GC
2018-2019

Network Technologies

"Behave like an engineer and ... be proud of being an engineer"

Ing. Giovanni CICCARESE
Dipartimento di Ingegneria dell'Innovazione
Università del Salento
Tel. 0832-297218
E-mail: gianni.ciccarese@unisalento.it

1

GC
2018-2019

Objectives

- The study of some fundamental aspects of the operation of modern computer networks, such as traffic control and quality of service, the support of wireless and mobile communications, security
- The analysis of some network technologies which represent the state of the art on the above issues
- The criteria for selecting the most appropriate technologies depending on their operating contexts.
  - Particularly, the criteria for designing network systems that meet given requirements in terms of performance, reliability and availability
- Exercises: a number of examples dealing with modelling of performance, reliability and availability of network systems

2

Reference books

GC 2018-2019

- J. Kurose e K.W. Ross, "Computer Networking. A Top-Down Approach", sixth edition, Pearson Addison-Wesley
- B.A. Forouzan, "Data Communications and Networking", fifth edition, McGraw-Hill
- P. Oppenheimer, "Top-Down Network Design", third edition, Cisco Press
- S. Convery, "Network Security Architecture", Cisco Press
- G. Bolch, S. Greiner, H. de Meer, K.S. Trivedi, "Queueing Networks and Markov Chains: Modeling and Performance Evaluation With Computer Science Applications", Wiley-Interscience
- K. S. Trivedi, A. Bobbio "Reliability-and-Availability Engineering", Cambridge University Press

3

Road map

GC 2018-2019

- Introduction
- Congestion and traffic control (in IP networks)
- Multicasting (in IP networks)
- IPv6
- Quality of service (in IP networks)
- Security
- Wireless and mobile networks
- Network Design

4

Introduction

GC 2018-2019

- The purpose is to provide an overview of some challenges that are complicating the task of ensuring acceptable application and service delivery
  - The way in which most enterprises do business is changing, so that the role of enterprise networks is changing
    - Network applications help an enterprise to increase productivity, profits
  - Typical requirements are:
    - The need for Performance and Quality of Service (QoS)
    - The need for Mobility and an immediate access to data, regardless of where the data is
    - The need for Reliability, Availability and Network Security
    - Of course, the need to reduce costs (CAPEX, OPEX)
  - Clearly, the most likely impact of poor performance and low availability of a business critical application is revenue loss

5

Application and service delivery challenges

GC 2018-2019

- Increasing number of business critical applications
  - A lot of application types
    - typical enterprises rely on hundreds of applications of different types
    - IP telephony (VoIP) and video are important applications to most businesses
    - A way to classify applications is whether the application is real-time, transactional or data transfer in orientation
    - The support of QoS is crucial
  - The widespread use of smartphones and tablets (see BYOD and BYOA later) has been driving the increase

6

Application and service delivery challenges

GC 2018-2019

The new 80/20 rule states that about 80% of a company's employees access applications over a WAN

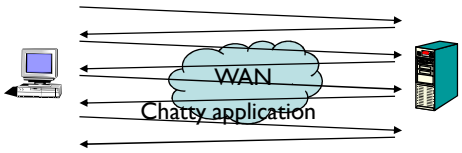
- Server consolidation
  - Many companies either have already consolidated or are in the process of consolidating servers out of branch offices and into centralized data centers
    - Higher utilization and lower costs
    - Better control over the company's data
    - Performance issues because chatty protocols and applications run over the WAN
- Data center consolidation
  - Many companies are also reducing the number of data centers they support worldwide
    - Additional WAN latency for remote users

7

Application and service delivery challenges

GC 2018-2019

- Chatty protocols and applications
  - A chatty application may require hundreds of turns (round trips) to complete a transaction
  - A relatively small increase in network delay can result in a significant increase of application delay (Response Time)
    - Example
      - let us assume that a given transaction requires 200 turns and that the round trip delay of the WAN is 100 msec
      - The application response time will be higher than 20 seconds



8

Application and service delivery challenges

GC 2018-2019

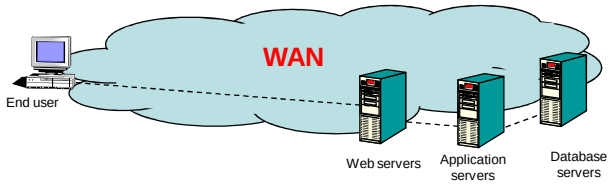
- "Webification" of applications
  - An application is accessed over the Internet or an Intranet and the user interface is a web browser
  - It is common for a web page to have a lot of objects
  - Although HTTP is not a chatty protocol, downloading a web page may require hundreds of round trips
  - The number of servers involved with a given user transaction is typically in the range of six to ten
    - Several of the servers typically reside in different data centers
  - The negative characteristics of the WAN (delay, jitter, packet loss rate) impact a web-based transaction multiple times

9

Application and service delivery challenges

GC 2018-2019

- Distributed applications
  - Today, a typical application consists of a Web tier, an application tier and a database tier, implemented on Web servers, application servers and database servers, respectively
  - It is becoming increasingly common to have these servers be virtualized within the same data center or in different ones
    - Virtual Machines (VMs) migrate to optimize and rebalance workloads, causing the physical end points of flows to change rapidly over time
    - It is very difficult to predict the end points of flows in order to correctly dimension the capacity of WAN links



10

Application and service delivery challenges

GC 2018-2019

- Most traffic is carried by TCP
  - The impact of RTT and packet loss rate on TCP performance

$$\text{TCP Throughput} < \frac{MSS}{RTT} * \frac{1}{\sqrt{p}}$$

[2]

MSS: Maximum Segment Size RTT: Round Trip Time p: packet loss rate

  - Small amounts of packet losses can significantly reduce the maximum throughput of a single TCP connection
    - If MSS is 1420 bytes, RTT is 100 ms and p is 0.01%, the maximum throughput is 1420 Kbyte/sec
    - If the packet loss rate increases to 0.1%, the maximum throughput drops to 449 Kbytes/sec
  - Some techniques are intended to lower the response time
    - WAN Optimization Controllers, Application Delivery Controllers, Internet optimization services, ...

11

Application and service delivery challenges

GC 2018-2019

- An example of what a well-known optimization company is currently offering

Application Performance

SharePoint Over **95%** data reduction **40X** faster response time	**Microsoft Office** Over **90%** data reduction **35X** faster response times
SVN (Subversion) Over **75%** data reduction **6X** faster response time	**SolidWorks PDM** Up to **90%** data reduction Over **30X** throughput improvement
File Transfer Over **99%** improvement Over **30X** faster response time	**Microsoft Exchange** Over **95%** data reduction Real-time replication across geography
Remote Desktop **400%** faster response time Better user-experience	**NetApp SnapMirror** More than **60%** bandwidth reduction **2X** higher throughput for data replication
HTTP Bandwidth utilization reduced **98%** **40X** faster response time	**Amazon Web Services** **8X** faster access to cloud services Extends reach to globally distributed offices
Images Data **de-duplication** benefits Faster application response times	**VoIP** **99.999%** service uptime End-to-end **QoS**
Oracle Data Guard **90X** higher link utilization **60X** improved performance for transfers	**Video** Stable core network and latency End-to-end **QoS**

12

Application and service delivery challenges

GC 2018-2019

- Mobility, BYOD and BYOA
  - The demand on WLANs for scalability is growing due to the rapid proliferation of new network devices (smartphones and tablets) and mobile applications
  - Many companies have already adopted the BYOD (Bring Your Own Device to work) concept, whereby employees use their own devices to access applications
  - Bring Your Own Application (BYOA): more and more employees using their own device source their own applications to do their job
  - Much stress is put on the available bandwidth
    - Particularly, the Signal-to-Noise Ratio (SNR) is degraded through both co-channel and adjacent channel interference
  - Adopting BYOD and BYOA increases a company's vulnerability to security breaches

13

High Availability and network security

GC 2018-2019

- Today, many enterprise managers report that service availability must be above 99.999 %
  - A "five-nines" availability (High-Availability) means an average downtime per year equal to 5.26 minutes
  - Companies would experience a severe loss of revenue or credibility if the service were down for even short periods of time
- Security has become very important as networks have become indispensable for business
  - The goal for security is linked to the goal for availability, as service cannot be available if security breaches are disabling network devices and applications
- When security and operational problems occur, networks must recover quickly (Resiliency)

14

System Downtime

GC 2018-2019

- Service Level Agreements (SLAs) often refer to monthly service downtime or availability

	Availability %	Downtime per year	Downtime per month*	Downtime per week
	99% ("two nines")	3.65 days	7.20 hours	1.68 hours
	99.5%	1.83 days	3.60 hours	50.4 minutes
	99.8%	17.52 hours	86.23 minutes	20.16 minutes
	99.9% ("three nines")	8.76 hours	43.8 minutes	10.1 minutes
	99.95%	4.38 hours	21.56 minutes	5.04 minutes
	99.99% ("four nines")	52.56 minutes	4.32 minutes	1.01 minutes
High Availability	99.999% ("five nines")	5.26 minutes	25.9 seconds	6.05 seconds
Very high Availability	99.9999% ("six nines")	31.5 seconds	2.59 seconds	0.605 seconds
Ultra high Availability	99.99999% ("seven nines")	3.15 seconds	0.259 seconds	0.0605 seconds

Business continuity and disaster recovery

GC 2018-2019

- ISO 22301 Business Continuity Management System (BCMS) standard
  - It has been developed to protect companies from the risks associated with service downtime which can occur due to unexpected disruptions or disasters (fires, floods, tornadoes, …)
  - ISO 22301 certification will guide a company on how best to architect for such eventualities

Software Defined Networking

GC 2018-2019

- The explosion of mobile devices, server virtualization, and advent of cloud services are driving the networking industry to re-examine traditional network architectures
  - Modern traffic pattern are incredibly dynamic and, therefore, unpredictable
  - To implement a network-wide policy (access, security, QoS, ..), IT operators may have to configure thousands of devices
    - Policies may be inconsistent
  - Due to complexity, today's networks are relatively static as IT operators seek to minimize the risk of service disruption
- Software Defined Networking (SDN) is an emerging network architecture where network's control plane (brain) is decoupled from forwarding plane (muscle)

17

Software Defined Networking (cont.)

GC 2018-2019

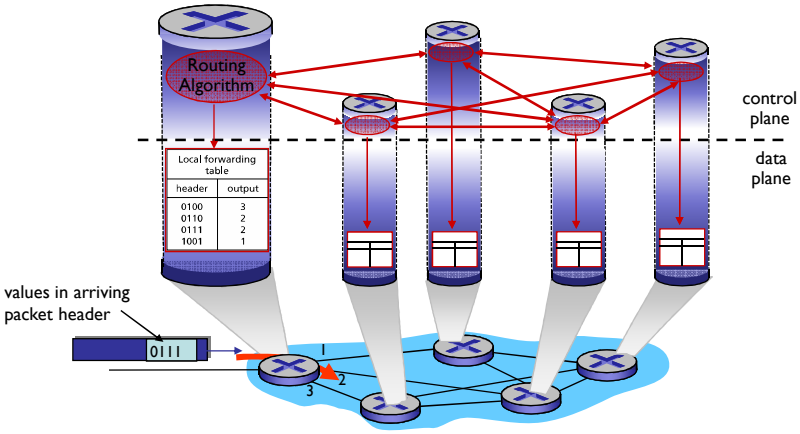
- SDN provides for the implementation of control plane to be open (and standard-based)
- The Open Networking Foundation (ONF) is the group that is most associated with the standardization and development of SDN
- Some important SDN use cases:
  - Dynamic QoS
  - Traffic Engineering
  - Role based access
  - Load Balancer services
  - Security services

18

Traditional approach: per-router control plane

GC 2018-2019

- Individual routing algorithm components *in each and every router* interact with each other in control plane to compute forwarding tables

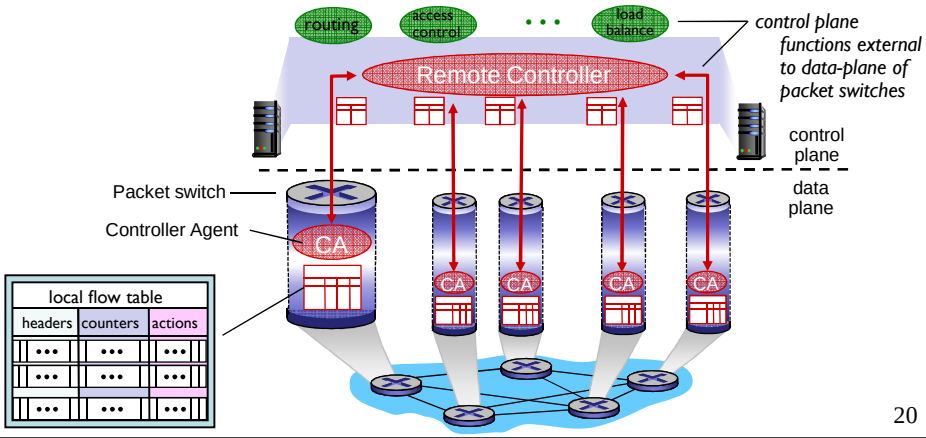


19

Control plane and data plane separation

GC 2018-2019

- A logically centralized software program (Remote Controller) controls the behaviour of an entire network
  - IT operators can program -and reprogram- the network in real time to meet specific business and user needs as they arise



20

The Openflow protocol

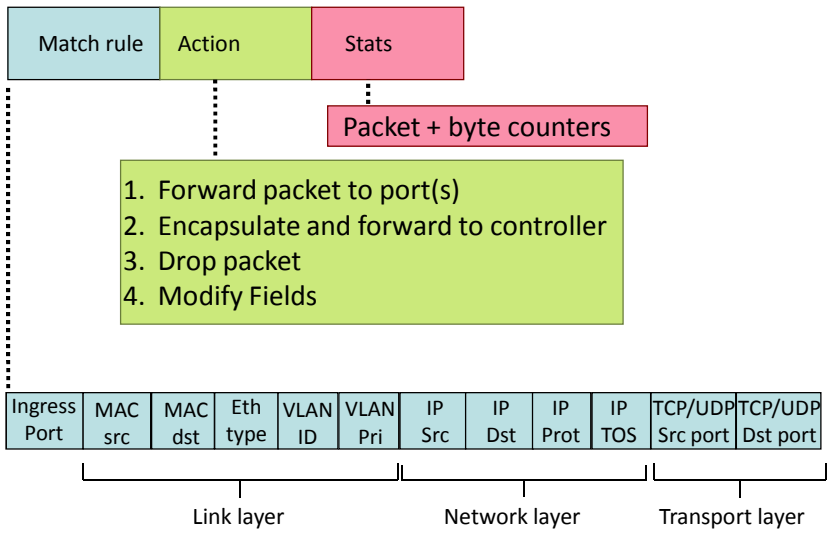
GC 2018-2019

- The Controller interacts with control agents (CAs) in packet switches to compute and distribute forwarding tables (called flow tables in SDN)
  - Examples of open source SDN controllers: Opendaylight, ONOS
- OpenFlow structures communication between the Controller and the CAs
  - The concept of flow is used to identify network traffic based on match rules programmed by the SDN control software
- The match-action paradigm
  - "Match" can be done on multiple header fields (up to 41) associated to different protocol layers
  - "Action" allows to define how traffic should be forwarded by the packet switch

21

OpenFlow: Flow Table Entries

GC 2018-2019



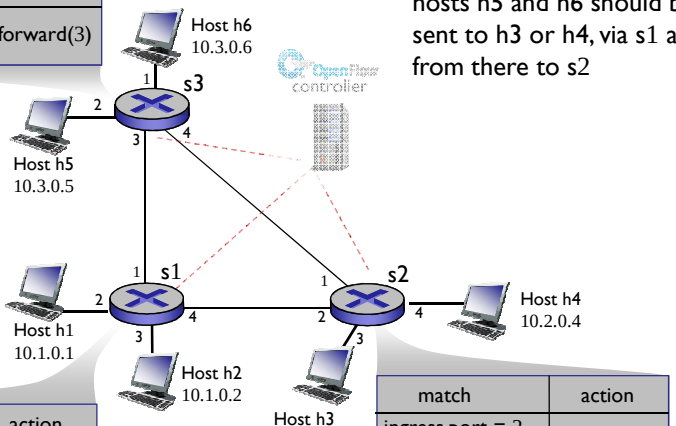
22

OpenFlow example

GC 2018-2019

Example: IP datagrams from hosts h5 and h6 should be sent to h3 or h4, via s1 and from there to s2

match	action
IP Src = 10.3.*.* IP Dst = 10.2.*.*	forward(3)



match	action
ingress port = 1 IP Src = 10.3.*.* IP Dst = 10.2.*.*	forward(4)

match	action
ingress port = 2 IP Dst = 10.2.0.3	forward(3)
ingress port = 2 IP Dst = 10.2.0.4	forward(4)

23

Network Functions Virtualization (NFV)

GC 2018-2019

- NFV is an initiative of the ETSI Industry Specification Group to virtualize network node functions, such as load balancers, firewalls, intrusion detection systems, WAN optimization controllers, ...
- Why NFV?
  - Network Operators' networks are populated with a large and increasing variety of proprietary hardware appliances
  - NFV allows to reduce complexity, make managing a network and deploying new capabilities easier, faster and cheaper
  - NFV is complementary to SDN, but not dependent on it (or vice-versa)
  - NFV is able to support SDN by providing the infrastructure upon which the SDN software can be run

24

References

GC 2018-2019

- [1] The 2015 Application & Service Delivery Handbook, produced by Webtorial (http://www.webtorials.com/content/2015/08/the-2015-application-service-delivery-handbook.html)
- [2] "The macroscopic behaviour of the TCP congestion avoidance algorithm", M. Mathis & alias, Computer Communication Review, volume 27, number 3, July 1997
- [3] Software-Defined Networking: The New Norm for Networks, Open Networking Function, (https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf)

25

References (cont.)

GC 2018-2019

- [4] Software-Defined Networking, Open Networking Function (https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/SDN-architecture-overview-1.0.pdf)
- [5] Network Functions Virtualisation – Introductory White Paper, http://portal.etsi.org/NFV/NFV_White_Paper.pdf
- [6] The 2015 guide to SDN and NFV, http://www.ashtonmetzler.com/2015_Guide_Complete.pdf

26