CPE654– Design and analysis of network systems

Spring 2017: Assignment 3

Name: Shruti Sharma
CWID: 10422506 (Spring 2017)

Problem 1: Show flows for each set of devices and applications below. Label each as either a uni- or bi-directional flow.

a. Client-server application: downstream (from server to client) – 1.2 Mb/s capacity; upstream (from client to server) – 15 kb/s capacity.

b. Streaming video (UDP) from video server to a subscriber's PC: 300 kb/s capacity, 40 ms delay (one-way).

c. Downloading pages from the web: downstream - 250 kb/s capacity, 5 second delay; upstream – 100 kb/s capacity.

d. Transaction processing from point-of-sale machine to server: upstream (from PoS machine to server) – 30 kb/s capacity, 100 ms round-trip delay; downstream – 50 kb/s capacity.

Solution: a) Client-server application: downstream (from server to client) – 1.2 Mb/s capacity; upstream (from client to server) – 15 kb/s capacity- *Bi-directional flow.*

b) Streaming video (UDP) from video server to a subscriber's PC: 300 kb/s capacity, 40 ms delay (one-way)- *Uni-directional flow.*

c) Downloading pages from the web: downstream - 250 kb/s capacity, 5 second delay; upstream – 100 kb/s capacity- *Uni-directional flow.*

d) Transaction processing from point-of-sale machine to server: upstream (from PoS machine to server) – 30 kb/s capacity, 100 ms round-trip delay; downstream – 50 kb/s capacity- *Bi-directional flow.*

Problem 2: You are developing a network for a company's on-line transaction processing (OLTP) application (e.g. a retail sales network). Their current system is a mainframe that has several terminals connected to it, either directly or through a terminal server, as in Figure 4.51 below. They are moving to a hierarchical client server network, where there will be multiple regional database servers, each acting in a client-server fashion and updating each other's regions via a database manager, as in Figure 4.52.

a. Show the probable data sources and sinks for both environments.

b. How does migrating from the mainframe environment to the hierarchical client-server environment modify the traffic flows in the network?

c. In what ways does the network environment improve the traffic flows?

d. What are some of the potential trade-offs between the two environments, for example, in security, management, and performance?

Solution: a) Show the probable data sources and sinks for both environments.

Mainframe environment is a strict client server model and the data source is the mainframe itself the sink would reside on the client. Figure 4.51.This is similar to a hierarchical C-S model since the databases are can be queried by location and all locations peer together. The Data Sinks and

Data Sources will be on each location's Database server. It is the Managers job to dump the sink into the data source for each database server.

b) How does migrating from the mainframe environment to the hierarchical client-server environment modify the traffic flows in the network?
Typically in a mainframe environment the flow would be client server between the terminals and the mainframe. However not the traffic flow will be client server from the clients to the database server per the location and the peer to peer flow between server from location to location to collate or merge the data.

c) In what ways does the network environment improve the traffic flows?
The improvement to traffic flow will be the splitting of the combined flows to a central location. Splitting the locations and geographically dispersing the units will split the combined flows over many client/servers.

d) What are some of the potential trade-offs between the two environments, for example, in security, management, and performance?
There are many tradeoffs... In a mainframe environment all of the clients are dependent on the flow of information from the mainframe, however now the flows are split between locations. Splitting the locations disperses the information and now we must employ a database management terminal to combine the information between database servers. The performance will increase in the Hierarchal C-S environment because the combined flows from clients are split between locations. Security is also now dispersed between locations rather than a central location in a mainframe environment which is must easier to maintain.

Problem 3: Give examples of external relationships between each of the following component architectures: addressing/routing, network management, performance, and security.

Solution: External Relationships:
–*Performance and Addressing*
• Performance is closely coupled with routing through mechanisms like DiffServ & IntServ, and RSVP. These are not simple protocols.
– *Performance and NM*
• Performance relies on NM to configure, monitor, manage, verify, and bill.
– *Performance and Security*
• Security mechanisms will affect negatively performance, especially those security mechanisms that are intrusive.
• If security mechanisms interrupt, terminate, or regenerate a traffic flow they seriously affect the ability to provide end-to-end QoS.

Optimizing the Reference Architecture

- Numerous trade-offs occur between addressing/routing, N.M., performance, security.
- High security leads to low performance – Security may have to take low profile in parts of the network.
- N.M. leads to low security – When management is a high priority, separate security component architecture for N.M. may be required.
- High Resolution N.M. leads to low Performance – Out-of-band N.M. a solution. –but, what about security?
- Simplicity in addressing/routing leads to low performance – Several performance protocols like DiffServ and RSVP are tightly coupled to the addressing scheme.

Architectural Considerations: Security

- Evaluate potential security mechanisms and think about where they apply within the network
- Determine external and internal relationships.
- Start simple and work toward more complex solutions:

– The access as well as distribution with their core architectural model we discussed before can be used as a starting point to apply security points.

– Security can be added at different points in the architecture.

– Security is increased from access to distribution to core areas.

- *External Relationships:*

– Security & Addressing

- NAT is an addressing scheme that helps security. Dynamic addressing interferes with address specific filtering.

– Security & Network Management.

- Security depends on Network Management – Security & Performance.
- These 2 are nearly always at odds. Security zones will affect the performance of that zone.

Architectural Considerations: Performance

- Start simple – BestEffort equivalent to DiffServ-IntServ
- From the flow analysis maps you know where performance requirements need to be applied in the network.
- Recall that the access/distribution/core architectural model separates network based on function.

– Core leads to bulk traffic leads to aggregated

– Distribution leads to flows to and from servers and aggregate traffic.

– Access leads to most traffic is sources and sinked here.

- Performance mechanisms that operate on individual flows (admission control, resource allocation, IntServ, ATM QoS) should be considered for access.

• Performance mechanisms that operate on aggregated flows (DiffServ, WFQ RED/WRED, and MPLS all fit in here) should be considered for core and distribution.

• External Relationships:
– ***Performance and Addressing***
• Performance is closely coupled with routing through mechanisms like DiffServ&IntServ, and RSVP. These are not simple protocols.
– ***Performance and NM***
• Performance relies on NM to configure, monitor, manage, verify, and bill.
– ***Performance and Security***
• Security mechanisms will affect negatively performance, especially those security mechanisms that are intrusive.
• If security mechanisms interrupt, terminate, or regenerate a traffic flow they seriously affect the ability to provide end-to-end QoS.

Architectural Considerations: NM
• Centralized/distributed monitoring
– Centralized: all monitoring data are sent from one monitoring node using either in-band or out-of-band-monitoring
– Distributed: local monitoring nodes
• Less NM traffic • In-band/out-of-band
• For a LAN start with one monitoring device per IP subnet. Estimate:
– Number of user and network devices to be polled
– Average number of interfaces / device, and the number of parameters to be collected
– Frequency of polling
– This combined rate should not be more than 10% of the capacity of the line. For Ethernet keep this at 5%.
• For a WAN start with a monitoring device per WAN/LAN interface.
• Local storage vs. archival
– Data usually kept locally, cached for easy retrieval (within hours). If not used this quickly then archive it.
• Selective copying of data
– Consider saving only every N iteration of data. N can range from 100 to 10000.
• Data Migration
– Usually occurs at night time from local to archive
• Metadata
– Additional information about the data is very useful. Data types time stamps etc.

External Trade-offs:
– Network Management and Addressing

- Management domain needs to be considered in the network architecture design.

– Network Management and Performance

- This is discussed before: how network data affects traffic flow and capacity.

– Network Management and Security

- Network management relies on a particular level of security to get access to the managed objects.

Problem 4. Please do Problem 6 in Chapter 5: (page 247)*

Consider the development of a demilitarized zone (DMZ), also known as an isolation LAN (iLAN), between 2 different networks (2 different autonomous systems (AS), managed by different organizations). The purpose of a DMZ is to separate and isolate the 2 networks. Briefly outline what you consider to be the most important addressing/routing, network management, performance, and security requirements and issues for a DMZ.

Solution: A DMZ should have a dis-jointed network addressing scheme from the organizations primary internal and public addressing scheme. This isolated LAN also needs to communicate data flows between the internal private network where a data source might exist and the internet where the customer or user will exist. From a network management and security stand point the network addresses of the DMZ needs to be excluded in firewalls to the internal servers and applications need to be encrypted between the data sources and data processors (web servers). Major issues for DMZ networks are security and the data that DMZ hosts can access.

Problem 5: Please do Problem7, Chapter 5 (Page247)*:

For Q5 (Problem 6, Chapter 5), what are some potential external relationships between addressing/routing, network management, performance and security for this DMZ? How do the component architectures need to work together to achieve the goal of effectively isolating and separating the two autonomous systems?

Solution: The external relationships between the client and server in respect to addressing/routing are the client needs to be routed from a public IP to a public IP and firewalled only to the application that the client needs to be accessing. As for the network management of the Client/Server in the location of the DMZ all firewalls between the Internet and DMZ and DMZ and Private network need to be configured a quality of service also needs to be established between the internet and DMZ and DMZ and Private network. This creates several locations for the hierarchical client server model.