NexTech 2009

Secure Multicast Communication

J. William Atwood

Distinguished Professor Emeritus
Computer Science and Software Engineering
Concordia University

Course overview

- Secure Multicast Communication
  - Overall motivation
- Overall Architecture
  - Motivation for using multicast
- Participant Access Control
  - Receiver Access Control, Sender Access Control
  - Policy Mechanisms
  - Mobility

..2

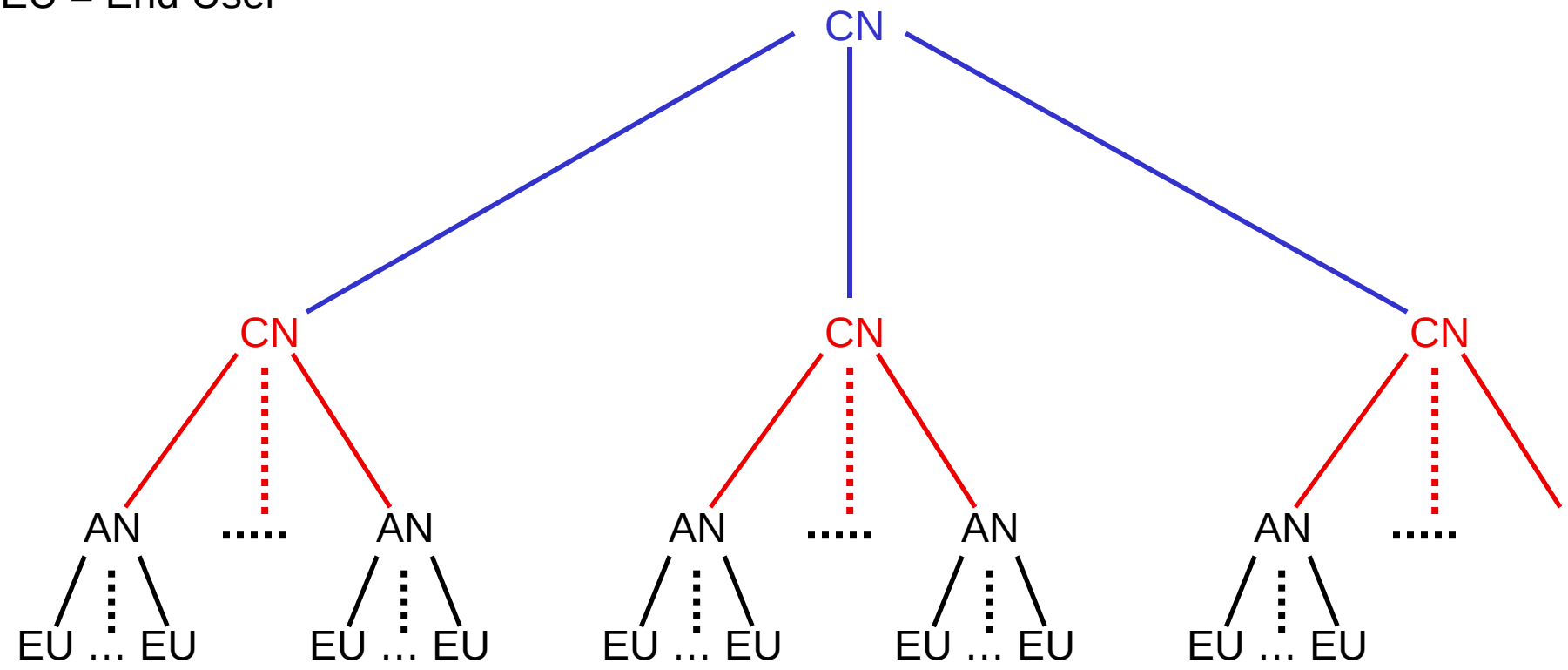
- Key Management
  - Proxy Encryption
  - SIM-KM
  - Authentication
  - Implementation
- E-commerce Interactions
  - Survey
  - Protection Profile
  - Protocols
- Control Plane Security

Results

- Many advantages for the End Users
- Potentially very lucrative for the Content Providers
- But, a growing challenge for the Network Service Providers and Content Servers

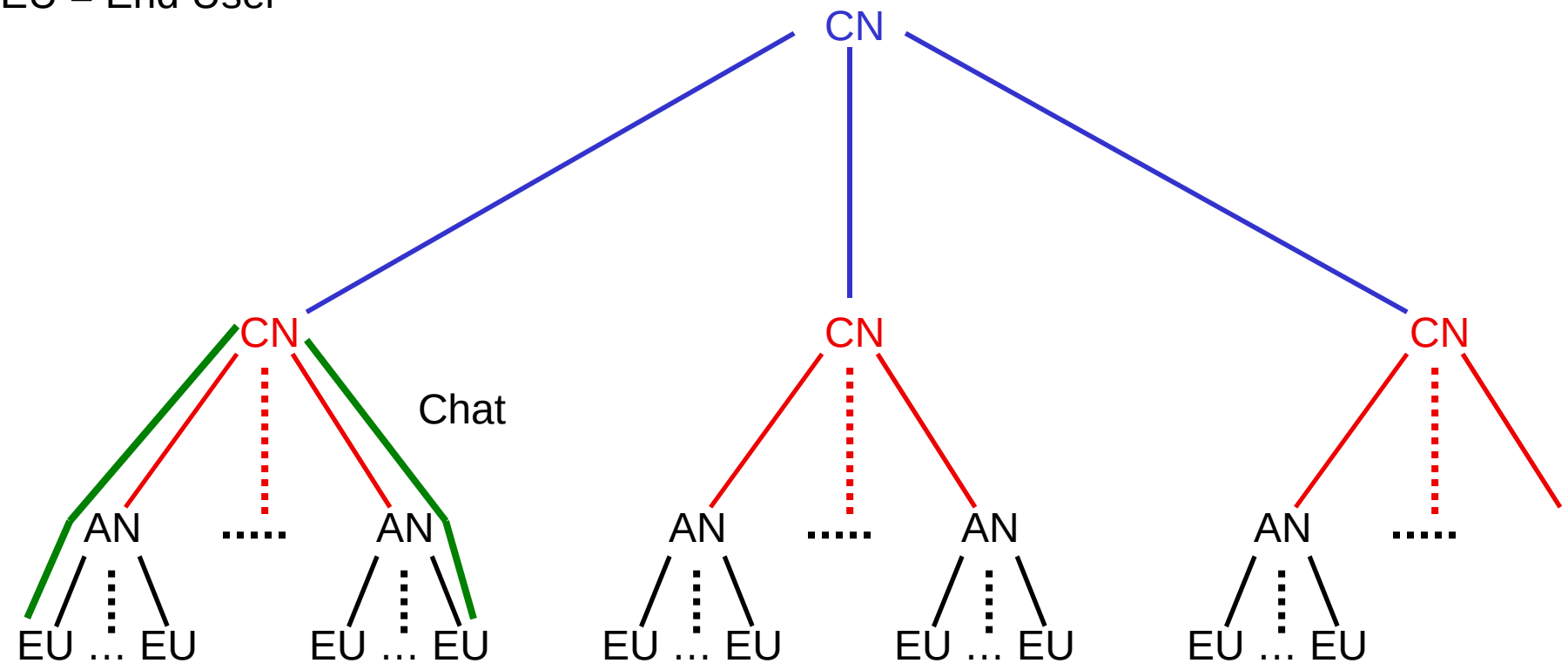
Network Structures

CN = Core Network
AN = Access Network
EU = End User



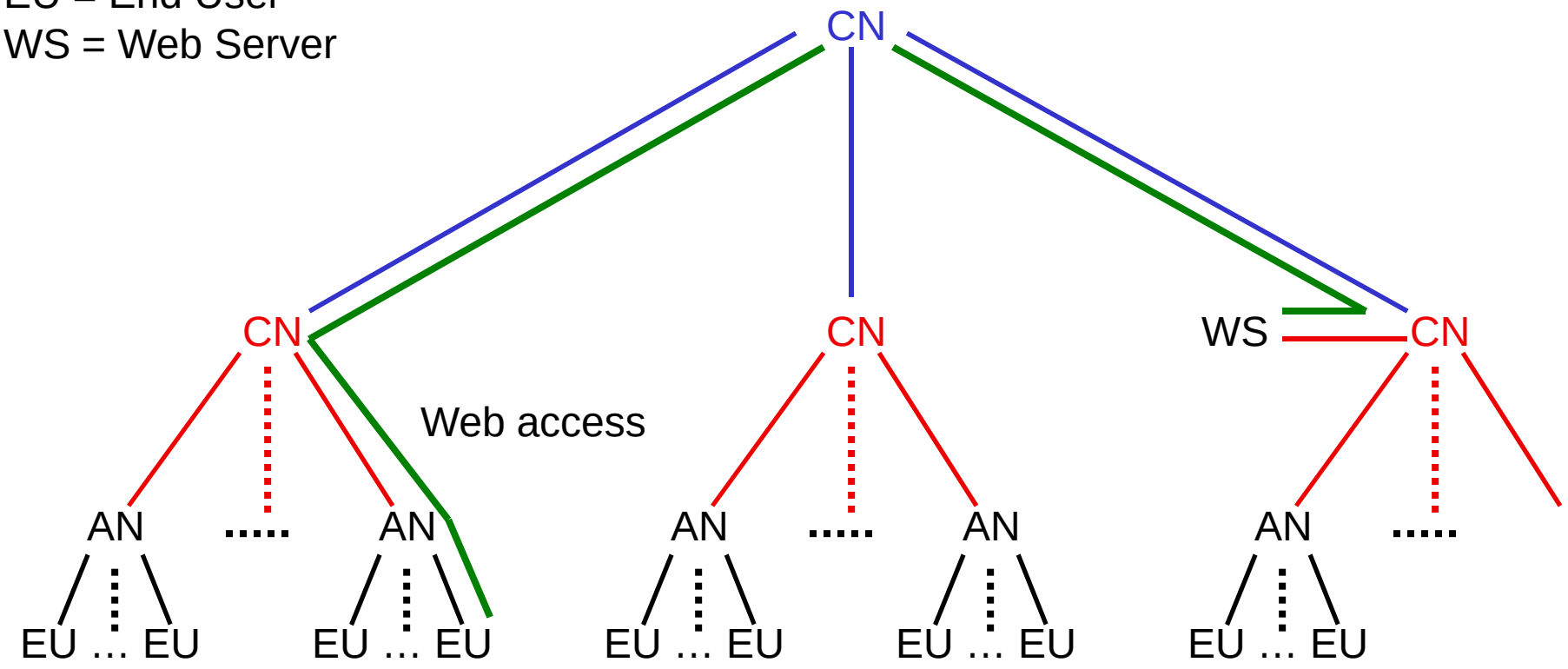
Communications Patterns 1

CN = Core Network
AN = Access Network
EU = End User



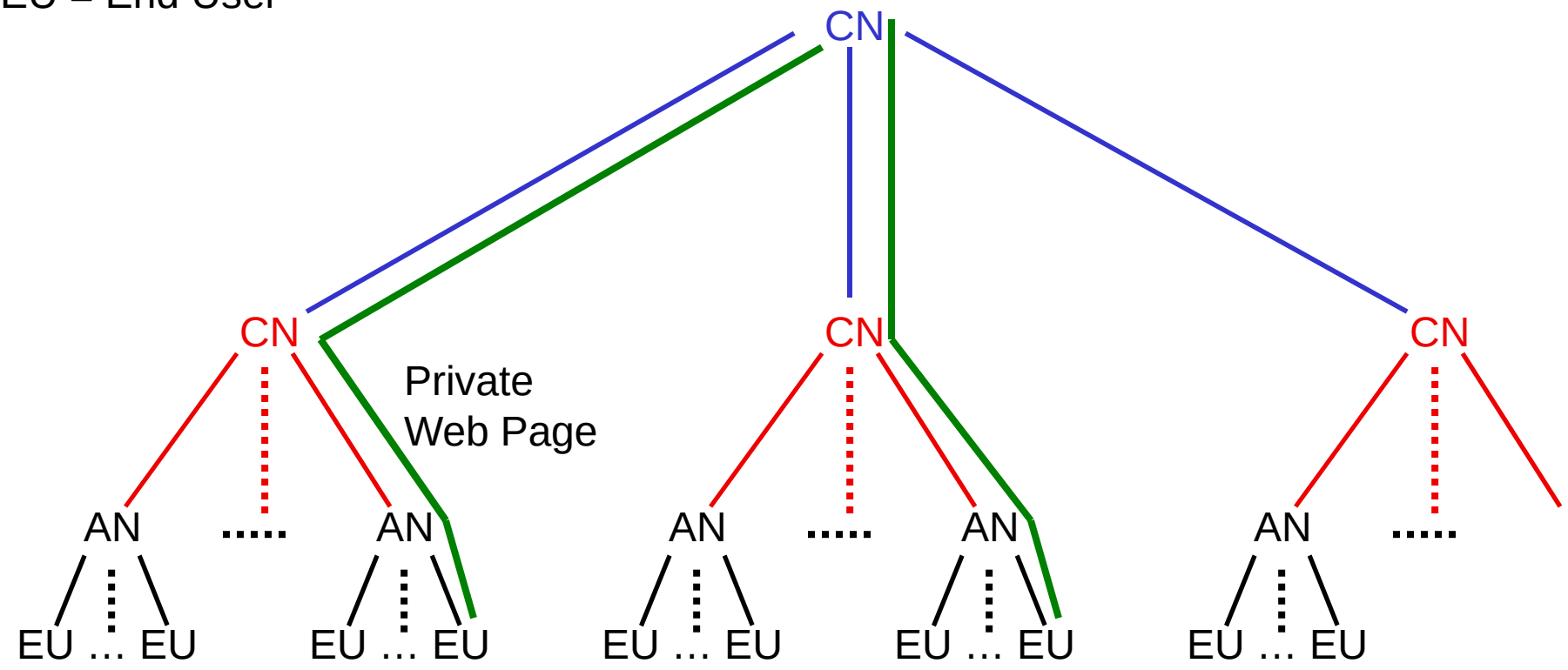
Communications Patterns 2

CN = Core Network
AN = Access Network
EU = End User
WS = Web Server



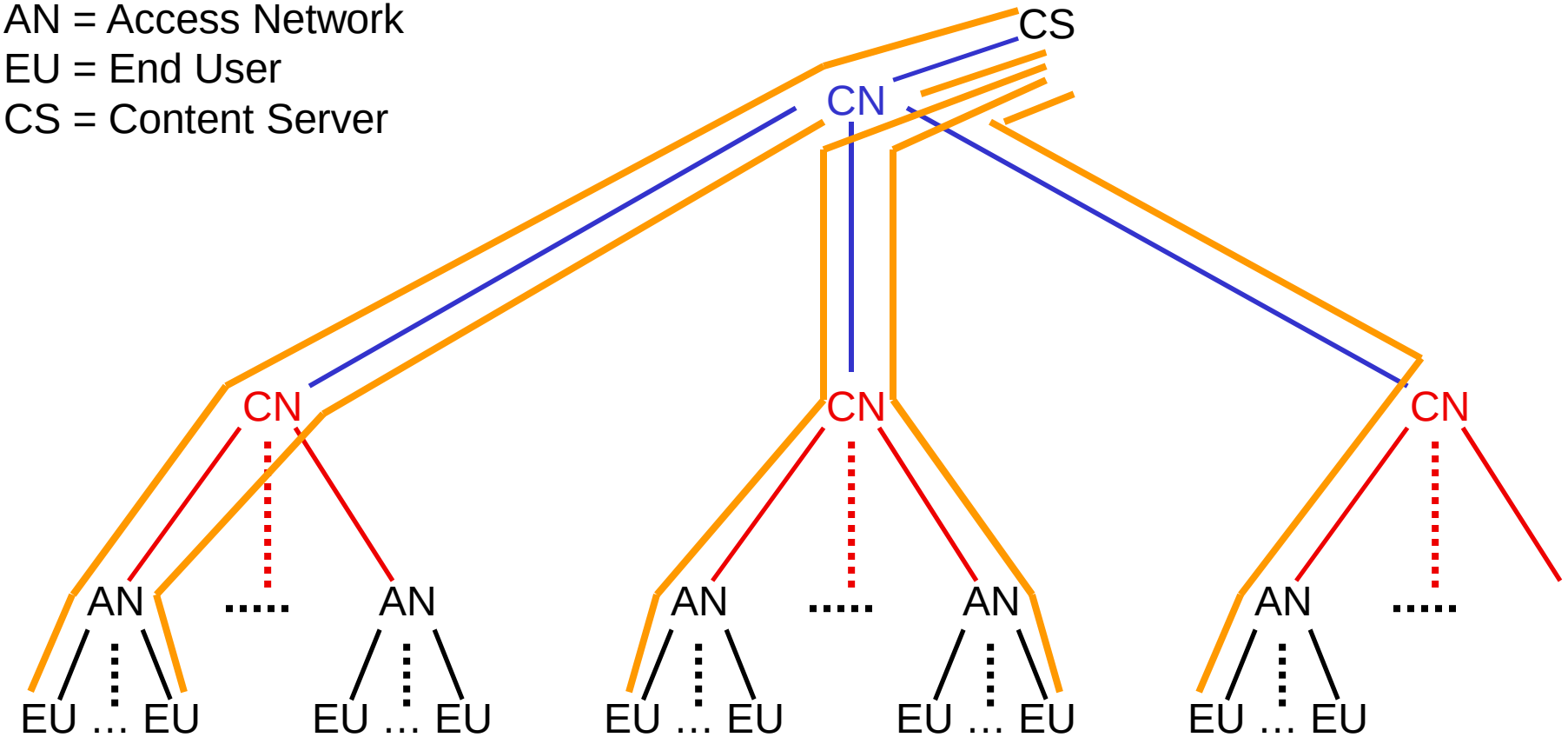
Communications Patterns 3

CN = Core Network
AN = Access Network
EU = End User



Communications Patterns 4

CN = Core Network
AN = Access Network
EU = End User
CS = Content Server

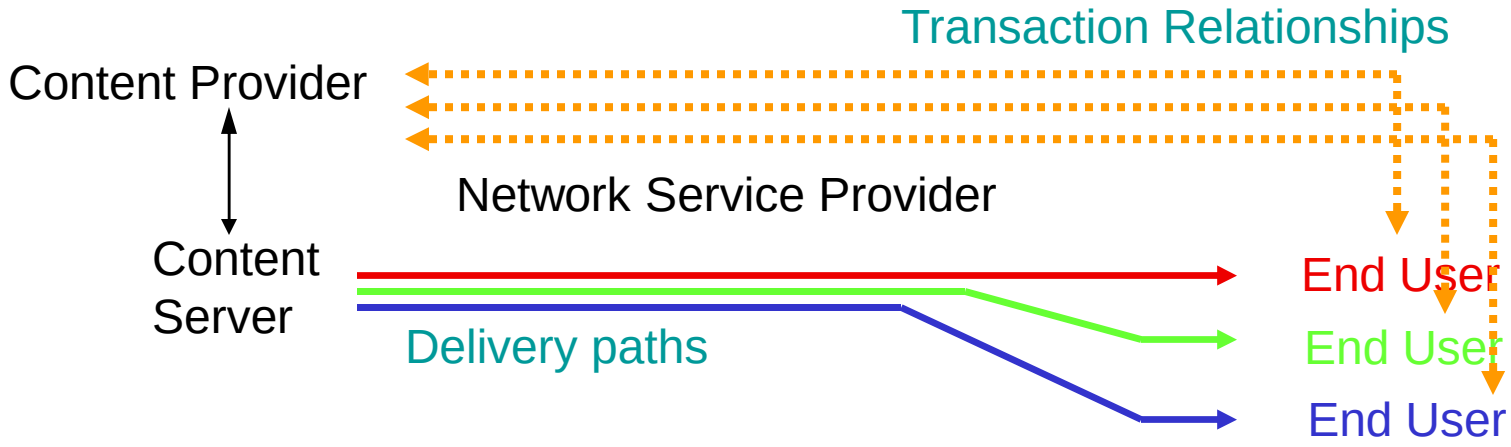


Summary

- Number & speed of Access Networks is growing
  - This puts more load on the Core Networks
- For “central server” applications
  - Even higher load on the Core Network
  - Very high load on the Content Server
- It is in these areas that a solution is needed

Today's Transaction Model

- Customer accepts offer from Content Provider
  - Encryption (defined by the Content Provider) is used to prevent theft
- Delivery is "over the network"
  - Network only "moves the bits"

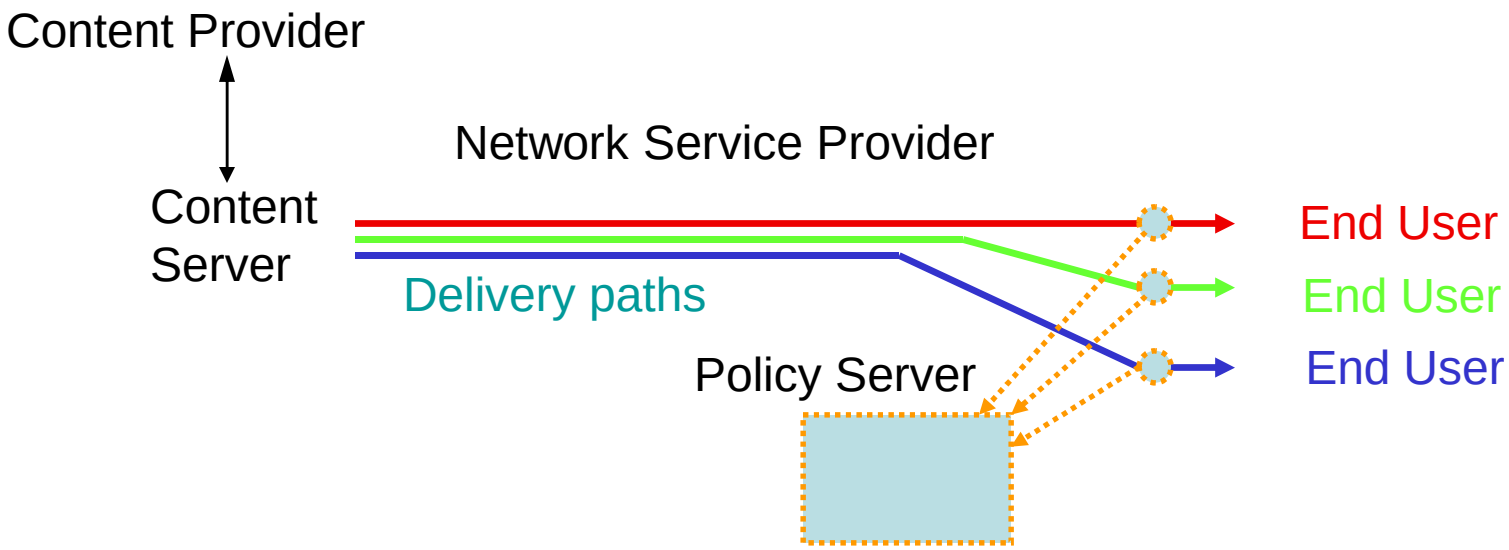


Network Service Provider View

- Network Service Provider controls access to “the (entire) network”
  - Network Service Provider only charges for “access to the network”
- Network Service Provider can deliver all services using “unicast” (one-to-one) communication
  - Each client (End User) has his/her own path

Access Control

- Two types of access control
  - Access to the service (controlled by the Content Provider, once per session)
  - Access to the network (controlled by the NSP, once per signon)



Tomorrow's Delivery Model

- As the Client Base increases, likelihood of simultaneous demands for identical material increases
- For "centralized" services, the network may saturate under heavy demand, and the Content Server is likely to reach an upper limit

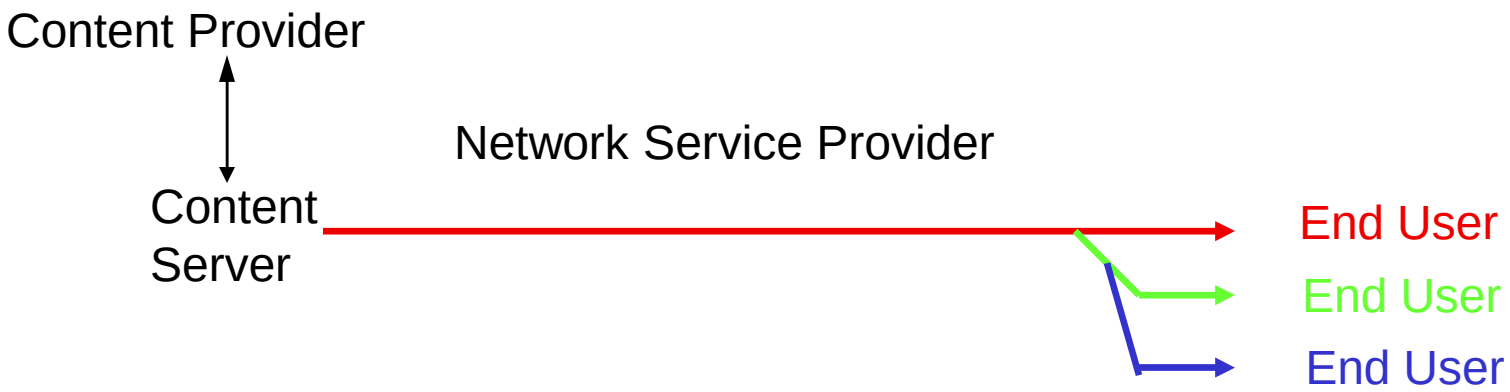
Multicast: A Solution

- Each End User shares common parts of the distribution path
- Each packet of the session flow only needs to be sent ***once***
  - Capacity of sender(s) does not need to grow
  - Capacity of the network can be smaller
- Core Routers must duplicate packets of a particular session

Standard Multicast

- Has been standardized for many years
- Multicast Advantages
  - Lower demands on the Content Server
  - Lower resource utilization in the network
  - → increase in scalability (= more revenue)

Building the Data Distribution Tree



Key Problem with Standard Multicast

- Loss of Control
  - The Data Distribution Tree has been built by the network, without consulting the Content Provider
  - The Content Provider does not know which End Users have received the session information
  - Vulnerable to fraudulent access by non-authorized Senders and/or End Users

Resolving the Problem

- Session
  - Defines the product that you purchased
  - Provides the keys for encryption
- Data Distribution Tree
  - Defines the network-level group
  - Joining will cause the End User's computer to be grafted onto the Data Distribution Tree
- Our solution is to take the existing ***network access*** protocol, and use it to control access to individual ***sessions***

Gaining Control 1

- For End Users
  - Combine the Session and Data Distribution Tree Join actions
  - Carry the session authorization on the DDT Join
- This allows the NSP to:
  - Determine who you are (authentication)
  - Determine that you are allowed to receive this session (authorization)
  - Record delivery of the product corresponding to a specific session (for accounting)

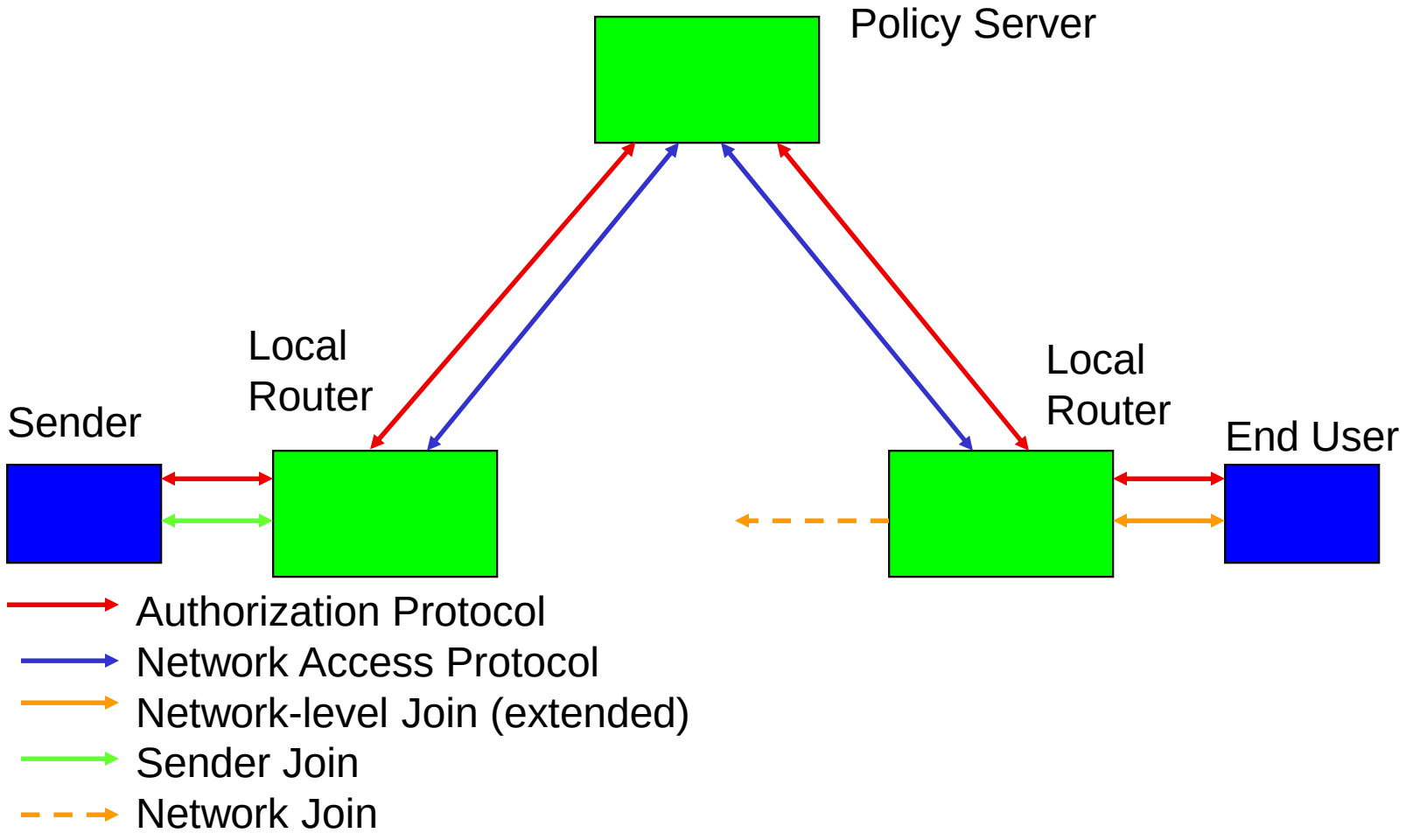
Gaining Control 2

- For Senders
  - We had to introduce a “Sender Join” action at the ***network*** level, to provide Sender Access Control for the Session
  - This then allowed us to use the extended standard network access protocols to allow managing a session
- Thus, the NSP can control and account for senders

Secure Multicast

- Achieving this control allows the NSP to “build a fence”
  - Control the End User access to the session
  - Control the Sender access to the session
- The Data Encryption Keys will be distributed only to legitimate participants
- The Data will only be accepted from a legitimate Sender, and will only be delivered to legitimate End Users.

Interior Communications



Other Issues Resolved

- Managing the Data Encryption Keys given multiple session participants
- Protecting the Data Distribution Tree against bogus data insertions
- Extending the Work to Multiple Administrative Domains
  - Senders will not always have the same Network Service Provider as the End Users
- Extending the Work to Mobile Environments

Current Issues

- Protecting the Neighbour Relationships among the Routers
  - To prevent intruders from altering the shape of the Data Distribution Tree
- Interfacing with the E-Commerce world
  - To collect the money

Technology Transfer

- Standardization to be done
  - Extensions to Network Level Join, to carry session credentials
  - Use of the standard (network-level) Authentication protocol to achieve session control
  - Application of a newly-defined extension to the standard Authentication protocol to permit “fast” mobile handoff
- Standardization in progress
  - Management of neighbour relationships for multicast routers

Future Work

- Digital Rights Management
  - Achieving control even after the session is over
- Implementation
  - Value-added routers: the XORP project
  - Extensions to existing protocols

Thank you!

- Questions?