

IGAP: IGMP for user Authentication Protocol

draft-hayashi-igap-00.txt

Tsunemasa Hayashi, hayashi@exa.onlab.ntt.co.jp

Daisuke Andou, dandou@ansl.ntt.co.jp

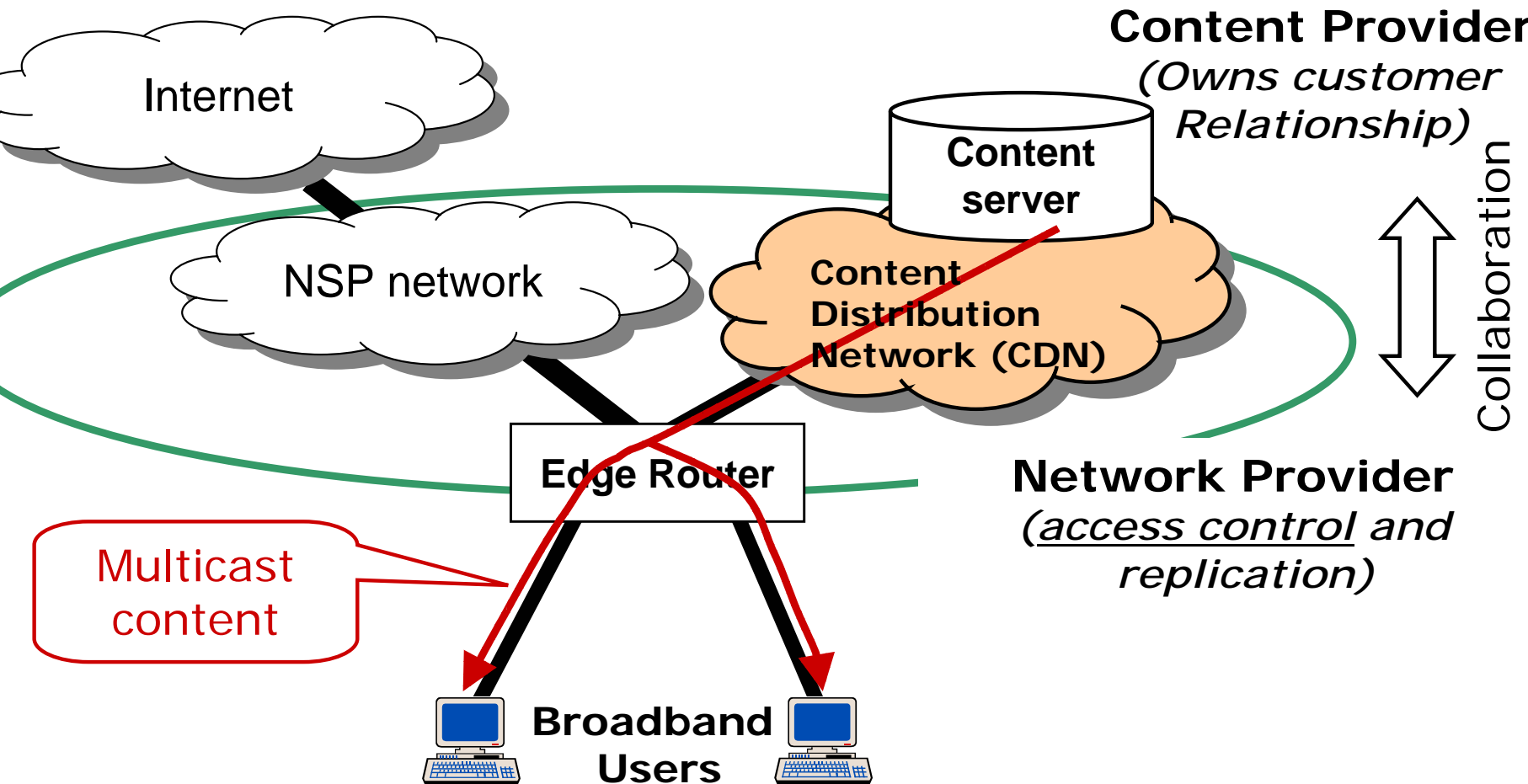
Haixiang He, haixiang@nortelnetworks.com

Wassim Tawbi, wtawbi@nortelnetworks.com

Teruki Niki, Niki@trl.mei.co.jp

2002/11/20

Network architecture



IP multicast in CDN

- Successful services need:
 - Access control to protect revenue source.
 - Limit scope to intra-domain multicast to avoid inter-provider issues.
 - Collaborations between content providers and network providers.
- Content providers need:
 - User-based subscription to services.
 - Outsource replication & user-based access control to network service providers.
- Network service providers need:
 - Simple mechanism to authenticate users & collect user usage information on behalf of content providers.
 - Who?, When?, Which group (content)?

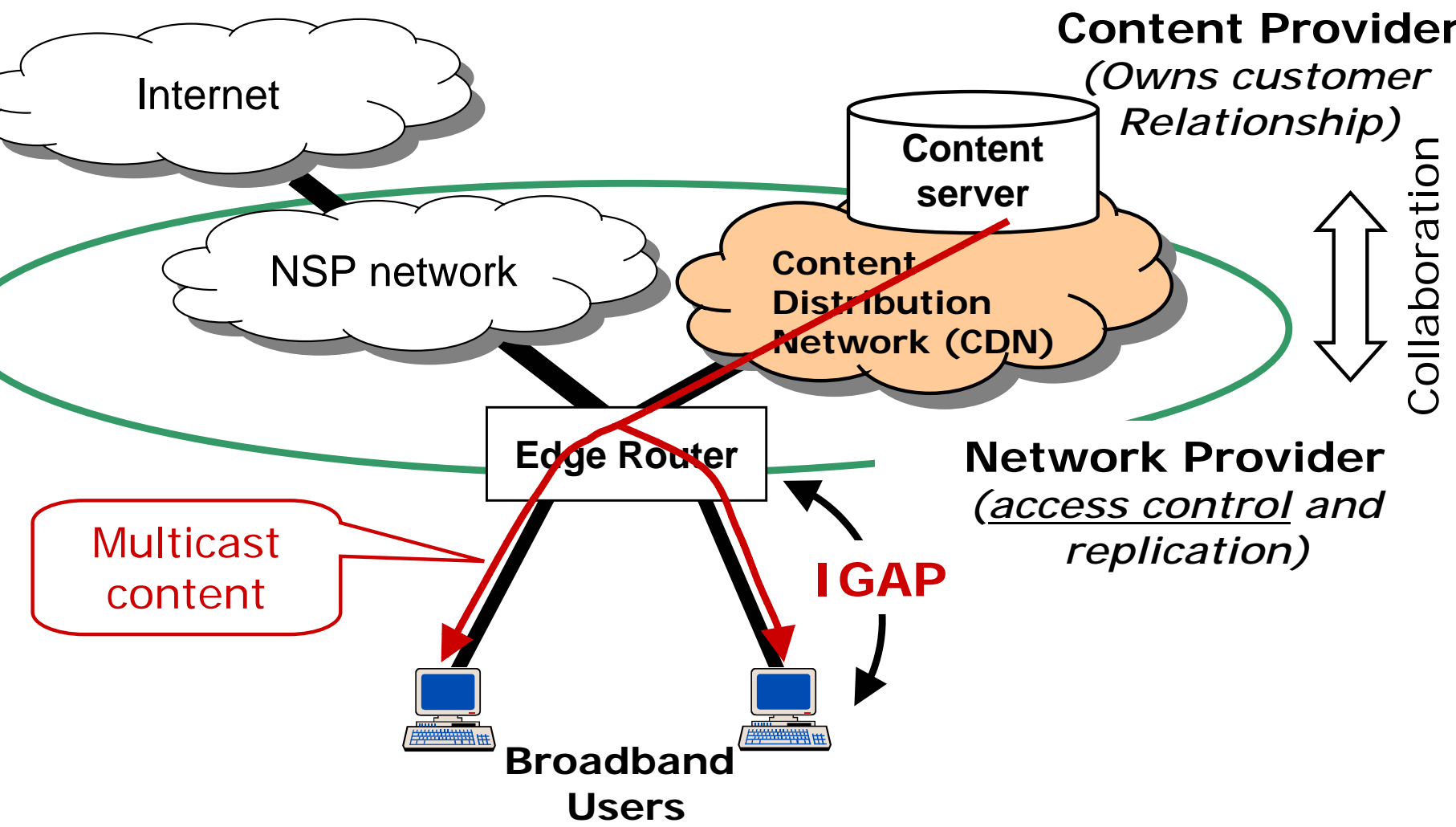
Current Situation

- No mechanism to control user access to multicast traffic.
 - Any user can join any multicast group
- No mechanism to collect user usage information.
- Multicast content security is being developed.
 - Can protect revenue source but,
 - Require a new key management infrastructure.
 - Cannot identify dynamically changing group membership
 - Doesn't address DoS problems (e.g. pulling 6Mbps TV stream).
 - Decoupling of key distribution and group membership complicates service assurance.
- Non-shared broadband access networks are widely deployed.
 - Access control is all that is required to protect revenue.

IGAP

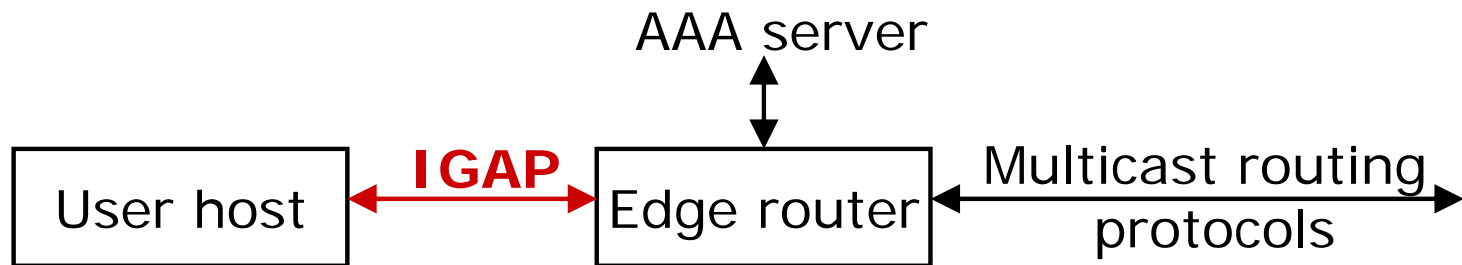
- Adds a protocol framework to transport user authentication information to IGMP.
- Enables providers to:
 - Enforce access control by a group, and by a user host
 - Collect per-user usage information.
 - Decouple user identity (logical identifier) from network operations
- Manages both group membership and user access as a unified process.
 - Group membership management is coupled with user access control in IP (network) layer operation.
 - User behavior is similar to the current multicast joining process with IGMPv2.

IGAP Context



IGAP design considerations

- Initially based on IGMPv2 due to deployment experience.
- Keep modifications as small as possible.
 - Hosts provide additional identification and authentication information into IGAP.
 - Routers authenticate membership state transitions with the content provider.
 - Additional notification capabilities are added.



- The interaction between edge routers and back-end AAA functions is out of scope.

Conclusion

- IGAP: Multicast Access Control
 - User based authentication
 - Initially derived from IGMPv2.

- Our request
 - to adopt IGAP as an I-D of magma WG.

(draft-hayashi-igap-00.txt)