SIMULATION & ANALYSIS OF A UNIVERSITY NETWORK SETUP

ALEXANDER HILLMER & LOTTE STEENBRINK

CONTENTS

ABSTRACT

In this report we evaluated a remote campus network connected to the main campus by a radio link. The Internet connection is located at the main campus. The evaluation was done by simulating the network. To model the network traffic properly we implemented common services like web browsing, FTP upload and video conferences. Additionally we assessed the possibility to add a CCTV service, which transfers a video stream to the main campus. At the end of this report, we are identifying bottlenecks and give an overview of possible improvements.

1 NETWORK SETUP AND IMPLEMENTATION

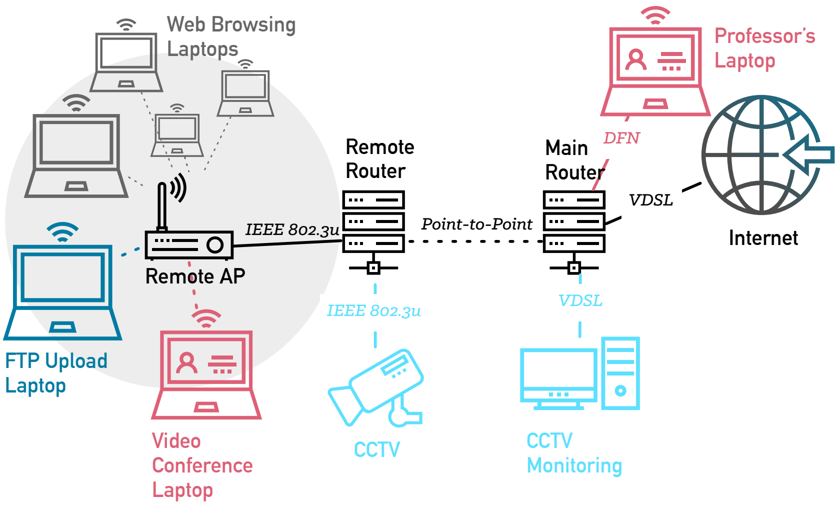


Figure 1: The Network Setup as simulated.[1]

To analyze the desired network setup, simulations were conducted. The simulated network was set up as illustrated in fig. 1. The following section discusses the implementation of the simulation and its configurations.

1.1 Applications

The network in question contains four different ways of using the network: video conference, FTP upload, web browsing and CCTV. Since all of these traffic types have different characteristics, dedicated applications which model their behavior were created.

VIDEO CONFERENCE The video conference traffic occurring bidirectionally between the Professor's Laptop and the Video Conference Laptop was modeled as a UDP application periodically sending messages of a fixed size. Packets arriving with a delay greater than a fixed maximum delay were discarded and considered lost.

FTP UPLOAD The FTP upload traffic flowing from one student's laptop to the Internet was modeled as a TCP based application which sends as much data at a time as it is allowed by TCP's congestion control algorithms. The size of the file uploaded using FTP was assumed to be endless, that is: the file upload continued over the course of the entire simulation, no matter the simulation time.

WEB BROWSING The web browsing traffic generated by all Web Browsing Laptops was modeled as a TCP application which sends HTTP requests of a fixed length to the Internet and receives varying-length responses. The idle period between two requests varies as well.

CCTV The application modeling the traffic flowing from the CCTV camera to the CCTV monitoring station is based on UDP. Similar to the video conference application, it also periodically sends messages of a fixed

[1] all icons by Icon Fair from the Noun Project.

size and ignores messages that have been delayed for too long. Its message size is significantly bigger, though, as can be seen in table 3.

For a detailed list of specific configuration parameters, see section 1.2.

1.2 Configuration Details

Video conference application	
Message length	1388 B payload + 12 B minimal RTP header = 1400 B
Packet send interval	40 ms
Maximum packet delay	100 ms
Web browsing application	
HTTP request length	8 KiB
HTTP response length	exponential($\mu = 671539$) [see section 1.3]
Idle interval	exponential(20 s)
CCTV application	
Message length	10KiB
Packet send interval	40 ms
Maximum packet delay	100 ms

Table 1: Application configuration parameters

Network	
PPP queue size	50 frames
WLAN version & bandwidth	IEEE 802.11g, 54 Mbit/s
Ethernet version & bandwidth	IEEE 802.3u, 100 Mbit/s
VDSL bandwidth	100 Mbit/s
VDSL delay	Internet: 30 ms CCTV Monitoring: 0 ms
DFN bandwidth & delay	100 Mbit/s, 5 ms
Maximum packet loss rate (video conference & CCTV)	5 %

Table 2: Network configuration parameters

Simulation	
Duration	1000 s
Repetitions	15
Number of laptops	1, 5, 10, 15, 20, 30, 40, 50 or 60

Table 3: Simulation configuration parameters

1.3 HTTP Traffic modeling

To model the size of the HTTP responses, the given trace file was analyzed in order to find a probability distribution that represents their data well.

After plotting the frequency of packet sizes found in the trace file (see Fig. 2), it was assumed that either a Poisson- or an exponential distribution could be a suitable theoretical distribution. The overall mean of the trace data is 671539. Using Pearson's χ^2 goodness of fit test, it was determined

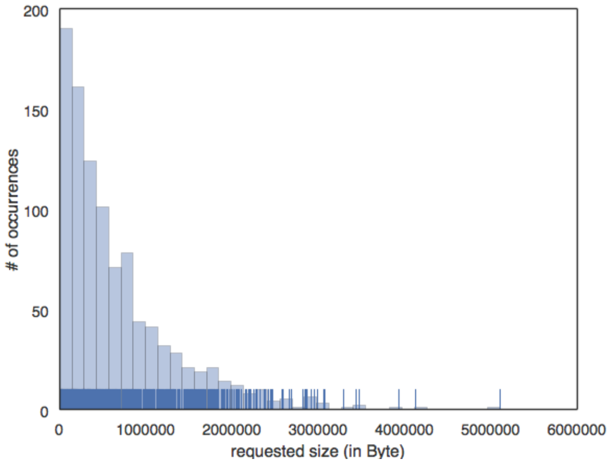


Figure 2: Frequency of packet sizes found in the trace file

that, when using an exponential distribution with mean 671539, the null hypothesis can be rejected with a 95% confidence level:

First, the sample data was divided into 100 intervals, where intervals with $\leqslant 5$ values were merged with their neighboring interval until the resulting interval contained more than 5 values, resulting in $k = 45$ intervals of observed data at the end.

Then, Pearson's χ^2 test for goodness of fit $\chi^2 = \sum \frac{(\text{Observed}-\text{Expected})^2}{\text{Expected}}$ was performed for both the Poisson and exponential distribution[2]. In both cases, $\lambda = 671539$ was used as the function's input value.

For the exponential distribution, the resulting values were

$$\chi^2 = 61.1437$$
$$\text{p-value} = 0.0222$$

leading to a rejection of the null hypothesis as $p < \alpha = 0.05$.
For the Poisson distribution, $\chi^2 = 9.3751 \cdot e^{20}$, suggesting that it is not a good fit.

This suggests that the exponential distribution is suitable to generate HTTP response sizes during the simulation.

1.4 Network behavior

In the following, the network behavior in terms of traffic and bandwidth utilization will be approximated roughly. This helps set up the simulation network as described in section 2 and enables the estimation of the maximum number of Web Browsing Laptops (also needed for the simulation).

1.4.1 *CCTV bit rate*

When sending packets of 10 kB of CCTV data every 40 ms, a bit rate of 2 megabits per second is generated:

[2] This was done using the Matlab script `ChiSquareTrace.m` which can be found among the files submitted with this report

$$\begin{aligned} \text{number of packets per second} \cdot \text{packet size} &= \text{bit rate} \\ \frac{1000ms}{40ms} \cdot 10kB \cdot 8bit &= 2Mbps \end{aligned}$$

1.4.2 *Video conference bit rate*

The professor's bidirectional RTP over UDP video conference generates a bit rate of 0,56 megabits per second. In each direction, a bit rate of 0,28 Mbps is achieved:

$$\begin{aligned} \text{number of packets per second} \cdot \text{packet size} &= \text{bit rate} \\ \frac{1000ms}{40ms} \cdot 1400B \cdot 8bit &= 0,28Mbps \end{aligned}$$

Where the 1400B packet size are 1388 B payload + 12 B minimal RTP header.

In conclusion, a total $2\text{Mbps} + 2 \cdot 0,56\text{Mbps} = 2,56\text{Mbps}$ of the point-to-point radio link's bandwidth are used constantly.

1.4.3 *FTP upload bit rate*

Since the FTP file transfer is a bulk upload rather than a continuous data stream, its bandwidth usage is not constant. Using TCP's congestion avoidance algorithms, the TCP connection taking care of the transfer will attempt to use as much of the available bandwidth as possible (until collisions occur). Therefore, the FTP traffic is not part of the network's baseline traffic.

2 SIMULATION PLAN

The overall goal of the simulation is to evaluate how the previously described applications perform and what the bottlenecks of the network are. First we identified potentially changing parameters of the network. These are the variables we can modify between different simulation runs. Afterwards we identified critical performance characteristics of the applications and performance metrics of the potential bottlenecks.

2.1 Simulation Parameters

The first parameter to look at is the amount of web browsing clients. We expect a decreasing performance with the amount of clients rising. The second part is the CCTV. To determine the influence of the CCTV on the network performance, we either include or exclude the CCTV from the simulation.

To determine the maximum number of clients to simulate, we looked at the scenario itself. An amount of 60 clients is a reasonable amount of students to be present in a $400m^2$ area. It can be assumed that they are surfing at the same time, if the lecture requires web research. To analyze the network thoroughly though, we need to make sure that the behavior with more clients does not change significantly. We found that it is not expected, that the behavior of the system changes significantly at a higher amount of clients, so we are able to extrapolate several network properties from the simulation results. To be able to extrapolate properly, we need to determine the incrementation of the amount of clients as well. To receive a well formed graph, we should work with a low increment, when the network behavior changes significantly. At low numbers, the traffic share is higher, therefore we need a low increment. At higher numbers we can increase it. The resulting numbers of clients we simulated are:

$$N \in \{1, 5, 10, 15, 20, 30, 40, 50, 60\}$$

To find a suitable duration of the simulation, we need to examine the behavior over time. We identified the browsing clients as the only application, whose behavior is depending on time. The mean time between HTTP requests is 20 seconds and it is exponentially distributed. The mean reply length is 671539 bytes and it is exponentially distributed as well. To get good results, we should include a high range of possible values in the simulation time. To calculate a reasonable expected highest value to take into account, we used the cumulative distribution function(CDF) of the exponential distribution:

$$y = 1 - e^{-\frac{1}{\mu}x}$$

If we want to include 0.95% of the random values, we need to calculate the upper bound of the waiting time and the reply length, by applying the CDF:

$$-\ln(0.05) * 671539B \approx 2MB$$

$$-\ln(0.05) * 20s \approx 60s$$

Our simulation showed, that the throughput for 60 clients goes down to 80000 bps. The expected time from simulation start to the end of the first request is therefore:

$$\frac{8\frac{b}{B} * 2MB}{80000bps} + 60s = 260s$$

To allow more of these requests, we set the maximum simulation time to 1000 seconds.

Throughout the simulation, we looked at the confidence intervals of several averaged values. We found that a repetition of 15 for each simulation combination produces a sufficient confidence level.

For the final simulation we end up with 9 different client and 2 CCTV settings, resulting in 270 simulation runs with a simulation duration of 1000 seconds.

2.2 Performance Characteristics

In the previous section we determined changing parameters between the simulation runs. The performance characteristics are the simulation measurements influenced by those parameters. The overall procedure is to record the measurements for every combination of parameters several times. Thus we have a set of 15 measurements for each combination. This allows us to calculate confidence intervals for each measurement. In the following we identify the performance characteristics of the implemented applications.

2.2.1 *Video Conference*

The video conference is based on UDP. Therefore packets can be dropped by the network permanently, reducing the quality of service. Additionally packets can be delayed. If a packet arrives too late, it can't contribute to the video stream anymore and is thus considered lost. The limit for the packet delay is 100 ms. If the packet loss rate is higher than 5%, the quality of the video conference is considered to be too bad. Thus the crucial characteristic to look at is the average packet loss rate of the video conference in both directions. Another characteristic is the average delay. Although you could expect it to be below 100 ms, when the average packet loss rate is sufficient, it is still an important value to rate the quality of service.

$$\frac{\text{lost packets} + \text{discarded packets}}{\text{sent packets}}$$

2.2.2 *Web Browsing*

The web browsing follows a simple request response model. The requests are carried out in a single session each. The important characteristic is how long the user has to wait until a response arrives. The response time is depending on the length of the response. For a greater length the user can cope with a longer response time. Therefore the crucial characteristic is the throughput the web client actually achieves. It is possible to measure the average throughput of the web clients. But this value is misleading, since the browsers do not use the medium at all times. To address this issue we measured the fraction of the simulation time a session was active. The calculation of the final throughput is thus:

$$\frac{1}{N}\sum_{i=1}^{N}\frac{r_i}{f_i * T},$$

$$\begin{aligned} \text{where } N &= \text{number of clients,} \\ r &= \text{received bits,} \\ f &= \text{fraction of the overall time,} \\ T &= \text{overall simulation time} \end{aligned}$$

To estimate the average response time, we can then further divide the average response length by the just acquired value. Todays response times for common home networks are usually below 5 seconds. For a temporary back-up solution such as the network at hand slightly higher response times can be considered acceptable. Therefore you can say that it is okay to wait for a response for 10 seconds.

2.2.3 *FTP Upload*

The FTP Upload is modeled as a continuous TCP stream to the Internet. It runs for the entire simulation. The only important characteristic is the average throughput. The user is just interested in the time the upload takes. We measured the average throughput by the total amount of bytes uploaded to the server divided by the simulation time.

$$\frac{\text{uploadedBits}}{\text{simTime}}$$

2.2.4 *CCTV*

The CCTV is used to monitor abnormal behavior at the remote campus. There are two characteristics, which can be considered. At first the delay of stream increases the reaction time of the staff. If the information arrives at the monitor one second late, it does not influence the reaction time of the staff in a significant way. Therefore it is negligible. As of the conference the average packet loss rate influences the quality of the video stream. If the packet loss rate is higher than 5% the video stream is considered not to be recognizable anymore. Therefore the packet loss rate should not exceed 5%.

2.3 Bottleneck Identification

Besides looking at the performance characteristics of the application, it is advisable to look at potential bottlenecks. We identified the wireless network at the remote campus and the radio link between the remote campus and the main campus as potential bottlenecks. The theoretical maximum bandwidth of 56 Mbps of the wireless network and a 12 Mbps bandwidth of the radio link are much smaller than the bandwidths of the remaining links. Thus it is not necessary to evaluate those.

2.3.1 *Radio Link*

To evaluate the radio link we need to consider two different characteristics. It is useful to determine how much bandwidth of the link is unused. Therefore we need to measure the average throughput. To receive even more information, we can look at the throughputs in each direction of the link. So we can identify the potential application, which is causing the traffic. In case the link is indeed a bottleneck, it is necessary to collect data about the packet drop rate. When the link is overloaded, the packets will be hold in a queue. When this queue is full. Incoming packets are dropped. We can use this drop rate to determine, if the link is a bottleneck. Since our applications require a sufficient packet delay, it is also useful to record the average queueing delay, to evaluate the influence of the link on the streaming delays. All of these measurements can be done at the Remote Router and Main Router to distinct between traffic directions.

2.3.2 *Wireless Network*

The practical throughput of a wireless network is much lower than the advertised theoretical maximum. This is due to collisions on the channel. So the wireless network can still be considered as a potential bottleneck, while its theoretical maximum bandwidth 56 Mbps is much higher than the 12Mbps of the radio link. To evaluate the wireless network channel, the same statistics as of the radio link can be considered. Additionally it is useful to look at the number of collisions to have a good metric to assess the issues caused by the channel.

3 SIMULATION EVALUATION

The following sections contain the separated evaluation of the network with and without CCTV. We would like to mention that we did the simulation with an important change of a parameter increasing primarily the performance of all applications depending on short network delays. We reduced the maximum PPP queue length to 50. We found, that large packets of the CCTV cause a tremendous amount of queueing delay due to high transmission delays of queued up packets. By decreasing the queue size the impact of accumulated CCTV packets at the Remote Router queue on the video conference is decreased.

3.1 Network with CCTV

This section contains the final evaluation of the network, when CCTV is included. We will start with an overview of the network behavior to be able to explain the behavior of the applications. After evaluating the application performances we continue with identifying and explaining bottlenecks.

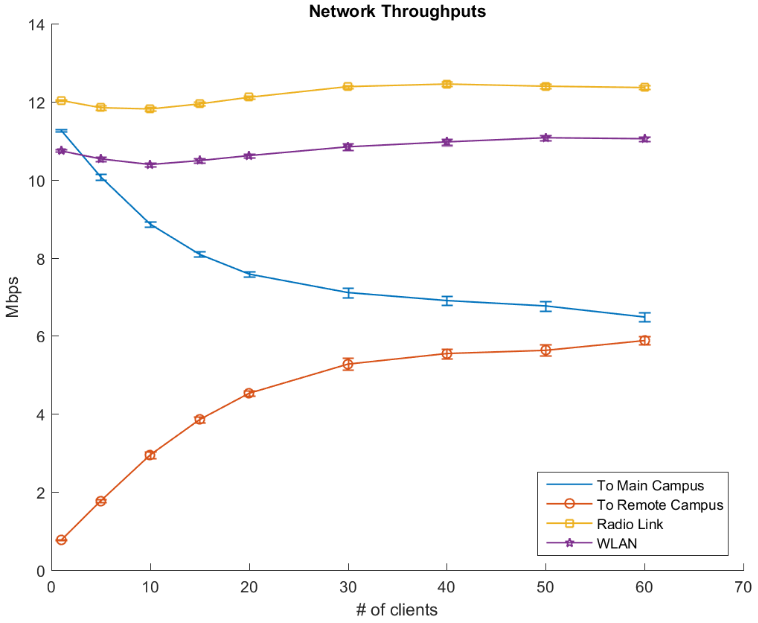


Figure 3: Throughputs of the important links of the simulated network including confidence intervals.

The network throughputs are depicted in fig. 3. As expected the total rate of the radio link is slightly above the rate of the WLAN. This is due to the steady load, which is added directly by the CCTV stream. The remaining bandwidth is composed of the steady load of the video conference, the web browsing and FTP upload traffic. With a rising number of clients the traffic directed to the main campus decreases and the traffic to the remote campus increases. This can be explained by looking at the application throughputs depicted in 4. With more clients the HTTP traffic uses a higher share of bandwidth. In general one can argue, that the major amount of HTTP traffic flows in the direction of the remote campus, while the traffic of the FTP upload flows to the main campus.

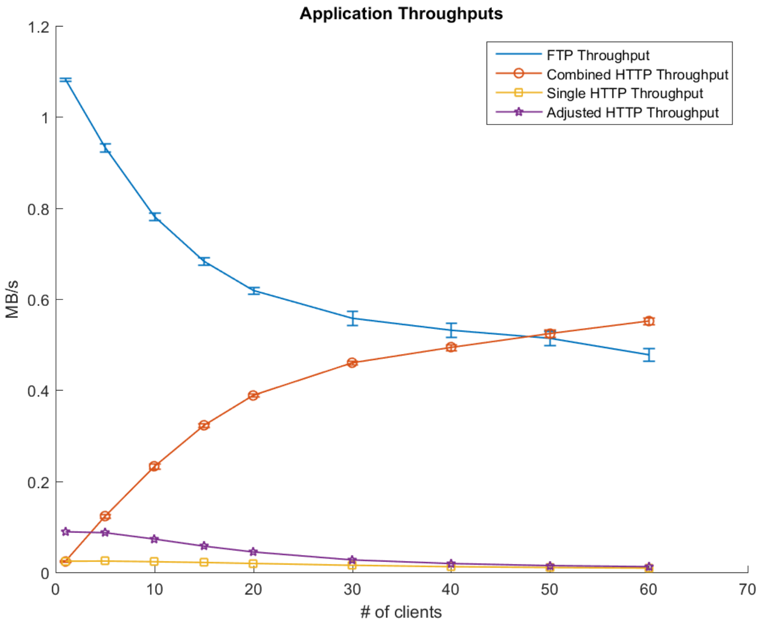


Figure 4: Average throughputs of the applications of the simulated network including confidence intervals.

3.1.1 *Application Performance*

In section 2.2 we identified the important performance characteristics of the implemented applications. In this section we will step through them and apply the simulation results.

The performance of the browsers and FTP upload is depending only on the throughput. The application throughputs were previously depicted in fig. 4. The FTP throughput is comparably high at every number of clients. When a low number of clients is surfing, the FTP upload almost uses the whole available bandwidth of the radio link. Only the steady load of the conference and the CCTV is slowing it down. With a bitrate of roughly 9 Mbps to 4 Mbps a good quality of service is achieved. But it is to be expected, that the FTP throughput decreases further with the number of clients rising above 60. Since a higher number of browsing clients does not fit the scenario, the FTP data rate does not set a maximum amount of clients.

The important value of the data rates of the browsing clients is actually the data rate for a single HTTP request. These values are depicted in fig. 5.

The adjusted data rate is calculated by applying the time a session was actually active instead of the whole simulation time.

If only one to five clients are using the network a comparably high data rate of roughly 100 KB/s is achieved. In combination with a mean reply length of 672 KB this results in an average waiting time of 6.7 seconds. This is already a really bad experience. You can argue that it is acceptable at the given circumstances. We argued before that an average waiting time of 10 seconds is acceptable in these circumstances. This time is exceeded, when more than 10 clients are using the network. The average HTTP Response Time is depicted in fig. 6. Therefore 10 clients provide a maximum of the proposed network configuration.

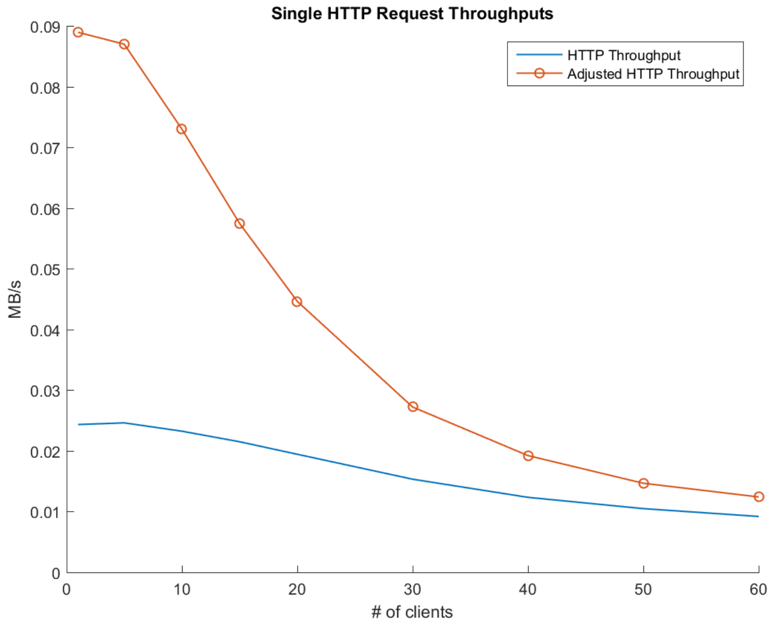


Figure 5: Throughput of a single HTTP request. The adjusted throughput takes into account the time a request was actually active.

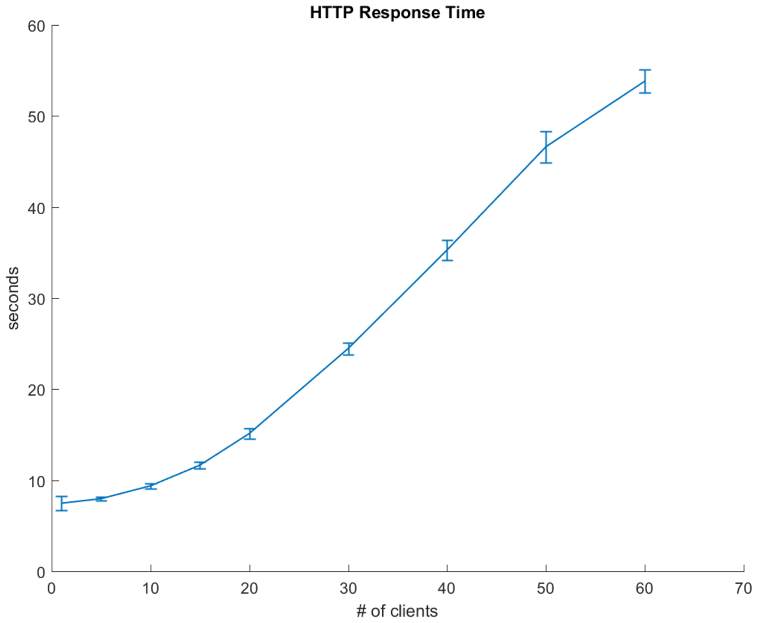


Figure 6: Response Time of a single HTTP request.

The performance characteristics of the video conference and the CCTV are the packet loss ratio and packet delays. The simulation results are depicted in fig 7 and 8 respectively.

The packet loss rates of the CCTV stream starts at a comparably high packet loss rate and decreases up to 0 for a higher number of clients. When a low number of clients is using the network almost all TCP traffic is directed

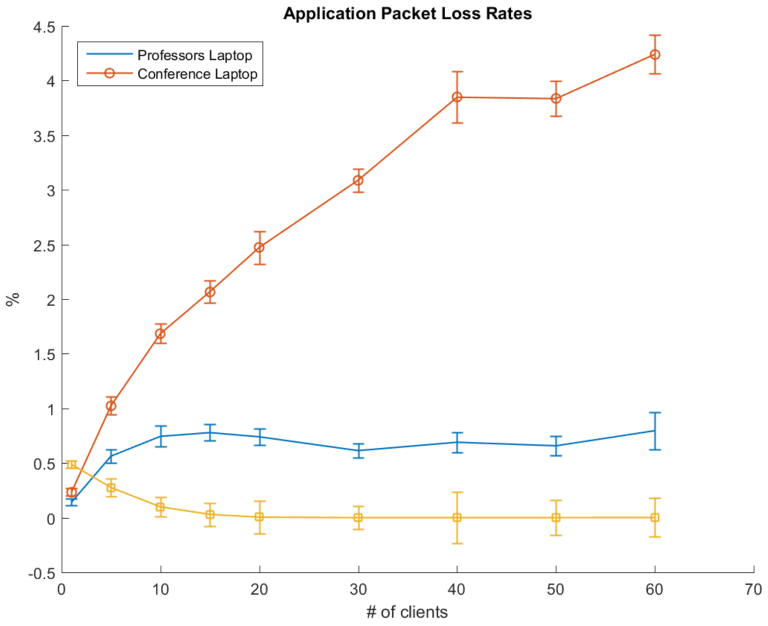


Figure 7: Packet loss rates of the applications of the simulated network including confidence intervals.

to the main campus. Therefore the congestion at the radio link causes the queues at the Remote Router to drop packets. Therefore increasing the packet loss rate of the CCTV stream. A packet loss rate of 5% is not exceeded at any amount of clients. Therefore a good quality is to be expected.

The packet loss rate of the stream directed to the professors laptop is low for a small number of clients and increases up to a rate of roughly 0.7% at 10 clients and keeps steady from there on. A possible explanation for the low loss rate at the beginning, while the loss rate for CCTV is high is, that the packet size of the video stream is much smaller than the CCTV stream packet size. While the CCTV packets arrive late due to transmission delay the video stream packets arrive faster and are therefore not considered lost.

The before mentioned loss rates are far below our threshold of 5%. Therefore they are not a limiting factor on the network. The packet loss rate of the stream received by the conference laptop however reaches a value of 4.2% at 60 clients. The overall graph suggests, that the 5% mark is exceeded at about 90 clients. Since 90 clients are an unrealistic number of clients considering the scenario, the performance of the stream can still be considered acceptable. The increase of the packet loss rate is caused by the increasing amount of traffic directed to the remote campus clients and therefore causing packet drops at the Main Router and access point queues.

The delay depicted in figure 8 is constantly low enough to be considered acceptable. The inverse behavior of the delays is caused by the direction of the expected traffic. At low client numbers only the queue at the Remote Router delays the packets. With an increasing number of clients the access point and the Main Router delay the packets due to the HTTP replies.

3.1.2 *Bottleneck Analysis*

The overall throughput of the network components was previously depicted in fig. 3. It shows that the radio link bandwidth is fully used at every

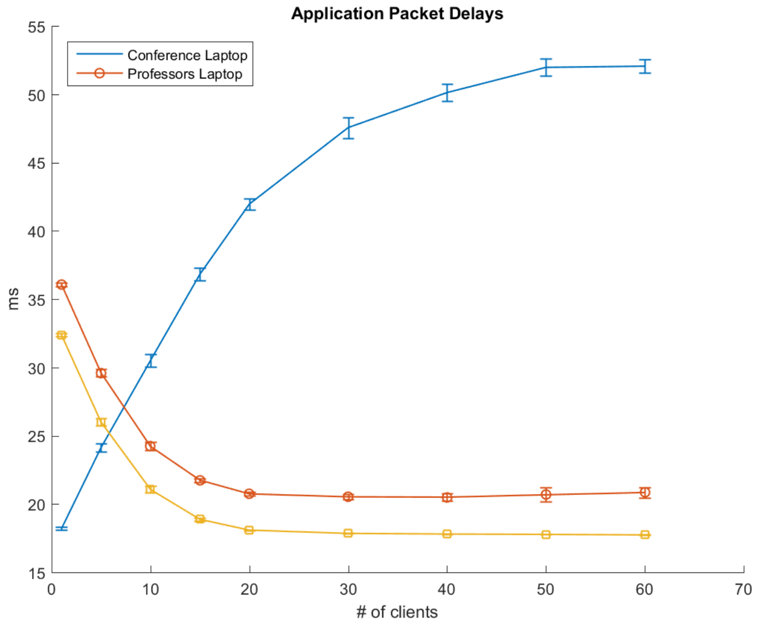


Figure 8: Average packet delays of the applications of the simulated network including confidence intervals.

number of clients. This is due to the TCP traffic caused by the FTP upload. The TCP protocol is designed to use all remaining bandwidth not used by steady load of the udp traffic. Since all TCP traffic is originated at the WLAN part of the network, it is expect that the WLAN throughput equals the throughput of the radio link without the steady load of the CCTV, which is connected directly to the Remote Router. The packet drop rates of the network queues are depicted in fig. 9.

The drop rate of the WLAN is increasing monotonously, while the Main Router drop rate increases more steeply, but decreases at a higher number of clients. The Remote Router queue is around zero regardless. This is due to the fact, that the main TCP traffic directed to the main campus is the FTP upload. Since it is only one stream, it can perfectly adapt to the available bandwidth. Furthermore it indicates that the WLAN is used at maximum capacity, because even the 8KiB HTTP requests should cause congestion at the Remote Router. The WLAN is therefore filtering the traffic originating from the remote campus. So the packets actually reaching the Remote Router do not get dropped anymore. This means a usable capacity of the WLAN of 10Mbit, which is the bandwidth of the radio link minus the data rate of the CCTV.

The steep increase of the drop rate at the Main Router indicates the impact of the HTTP requests. When a request reaches the Internet, the server initiates a reply, which causes a congestion at the Main Router, because the radio link is fully in use at all times. With a low number of clients the number of requests increases linearly. Therefore the drop rates at the Main Router increase linearly as as well. With the number of clients however the share of the bandwidth of each client decreases, this results in a longer session duration. A longer session duration means a decrease of the number of requests, since no new request is issued before the current request got served. This opposed effects increase the congestion at the Main Router

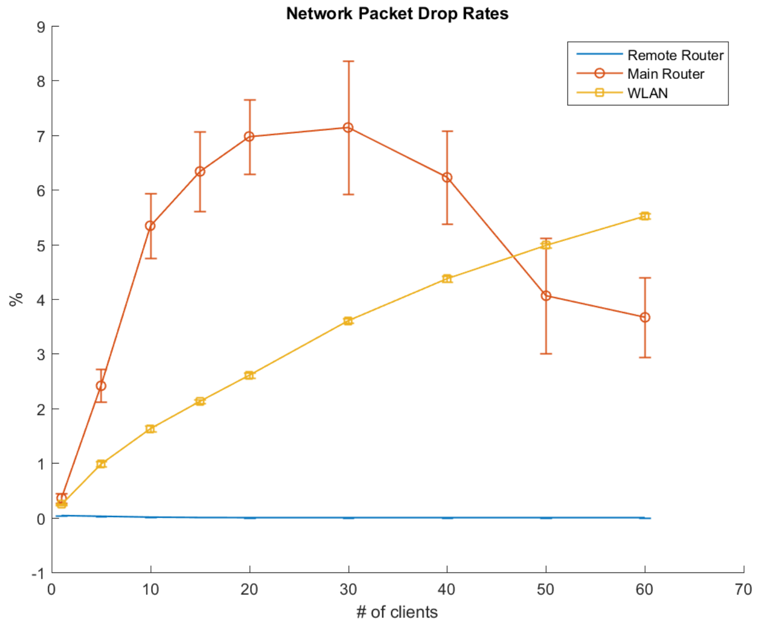


Figure 9: Average packet drop rates of the simulated network including confidence intervals.

up to 30 clients. Afterwards the secondary effect decreases the congestion caused by the primary effect.

These effects however have no impact on the drop rates of the WLAN. The monotonous increase is just due to the rising number of participants in the WLAN network causing more packets to be dropped.

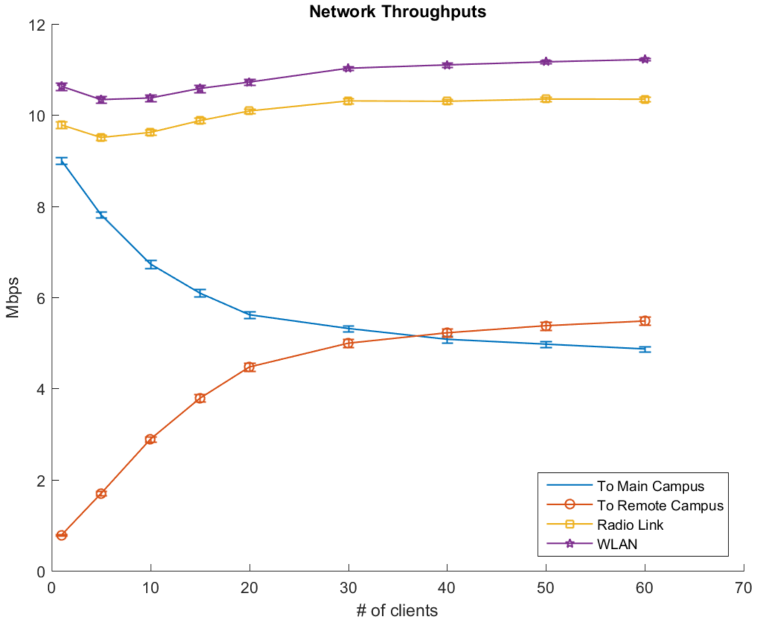


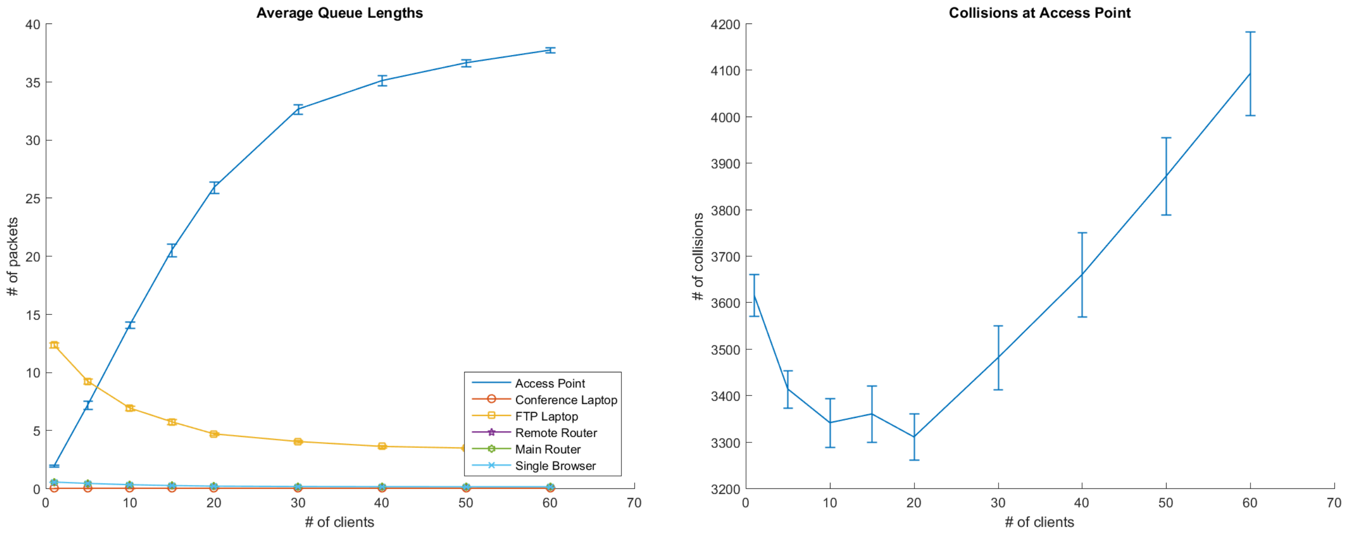
Figure 10: Average network throughputs

3.2 Network without CCTV

As a second measure, the same simulations were conducted without any CCTV infrastructure present. This section analyzes the simulation results of this configuration. First, the overall network behavior is discussed. Then, it focuses on the influence of FTP and web browsing applications on the video conference. Finally, possible bottlenecks are identified.

3.2.1 *Overall network behavior*

The throughput at different points in the network is illustrated in fig. 10. It can be observed that the radio link is never at full capacity. The traffic towards the Main Campus represents the sum of the FTP upload, HTTP requests and video conference traffic from conference laptop to professor. The traffic towards the Remote campus represents the sum of HTTP responses and video conference data from the Professor's Laptop towards the conference laptop. It can be seen that the throughputs are mostly inverse to each other, forming a steady ceiling of about 10 Mbit/s for $\geqslant 30$ clients.



(a) Average queue length

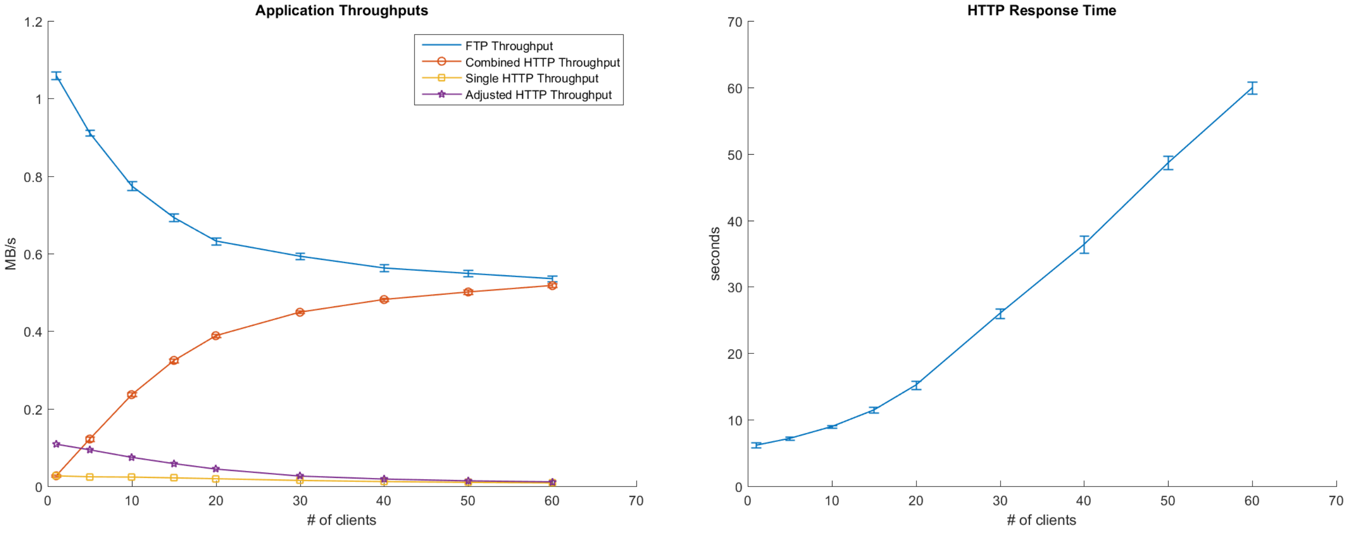
(b) Number of collisions in the WLAN

Figure 11: Remote Access Point data

Due to the aforementioned ceiling, it is worthwhile to inspect the WLAN and the Remote Access Point serving it more closely. As fig. 11a shows, the Remote Access Point queue length, i.e. the amount of data waiting to be sent to the WLAN clients, is the longest quickly after more than 5 HTTP clients have joined the network.

Fig. 12a summarizes the average application throughput with regard to the number of web browsing clients present in the network. In order to analyze the influence of the FTP and web browsing applications on the video quality, it is useful to first familiarize ourselves with the behavior of these applications.

THE WEB BROWSERS are the parameter continuously changing throughout the simulation, as detailed in section 2. Figure 12a shows that while



(a) Average application throughput

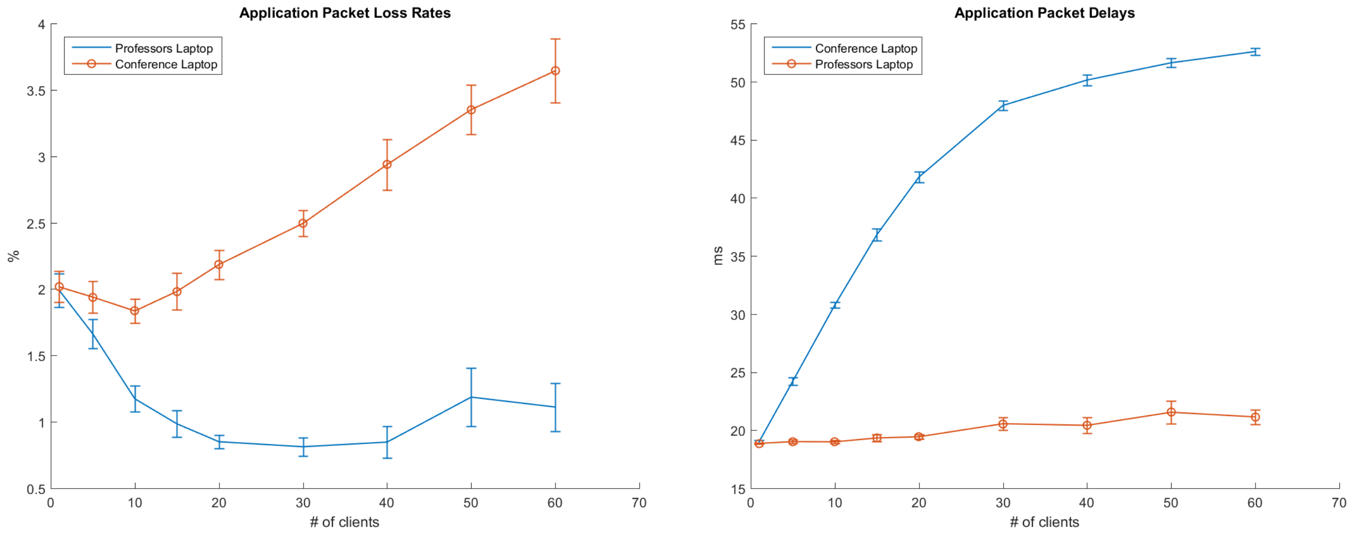
(b) Average browser session durations

Figure 12: Application data

the average overall HTTP traffic throughput rises with the number of web browsing clients, the average throughput achieved per browser decreases. Since bandwidth is limited, the TCP congestion control of each participant will negotiate a transmission rate that avoids collisions, throttling the overall transmission speed. Fig. 12b verifies this: The average session duration per browser increases with the number of clients. According to the criteria determined in 2.2, browsing quality declines quickly: At less than 15 active clients, the quality threshold of 10 s is surpassed. Notably, the session duration grows linearly with $\geqslant 20$ clients in the network.

THE FTP CLIENT , shown in fig. 12a as well, experiences a decline in throughput that is inverse to the increase in overall HTTP throughput. This also can be explained with TCP's congestion control mechanisms: the more bandwidth is used by web browsing clients, the more the FTP client is forced to react by limiting its bandwidth in order to avoid collisions. In short: the FTP client will use up as much bandwidth as you let them. It can be argued that the decrease in bandwidth is not as much of a nuisance as it is for the web browser users, since large file transfers are expected to take a while anyway.

THE VIDEO CONFERENCE has to be looked at as two distinct data flows: one going from the Professor's Laptop to the Video Conference Laptop, and one traveling the other way. This becomes apparent when looking at fig. 13, which depicts the average packet loss rate and delay for both directions in relation to the number of web browsing clients in the network. Note that the video conference is a UDP application periodically sending packets of a fixed size, and thus unaware of congestion or collisions.
Since it is known that the that the delays of the radio and DFN links are 10 and 5 seconds respectively, all application delays must be at least 15s. While the delay at the Professor's Laptop stays very close to this ideal value and only increases marginally when adding new clients, the delay at the



(a) Packet loss rates

(b) Delays

Figure 13: Average packet loss and delays of the video conference

conference laptop appears to grow logarithmically. This can be explained by examining the average queue length at the Remote Access Point (see fig. 11a): With an increased number of web browsing clients receiving large HTTP responses, the amount of data being sent from the access point into the WLAN increases as well. In combination with the outgoing traffic of the FTP client, increased contention for the wireless medium causes incoming data to aggregate at the access point, resulting in a higher delay at the conference laptop.

The packet loss at the Conference Laptop can be explained as a combination of collisions occurring in the WLAN, packet loss at the Main Router and an increase in HTTP response traffic. From 1 to 10 web browsing clients, the video conference sees a slight decrease in its loss rate from 2%. Around 0.5 to 2% of this initial loss rate can be accounted for by the Main Router's loss rate, as illustrated in fig. 14. All additional packet losses may be caused by collisions in the WLAN (see fig. 11b). Starting at 10 clients, the packet loss sees a steep increase, which correlates with the progress of the Main Router's packet drop rates. This increase, however, is dampened by the fact that with the number of web browsing clients, the amount of HTTP response traffic which shares the Main Router's queue with the video conference data rises as well. This way, less video data is discarded in total, as it makes up a smaller amount of the queue data.

3.2.2 *Identified bottlenecks*

The main bottleneck is the WLAN: as can be seen in fig. 10, its throughput stagnates around 10 Mbit/s, staying below the 12 Mbit/s the radio link would theoretically be capable of transmitting. However, even the radio link itself is not fully occupied. One cause for this may be the drop rate of the Main Router that can be seen in fig. 14 in combination with the increasing session durations shown in fig. 12b: Until its peak at 20 Web Browsing Laptops, the Main Router is confronted with more traffic caused by HTTP responses and video conference data flowing from the professor to the re-

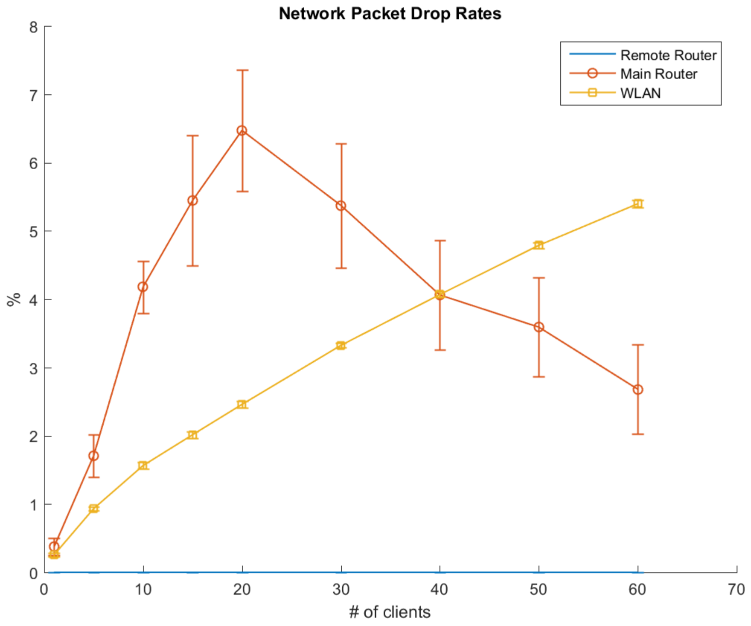


Figure 14: Packet drop rates at different points in the network

mote site than it can handle. After 20 clients, the increased session duration has caused an overall smaller number of sessions to be active, resulting in fewer data to be transmitted by the Main Router through the radio link. While this relieves the Main Router's queue, it also decreases the overall throughput of the radio link.

3.2.3 *Maxmimum number of web browsing clients*

When the video conference is key,the maximum number of web browsing clients is reached when either the average packet loss exceeds the maximum of 5% or the average delay exceeds the maximum of 100 ms.
Assuming client packet loss is linear starting at 10 clients, the video conference packet loss will exceed its maximum when ⩾ 90 web browsing clients are present. Even at 60 clients, the delay measured at the Conference Laptop does not significantly exceed half of the permitted maximum delay of 100 ms, as can be seen in Fig. 13a.When assuming logarithmic growth, unacceptable packet loss rates will occur long before the maximum delay threshold is reached.

When taking the students' web browsing experience into account, however, the maximum number of clients is reached far quicker with the current setup. The acceptable response time of 10s is already reached with <15 clients, as can be seen in fig. 12b.

4 RECOMMENDED CHANGES TO THE NETWORK

As shown in the previous section, the network at hand provides a satisfactory quality of service for video conference data with up to 90 students browsing the web in parallel. The web browsing experience, however, is sub-par as soon as $\geqslant 15$ clients are active. This is due to the fact that the Remote Access Point cannot provide more than 10 Mbit/s of bandwidth and is therefore the main bottleneck.

Based on these findings, we recommend to install additional access points if more than 15 students are expected to be active in the network. With more access points installed, the bottleneck would shift to the radio link, which therefore would need to be upgraded as well.

Additionally, limiting the bandwidth available to each individual user may improve the overall surfing experience as it prevents users such as the FTP client from unfairly occupying the channel at any time.

5 DISTRIBUTION OF TASKS

Simulation Implementation	Lotte
Simulation Execution	Alexander
Plotting	Alexander
Introductory text	Lotte
Simulation Plan text	Alexander
Evaluation with CCTV	Alexander
Evaluation without CCTV	Lotte

6 TERMINOLOGY

SIMULATION PARAMETERS Parameters changed between simulation runs

PERFORMANCE CHARACTERISTICS Measurements of the evaluation

RESPONSE TIME Time between browser request and fully received response

CDF Cumulative distribution function

LIST OF FIGURES

LIST OF TABLES