifying Customer Design Requirements
- Characterizing the Existing Network
- Designing the Network Topology and Solutions

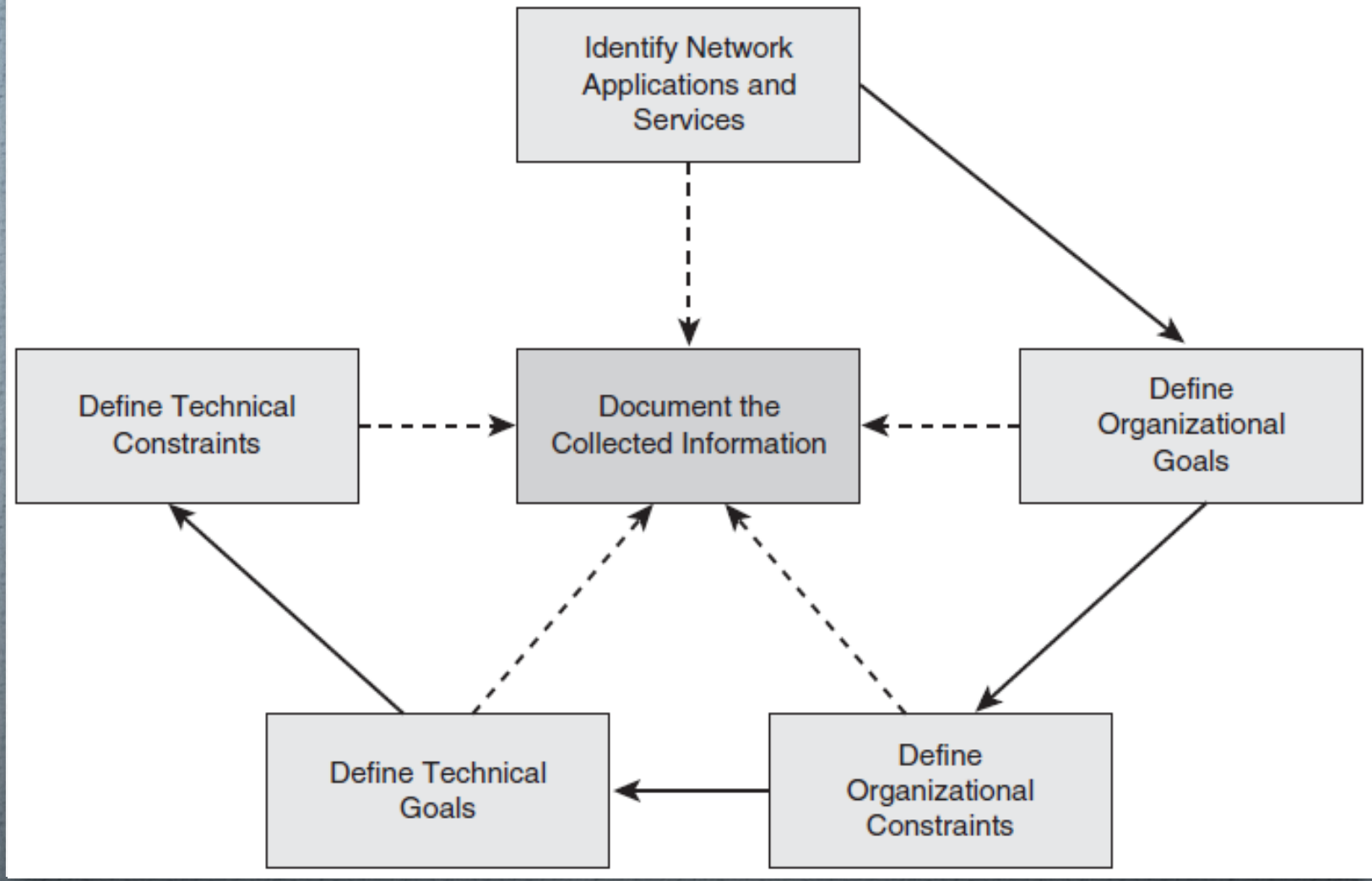
Identifying Customer Design Requirements

- You need to not only talk to network engineers, but also talk to **business unit personnel** and **company managers**.
- Networks are designed to **support** applications; you want to determine the network **services** that you need to **support**.

Identifying Customer Design Requirements

- The steps to identify customer requirements are as follows:
- Step 1. Identify network applications and **services**.
- Step 2. Define the **organizational** goals.
- Step 3. Define the possible **organizational** constraints.
- Step 4. Define the **technical** goals.
- Step 5. Define the possible **technical** constraints.

Identifying Customer Design Requirements



Identifying Customer Design Requirements

- After you complete these steps, you then *analyze* the data and *develop* a network design.
- You need determine the **importance** of each application. Is *email* as important as *customer support*? Is **IP telephony** being *deployed*?
- High-availability and *high-bandwidth* applications need to be **identified** for the design to **accommodate** their network requirements.

Identifying Customer Design Requirements

- A table *identifying applications* should **list** the following:
- ■ Planned application types: Such as email, collaboration, voice, web browsing, file sharing, database
- ■ Concrete applications: Such as Outlook, MeetingPlace

Identifying Customer Design Requirements

- Business **importance**: Labeled as critical, important, or unimportant
- Comment: Any *additional information* critical to the design of the network

Identifying Customer Design Requirements

- Planned **infrastructure services** should also be gathered.
- Network services include *security*, *quality of service* (QoS), network management, high availability, unified communications, mobility, and virtualization. (Task)

Identifying Customer Design Requirements

- For **organizational goals**, you should identify whether the company's goal is to *improve* customer support, *add* new customer services, *increase* competitiveness, or *reduce* costs.
- It might be a *combination* of these goals, with some of them being more important than others.

Identifying Customer Design Requirements

- Some organizational goals are as follows:
- ■ Increase competitiveness
- ■ Reduce costs
- ■ Improve customer support
- ■ Add new customer services

Identifying Customer Design Requirements

- **Organizational constraints** include *budget*, *personnel*, *policy*, and *schedule*. The company might **limit** you to a certain **budget** or **timeframe**.
- The organization might require the project to be completed in an unreasonable *timeframe*. It might have limited personnel to support the assessment and design efforts, or it might have *policy limitations* to use certain *protocols*.

Identifying Customer Design Requirements

- **Technical goals** support the organization's objectives and the supported applications.
- Technical goals include the following:
- ■ *Improve* the network's *response-time throughput*
- ■ *Decrease* network *failures* and *downtime* (high availability)

Identifying Customer Design Requirements

- Simplify network management
- Improve network security
- Improve reliability of mission-critical applications
- Modernize outdated technologies (technology refresh)
- Improve the network's **scalability**

Identifying Customer Design Requirements

- Network design might be *constrained* by *parameters* that limit the solution.
- **Legacy applications** might still exist that must be supported going forward, and these applications might *require* a legacy protocol that may limit a design.

Identifying Customer Design Requirements

- Technical constraints include the following:
- ■ Existing **wiring** does not support new technology.
- ■ Bandwidth might not **support** new applications.
- ■ The network must support exiting **legacy** equipment.
- ■ Legacy applications must be supported (application **compatibility**).

Network Design Methodology

- Cisco Architectures for the Enterprise
- PPDIOO life cycle
- Identifying Customer Design Requirements
- Characterizing the Existing Network
- Designing the Network Topology and Solutions

Steps in Gathering Information

- information. Here are the steps for gathering information:
- Step 1. Identify all existing organization information and documentation.
- Step 2. Perform a network audit that adds detail to the description of the network.
- Step 3. Use traffic analysis information to augment information on applications and protocols used.

Steps in Gathering Information

- When gathering exiting *documentation*, you look for **site information** such as site *names*, site *addresses*, site *contacts*, site *hours* of operation, and building and room access.
- Network **infrastructure information** includes *locations* and *types of servers* and network *devices*, data center and closet locations, LAN wiring, WAN technologies and circuit speeds, and power used.

Steps in Gathering Information

- **Logical network information** includes IP addressing, routing protocols, network management, and security access lists used.
- You need to find out whether voice or video is being used on the network.

Network Audit Tools

- When performing a network audit, you have three primary sources of information:
- ■ Existing documentation
- ■ Existing network management software tools
- ■ New network auditing tools

Network Audit Tools

- After gathering the existing documentation, you must obtain **access** to the existing management software.
- The client may already have CiscoWorks **tools** from which you can obtain hardware models and components and software versions.
- You can also obtain the existing router and switch *configurations*.

Network Audit Tools

- The network audit should provide the following information:
- ■ Network device list
- ■ Hardware models
- ■ Software versions
- ■ Configuration of network devices
- ■ Auditing tools output information

Network Audit Tools

- Interface speeds
- Link, CPU, and memory utilization
- WAN technology types and carrier information

Network assessment

- In **small** network, you might be able to obtain the required information via a manual assessment.
- For **larger** network, a manual assessment might be too **time-consuming**. Network assessment tools include the following:
- ■ Manual assessment
  - ■ Manual commands: Review of device configuration and operation though the use of show
  - ■ Scripting tools

Network assessment

- When performing manual auditing on network devices, you can use the following commands to obtain information:
- ■ show tech-support
- ■ show processes cpu (provides the average CPU utilization information)
- ■ show version

Network assessment

- show processes memory
- show log
- show interface
- show policy-map interface
- show running-config (provides the full router or switch configuration)

show version command

- This command shows:
- The operating system version,
- The router type,
- The amount of flash and RAM memory,
- The router uptime, and interface types.

NetFlow

- Provides extremely granular and accurate traffic measurements and a high-level collection of aggregated traffic.
- The output of **NetFlow** information is displayed via the ***show ip cache flow*** command on routers.
- The next table shows a description of the fields for **NetFlow** output.

NetFlow

Field	Description
Bytes	Number of bytes of memory that are used by the NetFlow cache
Active	Number of active flows
Inactive	Number of flow buffers that are allocated in the NetFlow cache
Added	Number of flows that have been created since the start of the summary
Exporting flows	IP address and User Datagram Protocol (UDP) port number of the workstation to which flows are exported
Flows exported	Total number of flows export and the total number of UDP datagrams
Protocol	IP protocol and well-known port number
Total flows	Number of flows for this protocol since the last time that statistics were cleared
Flows/sec	Average number of flows this protocol per second
Packets/flow	Average number of packets per flow per second
Bytes/pkt	Average number of bytes for this protocol
Packets/sec	Average number of packets for this protocol per second

Network Analysis Tools

- To obtain application-level information, the IP packet needs to be further **inspected**.
- Cisco devices or dedicated hardware or software analyzers **capture packets** or use Simple Network Management Protocol (**SNMP**) to **gather** specific information.

Network Analysis Tools

- Network analysis tools include the following:
- ■ **Netformx DesignXpert Enterprise**: An integrated desktop tool for discovery, design, configuration, quoting and proposing integrated communications network solutions.
- ■ **CNS NetFlow Collector Engine**: Cisco hardware that *gathers* every flow in a network segment.

Network Analysis Tools

- **Cisco Embedded Resource Manager (ERM)**: Allows for granular *monitoring* on a task basis within the Cisco IOS software. It monitors the internal system resource utilization for specific resources, such as the buffer, memory, and CPU.
- **Third-party tools**: Such as Sniffer, AirMagnet Wifi Analyzer, BVS Yellowjacket 802.11, NetIQ Vivinet Assessor, Netcordia NetMRI, and SolarWinds Orion.

Network Checklist

- The *network checklist* can be used to determine a network's health status:
- ■ *New segments* should use *switched* and not use dated hub/shared technology.
- ■ *No WAN links* are *saturated* (no more than *70 percent* sustained network *utilization*).
- ■ The *response time* is less than 100ms (one-tenth of a second); more commonly, less than 2ms in a LAN.

Network Checklist

- ■ No segments have more than 20 percent broadcasts or multicast traffic. Broadcasts are sent to all hosts in a network and should be limited. Multicast traffic is sent to a group of hosts but should also be controlled and limited to only those hosts registered to receive it.
- ■ No segments have more than one cyclic redundancy check (CRC) error per million bytes of data.
- ■ No segments have more than one cyclic redundancy check (CRC) error per million bytes of data.

Network Checklist

- ■ On the *Ethernet segments*, less than 0.1 percent of the packets result in *collisions*.
- ■ A *CPU utilization* at or more than *75 percent* for a 5-minute interval likely suggests network problems. Normal CPU utilization should be much lower during normal periods.
- ■ The number of *output queue drops* has not exceeded 100 in an hour on any Cisco router.

Network Checklist

- The number of *input queue drops* has not exceeded 50 in an hour on any Cisco router.
- The number of *buffer misses* has not exceeded 25 in an hour on any Cisco router.
- The number of *ignored packets* has not exceeded 10 in an hour on any interface on a Cisco router.
- *QoS* should be *enabled* on network devices to allow for *prioritization* of *time-sensitive* or bandwidth-sensitive applications.


End


Thank You