



**NETFLIX**

---

*A Network Perspective*  
**Matthew Kramer**

# CONTENTS

- About
- Protocols
- Content Delivery
- Packet Analysis
- Conclusion
- References

# ABOUT

# ABOUT

Netflix is a web-based service that streams movies and television shows to your devices.

A monthly subscription provides users access to the entire catalog of titles available in their region.

Netflix may be watched on smart televisions, desktop computers, mobile phones, tablets, and other digital media players.

# PROTOCOLS

# NETWORK PROTOCOLS

Content streamed from Netflix always uses the Transmission Control Protocol, or TCP.

This protocol provides:

- network buffering,
- transmission guarantee,
- bandwidth probing, and
- congestion control.

Each of which helps to provide smooth playback without impeding other traffic on the network.

# TCP FEATURES

Network buffering allows data being sent from Netflix servers to be stored temporarily until it is ready to be used.

Transmission guarantee assures that each frame arrives intact and in the order it was sent. However, frames may still be dropped if arrive too late due to network delay.

# TCP FEATURES

Bandwidth probing allows the network to determine how much bandwidth is available between server and client so that it can fetch the content as quickly as possible without affecting other traffic.

Congestion control is used by Netflix servers to adjust how traffic is sent through the network in order to avoid congesting the network.



# STREAMING PROTOCOL

Netflix uses the Dynamic Adaptive Streaming over HTTP (DASH) protocol in order to deliver the videos from the server to the client.

In this protocol:

- Content is encoded at different levels of quality
- Content is segmented before being sent
- Clients request one segment at a time using HTTP
- Quality of future segments are determined by bandwidth measurements from previous segments

# CONTENT DELIVERY

# CONTENT DELIVERY

In order to deliver content to clients, Netflix uses third-party infrastructure through Content Delivery Networks, or CDNs.

These CDNs (Akami, LimeLight, and Level-3) serve video streams to Netflix clients, eliminating the need for Netflix to have network infrastructure of its own.

Netflix alone handles user account registration and payment information. However, Amazon Cloud is used to manage user sign-in, CDN routing, logging, and Digital Rights Management, or DRM.

# PACKET ANALYSIS

# PACKET ANALYSIS

The process of accessing and streaming content from Netflix consists of five primary phases:

1. User Authentication
2. Device Authorization
3. Instruction Fetching
4. Content Streaming

# USER AUTHENTICATION

Ensures that the viewer is a Netflix subscriber and has proper privileges.

Typically managed at the browser-level by cookies.

Users login to their Netflix accounts and the server sets the browser cookies that it needs.

Netflix also verifies that the user is in a geographical location that allows for playback of the requested content by checking their IP address.

# PROCESS OF USER AUTHENTICATION

1. Browser requests a video page

```
GET http://www.netflix.com/WiPlayer?movieid=XXXXXXX[1]
```

2. Javascript checks that Silverlight is installed
3. If not installed, browser downloads Silverlight

```
GET http://www.netflix.com/pages/watchNow/player/silverlight/SLPlayer.xap[2]
```

4. Silverlight notifies server that it is ready

```
POST http://www.netflix.com/SilverlightEvent[3]
```

# DEVICE AUTHORIZATION

Identifies the device the user is attempting to stream content to and ensures that they have not reached the per-account limit of six devices.

Netflix servers connect the cookies created in the user authentication phase to link the account to the device.

If authorization is successful, the server sends a response to the user with a header for the client to use on all future messages to the server. This header contains information about both the user account and authorized device.



# PROCESS OF DEVICE AUTHORIZATION

1. Player requests cross-site interaction with the Netflix controller

```
GET https://agmoviecontrol.netflix.com/clientaccesspolicy.xml
```

2. Browser verifies identity of Netflix controller with Verisign

```
POST http://ocsp.verisign.com/
```

3. Player begins interaction with Netflix controller by sending a ping

```
POST https://agmoviecontrol.netflix.com/nccp/controller
```

# INSTRUCTION FETCHING

Player retrieves information from Netflix servers about how to play the content and where to get the data.

The server returns generic information about the content to be played, including the title, cast, runtime, and other related data. The player then uses this data to display the content information and return the user to a bookmarked time if they are continuing their viewing.

In this phase, there are little to no security checks. The CDNs simply return the files to anyone who requests them within the time of expiration associated with the URI.

# PROCESS OF INSTRUCTION FETCHING

1. Player requests information about the movie and user

```
POST https://agmoviecontrol.netflix.com/nccp/controller HEADER: X-CTicket=...  
POST-DATA: 'moviemetadata', with movie ID
```

```
POST https://agmoviecontrol.netflix.com/nccp/controller HEADER: X-CTicket=...  
POST-DATA: 'usermoviemetadata', with movie ID
```

2. Player requests information about streaming servers and where to find the files to stream the content

```
POST https://agmoviecontrol.netflix.com/nccp/controller HEADER: X-CTicket=...  
POST-DATA: 'authorization' (a misnomer), with movie ID
```

# PROCESS OF INSTRUCTION FETCHING

3. Server returns a long message containing the location of the files

```
<nccp:downloadurl>  
  <nccp:expiration>1238103632</nccp:expiration>  
  <nccp:cdnid>4</nccp:cdnid>  
  <nccp:url>  
    http://netflix-274.vo.llnwd.net/s/s1/911/11748911.bif?p=53&e=123810  
    3632&h=2beb62b1de51b4872978787fc98d075b  
  </nccp:url>  
</nccp:downloadurl>
```

4. Player begins downloading the streaming files from the specified locations, using the CDN recommended by the Netflix controller

```
GET http://netflix-274.vo.llnwd.net/s/s1/373/447071373.wmv/range/0-23?p=54&e=...
```

# CONTENT STREAMING

Player talks directly to the Netflix streaming servers who serve the content to those clients who requested it.

The CDNs will give content to whoever requests them with a valid URI, but only within a window of time before a defined time of expiration closes it.

# PROCESS OF CONTENT STREAMING

1. Silverlight player begins playback, continues downloading content, and notifies the server of its success

```
POST http://www.netflix.com/SilverlightEvent
```

2. Player contacts Netflix servers regularly to transmit playback data and other information

```
POST https://agmoviecontrol.netflix.com/nccp/controller HEADER: X-CTicket=...  
POST-DATA: 'logblob', with logging data AND sequence number
```

# 25-40%

OF ALL INTERNET TRAFFIC IS VIDEO STREAMING

# CONCLUSION



# CONCLUSION

While video streaming represents a large fraction of internet traffic, very little is known about how this is accomplished.

Netflix uses DASH and TCP to quickly and reliably stream content to devices for users to watch.

While Netflix itself does not have the infrastructure to support its users, it leverages the infrastructure of CDNs to distribute content servers.

# REFERENCES

Packets located in attached text document

Network Characteristics of Video Streaming Traffic, ACM CoNEXT 2011

Ros Belle, Netflix Uncovered, 2013

Pomelo LLC, Analysis of Netflix's Security Framework, 2009