



The CastGate project

“Enabling Internet multicast for content distribution”

Prof. Marnix Goossens
Dr. Pieter Liefoghe
Arnout Swinnen

Vrije Universiteit Brussel
ETRO-TELE research group
Brussels, Belgium

The CastGate project

Mission: obtain a **breakthrough** in the enabling of **IP multicast** in the **general, public** Internet to allow it to be used by **content providers** for their content distribution.

Method: provide **temporarily, pragmatic** “work-arounds” for **content providers** to the **practical problems** currently preventing them from using IP multicast.

Operation modes:

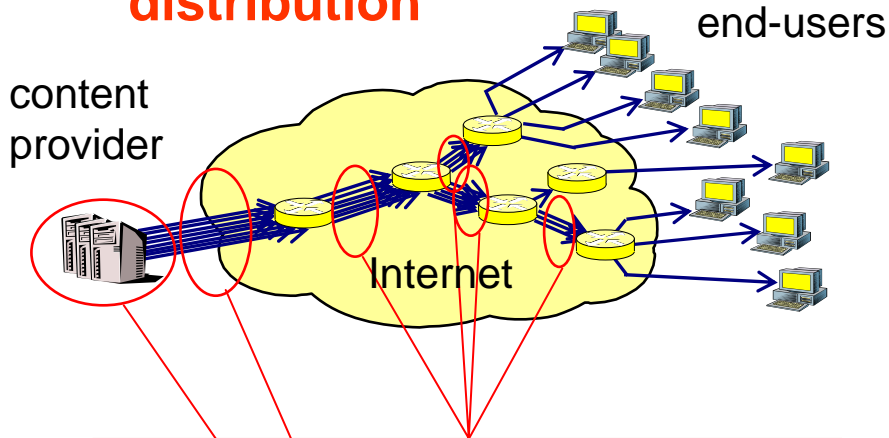
- **Private:** to extend private multicast distribution in a multicast enabled network (e.g. an intranet) to customers in the public Internet
- **Public:** to allow public use of multicast in the public Internet

Keys to success:

- “work-arounds” must operate **automatic** and **transparent** at the **end-user’s** side
- for public operation: some (public funded, research) network operators **volunteering** to **offer free, public multicast access** through tunneling

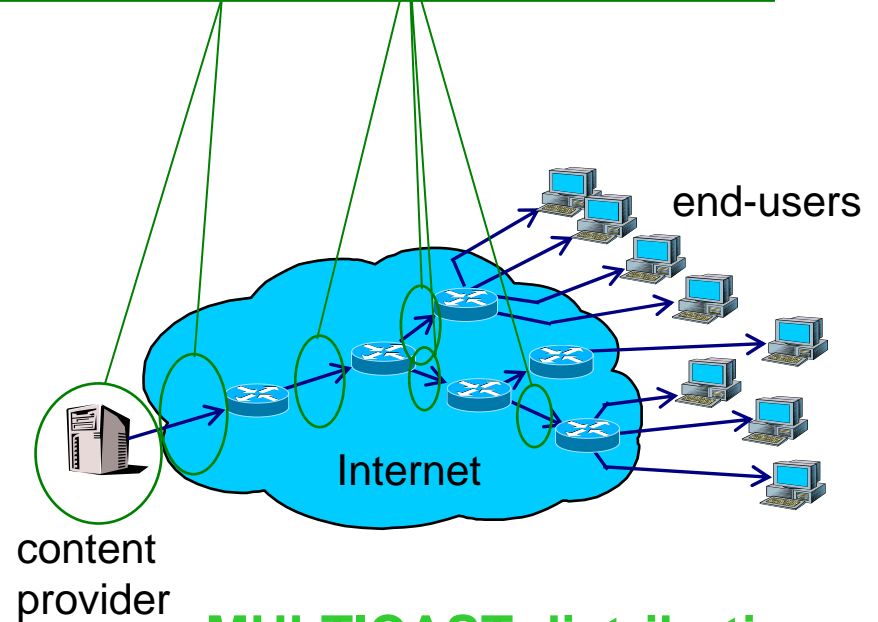
UNICAST versus MULTICAST distribution in the Internet

Current UNICAST distribution



1. Server and Internet connection of content provider needs to support only one single stream.
 2. Necessary duplication of information is performed by the Internet, and deferred to be as close as possible to the end-users

1. Server and Internet connection of content provider needs to support only one single stream.
 2. Necessary duplication of information is performed by the Internet, and deferred to be as close as possible to the end-users



MULTICAST distribution

IP multicast: evolution

- Started in the context of “many-to-many” communications (“or rather “few-to-few”, cfr. multi-party video-conferencing over narrowband connections)

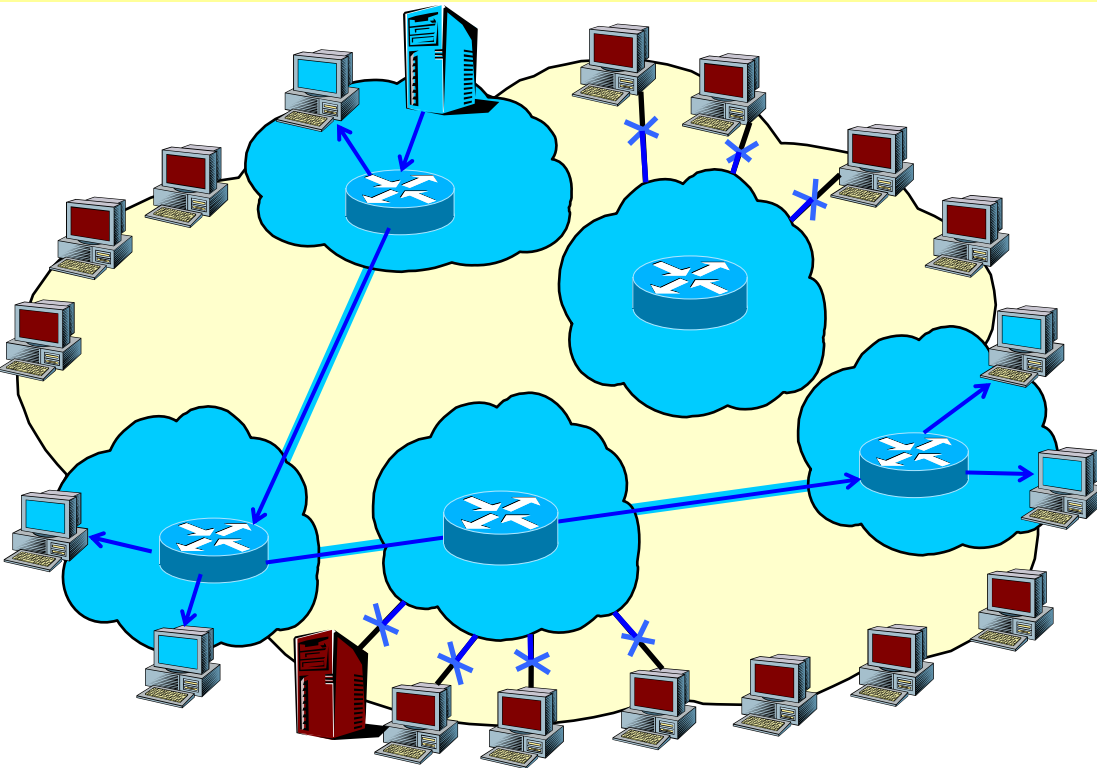


- Now probably much more important for “one-to-many”, large(r) scale content distribution (audio and video broadcast, e-paper distribution, e-learning, etc.)

IP multicast: “reality-check”

👍 IP multicast is DEFINED for more than a decade, and is IMPLEMENTED in most current computer and networking systems; most content distribution end-user applications (e.g. multimedia players such as WMP, QuickTime, etc...) are “IP MULTICAST READY”

- 👍 IP multicast is DEFAULT ENABLED in most computer systems and LANs
- 👍 IP multicast is ENABLED internally in the back-bones of many network operators
- 👎 IP multicast is NOT ENABLED in the access networks of most (commercial) ISPs

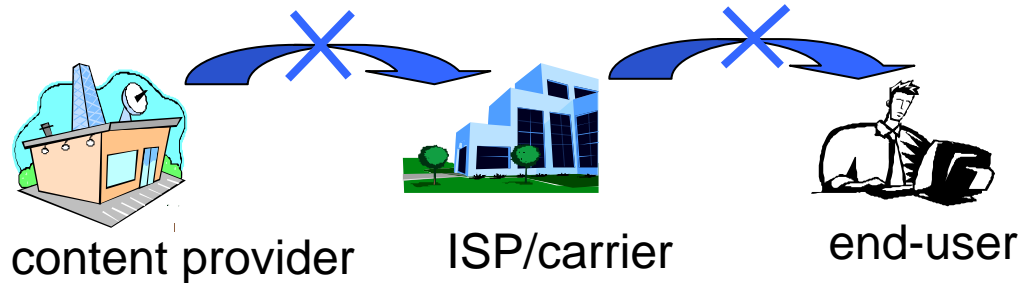


=> IP multicast is technically ready to be used, but practically blocked in the access networks of the ISPs

Why do ISPs not provide IP multicast?

Economical reasons

1. the “chicken-and-egg” problem

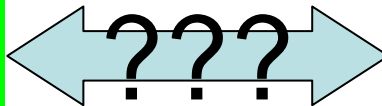


ISP/carrier does not enable IP multicast towards content provider nor end-users since there is insufficient IP multicast traffic to make enabling a profitable operation

Content provider does not send in IP multicast, since the content provider nor its end-users have access to it

2. the IP multicast “bussiness” model for the ISP/carrier?

IP multicast reduces the internal load in the network of the ISP/carrier



content provider pays only for one transmission, but generates traffic for multiple connections...

Why not provide IP multicast? (cont.)

Technical reasons

- Current ASM (“many-to-many”) issues:
 - complex routing (interdomain)
 - “open door” to “Denial-of-Service” attacks

SSM (“one –to-many”) offers solutions, but slow in development (IGMPv3 support in OS, content distribution applications,...)
- Unidirectional flow without congestion control -> possible “flooding” of “shared capacity” access network configurations (shared media, ADSL concentrators,...) by inadvertent usage
- Smaller issues such as fragmentation, errors, etc...

Who gains from multicast?

- First and most, the CONTENT PROVIDER: only server- and Internet capacity for ONE stream required -> *significant cost reduction*
- Later, the NETWORK OPERATOR: reduction of network capacity cost due to reduction in internal network load, mostly in back-bone and the peering links, *on condition that there is sufficient IP multicast traffic*
- END-USER: usually *does not really care*, and gets no direct (technical) benefits...but there is an indirect bonus: capacity saved by content providers will be used by them for higher quality and greater diversity of content

=> driving force behind enabling IP multicast will first be the content provider...

Do we need IP multicast?

IP multicast has been dormant for many years, so do we *really* need it?

In view of the emerging multimedia content distribution on the public Internet, multicast support is now URGENTLY required...

Many potential initiatives (long range radio and television broadcasts, live-concerts, e-learning, etc) are blocked by the prohibitive high cost and/or the technical impossibility (e.g. large scale distribution of television quality video) of unicast distribution.

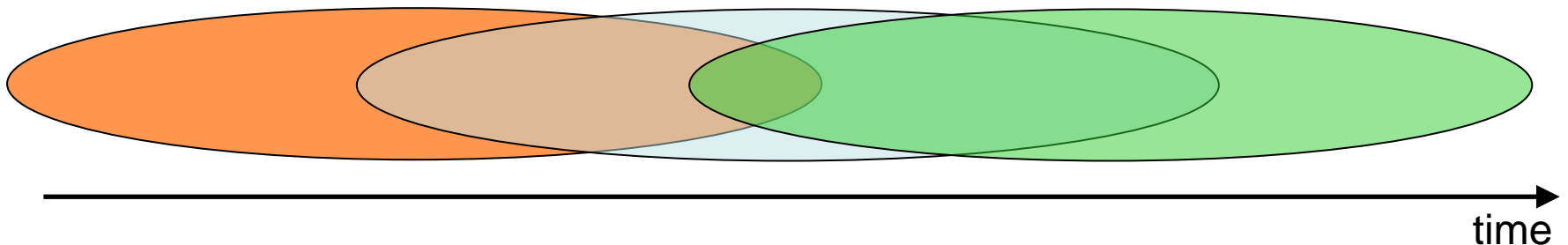
Multicast for what?

- NOT for very large scale local radio and television distribution. The Internet can not provide a guaranteed service... Radio and television are using other technologies for their local digital radio and television broadcasts (e.g. distribution servers in the local access loop)
- Maybe for (a small number of) “long-distance” clients of those radio and television broadcast stations
- Probably essential for smaller scale content distribution by smaller organisations (cultural organisations, Universities,...)
- Content distribution in the context of individual, “personal” multimedia

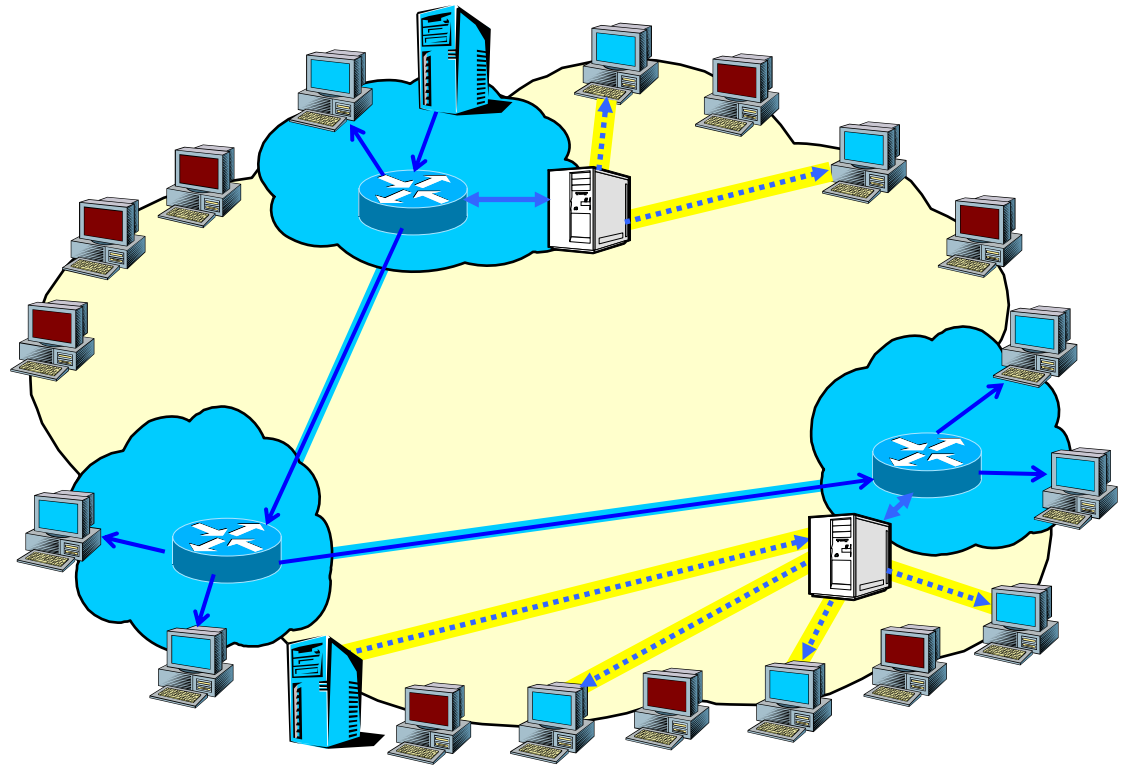
The CastGate project

In the absence of native IP multicast connectivity for their customers (and themselves), CONTENT PROVIDERS must be provided with the possibility of distributing using IP multicast, and arranging – temporarily - “simulated” IP multicast access for their content to their customers not having native IP multicast access (now often about ALL of them).
The use of IP multicast by content providers will increase IP multicast traffic on the Internet, and a consequent (gradual) enabling of native IP multicast access by network operators.

NO IP multicast → “Simulated” IP multicast → Native IP multicast



Simulated access: IP multicast access through “tunneling”



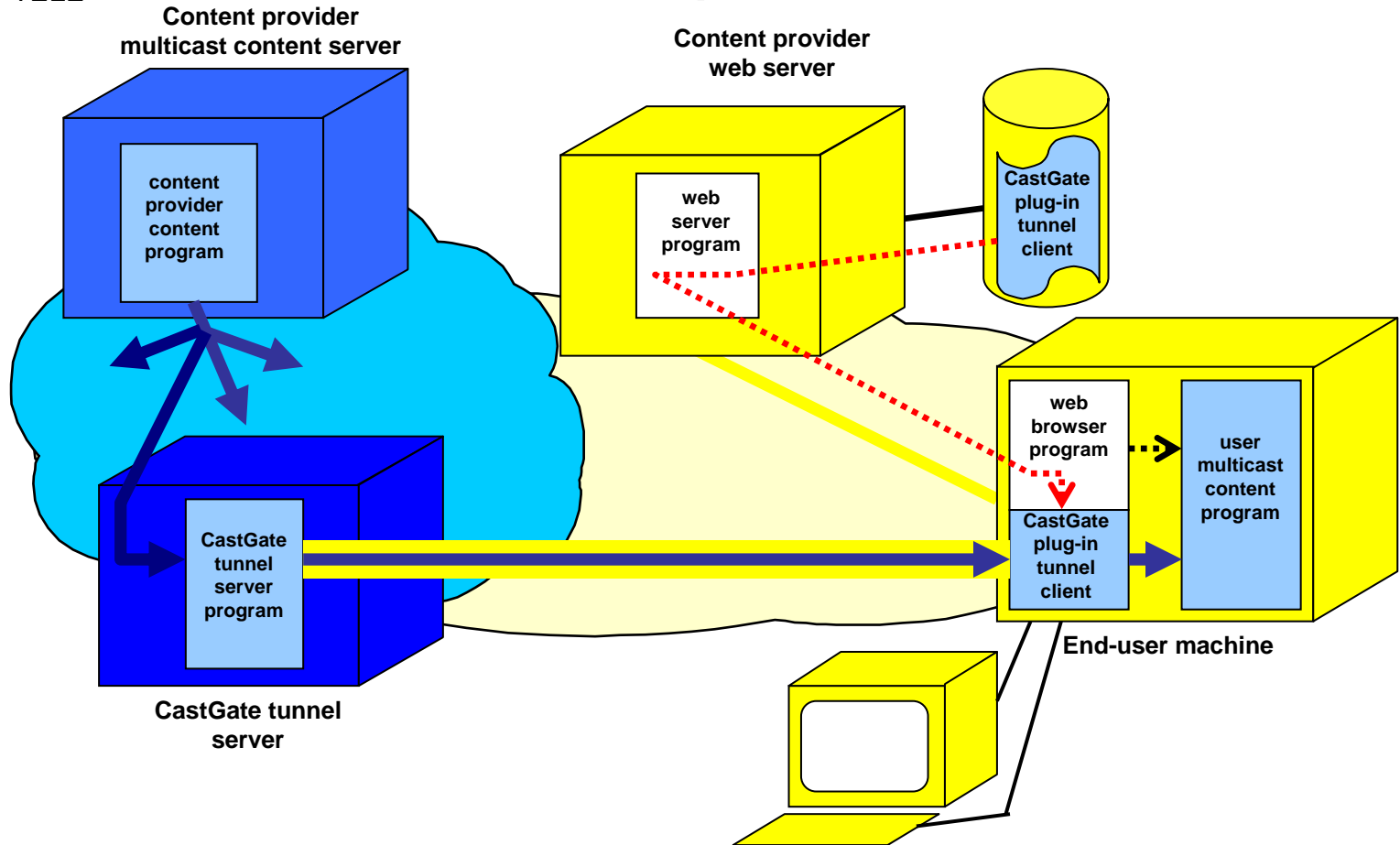
Tunnel servers connected in the IP multicast enabled part of the Internet allow stations to set up unicast tunnels to them over which the multicast traffic can be forwarded.

“Real-world” requirements of a system for simulated access...

To have any “real-world” chance of success, the following conditions must be met for a system providing “simulated” access:

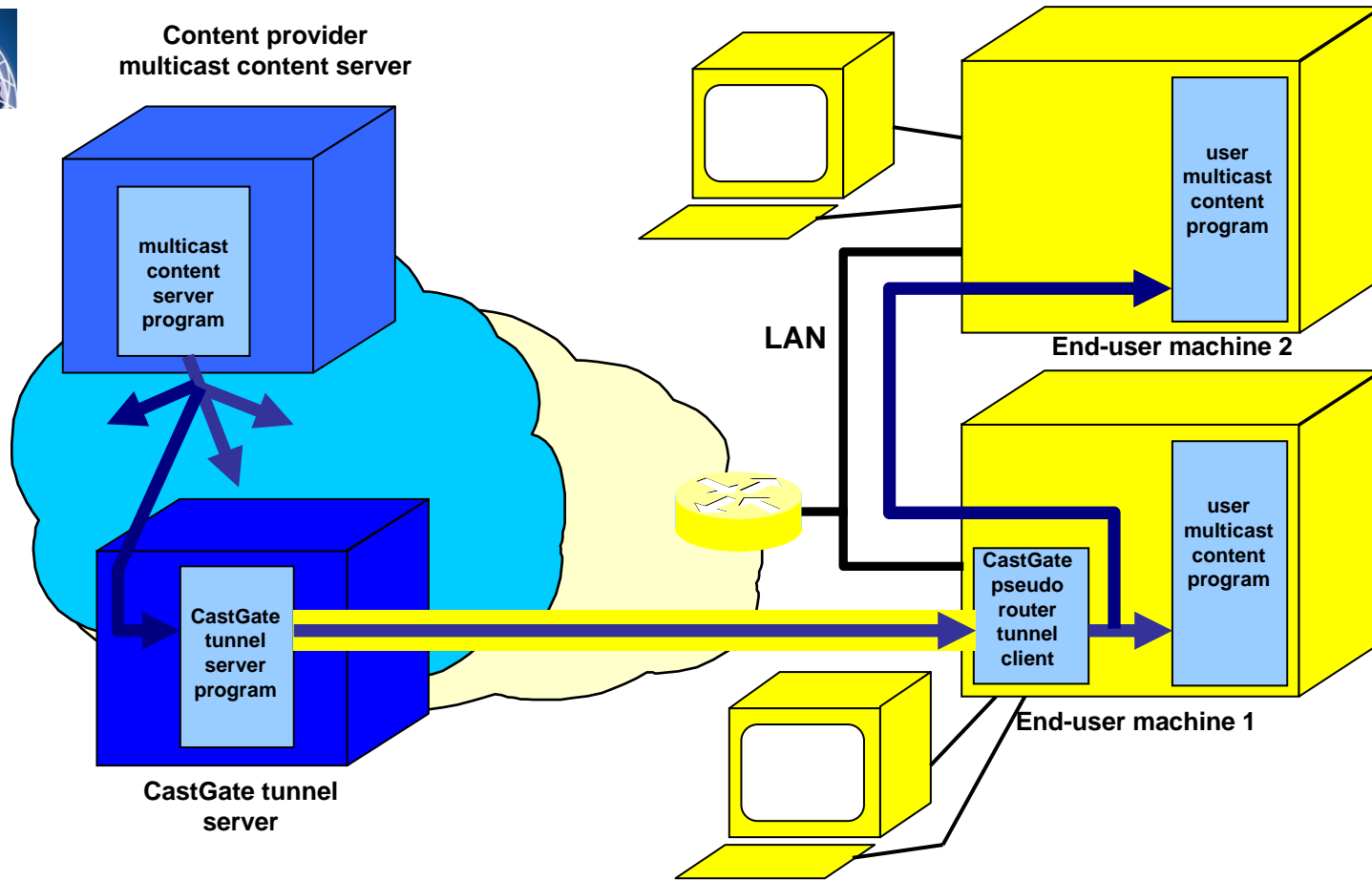
- operate within the normal, unmodified Internet infrastructure
- its operation must be transparent and automatic to the end-user (*having the end-user download and install something is often already too high a threshold!*)
- not require changes to the operating system nor to the multicast applications
- *active* participation from each and every network provider can NOT be assumed!
- public, free tunnel servers should be available
- restrictions resulting from (standard) firewalls and other security measures must be taken into account

Automatic transparent, (limited) user operation



Transparent user operation is obtained by downloading the tunnel client software as a browser “plug-in”. The type of OS and browser is automatically detected, and the appropriate plug-in is installed. No user intervention – apart from allowing the plug-in download – is required.

Full transparent multicast user access



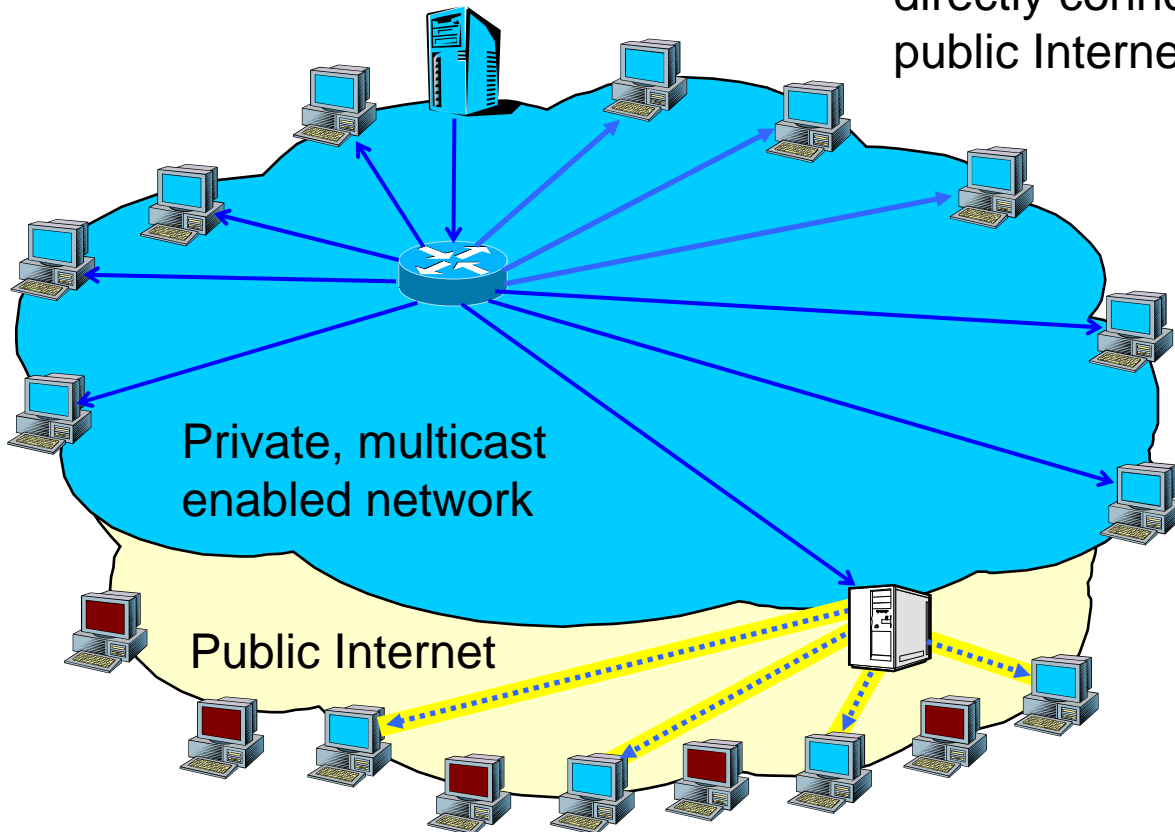
A module to be downloaded and installed by the user (or the content provider) allows FULL transparent access to multicast for the machine internally, and the other machines on the same LAN.

CastGate main features

- Clients can receive in ASM and SSM, and send in ASM (“manually managed” sending in SSM is in development)
- Tunnels operate in “bridged” mode rather than “routed” (routed would require network operator cooperation)
- tunneling default masqueraded as HTTP-TCP traffic to avoid problems with Firewalls and NATs; UDP tunneling is an option
- Auto-selection CastGate browser plug-in “package” of tunnel clients, automatically selecting the right plug-in in function of client’s OS and web browser used
- “Zero configuration”, but configuration still possible if required
- Tunnel servers can set “access” scope based on geographical location and/or net/host id of clients
- Tunnel servers can restrict access to specific multicast “channels”
- Public or private operation

CastGate private operation

When using multicast content distribution in a network that is multicast enabled, private operation of CastGate allows to distribute the same content to members that are not directly connected but have access through a public Internet connection.



E.g. a University that distributes internally using multicast over its university network can make the multicast content available to people residing "off-campus".

Free, public tunnel servers?

The whole operation is based on the assumption of public, free tunnel servers (and associated network capacity) being available... Who will provide them?

Here is an **important role** for the **publicly funded research, education and government networks**. If they offer to run tunnel servers and a fraction of their network capacity for the benefit of the Internet community, at least small to medium scale content distribution using multicast will become possible... BELNET, the academic and research network in Belgium – generously – paved the way, by offering 2 public tunnel servers @ 1Gbit/sec each.

Why would they do so???? Because:

- the Internet is a legacy of the academic community, and we still have a commitment to its evolution
- these networks are being paid with public funding, and there is a (implicit) responsibility to provide a **public** service when the occasion arises

- Tunnel servers and “pseudo-router” clients available for Linux and Windows
- Tunnel database servers is machine independent
- Browser plug-in client available for Internet Explorer and Netscape/Mozilla based browsers
- Java applet browser client for other web browsers (but requires Java VM to be installed)
- Reliability and machine independence should be improved
- Documentation is a mess...

Work in progress

- Additional porting (e.g. Apple Mac support)
- SSM:
 - (managed) SSM transmission through CastGate tunnel servers
 - allowing SSM reception with ASM-only applications
- Electronic Program Guides
- Tracking and access control for content providers of content distribution using IP multicast (hybrid operation, unicast control, multicast data)
- Massive multicast “Content-on-Demand” distribution (hybrid operation, unicast control, multicast data)
- IPv6 multicast bridging to the general, public IPv4 Internet

Conclusions

- CastGate is yet another multicast tunneling method such as LiveGate, AMT, etc...
- The main differentiation is:
 - the focus is towards “pragmatic” rather than technically optimal (but not always entirely practical?) solutions
 - targeted at content providers, NOT network providers
- With support from the (public funded) networks volunteering to provide a free, public multicast tunnel service, we maybe can finally break the “deadlock” holding back IP multicast deployment in the general, public Internet



CastGate contact information

www.castgate.net

support@castgate.net

Automatic and transparent?

Demo of a residential user **WITHOUT native multicast connectivity** accessing a local television broadcast station sending in **IP multicast** on the public Internet.

(Remark: the end-user uses **a standard** computer system **without** any specific multicast software tools installed...)

[Recorded CastGate demo](#)

