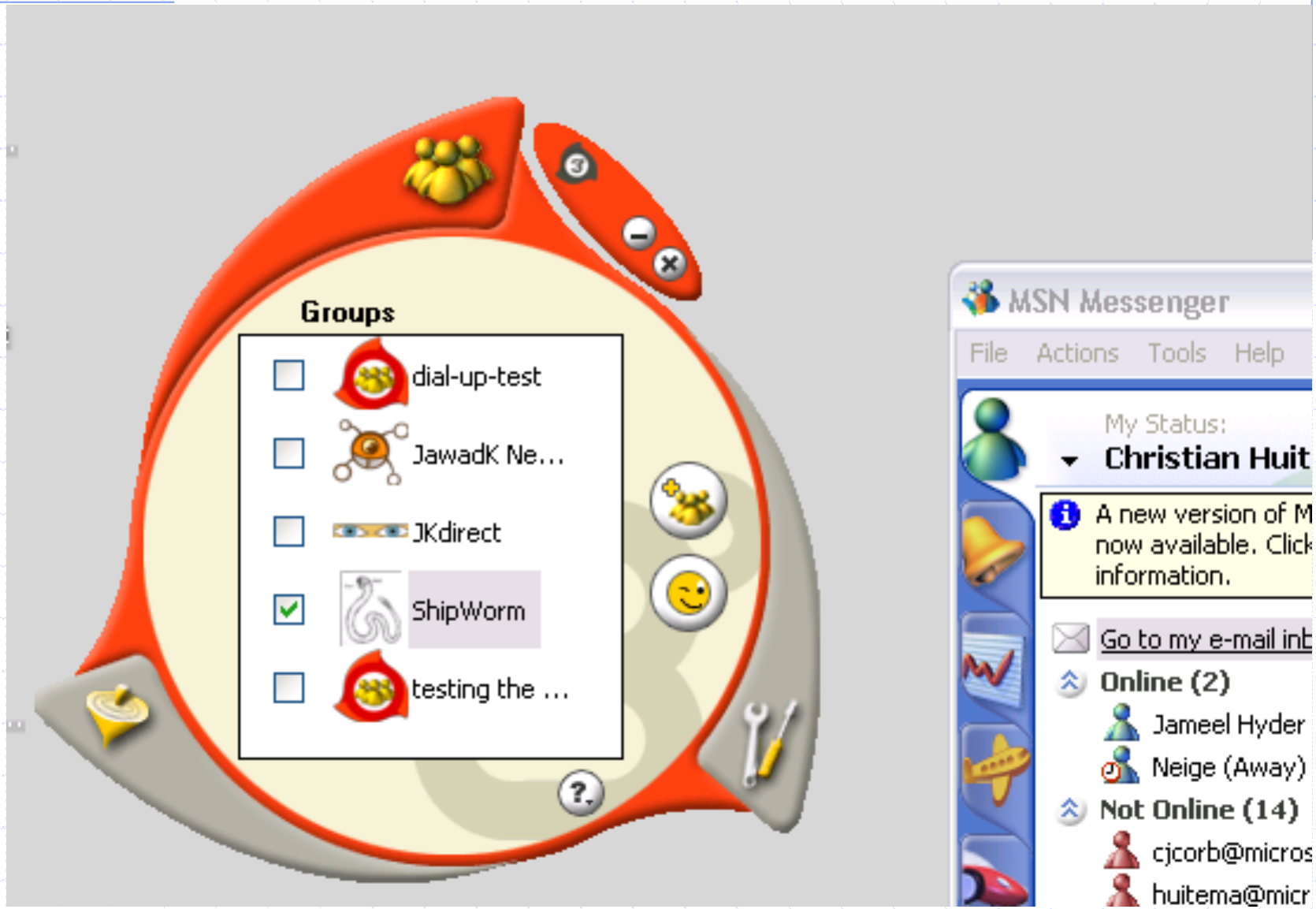
Le Pair-à-pair et les Nouvelles Applications de l'Internet

Christian Huitema
Architecte
Windows Networking & Communications
Microsoft Corporation

Welcome to 3 Degrees, P2P & IPv6



Pair-a-pair & Windows

- Du prototype (Fin 2000) au produit (2003)
  - Outil de développement disponible sur MSDN
  - Déploiement (bêta) de “3 Degrees”
  - Progression vers “RTM”
- But: développement d’ applications P2P
  - Centrage vers les interactions « de groupe »
    - (3 Degrees plutôt que Kazaa)
    - « messages instantanées P2P »
  - Internet, réseau d’entreprise, ad hoc
  - Ne doit pas requérir de serveur

Architecture

- Quatre composants principaux
  - IPv6
  - Service de noms P2P
  - Réplication de données sur un graphe
  - Gestion d'identite et de droits d'acces
- Pour répondre a trois questions
  - Déploiement
  - « scalability »
  - Sécurité

Déploiement d'une nouvelle infrastructure

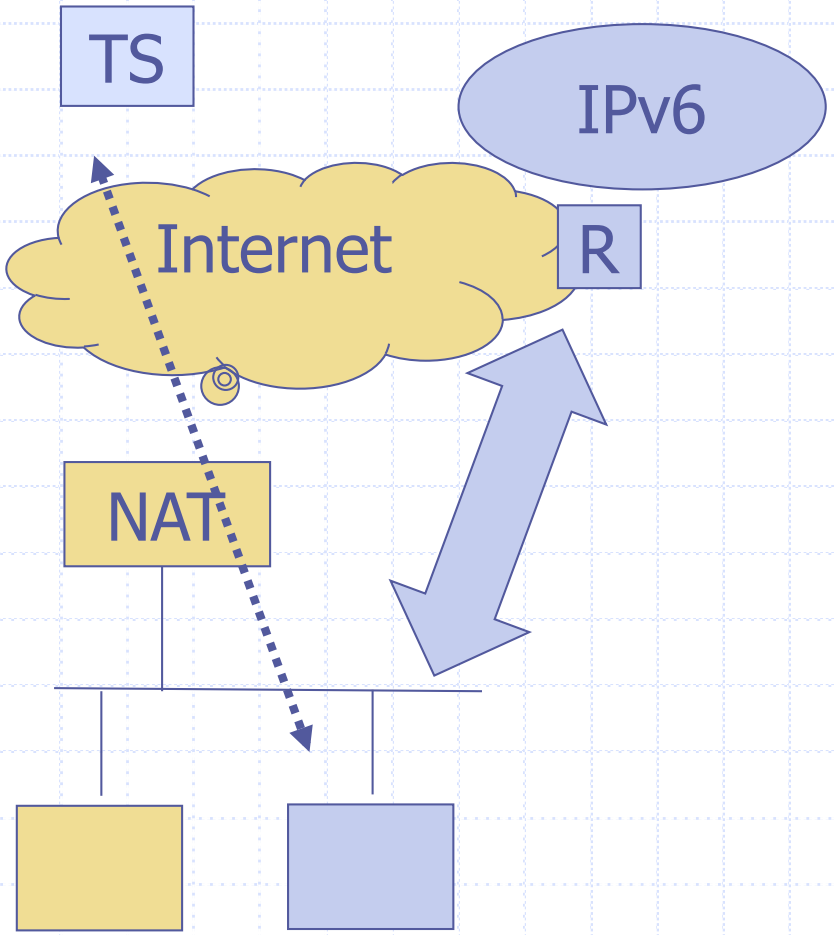
- Quelques échecs célèbres
  - RSVP:
    - tous les routeurs doivent être modifiés avant d'obtenir le service
  - IP multipoint
    - Déploiement incrémental (MBONE), mais justification économique faible
- On ne peut pas « bouillir l'océan »
  - Le déploiement doit procurer un bénéfice immédiat pour chacun des acteurs

Déploiement & pair à pair

- Généralement possible
  - Application distribuée, chaque acteur bénéficie du résultat.
- Mais ...
  - Distribution implique connectivité:
    - NAT, Firewalls
  - Certaines formes de distributions requièrent des services centraux

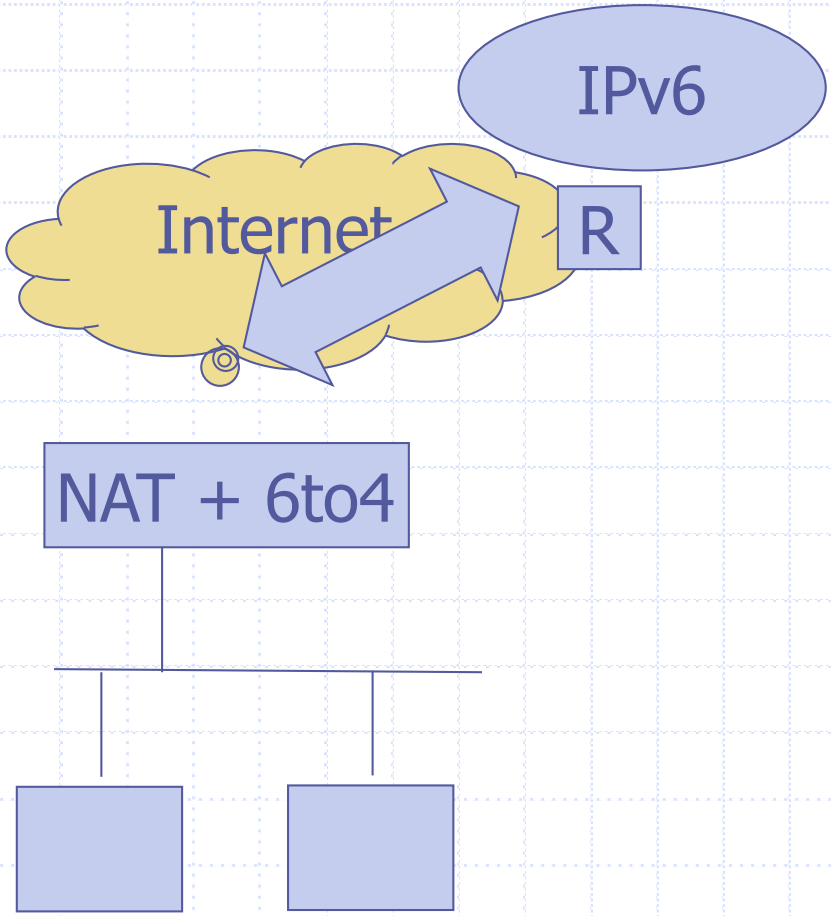
    Serveur de noms, catalogues

Pair à pair et connectivité: IPv6, Teredo



- IPv6 fournit des adresses globales
- Phase 1: Teredo
  - IPv6 > UDP > IPv4
- Déploiement :
  - Serveur « minimal »
  - Logiciel dans les PC
  - Relais

Déploiement de IPv6

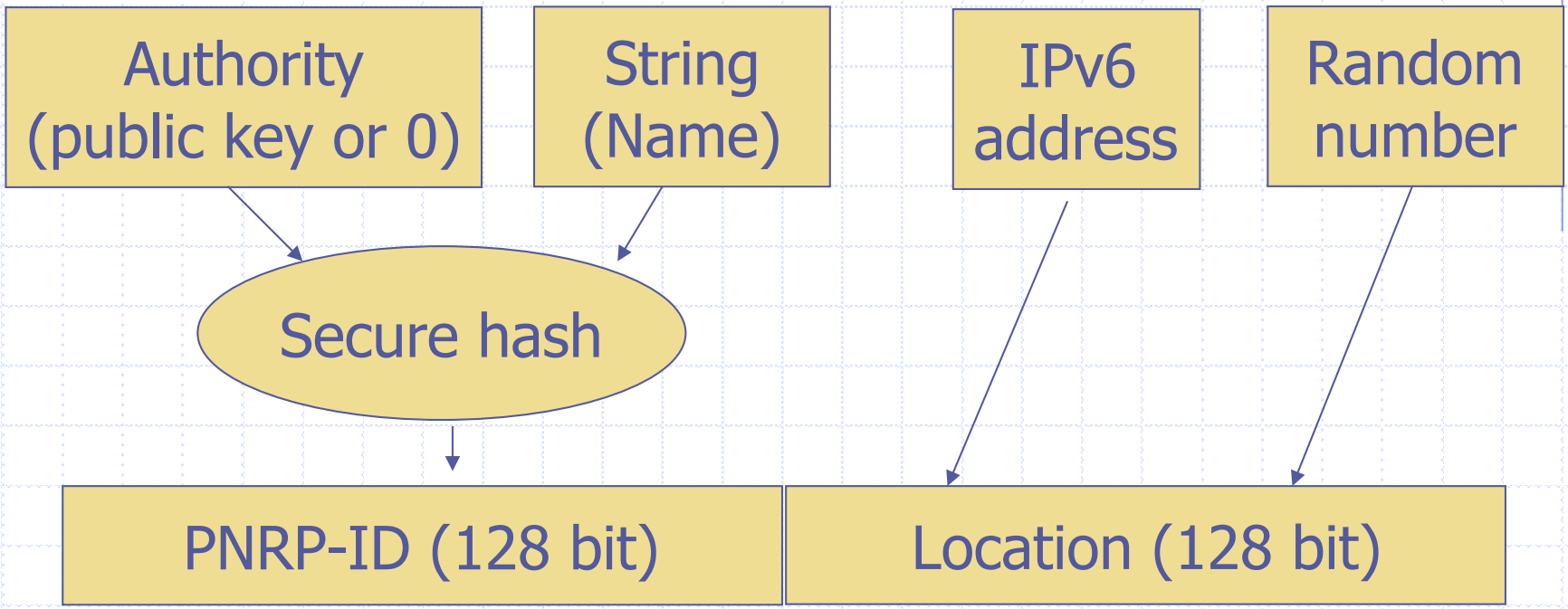


- Phase 2: 6to4
  - IPv6 > UDP > IPv4
- Déploiement :
  - Logiciel dans les NAT
  - Relais
- Motivation : P2P
- Phase 3: « natif »

Scalability, Robustesse

- Service de noms
  - Des milliards d'agents repartis sur tout l'Internet
- Graphes et groupes
  - Des millions de groupes, de taille variable
- Présence intermittente
  - Les pairs vont et viennent...

Résolution de noms pair à pair: PNRP



Chaque point maintient un cache de “PNRP records”.

Le routage est basé sur le cache.

Le cache est géré comme une table de hachage distribuée

Entrée PNRP

- Identifiant PNRP & location,
- Hachage de la clef publique de l'autorité,
- Hachage du nom,
- Adresse(s) IPv6 du point de publication,
- Adresse(s) & port de la ressource
- Clef publique du point de publication,
- Signature de l'entrée par la clef privée du point de publication
- Si nécessaire, certificats liant le point de publication à l'autorité.

Gestion du hachage distribué de PNRP

- Maintenance du cache
  - Acquisition d'entrées lors du traitement des requêtes
    - Garder les plus fiables et les plus proches en priorite
  - Organisation en niveaux
    - Niveau = fraction de l'espace, centrée sur le nom local
    - Chaque niveau est un cinquième du précédent
    - 10 entrées par niveau (redondance, randomisation)
  - Maintenance par « inondation » du dernier niveau
  - Utilisation d'un « seed server » pour l'initialisation (premier pair) et la détection de partitions
- Chaque point peut publier plusieurs noms

Support des groupes

- Les applications intéressantes incluent plusieurs pairs
  - Partage de fichiers,
  - Groupes de discussions,
  - Publication de données vers des grands groupes.
- On ne peut pas compter sur IP multipoint, mais le multipoint « par application » est problématique
  - Les nœuds du graphe ne sont pas fiables,
  - Les nœuds sont à la marge du réseau,
  - Le graphe « logique » ne reflète pas forcement la topologie du réseau.

Support des groupes, gestion de graphes

- Notre solution: graphes pair à pair
  - Construction progressive a partir de points de contact (publiés dans PNRP)
  - Transmission robuste & redondante (inondation)
  - Adaptation continue à la topologie par calcul d'une « fonction d'utilité »
  - Protection contre les partitions
- Chaque noeud maintient une copie de la « base de données » du graphe

Sécurité & pair à pair

- PNRP, service de noms distribués
  - Publication de fausses données (spoofing)
    - Protection: signature des entrées
  - Déni de service
    - Protection: randomisation, redondance, gestion du cache
- Groupes et graphes
  - Accès non autorisé, déni de service
    - Protection: contrôle d'accès, chiffrement des transmission, signature des messages

Sécurité des groupes pair à pair

- On ne peut pas compter sur des serveurs
  - On doit utiliser des « clefs publiques »
  - On ne peut pas utiliser une « autorité centrale de certification »
- Notre solution: « certificats de groupe »
  - Un pair crée un groupe, choisit clef publique et privée
  - Invite d'autres pairs a joindre le groupe
  - Donne aux pairs un « certificat », utiliser pour contrôler l'accès au groupe

P2P & .Net

- Les services P2P seront utilisable dans « .Net framework »
- IPv6
  - Service de réseau System.Net
- PNRP
  - Publication d'URL P2P pour services web
- Certificats P2P
  - Sécurisation de transactions, WS-Security
- Graphes & groupes
  - Services web multipoints

Travaux Futurs

- Expérimenter & étudier
  - Déploiement de quelques applications de tests
  - Commentaires des premiers utilisateurs
- Nouveaux algorithmes
  - Par exemple, diminuer les transmissions redondantes dans les graphes
- Nouveaux services
  - Recherches dans un graphe, catalogues distribués
  - Diffusion de fichiers, de multi-media

Pour en savoir plus

- Windows XP Peer-to-Peer Update, Peer-to-peer toolkit
  - http://msdn.microsoft.com/downloads/list/winxppeer.asp
- Internet P2P research group
  - http://www.irtf.org/charters/p2prg.html