IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 1, January 2025

DOI: 10.17148/IJARCCE.2025.14112

PRIORITIZATION OF CHARGEABLE TRAFFIC AND NETWORK SECURITY NITTY-GRITTIES

E. G. Okereke[1], E. G. Chukwu[2], O. P. Ekwe[3], C. N. Asogwa[4], E. L. Anozie[5], & A. A. Umaru[6]

Department of Computer Science, University of Nigeria Nsukka, Enugu State[1]

Department of Computer Science, University of Nigeria Nsukka, Enugu State[2]

Department of Computer Science, University of Nigeria Nsukka, Enugu State[3]

Department of Computer Science, University of Nigeria Nsukka, Enugu State[4]

Department of Computer Science, University of Nigeria Nsukka, Enugu State[5]

Department of Computer Science, University of Nigeria Nsukka, Enugu State[6]

Abstract: In order to carry real-time traffic like video, IP networks, especially intranets recently began to deal with different levels of priority for communication flows. Traffic prioritization is the key to meeting the demands of real-time traffic, which are much more stringent than mere data traffic, such as file transfers. Now that the question: "How should we specify different levels of priority?" is reasonably understood, the challenge is to answer this new one: "How should we charge for these different levels of priority by understanding Network Security?"

This document discusses the introduction of Quality of Service (QoS) in the corporate network of a large industrial enterprise. Its main contributions are a charging model for different types of traffic with different levels of priority, a network simulation for verifying the impact of a QoS implementation and detailed understanding of network security nitty-gritties.

I. INTRODUCTION

Traffic on corporate networks is increasing fast. This is partly due to the introduction of many new applications in the market offering services such as videoconferencing, multimedia, and other bandwidth-demanding services. It may also be due to the increasing use of the Internet and the fact that more and more tasks are performed by computers. In addition, today's applications are more demanding, largely because there is an important cost trade-off between fast and efficient programme. This increase in the traffic negatively affects the performance of corporate networks. During peak hours, this can result in congestion and therefore in insufficient service levels for business-critical applications. To support this new amount of traffic and, more importantly, to ensure the operation of critical applications on the intranet, some measures must be taken.

There are different approaches for solving these problems. The first solution that springs to mind is increasing the bandwidth of the network by allocating more resources. This would, of course, solve the problem in the short term. Since a corporate network is often differently loaded during different times of the day, with peak hours occurring during office hours, we need to increase the bandwidth to support the maximum load under the worst conditions to be able to guarantee proper operation. This can result in an inefficient use of resources, so this we explored complementary solutions in this thesis.

To be able to guarantee a certain level of service to business-critical applications, we need to introduce Quality of Service (QoS) in the network. QoS aims to guarantee that a certain application is provided with the network resources that it needs for proper operation, e.g., bandwidth and response time. During peak hours, critical applications must have priority over less critical tasks such as, in many cases, Web browsing or FTPs. There are many different ways of implementing QoS in a network; we will explore some of the most popular.

When we let some applications have a higher priority than others, we must also introduce some incentives to prevent the abuse of the high priority class. Otherwise, we might come to a stage where all applications request the highest priority, which would bring us back to square 1. This thesis explores the introduction of usage-based charging on a

This work is licensed under a Creative Commons Attribution 4.0 International License

DOI: 10.17148/IJARCCE.2025.14112

corporate network. Network resources are very expensive to an enterprise, and their use should be divided between its different business units. By introducing usage-based charging in the network, these costs can be fairly shared on a usage basis. Clearly, fairness is a function of the corporate aims and the pricing formula used.

The introduction of QoS and charging requires a well-defined policy for the network. The enterprise must formulate a policy for the use of its network in a cost-efficient way. There are many different parameters to network policing. What applications should be allowed a certain QoS? At which hours are which users allowed to use how much bandwidth of the network? Who should be charged and at what price? There are other aspects to policy-based networking such as security, but these are beyond the scope of this thesis.

This project aims to clarify the need for introducing QoS and charging in a large corporate intranet. It will focus practically on tests for implementation of QoS and charging in a large multinational enterprise.

II. PRESENTATION OF XPERTECH SOLUTIONS GROUP (XSG)

2.1 Xpertech Solutions Group in Brief

This is a leading force in ICT and renewable energy, providing a comprehensive range of services, including computer hardware, software, security systems, and professional ICT solutions, alongside renewable energy offerings. Our expertise is centered on delivering solutions that align with and enhance business objectives.

Supported by a highly skilled management team and staff with a combined experience of over 250 years, we excel in deploying solutions across various sectors such as oil & gas, government, banking, education, and real estate. Our team's diverse background, encompassing both service provision and consumer perspectives, drives a strong customer-centric approach in all our engagements.

Expertise drives our mission-critical ICT and renewable energy solutions. Using proven assets and advanced technologies, we provide clients a competitive edge in today’s fast-changing landscape. By addressing each client’s unique needs, we deliver tailored, effective solutions, avoiding generic approaches.

We are dedicated to offering innovative solutions that empower and transform businesses. Whether it’s enhancing revenue, improving efficiency, engaging customers, securing operations, or ensuring reliable energy supply, we provide the products, solutions, and expertise needed to tackle complex technological challenges.

Our mission is to empower businesses by leveraging ICT solutions as strategic assets and integrating renewable energy for uninterrupted operations. We offer services like network infrastructure, connectivity, security systems, productivity tools, business continuity, software development, training and so on.

2.2 Physical Network Structure

Xpertech’s corporate network, henceforth referred to as the XSG, consists of several large area sites interconnected worldwide as shown in Figure below. Smaller area sites are, in turn, connected to a larger area site. The XSG comprises roughly 500 routers and 300 Frame Relay lines plus a number of leased lines. We count about 40.000 end users in the complete network. Investigations have shown that to support a number of users with application server services, printers and other networking equipment, we need about 1.3 host stations per user. In the entire XSG we have about 52.000 host stations

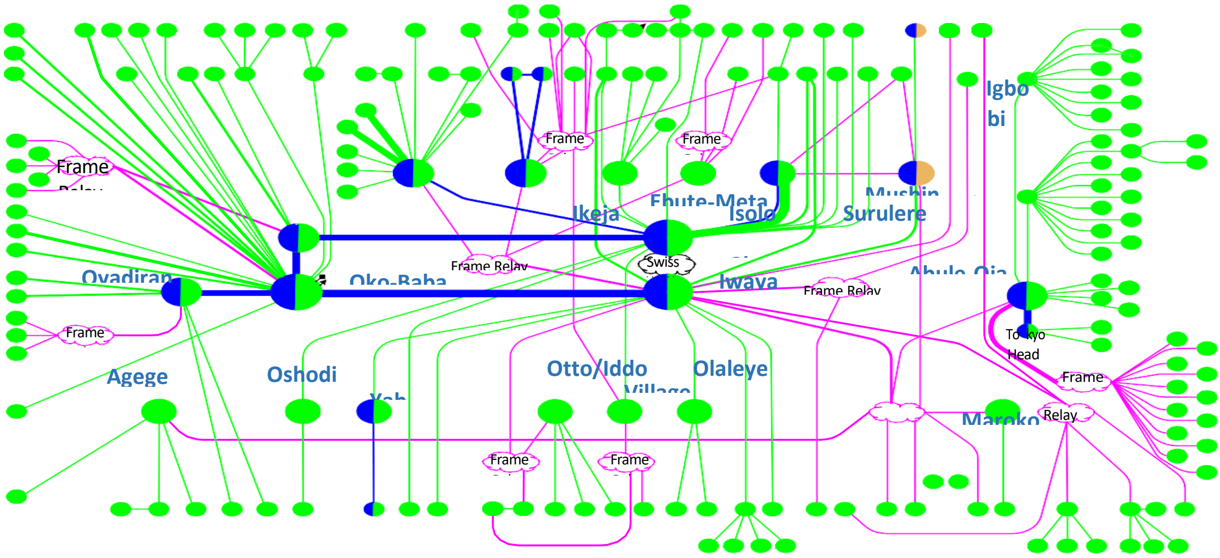


Figure 2-1: Xpertech Solutions Group

The site at which this research is carried out is located in Logos, Nigeria. The LANs of the two locations are interconnected via an ATM backbone and form one site. The physical structure of this site is shown in Figure below. This site has 7600 end users and about 10.000 host stations. The routers in the squares marked with core, connects this site with the rest of Xpertech Solutions Group.

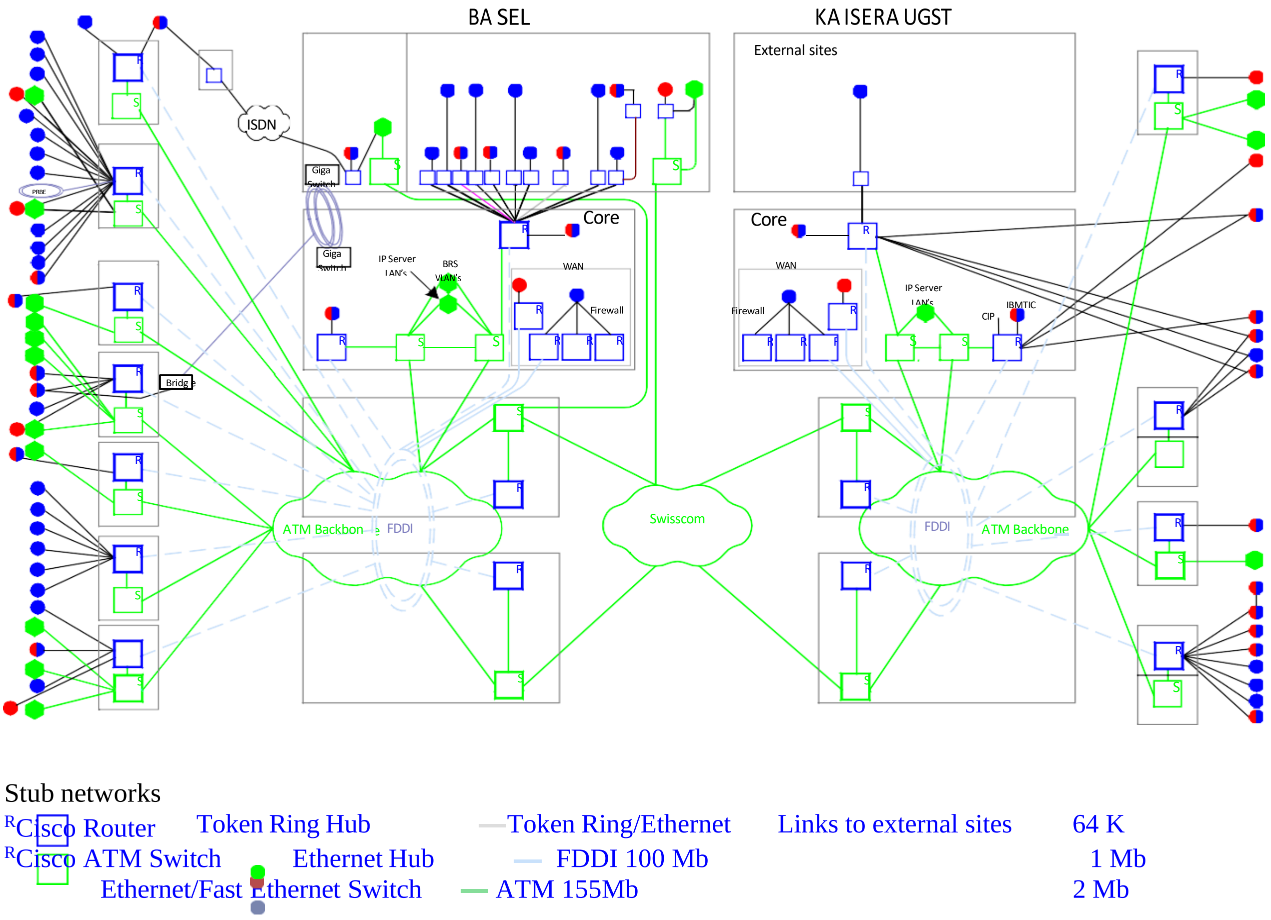


Figure 2-1: Xpertech Solutions Group

DOI: 10.17148/IJARCCE.2025.14112

III. QoS IN IP NETWORKS

3.1 What QoS Means

It means Quality of Service and it is the term that describes the methods for introducing a differentiated service model in the networks. All applications used over the network are not created equal. Some applications need more predictable service than others do, as for instance interactive applications such as telnet. Some applications are more sensitive to delay or delay jitter than others are, as for instance telephony over the Internet. Some applications are very sensitive to packet loss, as for instance router configuration messages via ICMP. It is clear that we might get our network to work better if we somehow could organize all this instead of just sending everything into the network on a first come first served basis.

QoS is the term used for this organization. By differentiating one type of traffic from another we could provide them with different service levels. There are several methods for doing this, and we will describe the most popular further down in this chapter.

3.1 Why QoS is Important

Good functioning of the applications used on the company intranet is crucial for business. A company cannot afford badly functioning of business-critical applications.

Traffic on company intranets is increasing very fast. This is probably due to the introduction of a large amount of new applications in the market offering services such as videoconferencing, multimedia, and other bandwidth-hungry services. It may also be due to the increasing use of the Internet.

Network equipment and links are costly resources in a corporate network. The solution for supporting higher amounts of traffic might not always be to increase the size of the pipe once the network gets congested. As we must deal with the network congestion in a cost-efficient way, this thesis explores an alternative solution.

Apart from supporting the needs for the applications, there is also a policy point of view. Business policy might aim to give certain business-critical applications higher priority or even reserve bandwidth for them. Such a management facility is commonly called “controlled link-sharing”.

3.2 How to Measure QoS

Packets in a flow from a sender to one or more receivers will be affected by network characteristics on the way. There are four very important characteristics of a packet flow; bandwidth, delay, jitter, and reliability, as described by Mills C. et al (2021).

Bandwidth is the maximal data transfer rate available to a flow between a sender and a receiver. The upper bound of the bandwidth available is the physical link capacity of the link with the lowest capacity on the path between the end-points in a simple topology. In more complex topologies several links could run in parallel between end-points and the upper bound on the bandwidth gets more complicated to calculate. Other flows may also be using parts of the path between the end- points, reducing the bandwidth available to the flow in question.

Delay is the time it takes for a packet to travel from a sender, through the network, to the receiver. Delay is due not only to transmission links, but is also increased by router holding time. If the packet has to be queued in the router it will experience higher delay.

Jitter is the variation of the delay. Mathematically it is the absolute value of the first derivative of the sequence of individual delay measurements.

Reliability measures the probability that the data arrives properly at the receiver. Errors can be introduced either on the physical link layer where a bit or a number of bits get changed during transmission, (bit-errors and burst-errors). Or, routing and protocol processing in the system can introduce degradation in reliability, as the order of the packets can be changed (packet reordering) or packets can be lost (packet loss).

These are characteristics that are directly measurable and that can be modeled mathematically. Now we have to remember that behind each flow is a transfer protocol and an application. Different types of protocols and applications behave differently when encountering the limitations described above. Taking the jitter parameter as an example: A user doing a file transfer would not experience any degradation in quality, although the TCP protocol might work a bit inefficiently. A user talking on the telephone over IP, on the other hand, would experience degradation in quality due to the loss of signal.

Tools are evolving to measure application specific response-times, taking into consideration the user need at the moment. Examples of such tools are ETEWatch from Candle Corp. and Smartwatch from Landmark Systems Corp. Packages that work only with one specific application are for example Stopwatch Pro from Envive and Luminate for SAP/R3 from Luminate Software Corp, both of which analyze SAP R/3. DataCom by Stallings, W. (2022) recently published an evaluation of response- time measurement tools.

3.3 QoS Models

The above mechanisms help us use our network efficiently, but they do not let us differentiate certain traffic from other. Differentiation would be preferable, since different users or applications have different needs. The following paragraphs discuss the two most important QoS models for introducing different levels of service for network traffic: differentiated services and integrated services.

3.3.1 Differentiated Services

There is an IETF Working Group called DiffServ according to Postel, J. (2019) that is working with a differentiated services model on the Internet Blake, S. et al (2018). Differentiated services aims to give some traffic flows better service than others. To distinguish between flows we need a way to mark packets with a priority. The priority can be used either to let some traffic flows have precedence over others by reordering packets in the queue so that higher priority packets get sent first. Or, the priority could serve as a discard preference. A packet with a lower priority level would be discarded more easily in the event of congestion than a packet with higher priority.

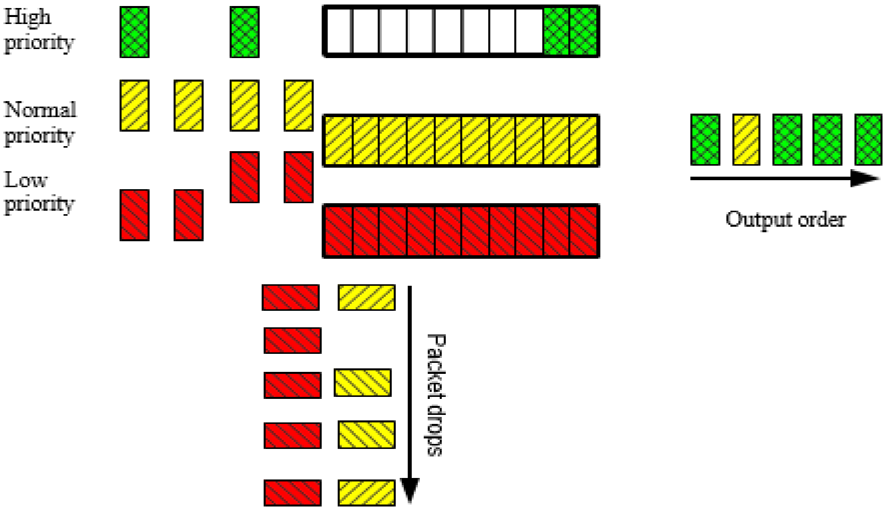
The most common way to mark packets is via IP Precedence, as described in the initial Internet Protocol RFC, Zappala, D. (2019). A subfield of the TOS (Type of Service) octet in the IPv4 header is used for this. The three leftmost bits in the TOS field are used, giving a possible maximum of eight different priority levels. The priorities are set as 0 for lowest priority and 7 for highest. The IETF Working Group proposes as an extension to use the complete TOS-field as priority field. They propose to call the field for the Differentiated Services (DS) field, UCB/LBNL/VINT (2020). Six bits are used for setting priority, giving a possible maximum of 64 different priority levels. The two leftover bits are reserved for future use.

The idea of differentiated services is to set the priority level of the packet when it enters the network. This is done by a packet classifier. A packet can be classified as a certain priority by examining its source and destination IP address and/or by other information found in the packet header such as a TCP or UDP port number. The network manager has to define a policy for what traffic should be classified as what priority level, then the core network has only to implement scheduling algorithms to queue and forward the packets to their destinations. It is especially important to apply those mechanisms at network bottlenecks, as it is in these areas where congestion is most likely to occur.

The basic modification of the single level FIFO queuing algorithm to enable differentiated services is to divide traffic into a number of categories, and then provide resources to each category in accordance with a predetermined allocation structure, implementing some form of proportional resource allocation.

A basic modification of the FIFO structure is to introduce Priority Queues. The idea is to create a number of distinct queues for each interface and associate a relative priority level with each one. Packets are scheduled from a particular priority queue in FIFO order only when all queues of a higher priority are empty. In such a model, the highest priority traffic receives minimal delay, but all other priority levels may experience resource starvation if the highest precedence traffic queue remains occupied. See Figure 3-1 for the scheduling principle. Note how the low priority traffic gets completely starved by the two higher priority traffic flows. This model is simple to implement, but to ensure that all traffic receives some level of service we need more sophisticated scheduling algorithms.

© IJARCCE This work is licensed under a Creative Commons Attribution 4.0 International License



A more sophisticated method would be to classify each traffic flow as belonging to its own queue. This could be done by differentiating flows by criteria such as source and destination address, source and destination port, ProtocolID, and TOS field. The router assigns each flow its own queue. It then applies its scheduling mechanism to these queues, so that the packets gets scheduled on a per flow basis.

We would service each queue in order to its relative weight. This approach is called General Processor Sharing, GPS. The equation for calculating the bandwidth received for each flow would be:

$$BW_{MyFlow} \quad \frac{(\Pr ec_{MyFlow} \quad 1)}{_{i} \; (\Pr ec_{Flowi} \quad 1)} \quad BW_{total}$$

BW_{MyFlow}	The share of the bandwidth allotted to the flow in question.
$Prec_{MyFlow}$	The IP precedence set for the flow in question
$_{i} \; (\Pr ec_{Flowi} \quad 1)$	The sum of the (IP precedence + 1) for all flows.
BW_{total}	The total bandwidth available on the link.

We could use a weighted round-robin scheduling algorithm to service each queue. As an example we use four queues with priority 3, 1, 0, and 0. Our weighted round robin schedule will send four packets from queue number one, two packets from queue number two and one packet each from queues number three and four. Then we start over by sending packets from queue number one again. See Figure 3-2 for the scheduling principle. When packets are equally large, this mechanism fairly shares the bandwidth between all flows on our link. When packet sizes vary we would come to a situation where a flow with larger packets would occupy more bandwidth than a flow with smaller packets of the same priority. To avoid this, we would be better off using a deficit weighted round-robin algorithm, which modifies the round robin algorithm to use a service quantum unit.

This is also known as a bit-wise round-robin algorithm. A packet is scheduled from the head of a weighted queue only if the packet size minus the per-queue deficit counter is less than the weighted quantum value. The next packet in the queue is tested using a weighted quantum value, which has been reduced by the size of the scheduled packet. When the test fails, the remaining weighted quantum size is added to the per-queue deficit counter and the scheduler moves to the next queue. This algorithm performs with an average allocation that corresponds to the relative weights of each queue on a bandwidth basis.

DOI: 10.17148/IJARCCE.2025.14112

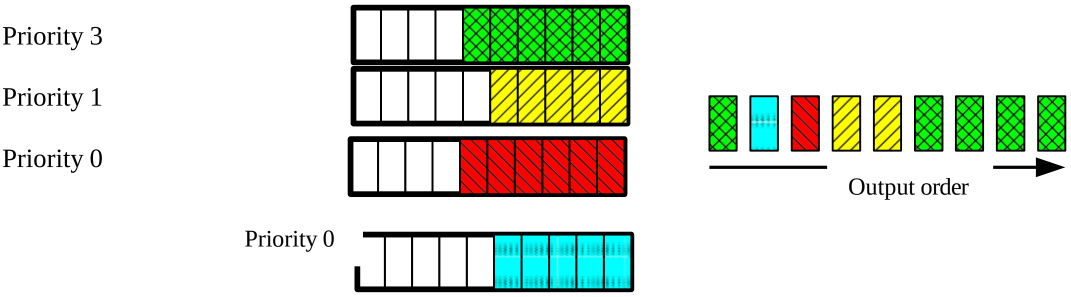


Figure 3-2: Weighted Round Robin Queuing

IV. QoS IN XPERTECH SOLUTIONS GROUP

4.2 Motivation

There are several applications considered as business critical on Xpertech Solutions Group. Considered the increasing load on the network there is a wish for introducing a more consistent service for these applications, especially during peak hours. The desire is to have fast response times for the applications used. The applications that are considered as business critical at the moment are: SAP, Oracle Clinical, and two more Oracle database applications. There is no intent to differentiate between users.

4.2 Differentiated Services in the XSG

The model chosen by Xpertech Solutions Group to evaluate is the differentiated service model using IP Precedence and WFQ. Using the differentiated service model on the XSG would mean assigning the above applications a certain priority and applying a queuing mechanism that recognizes these priorities. On Cisco routers, the preferred method for doing this is using IP Precedence and WFQ. Since Xpertech has almost exclusively Cisco routers this seems to be the obvious way to go.

For determining what flows/packets belong to a certain application on the network we need to work out what characterizes these flows. At a minimum we could look for the application servers IP addresses in the Source or Destination address field in the IP header of the packets. If we want more granularity we could also look in the Source or Destination port field in the IP header for application specific ports. This is useful if more than one application is active on a server. It should be noted, though, that not all applications use specific port numbers. Some applications simply use a range of ports that are free, which are negotiated in the first connection. Also, the Cisco IOS 11.2 release does not support differentiating packets on a port number basis when setting the priority level.

Installation consists in gathering data about application servers’ IP addresses and configure the key routers for marking packets with IP precedence and for enabling WFQ. See further down in this section for commands used for doing this.

Advantages with this model are that it is fairly simple to implement and does not require additional hardware or software. Benefits are that business-critical applications should get priority over best- effort traffic.

Disadvantages are that we have to keep a record of all server addresses and update the router configuration if they change. With a good database this could be done automatically by scripts if the security issue about who can log in to a router can be solved.

4.3 Tests of QoS XSG

It was decided to test this model both in a network laboratory (NetLab) with real hardware and in a network simulator, which was part of this thesis project. See chapter *5 Simulation of QoS Benefits* for the simulation.

The goal of the tests was to verify the functionality of the WFQ and IP Precedence on the Cisco routers and to estimate the effect of introducing QoS in the Xpertech Solutions Group. A test network topology was set up, as shown in Figure 4-1.

DOI: 10.17148/IJARCCE.2025.14112

It was decided to use FTP and Ping for the functional tests, and to use the application SAP R/3 for testing the benefit for a real application when introducing QoS. There are at least two good reasons for choosing SAP R/3 as a test application. First, it is a productive application where we can see the benefits directly. Second, in SAP there is a possibility to record macros, which will simplify the test process. We can record a typical SAP transaction and save as a macro. The next time we want to run it, we do not need to go through the complete process again, but merely select the macro to run. It can either be run in the background or in the foreground, where each step in the macro is confirmed by a key press.

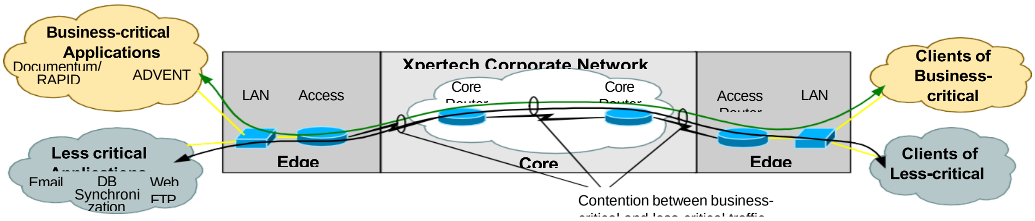

Business-critical Applications
Documentum/ RAPID
ADVENT
Less critical Applications
Email
DB Synchronization
Web
FTP
Xpertech Corporate Network
LAN
Access
Edge
Core Router
Core Router
Core
Access Router
LAN
Edge
Clients of Business-critical
Clients of Less-critical
Contention between business-critical and less-critical traffic

Figure 4-1: NetLab test setup

4.4 Test results

The tests in the NetLab according to Xpertech. *QOS project (2019)* and the tests with the network simulator show that the business-critical applications would benefit from a scenario with WFQ and IP Precedence. Test results show that it is important to characterize the traffic pattern of the application intended for prioritization, as the benefit from this QoS model varies with parameters such as packet size and throughput. Chapter 5 discusses this issue further. It was decided to implement this variant of differentiated services in the XSG.

The NetLab tests also discovered that we increase the load on the CPU on the routers largely when using Cisco IOS 11.2 and classifying packets. Using Cisco IOS 11.3 shows a much more moderate increase in CPU load, why an upgrade is recommended before deploying these services on the routers that should do the classifying of packets.

V. SIMULATION OF QOS BENEFITS

The purpose of this simulation is to verify the impact of introducing QoS in the form of IP Precedence and WFQ on Cisco routers in the corporate network. The theoretical result coming out of this test is checked against the tests carried out on hardware in the NetLab.

5.1 Simulation Model

For the test setup, five parts need to be included in the model:

- The **network topology** includes the network host stations, the routers, and the links between these entities. The configurable parameters of the links are duplex, bandwidth, and delay.

- The **queuing mechanism** will be configured to work on the router nodes in the network. The mechanism we will use is WFQ. The queuing mechanism controls the output on the link.

- The **traffic flows** are established between host machines in the network. Traffic flows will be used for generating background traffic and to simulate FTP and SAP traffic on the network.

- The **traffic classifier** will be used to work on the edge routers of the network. The purpose of this classifier is to set the IP Precedence bits on the packets belonging to the flows to be prioritized.

- The **measurement mechanism** will be used for measuring flow start and end times. We need this to be able to compare flow statistics with and without QoS applied.

These five parts should be considered when choosing the Network Simulator to work with.

DOI: 10.17148/IJARCCE.2025.14112

5.2 Choice of Simulator

Due to the relatively short time for the simulation, I did not have time to make a thorough evaluation of different simulators, so I chose to rely on recommendations of others. Also, since my budget for this was zero, it limited the possible choices. At EPFL we had an old version of a commercial simulator called OpNet, but it was available neither at Adventis, nor at Xpertech. A new license for this simulator costs around $100'000. The simulator, which was recommended by EPFL staff, was the UCB/LBNL/VINT Network Simulator - NS v.2 (version 2) according to Postel, J. (2015), hereafter referred to as ns.

This simulator is a discrete event simulator targeted at networking research. It was developed at the University of California, Berkeley. The first implementations of nswere developed primarily on Unix (SunOS, FreeBSD, and Linux), but ns was also ported to Windows-95 and NT. It is free of charge and can be downloaded from <http://www-mash.cs.berkeley.edu/ns/>.

The simulator is written in C++. As a command and configuration interface it uses OTcl, which is an object-oriented version of Tcl. My study of the nsdocumentation according to Jander, M. (2018) showed that it should be possible to implement the above elements and to conduct the tests we have set up.

5.3 Implementation: The Simulator

In ns,the network topology is represented by nodes and links. The links connect the nodes with each other. The nodes represent both the routers and the host stations. The links can be configured for a certain delay and bandwidth. One-way links or full duplex links can be used.

The queuing mechanisms in nsare configured per link. This gives the same functionality as if they were implemented on an interface port of a router. The queuing schedule is applied to the packets before they are sent to the receiver side of the link.

The traffic flows are set up by agents that sit on the nodes in the nstopology, and applications connected to these agents. The agents represent the transport layer. There are implementations of TCP and UDP, which is enough for our tests. Applications are representing the upper layer protocols. There are implementations of a File Transfer Protocol (FTP) and Constant Bit Rate traffic (CBR) as applications. I have configured a Client/Server application model for the SAP traffic in OTcl. Each agent, and therefore traffic flow, can be assigned a FlowId. The queuing mechanism, for instance, uses this FlowId when setting up the queues.

I did not find an implementation of a Packet Classifier in ns. Instead, nsoffers the possibility to assign a priority to the node agents. This way the traffic flow created by the agent will have a certain priority already from the beginning. This change of idea does not matter for our simulations, since it was not the Packet Classifier itself that was to be tested. The important thing is that we can set the priority of certain flows.

When run, nsproduces a log file. In the log file, we find information about each packet in the simulation, and what happens to it. The packet can be sent, received or dropped, for example. Timestamps are associated with these entries. In addition, nsprovides a discrete clock mechanism that can be used within applications to signal a start or stop time for example. This gives us the possibility to measure the traffic flows, as we wanted.

DOI: 10.17148/IJARCCE.2025.14112

5.4 Test Model Setup

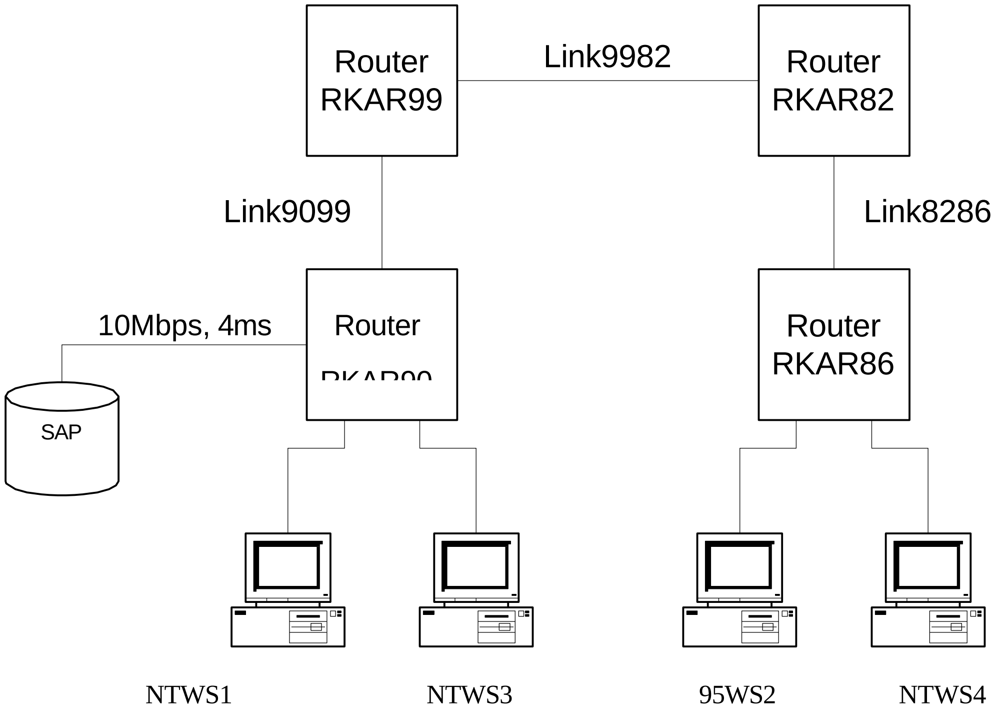


Figure 5-1: Topology setup in ns

Figure 5-1 shows the test topology that I configured in the simulator. Background traffic is run between the stations NTWS3 and NTWS4. FTP traffic is run between stations 95WS2 and NTWS1. SAP traffic is run between stations 95WS2 and SAP Server.

Background traffic is created by 15 concurrent UDP flows. The packet size of the UDP datagrams is 1310 bytes. Each flow sends a packet every 0.02 seconds. This creates a total load of 7.5 Mbps in each direction in the test network.

NB: Two types of applications will be tested:

- FTP File Transfer of a 100 kbytes file

- SAP macro zb160172. This macro creates a new test user in SAP and deletes the same user again. It consists of 7 screens. The macro starts by sending one packet from the client to the server. The server returns one packet to the client and this continues for 7 rounds. The packet sizes vary between 40 and 931 bytes.

For each test, three cases will be run:

- Baseline: The application will run without any background traffic to disturb it.

- Background: The application will run together with the background traffic.

- Priority: The traffic from the application will be prioritized and run together with the background traffic.

© IJARCCE This work is licensed under a Creative Commons Attribution 4.0 International License

DOI: 10.17148/IJARCCE.2025.14112

The tests are conducted in four different configurations, as shown in Table 5-1.

	Link 9099	Link 9982	Link 8286
Configuration 1	**64 kbps, 1 ms**	**2Mbps, 1 ms**	**64 kbps, 1 ms**
Configuration 2	**64 kbps, 1 ms**	**2Mbps, 50 ms**	**64 kbps, 1 ms**
Configuration 3	**10 Mbps, 1ms**	**2Mbps, 1ms**	**10 Mbps, 1ms**
Configuration 4	**10 Mbps, 1ms**	**2Mbps, 50ms**	**10 Mbps, 1ms**

Table 5-1: The four configurations in the test setup

5.5 Test Results

5.5.1 FTP and SAP test

File Transfer 100k	Baseline (seconds)	Background (seconds)	Increase of RTT
Configuration 1	**13.9**	**231.9**	**1568%**
Configuration 2	**14.4**	**229.6**	**1494%**
Configuration 3	**0.49**	**9.64**	**1867%**
Configuration 4	**1.11**	**10.25**	**823%**

Table 5-2: Round Trip Time for FTP File Transfer of a 100 kbytes file.

SAP macro zb160172	Baseline (seconds)	Background (seconds)	Increase of RTT
Configuration 1	**0.98**	**5.29**	**440%**
Configuration 2	**1.76**	**5.65**	**221%**
Configuration 3	**0.18**	**0.24**	**33%**
Configuration 4	**0.96**	**1.04**	**8%**

Table 5-3: Round Trip Time for SAP macro zb160172

An FTP File transfer takes 9-20 times longer when encountering background traffic depending on the configuration. The mathematical result should be 16, since the bandwidth should be shared equally between the 16 flows. The deviation from this result could be explained by:

- TCP setup time. The FTP flow is not running at maximum speed until the maximum TCP window size is fixed.

- For configuration 4, the link delay is more important when running the baseline test than when running the background test. The background traffic introduces more delay to the FTP flow than the link itself, and the result converges with that of the configuration 3 test.

© IJARCCE This work is licensed under a Creative Commons Attribution 4.0 International License

DOI: 10.17148/IJARCCE.2025.14112

-

The SAP macro takes 3-5 times longer when encountering background traffic for the configurations 1 and 2. For the configurations 3 and 4 we can see almost no difference. This time, the deviation from the mathematical result can be explained by two facts:

- SAP traffic gets more bandwidth than it needs. This is why we can see almost no difference in the configurations 3 and 4. The SAP traffic gets a share of the bandwidth equal to 2Mbps/16 = 128kbps, which is actually more than the 64kbps it receives in the configurations 1 and 2 without background traffic. We note that it is consequently faster in configurations 3 and 4 with background traffic.

- The SAP traffic benefits from the WFQ mechanism because it is an interactive flow. When its packets arrive in the queue they get scheduled quite soon, since the last SAP packet was sent quite some time before.

VI. CHARGING IN XPERTECH SOLUTIONS GROUP

6 .1 Motivation

The Xpertech Solutions Group (XSG) is structured around a backbone with main sites connected to it. Smaller sites are connected to the main sites, and could, in turn, have “child sites” connected to them. Each site has costs for Wide Area Network (WAN) implementations such as links and WAN routers. It is not at all sure that the site that implements or maintains a link or other WAN equipment is the only site using it, since the site might serve as an interconnecting entity between other sites. This cost must then be divided by those who benefit from it.

The organization of the company is not constrained by the network structure. Business units can be a division of a site, as well as span over site or country boarders. Each of these units uses the WAN differently. This is why it is important to fairly divide the WAN costs between them.

With the introduction of QoS in the XSG, some traffic will be given a higher priority than other traffic. It is also very important to be able to charge for this.

6.1.1 Today’s Model of Charging

The model used for dividing the costs for the XSG today is a weighted subscription-based charging. Thus, each business unit pays a share of the cost based on the number of employees it has and a weighting factor that takes into account how much load they put on the network. This weighting factor is estimated by some network monitoring and general knowledge about network usage, but no real-time measurements are taken into account.

6.1.2 Customer Requirements Analysis

In 1998, a customer requirement analysis was performed by a consulting firm (At Rete[1]) for Xpertech. The customers are, in this case, the business units of the Xpertech organization. The results of the analysis were that the current cost division is perceived as unfair, and that there is a wish for a new charging model. The cornerstones of the expected new model are that it should be fair, accurate, simple, flexible, and efficient:

- Fair in the sense that the costs should be fairly divided by the actual users of the WAN.
- Accurate in the sense that the charging should be based on accurate data. Thus, the usage of resources in the XSG should be measured before they can be charged for.
- Simple in the sense that it should be easy to understand the algorithm and to calculate the share of the cost for each cost center. This is very important for budgeting.
- Flexible in the sense that it should be easy to recalculate the charging algorithm when the structure of the network or the organization change.
- Efficient in the sense that the cost of implementing the charging structure should not be so large that it outweighs the benefits.

6 .2 IP Address Resolution Issues on XSG

For user-based charging, the main issue is: How to recognize end users? From an IP packet in a flow, we can get the

DOI: 10.17148/IJARCCE.2025.14112

source and destination IP addresses and the source and destination ports. From this information we would like to resolve who the owner of the flow in reality is. This could be a user or an application server, for example.
In Xpertech's network, as described in section 2.4, an IP addresses is registered to the MAC address of the network device, and therefore to end user and cost center. This data is stored in a Network Management database, and it is accurate in 80% of the cases, since not all addresses have been registered with the Network Management Tool application. In the cases where DHCP is used, there are scripts running every six hours to update the Network Management database with the IP addresses mapped to MAC addresses. The default lease time for an IP address is 7 days, which means that if a machine is used more often than once a week, it will retain its IP address from time to time. We should however be aware that this information might be inaccurate for a small fraction of the end-stations during intervals shorter than 6 hours. Server addresses are static, and a database is being built up to add additional information about application servers, such as source and destination TCP or UDP ports of the application.

If we manage to resolve the IP address to the machine ID, then we still might have a problem if different users share the same machine. If these users belong to the same cost center, this issue is probably not so important, but if this is not the case, then we have to find a way to split the cost for this machine between its users.

In case the IP address belongs to an application server, we must conclude whether only one application is active on the machine, or if we might have more than one. If we have more than one application on the same machine, we might try to resolve which one is active in thy flow by looking at the port numbers they use. This may work in some cases, but there are also applications that simply use a range of ports that are free, which are negotiated in the first connection. In these cases it is not possible to identify the application by the port numbers used. Again, if the applications belong to different cost centers, we will have to find a way to split the cost for this machine.

To resolve the problems related to the user IP addresses, we suggest one of the following:

- Update the database that ties IP address to users and make sure it is regularly maintained. The charging application needs to interact with this database.

- Install a user registration utility that interoperates with the NT logon server, for example the Cisco User Registration Tool (URT), IETF DiffServ Working Group (2019). The charging application can then interact with the URT database.

To resolve the problems related to the server IP addresses we suggest to install the two applications on different machines if we cannot resolve the problem by simply splitting the cost equally over the applications.

Other implications concerning IP address resolution are related to traffic via a proxy server, and multicast traffic, where the real source or destination address is not visible. To resolve these addresses to the real source or destination address we need to interact with other units on the way, such as proxy servers or multicast routers. This type of traffic represents about 5-10% of the total WAN traffic during daytime, and normally less than 1% during night. We suggest to apply flat-rate charges for this type of traffic for the moment, not to complicate the charging model with too many database interactions.

6 .3 Evaluation of scenarios for implementing charging in the XSG

The following sections discuss different scenarios for implementing charging in the Xpertech Solutions Group. We start by confirming a distributed approach to the charging model in section 7.3.1. In sections 7.3.2 and 7.3.3, we look at different scenarios for charging. These include both flat-rate and usage-based charging models.

6.3.1 Distributed Approach

The XSG is a large network interconnecting distant sites. The WAN links connect these sites together and it is on these links that we can measure WAN activity. The ends of a WAN link belong to two different sites, and therefore it makes sense to use a distributed model to describe the charging model for the XSG with the sites as independent charging domains.

For this distributed model, we can separate the charging of WAN costs in two steps:

1. divide overall cost of WAN between sites (Intersite Charging); and
2. let each site charge back its costs to the appropriate granularity (charging within the site)

The term charging within the site should not be confused with charging for traffic within the site. The costs allocated to a site by the intersite charging are distributed to business units within the site at the proper granularity. If these tasks are independent, we can imagine different scenarios for both cases and combine them for optimal efficiency. Also, the benefit of separating these two tasks is that each site can possibly use different methods for charging within the site depending on their needs.

6.3.2 Intersite Charging

This is the first step of the distributed model as described in section 7.3.1. We have set the accountable entity to a site and we will now discuss the parameter 1 in section 6.2.2 – what should be charged for, and how?

6.3.2.3 Calculated fixed price Intersite charging

The idea of this scenario is to distribute Xpertech's total costs for the WAN to sites, depending on the bandwidth of their access links. In the hierarchy of the XSG, sites belong to an area and areas belong to a region. We define links between sites as area links, regional links or backbone links. An area link is connecting two sites within an area. A regional link connects two sites within different areas, but within the same region. A backbone link connects two sites from different regions. We collect information about all the links from each site and classify the links according to the above criteria.

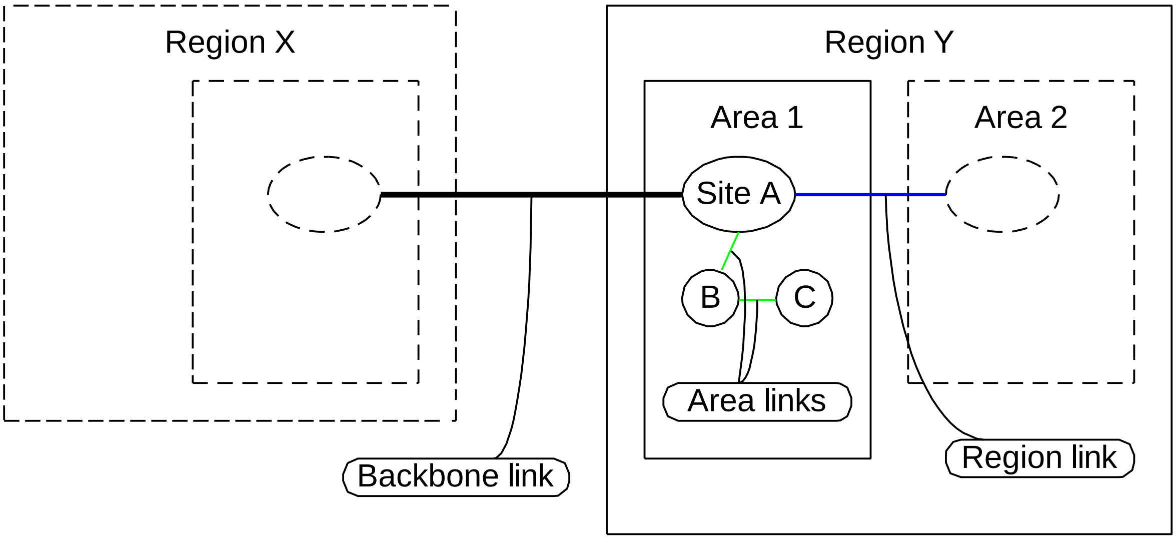


Figure 7-1: Link definitions

For each region, we calculate the total bandwidth of the backbone links connecting to the region. The sum of the bandwidth for backbone links for all regions make the network's total of backbone links. The share of the cost for the backbone that is allotted to a region is calculated as follows:

$$\text{Region's share of total cost} \; \square \; \frac{\text{Region's total of backbone links}}{\text{Network total of backbone links}}$$

This work is licensed under a Creative Commons Attribution 4.0 International License

The same calculations are made for dividing regional costs to areas. The share of the cost that should be allotted to an area within the region is calculated as follows

$$\text{Area's share of regional costs} \;\square\; \frac{\text{Area's total of regional links}}{\text{Region's total of regional links}}$$

The last step, to get to the sites share of the WAN costs, is calculating on a sites area links.

The Share of the cost that should be allotted to a site within the area is calculated as follows:

$$\text{Site's share of } \overset{\text{Areas costs}}{\square} \; \frac{\text{Site's total of area links}}{\text{Area's total of area links}}$$

This way we have allotted each site a fraction of the total WAN cost. If we take for example a site A, which belongs to the area B and to the region C. Region C uses 30% of the backbone links. Area B uses 50% of the regional links and site a uses 10% of the area links. We get the following equation: Regional cost

Costs for site a □ 0.1□ □Local area cost □ 0.5□ □Regional cost □ 0.3□ Backbone cost□□

Advantages of this scenario are that it is simple and flexible. When adding a link, we need to update the table and then we get the new portions for each site. It is quite fair for the end sites since the bandwidth of their access links should correspond to the load they impose on the network. It is not so costly to implement since it does not require any measurement equipment at all. It should be quite efficient.

Disadvantages are that it is not accurate since we are not doing any measurements. It is unfair to a site that serves as an interconnecting site that forwards traffic from one site to another. This site will be charged too much, since the bandwidth of its links is proportional to its own load plus the load of the traffic that it is forwarding. There are no incentives for use of the network in a cost-efficient way

6.3.2.3 Usage-Based Intersite Charging On A Per-Hop Basis

The idea with usage-based intersite charging is to allocate the costs of the XSG to the different sites depending on how much they are using the network. To be able to do this, we first have to define usage of the network.

To define usage of the network as resource utilization would mean to account for every traversed link and router of a flow. This is the model described in 6.3.2, with autonomous charging domains. In this scenario, we would need to measure traffic at every site border. Each site would then need to account for the traffic flows starting or ending on the site and for the flows traversing the site.

For each link, the site would exchange bills with the adjacent site on the other side. This could be done either explicitly between sites, or implicitly by sending the statistics to the Network Management group. The latter then distributes the aggregated bills back to the sites.

The setup consists in installing measurement equipment at each site border and defining the contracts between the sites. This includes the mapping of IP addresses to sites and the implementation of an automated process for updating. The flexibility of this scenario is dependent on how we could implement the algorithm for setting up the contracts and how we could automate the process of keeping a table of IP addresses.

The advantages of this scenario are that it is fair and accurate. The accounting for use of prioritized traffic is possible by differentiating flows by end-point attributes. We can also set different tariffs for the links depending on the time of day they are used. This scenario invites use of the network in a cost-efficient way.

The disadvantages are that it is not at all simple. It is costly to implement and therefore the efficiency must be carefully calculated.

DOI: 10.17148/IJARCCE.2025.14112

6.3.2.3 Usage-based intersite charging on a per-access basis

Another way of defining the usage of the network is on a per-access basis: we apply the same tariff, no matter how far data is transferred. This model is a little less fair from a cost division point of view, since short distance users are billed as much as long distance users, who use more resources. Nevertheless, if we see the WAN as a communication medium that everyone should have access to for the same price per load, then this model makes sense.

In this scenario, we measure only traffic starting from or ending at our site. We measure the traffic we send and receive on the network and get charged for it by Network Management. The security aspect is very important here. The site itself cannot be responsible for the measurement equipment, since this will be the basis for its bills.

The setup consists in installing measurement equipment at each site border and in solving the security issues related to who is responsible for the measurements.

The advantages of this scenario are that it is accurate, flexible, quite simple and quite fair. It enables the accounting for use of prioritized traffic by differentiating flows by end-point attributes. We can also set different tariffs for the links, depending on the time of day it is used.

The disadvantages are that it is costly to implement and therefore the efficiency must be well calculated.

VII. THE NITTY-GRITTIES OF NETWORK SECURITY

These are the various technologies, policies, and procedures that work together to create a secure environment for data transmission and communication. These measures are put in place to prevent cyber threats, such as hacking, data breaches, malware infections, and denial-of-service attacks.

7.1 Technologies that Create a Secure Environment for Data Transmission and Communication

The most important aspect of any company's cyber security strategy revolves around how to keep enterprise data protected and how to prevent data loss. This includes data at rest, in transit and in use.

Data security technologies come in a variety of forms, including the following:

- firewalls
- authentication and authorization
- encryption
- data masking
- hardware-based security
- data backup and resilience
- data erasure

Each of these has the same goal: keeping data safe and protected.

a. Data Security and Its Importance

Data security refers to the practice of protecting data from theft, loss or unauthorized access throughout its lifecycle.

Data breaches are a continuing issue for organizations. A Thought Lab report found a 15.1% rise in the number of data breaches and cyber-attacks in 2021 over 2020. Data breaches not only expose enterprise data, but also open companies up to lawsuits and fines.

Data security practices, policies and technologies are also key to keeping internal users from conducting inappropriate actions with any data.

Data security is important because it helps with the following:

- Keep intellectual property safe;
- Prevent financial losses;
- Maintain customer trust; and
- Ensure compliance with several regulatory standards is met.

The last point is significant because organizations have a variety of industry and federal regulations with which to comply, from GDPR and CCPA with the Sarbanes-Oxley Act and PCI DSS.

b. Types of Data Security Technologies

Data security is paramount because attackers relentlessly look for any and all vulnerabilities to infiltrate corporate networks. To keep data properly protected, enterprises can use the following seven technologies.

DOI: 10.17148/IJARCCE.2025.14112

Firewalls

A firewall is the initial security layer in a system. It is designed to keep unauthorized sources from accessing enterprise data. A firewall serves as an intermediary between a personal or enterprise network and the public internet. Firewalls use pre-configured rules to inspect all the packets entering and exiting a network and, therefore, help stop malware and other unauthorized traffic from connecting to devices on a network.

Different types of firewalls include the following:

- Basic packet-filtering firewalls
- Circuit-level gateways
- Application-level gateways
- Stateful inspection firewalls
- Next-generation firewalls

Authentication and authorization

Two processes are used to ensure only appropriate users can access enterprise data: authentication and Authorization. Authentication involves users providing proof that they are who they claim to be. This proof can be providing a secret, such as password or PIN, or biometric authentication. Depending on the authentication scenario, users may be required to provide one or more additional factors when signing in, known as two-factor authentication or multifactor authentication (MFA). Step-up authentication maybe also be required if a user attempts a more restricted action after successfully logging in initially.

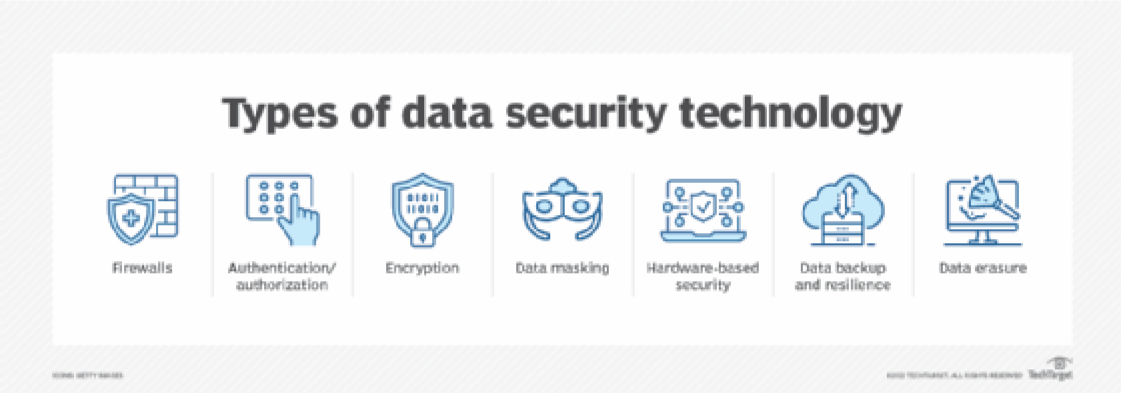
Examples of authentication are the following:

- passwords/PINs
- MFA
- biometric scans
- behavioral scans

Once users have proven their identity, authorization determines whether the user has the appropriate permissions to access and interact with specific data. By authorizing users, they gain permissions within the system to read, edit and write different resources.

Examples of authorization are the following:

- principle of least privilege access
- attribute-based access control
- role-based access control


Types of data security technology
Firewalls
Authentication/ authorization
Encryption
Data masking
Hardware-based security
Data backup and resilience
Data erasure
TechTarget

Data encryption

Data encryption converts data into coded cipher text to keep it secure at rest and while in transit between approved parties. Encrypting data ensures only those who have the proper decryption key can view the data in its original plaintext form. Encrypted data is meaningless if captured by attackers.

Examples of data encryption are the following:

- Asymmetric encryption, also known as public key encryption; and
- Symmetric encryption, also known as secret key encryption.

Keeping data at rest protected involves endpoint encryption, which can be done via file encryption or full-disk encryption methods.

Data masking

Data masking obscures data so that, even if criminals exfiltrate it, they can't make sense of what they stole. Unlike encryption, which uses encryption algorithms to encode data, data masking involves replacing legitimate data with similar but fake data. This data can also be used by the company in scenarios where using real data isn't required, such as for software testing or user training.

Tokenization is an example of data masking. It involves replacing data with a unique string of characters that holds no value and cannot be reverse-engineered should it be captured by bad actors.

Other examples of data masking are the following:

- data deidentification
- data generalization
- data anonymization
- pseudonymization

Hardware-based security

Hardware-based security involves physical protection of a device rather than relying solely on software installed onto the hardware. Because attackers target every IT layer, companies need protections built into the silicon to ensure hardened devices.

Examples of hardware-based security are the following:

- hardware-based firewalls
- proxy servers
- hardware security modules

Hardware-based security often runs isolated alongside the main processor, such as with Apple's Secure Enclave.

Data backup and resilience

Organizations should save multiple copies of data, especially if they want to fully recover following a data breach or other disaster. With data backups in place, companies can resume normal business functions faster and with fewer hiccups. To ensure data resilience, organizations need protections in place to keep the backed-up data secure and ready for use.

One example of data backup protection is data vaulting, which creates air-gapped versions of backed-up data. Organizations should also follow a 3-2-1 backup strategy, which results in at least three saved copies of data in different locations.

Other types of data backup protection include the following:

- redundancy
- cloud backup
- external hard drives
- hardware appliances

Data erasure

It is important organizations properly delete data and ensure that deleted data is not recoverable. Known as data erasure, this process involves completely overwriting stored data so that it cannot be recovered. Also known as data destruction, data erasure often involves turning data illegible after erasing it.

Organizations must be able to properly destroy data, especially in the wake of regulations such as GDPR, which stipulate customers can request the erasure of their personal data.

DOI: 10.17148/IJARCCE.2025.14112

Other types of data erasure include the following:

- data wiping
- overwriting
- physical destruction
- degaussing

7.2 Policies to Create a Secure Environment for Data Transmission and Communication

These are set of guidelines, rules, and standards organizations establish to manage and protect their data assets. It provides a framework for ensuring that data is handled, stored, transmitted, and accessed in a way that maintains its confidentiality, integrity, and availability.

10 Must-Have Information Security Policies for a Networking Company

In this discuss, we shall be stating the common policies various networking companies would have, the purposes of the policies and the applications areas or the personnel's that adheres to those policies:

S/N	POLICIES	PURPOSE	APPLICATIONS
1	Acceptable use Policy	Defines the acceptable conditions for using an organization's information	All of the organization's users accessing computing devices, data assets, and network resources
2	Network Security Policy	Outlines principles, procedures, and guidelines to enforce, manage, monitor, and maintain data security on a corporate network	All of the organization's users and networks
3	Data Management Policy	Defines measures for maintaining the confidentiality, integrity, and availability of the organization's data	All users as well as data storage and information processing systems
4	Access Control Policy	Defines the requirements for managing users' access to critical data and systems	All users and third parties with access to the organization's sensitive resources
5	Password Management Policy	Outlines requirements for securely handling user credentials	All users and third parties possessing credentials to your organization's accounts
6	Remote Access Policy	Defines requirements for establishing secure remote access to an organization's data and systems	All users and devices that access your organization's infrastructure from outside the corporate network
7	Vendor Management Policy	Governs an organization's third-party risk management activities	All vendors, suppliers, partners, and other third parties accessing your corporate data and systems

DOI: 10.17148/IJARCCE.2025.14112

8	Removable Media Policy	Outlines rules for using USB devices in your organization and specifies measures for preventing USB-related security incidents	All users of removable media
9	Incident Response Policy	Guides the organization's response to a data security incident	The organization's security officers and other employees, information systems, and data
10	Security Awareness And Training Policy	Establishes your organization's requirements for raising employees' security awareness and conducting corresponding training	Security officers and other staff organizing cyber-security awareness training sessions.

7.3 Procedures to Create a Secure Environment for Data Transmission and Communication

This can include using firewalls to block unauthorized access, implementing intrusion detection systems to monitor for and prevent cyber-attacks, and using encryption to protect sensitive information transmitted over the network.

The protection of data is a crucial concern for individuals, businesses, and organizations of all sizes. With the increasing reliance on technology for storing and transmitting sensitive information, the threat of data breaches and theft has become a major issue. In 2022, there were more than 2000 publicly disclosed data breaches, with 60% being a result of hacking. Affected companies and individuals were at risk of financial and reputational losses, compromised data, and sometimes legal liability.

To mitigate these risks, several methods have been developed to protect data from unauthorized access and manipulation. We will therefore list the top 5 methods of protecting data and discuss them briefly:

TOP 5 METHODS OF PROTECTING DATA

Looking to protect your precious business or client data? Here are the top 5 methods:

01 Encrypt your sensitive data

Encryption involves converting sensitive information into a coded form, making it unreadable to anyone without the proper decryption key. Utilize encryption when storing or sharing sensitive data to preserve its confidentiality.

02 Improve network security

Network security refers to the measures used to protect information and assets stored on computer networks from unauthorized access, theft, or damage. This can include using firewalls to block unauthorized access, implementing intrusion detection systems to monitor for and prevent cyber-attacks.

03 Implement access controls

Access control is a method of restricting access to sensitive information to only authorized users. This can be achieved through the use of passwords, multi-factor authentication, and role-based access control. These methods ensure that only those with the proper authorization can access sensitive data, reducing the risk of data breaches and unauthorized access.

04 Backup your data

Backing up data regularly ensures that data is preserved in the event of data loss or corruption. By creating copies of data and storing them in a secure location, organizations can quickly recover their data in the event of a disaster.

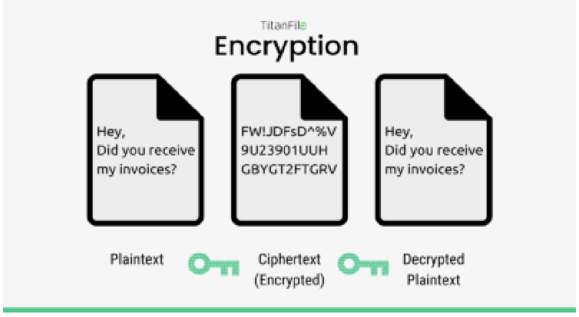
05 Improve physical security

Physical security involves the measures used to secure physical devices and facilities that store sensitive information. This can include locking devices in secure storage cabinets or vaults, implementing access control systems with biometric authentication or key cards, and installing security cameras and alarms in sensitive areas.

DOI: 10.17148/IJARCCE.2025.14112

1. Encryption

Encryption is a fundamental component for protecting personal data. It involves converting sensitive information into a coded form, making it unreadable to anyone without the proper decryption key. Only the authorized user, who possesses the decryption key, is able to decode and view the information. This method is widely used to protect sensitive data during transmission over the internet, as well as to secure data stored on devices, such as laptops and mobile phones. Additionally, encryption algorithms, such as AES and RSA, are used to scramble the data, making it virtually impossible for unauthorized users to access it.



2. Backup and Recovery

Backing up data regularly is an important aspect of data protection, as it ensures that data is preserved in the event of data loss or corruption. By creating copies of data and storing them in a secure location, organizations can quickly recover their data in the event of a disaster. Many companies use cloud-based storage services, such as TitanFile, as they provide a secure and reliable way to store and recover data. As well, experts recommend using the 3-2-1 method for backing up data. The 3-2-1 data backup method involves backing up **three** copies of data on **two** local devices (i.e. original device, external hard drive) and **one** off-site (i.e. cloud-based).

3. Access Control

Access control is a method of restricting access to sensitive information to only authorized users. This can be achieved through the use of passwords, multi-factor authentication, and role-based access control. These methods ensure that only those with the proper authorization can access sensitive data, reducing the risk of data breaches and unauthorized access.

4. Network Security

Network security refers to the measures used to protect information and assets stored on computer networks from unauthorized access, theft, or damage. This can include using firewalls to block unauthorized access, implementing intrusion detection systems to monitor for and prevent cyber-attacks, and using encryption to protect sensitive information transmitted over the network. Regular software updates and employee training can also play an important role in reducing the risk of cyber-attacks.

DOI: 10.17148/IJARCCE.2025.14112

5. Physical Security

Lastly, physical security is another important component of data protection, as it involves the measures used to secure physical devices and facilities that store sensitive information. This can include locking devices in secure storage cabinets or vaults, implementing access control systems with biometric authentication or key cards, and installing security cameras and alarms in sensitive areas. Portable devices, such as laptops and mobile phones, are also vulnerable to theft or loss and can be protected with encryption, secure passwords, and remote wipe capabilities.

CONCLUSION AND BENEFITS FOR THE STUDENT

Conclusion

This thesis was centered on two related projects at Xpertech: one concerning the introduction of QoS in the network, and another concerning the charging for the use of network resources.

In the QoS project, we have tested a model for differentiated services on XSG. The model is based on IP Precedence and Weighted Fair Queuing, which are standard components in Cisco routers today. The tests were successful, and it has been decided to deploy this model in XSGs. Apart from assisting in the testing of the hardware, carried out by Xpertech, I have provided an additional test environment using a network simulator.

In the charging project, this thesis provides an extensive study of how charging is deployed in IP networks today. It also explores different scenarios for charging in XSG, and proposes a solution with possible further enhancements in the long term. The proposed scenario combines flat-rate charging and usage-based charging with a fine granularity (end user).

On the hand, the trend of imputing network security research topics design to simulation, is becoming quite performance towards any kind of threat. With that data, you can work towards enhancing your systems' efficiency. We encourage the exchange of authentic research data while maintaining professional secrecy.

Benefits for the Student

This project has been carried out in collaboration with several institutions. The author is enrolled at KTH, Stockholm, and he conducted this thesis as an exchange student at EPFL, Lausanne. Moreover, this thesis was an industrial project in collaboration with Adventis, a consulting company specialized in telecommunications, and their customer Xpertech, a large industrial corporation in the pharmaceutical business. During the startup of the project, we realized that the challenges of this project were not all technical, as the wishes of a university do not necessarily meet those of an industrial. Coping with and solving these occasional divergences proved to be a very valuable experience.

It was also a great experience to work in a large enterprise with a high-tech corporate network. This has given me a much deeper knowledge in the field of network management, and experience with modern networking products used in the industry today. These include Cisco hardware, Cisco software, and network management applications such as

DOI: 10.17148/IJARCCE.2025.14112

Cabletron Spectrum, HP Openview Network Node Manager, HP Openview Netmetrix, and NetScout.
It has also been very inspiring to work with a consulting company, where the environment is dynamic and offers many possibilities and challenges. Responsibility and initiative are key words in such enterprises.\

Last but not least, this project gave me the opportunity to develop many technical skills, especially in IP networking and QoS, which are hot topics on the market today. I have also gained a good experience in the field of network simulation.

REFERENCES

[1]. At Rete, Xpertech. QOS project: “Limited CoS” tests. Xpertech internal project document. March 1999
[2]. S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang and W. Weiss. RFC 2475. An Architecture for Differentiated Services. IETF, December 1998.
[3]. IETF DiffServ Working Group. Available at:
[4]. <http://www.ietf.org/html.charters/diffserv-charter.html>, March 1999.
[5]. M. Jander. “Clock Watchers”. Data Communications International, September 21, 2018.
[6]. C. Mills, D. Hirsh and G.R. Ruth. RFC 1272. Internet Accounting: Background. IETF, November 2021.
[7]. J. Postel. RFC 768. User Datagram Protocol. IETF, August 2019.
[8]. J. Postel. RFC 793. Transmission Control Protocol. IETF, September 2015.
[9]. W. Stallings. Data and Computer Communications. 5th Edition. Prentice Hall, Upper Saddle River, NJ, USA, 2022.
[10]. UCB/LBNL/VINT. Network Simulator: Scenario Generation. Available at:
[11]. <http://www-mash.cs.berkeley.edu/ns/ns-scengeneration.html>, October 2020.
[12]. D. Zappala. Topology Generation for Network Simulation. Available at:
[13]. <http://www.cs.uoregon.edu/~zappala/topology/>, October 2019.