Challenges and Opportunities in Deploying IPv6 Applications

Marc Blanchet

CTO, Hexago

(Director, North American IPv6 Task Force
Member of the Board and Technical Directorate, IPv6Forum)

{mailtoIsip}: Marc.Blanchet@hexago.com

Plan

- Some IPv6 benefits TODAY
- Ubiquitous IP
- Challenges
- Incremental deployment
- TSP tunnel broker
- Case studies with real examples

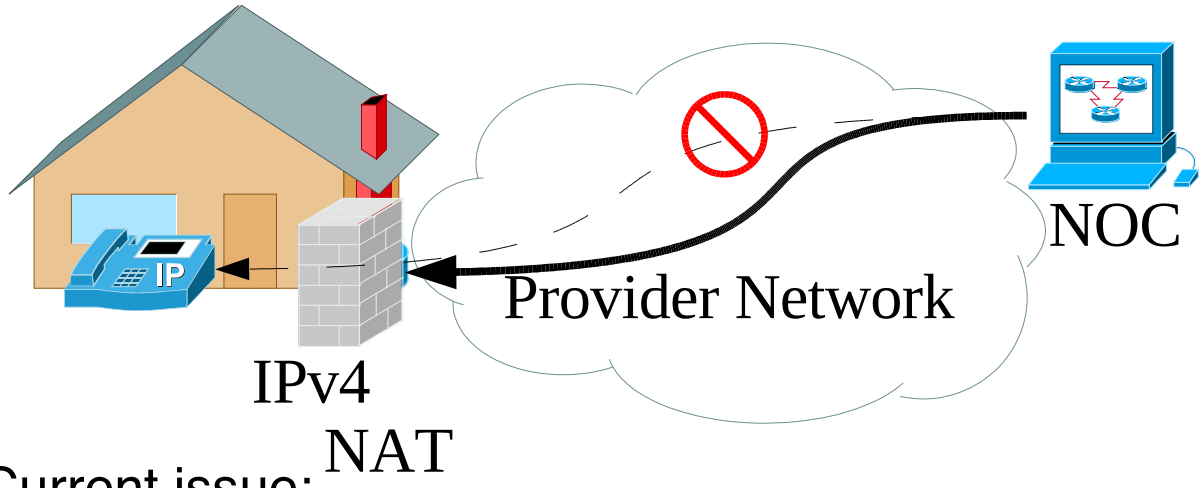
- Warning: Real world examples in this presentation!

Some IPv6 Benefits Today

- Network Management
  - Visibility/Management/Support of nodes/users
    - Remote sites
    - Broadband users and applications
  - Manageable and Unique Private Address Space
- VoIP Deployment
  - Enables End to End (P2P) VoIP
  - Lightweight SIP infrastructure
- IP security Deployment
  - End to End, anywhere.
  - Mobile nodes and networks
  - Secure VoIP
- Ubiquitous IP
  - Mobility using any link access and any IP version

Network Management

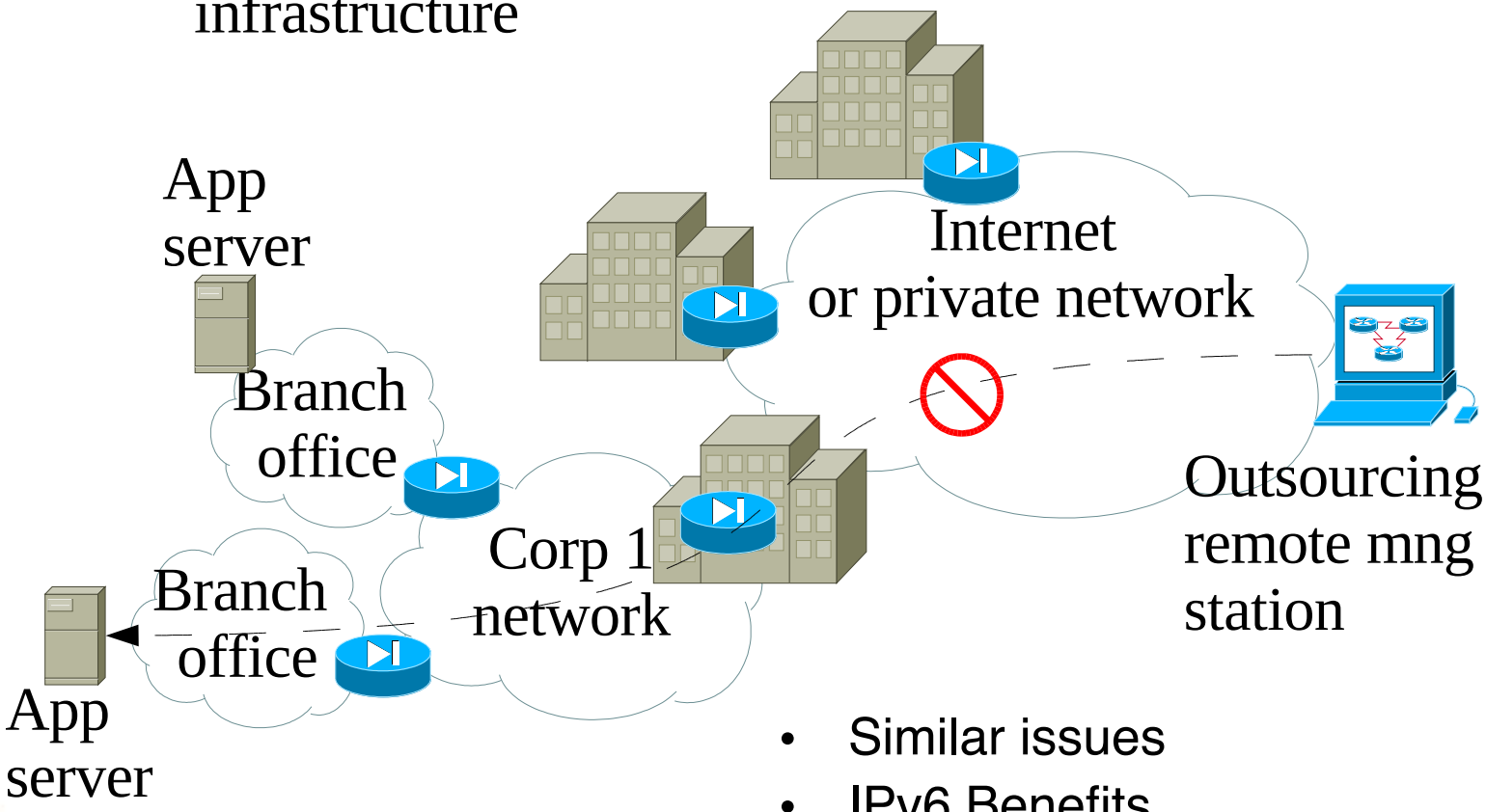
Provider deploying broadband VoIP services



- Current issue:
  - IPv4 NAT disables visibility.
  - Business consequence:
    - Can't answer a support call. High support costs ($$$), loose customers.
    - Can't deliver SLA. Can't sell higher price with higher margin.
- IPv6 Benefits:
  - Visibility/Reachability
  - Support

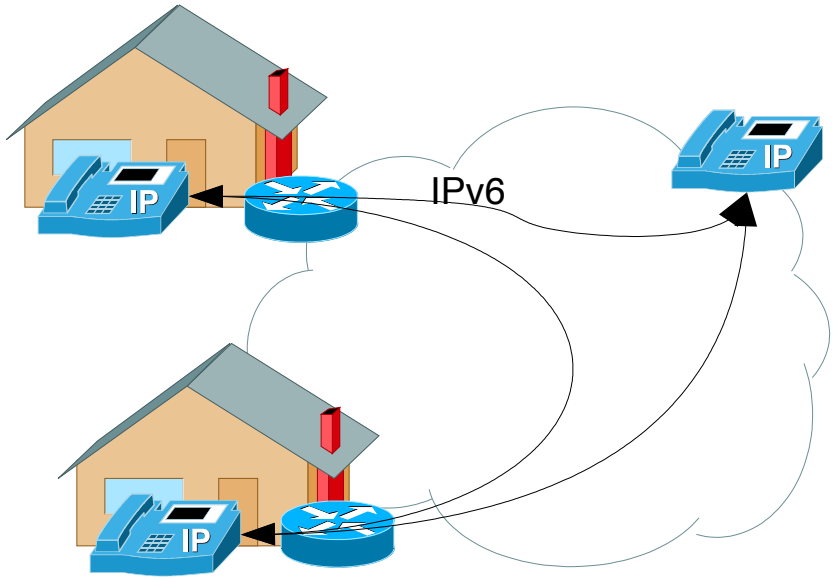
Network Management (2)

Outsourcing company doing remote management of infrastructure



- Similar issues
- IPv6 Benefits
  - Visibility/Reachability
  - Unique Private Addressing

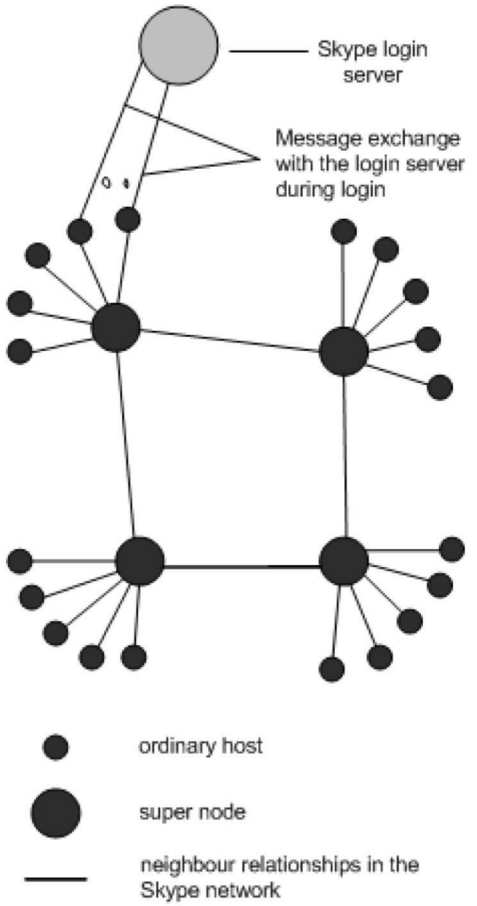
VoIP E2E deployment



- Issue: If home gateway is IPv4 NAT, no E2E/P2P VoIP. needs a SIP proxy architecture with NAT traversal.
- Business consequence:
  - Much heavyweight architecture: bigger servers, bigger bandwidth, etc... Higher costs.
- IPv6 benefits: reachability, P2P, lightweight VoIP.

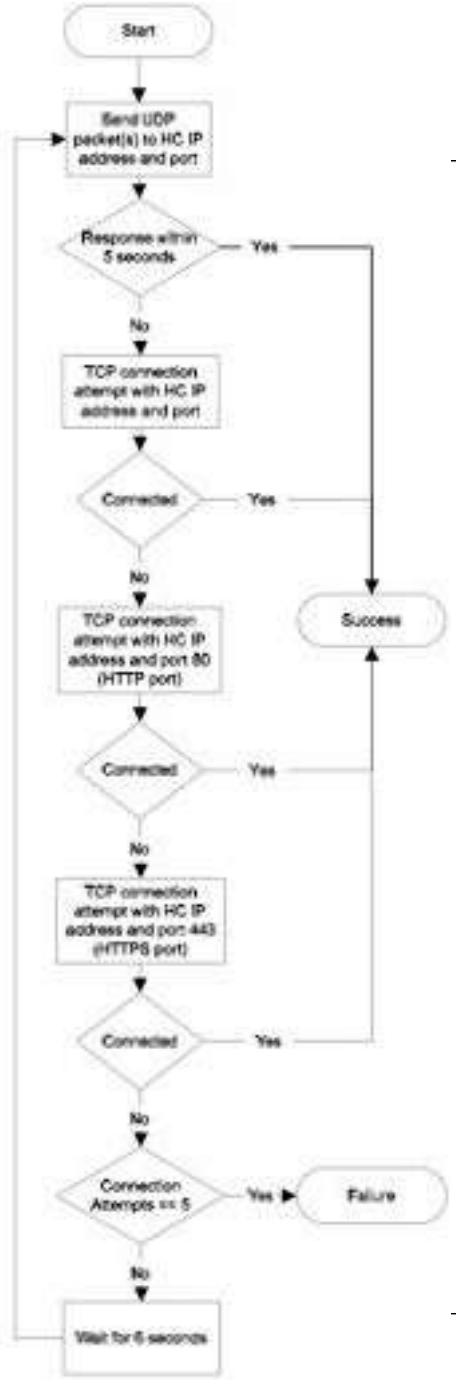
Alternative to SIP and NAT issues?

- Skype model:
  - Not peer-to-peer!
  - Through «super-nodes »
  - Super-node are proxies carrying voice traffic
  - Trapezoide: user1->sn1->sn2->user2
  - Any user computer can be elected as supernode, without the consent of the user and without noticing!!! You may be elected if you have a public IPv4 address and some cpu.
  - When supernode is elected, it receives and forwards traffic from many skype nodes.
    - Consequence: your bandwidth is used by others, not for you, and without knowing!
    - Universities with public addresses and a lot of cpus do not like it at all!
    - Consequence: trying to block skype use.
- Why Supernodes: because of NAT.



Skype NAT traversal

- Technique:
  - 1) try udp
  - 2) if no success, try tcp
  - 3) if no success, try tcp on port 80 (http)
  - 4) if no success, try tcp on port 443 (https)
  - 5) if no success, go to 1)
- Consequence:
  - Application has very complex logic for getting basic connectivity
  - Logic will have to change as firewalls and NATs are changing behaviors (a new implementation of a NAT might just block this process)
  - Security bypassed.
  -
  -
  - Ref: http://www.cs.columbia.edu/~library/TR-repository/reports/reports-2004/cucs-039-04.pdf



Skype Lessons

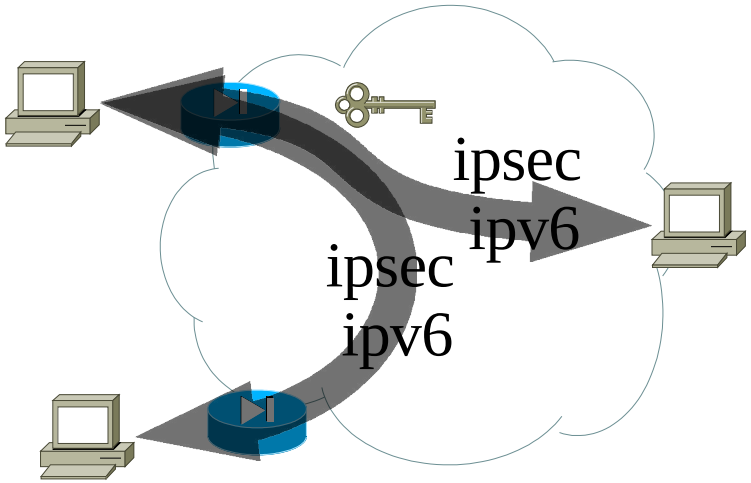
- Skype showed demand for P2P. New opportunity. Good
- NAT disabled P2P. Not good!
- Skype architecture is based on stealing someone else bandwidth, without their consent, for other parties to use. Not good!
- Skype nat traversal method is:
  - Complex. Higher costs of development, support, etc... Not good.
  - Fragile. To any changes. Higher costs of support, development. Not good.
- Business consequence:
  - On current IPv4 networks, if your application needs P2P, then the Skype technique is probably the most effective to get nat traversal, even if it is fragile and far from perfect.
  - So you will end up doing similar techniques, with all the consequences, present and future.

NAT is killing innovation!

- Prior to Skype and SIP, there was SpeakFreely.
- The author stopped development because of proliferation of NATs, that cause the application to stop working.
- NATs are killing Internet innovation!
- Here is an excerpt from his EOL note:
- « “**The Internet of the near future** will be something never contemplated when Speak Freely was designed, **inherently hostile to such peer-to-peer applications**. I am not using the phrase "peer to peer" as a euphemism for "file sharing" or other related activities, but in its original architectural sense, where all hosts on the Internet were fundamentally equal. Certainly, Internet connections differed in bandwidth, latency, and reliability, but apart from those physical properties any machine connected to the Internet could act as a client, server, or (in the case of datagram traffic such as Speak Freely audio) neither--simply a peer of those with which it communicated. Any Internet host could provide any service to any other and access services provided by them. **New kinds of services could be invented as required**, subject only to compatibility with the higher level transport protocols (such as TCP and UDP). **Unfortunately, this era is coming to an end**.” [SpeakFreely]

REF: http://www.fourmilab.ch/speakfree/unix

IP Security E2E deployment



- Issue: If IPv4 NAT, no E2E/P2P security. Multiple NATs in sequence in corporate networks.
- IPv6 benefits: reachability, P2P, E2E.

Ubiquitous IP

- Multiple access technologies
- Multiple IP versions
- Various scenarios
-

Multiple Link Access Technologies

- Mobile/portable devices have multiple link access technologies:
  - Fixed: 802.3+... (Fixed Ethernet at all speeds)
  - Wireless: 802.11, GPRS, 3G, W-CDMA, Bluetooth, WiMAX, ...
  - (fixed will always be « better »: bandwidth, signal, price, ...)
- « Smart » devices (and users!) move dynamically to the « best » link (depending on criteria: bandwidth, price, signal strength...)
- 1st common network protocol layer: IP
- Each move requires authentication to the new network and reconfiguration of the IP stack (i.e. IP address/gateways/DNS servers, ...)
- An application cannot manage the changes. It is handled by the networking stack in the operating system.
- Need to handle mobility at the IP layer.

Multiple IP Versions

- In these access networks:
  - Most (all?) have IPv4
  - Some have IPv6 (with IPv4, maybe at different service levels)
  - Most are moving to IPv6 (by some speed)
  - For the next years, very few, but some are/going to be IPv6-only (given applications requirements and IPv4 limitations)
- Change of IP protocol version requires configuration of the IP stack and re-establishment of network connections
- An application cannot manage the changes. It is handled by the networking stack in the operating system.

Multiple Links and IP Versions

- Reality: combinations of links and IP versions on the same mobile device, moving over multiple networks
- Examples:
  - 802.3-IPv4-IPv6
  - 802.11-IPv4
  - GPRS-IPv4
  - 3G-IPv6
  - ...

Handoff Speed

- Speed to move to a new link access technology should be fast
  - from the user point of view
  - and from the application point of view
- But, handoff involves:
  - Authentication
    - Roaming authentication between different link access technologies are not available.
    - Currently involves different authentication protocols/access (i.e. 802.11 hotspots with web-ssl authentication).
    - May be very slow especially if requires manual user intervention (finding that he needs to (re)start his browser, click, find his authentication credentials in some file, fill in, click, ...)
  - Mobility detection
    - To be optimal, requires help of the link access to pass information to the IP stack. (ex: frequent router advertisements).
    - Not all access may/should provide this service. (i.e. 802.3 fixed ethernet might not be set to help mobile devices)
  - IP stack reconfiguration
  - May require manual interface card installation

Summary: Ubiquitous IP

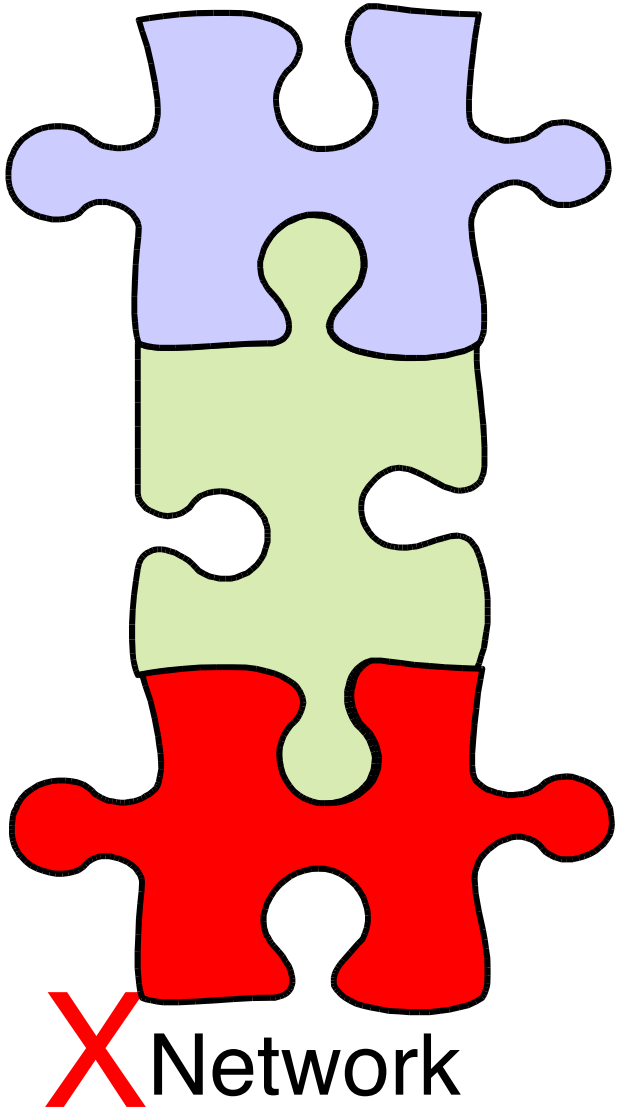
- Multiple network access technologies
- Multiple IP versions
- Different combinations while moving from one network to another
- Handoff speed is relative to many factors
- Application and user should be unaware of all these.
-
- Ubiquitous IP: capability to be always IP connected to both IP versions, on any link access, so applications are always working and unaware of mobility.

Challenge

- Commonality:
  - Applications/IP starts at the end node.
    - IPv6 has to reach all end nodes involved for an application.
  - Reachability of end nodes
    - Network management
    - « server » nodes
- In order to bring these benefits TODAY, all nodes should have:
  - IPv6-enabled applications
  - IPv6-enabled IP stack/operating system
  - IPv6 connectivity
- Requirements of these previous applications:
  - Stability of IPv6 address
  - Management

IPv6 Deployment Blocks

Applications



Operating System

X Network

Only when all blocks are IPv6 ready, one can use IPv6 services.
=> Planning and scheduling are key.

Routers, servers, VPN, Firewall, etc...

Application and OS: How to Deploy

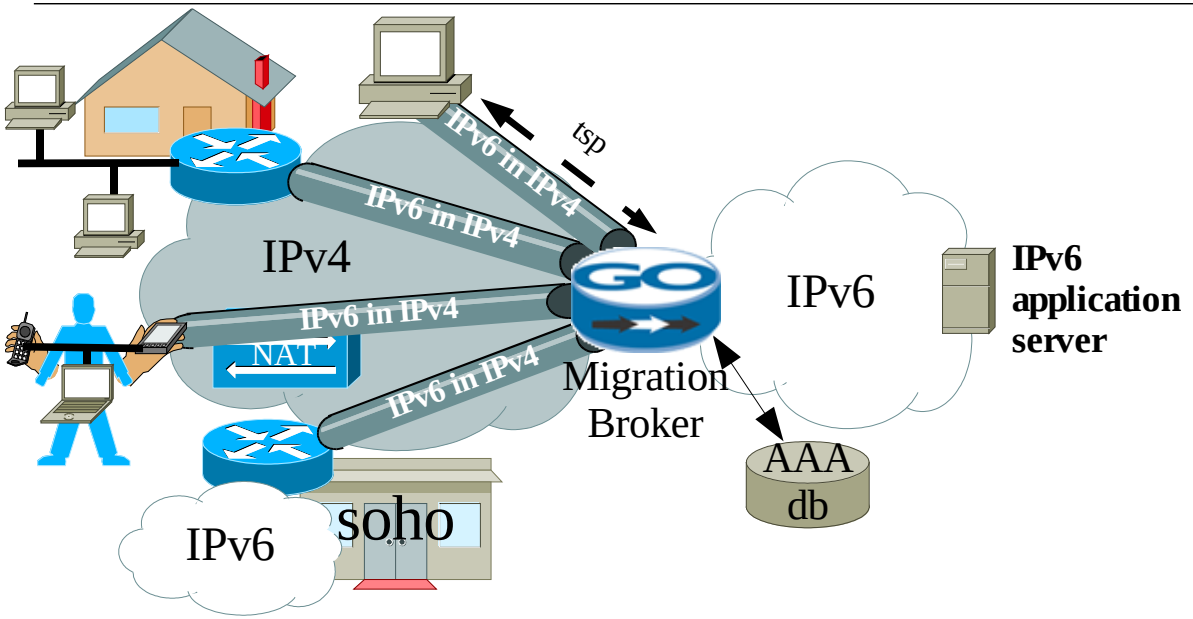
- Application:
  - If you have access to source code, then modifications are « straightforward ».
    - Quake porting to IPv6: 350K C source code, 1 file for networking, 2 days including setup and test.
    - Dependency on the OS.
  - If you don't have access to source code, then ask the vendor.
- Operating System (OS):
  - IP stack is part of the OS.
  - Most current OS are IPv6 ready.
  - Upgrade path needed for older OS.
- Usual case:
  - « slow » conversion to IPv6
  - Incremental conversion and deployment
  - Project by project, application by application, ...

How to deploy

- Delivering IPv6 connectivity:
  - Upgrade everything
  - Deploy incrementally:

Per host/per application:
One host-application at a time, as needed.
Have some IPv6 native backbone to aggregate traffic, deploy addressing, etc..
IPv6 access through the IPv4 network
Use transition technique (TSP tunnel broker) to give IPv6 connectivity to the « far » hosts
In an efficient network-wise way
TB: while providing controlled and managed deployment.
TB: security, AAA, IPv6 address delegation are key
Low upfront costs while providing early service

TSP Tunnel Broker



- TSP Tunnel Broker has:
  - Tunnel Setup Protocol: signaling protocol for establishing the tunne
  - TSP client on host or home gateway
  - TSP tunnel broker:
    - establish the tunnel end point
    - NAT traversal
    - Prefix delegation
    - AAA

TSP Tunnel Broker

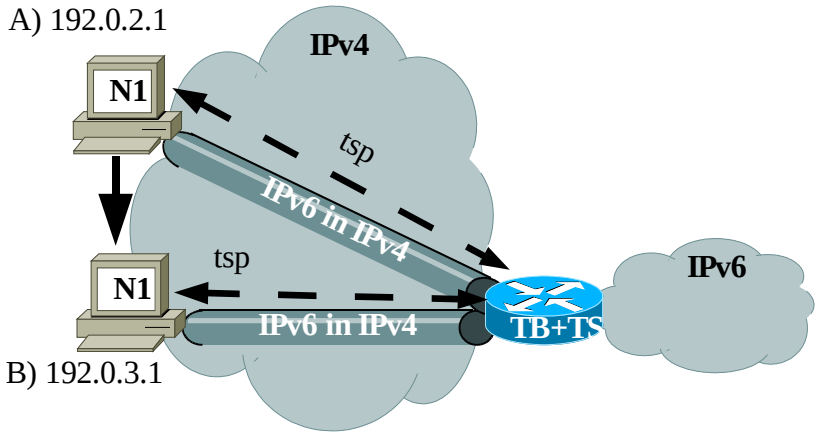
- TSP: Tunnel Setup Protocol
- Control channel
  - To negociate and establish the tunnel
- between
  - a TSP client
    - who needs IP connectivity
      - such as IPv6 when only IPv4 is available
  - And a TSP tunnel broker,
    - behaving as an IPv6 network access server
    - offering IPv6 in IPv4 tunnels
    - detecting NATs and providing tunnels over NAT
    - offering network prefixes to networks (such as home, personal, org)
    - authenticating, authorizing and accounting users and traffic
- TSP client:
  - Lightweight (small footprint for embedded such as mobile phone, PDA, sensors, home gateways)
  - On a user PC, acts as a driver: i.e. Automatic, no user intervention.

TSP Capabilities

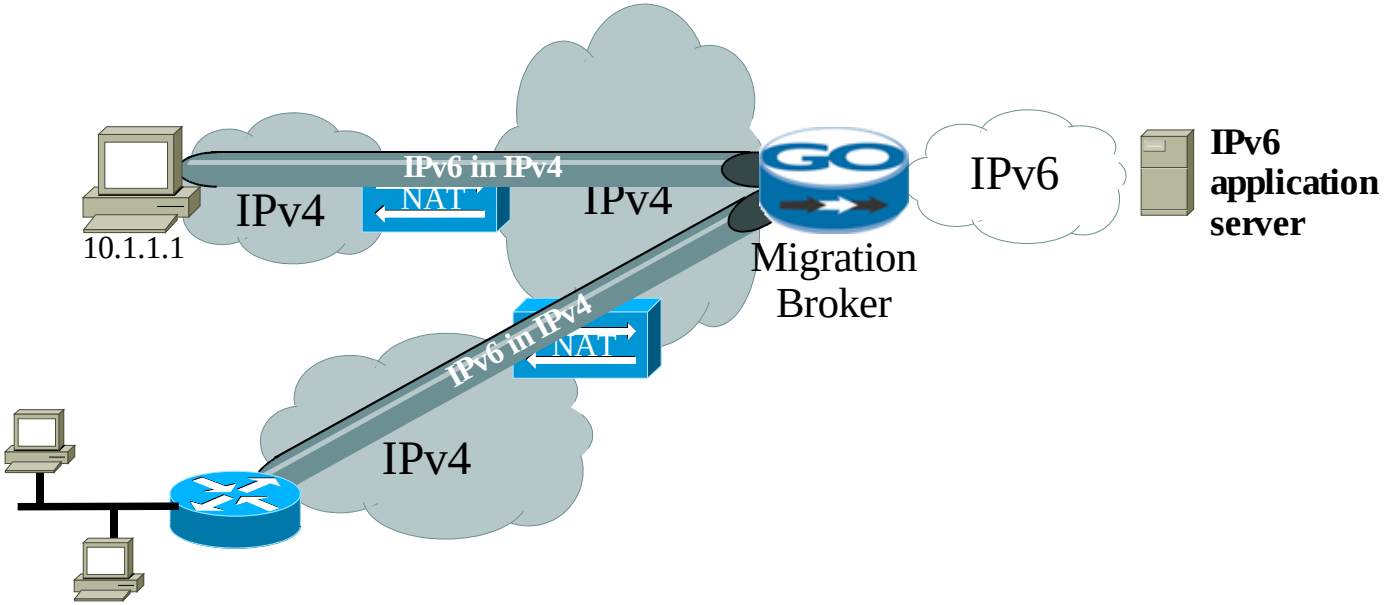
- Tunnel types:
  - IPv6 in IPv4
  - IPv6 in UDP-IPv4 (a NAT is in the path)
  - IPv4 in IPv6
- Permanent or temporary IPv6 address
- Prefix delegation
- IPv4 Mobility/change of address detection
- Mobile networks
- DNS automated registration
  - tunnel end-point name (AAAA record)
  - Inverse tree delegation for assigned prefix (NS record)
- Keepalive/Heartbeat

TSP moving node

- When changing IPv4 address, TSP re-establish automatically the IPv6 tunnel



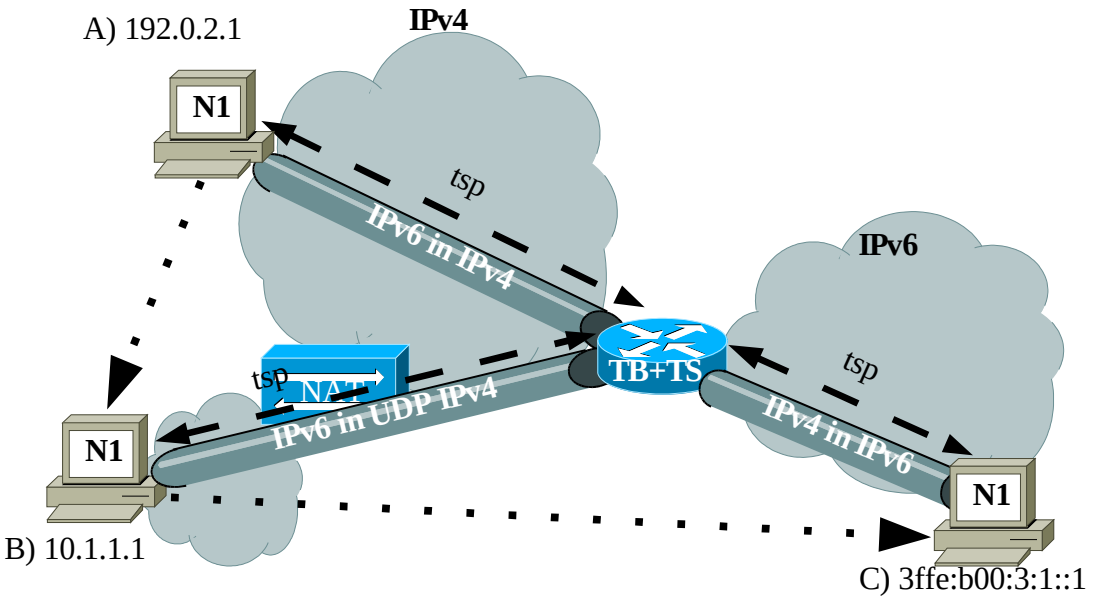
Connecting IPv6 over NAT



- Migration Broker connects:
  - IPv6 nodes and networks
  - located behind a NAT
  - enabling applications to be deployed, otherwise impossible with NAT

TSP: Ubiquitous IP

- Also enables IPv4 in IPv6 tunnels
- Mobile node/network with:
  - IPv4 with reachable address
  - IPv4 behind a NAT
  - IPv6 network
- TSP tunnel broker provides both IP protocols in all cases.



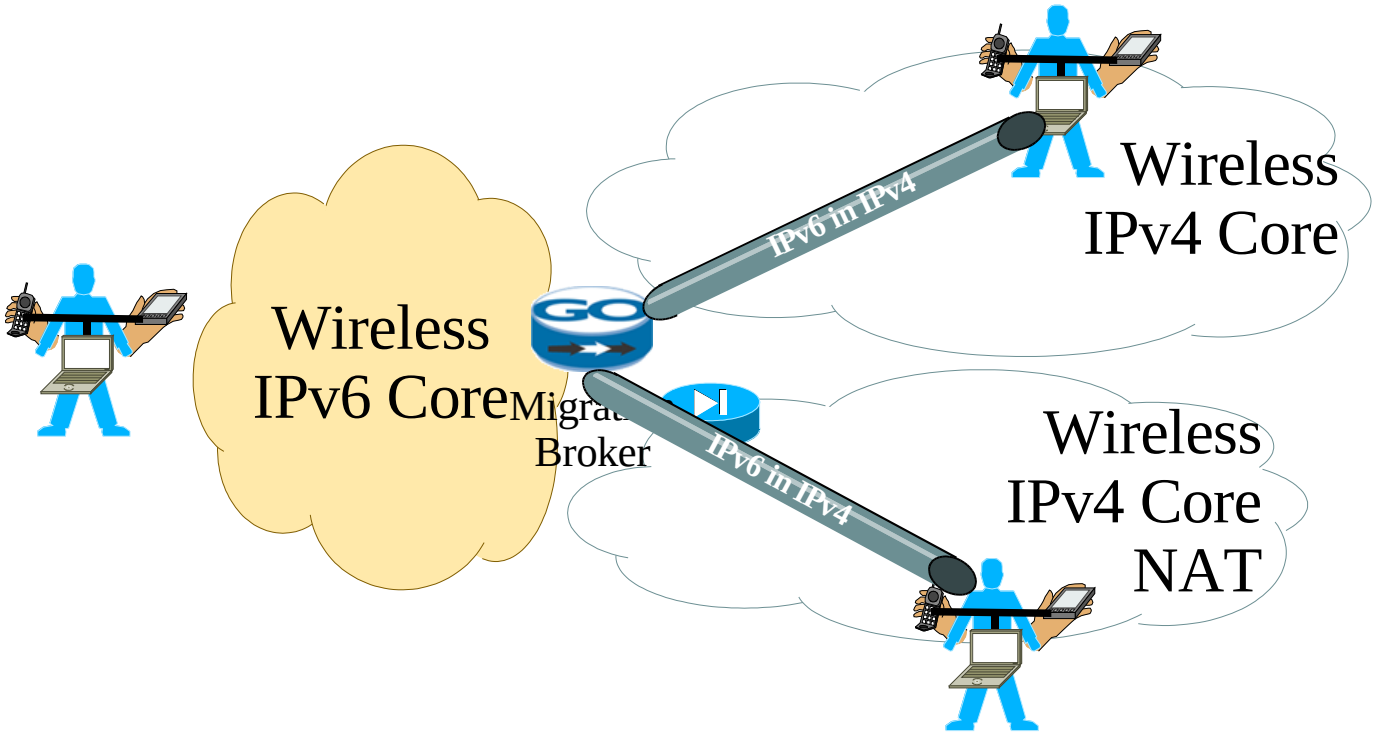
Case Studies

- Examples of customers:
  - Wireless provider
    - Mix of IPv4, IPv4 with private address space (NAT) and IPv6 networks
    - Need a transition tool handling all cases: Ubiquitous IP.
    - Example of application: mobile videoconferencing
  - Broadband provider
    - IPv6 E2E applications deployment to the home
    - Network management and support of home premises
  -

Wireless Provider

- Need:
  - Mobility application.
  - Using MobileIPv6
  - Connecting networks for the mobile node are:
    - IPv4-only with global address
    - IPv4-only with private address
    - IPv6
  - Goal: Ubiquitous IP
- Solution:
  - IPv6 in IPv4 tunnels with NAT traversal, with AAA.
  - Hexago Migration Broker
  - TSP client in mobile node.

Wireless Provider Network

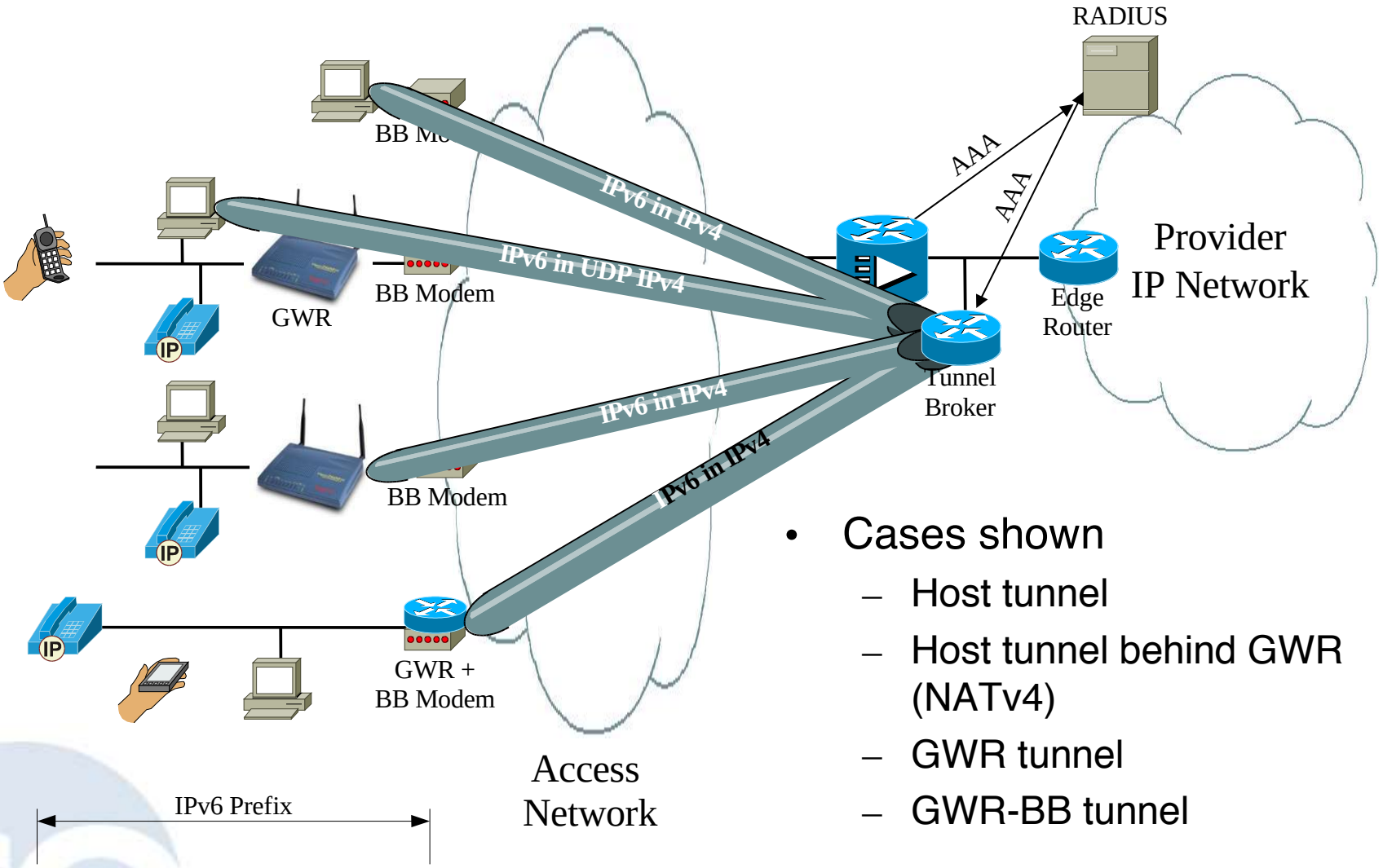


- Provides ubiquitous IP for the application.
- Mobile videoconferencing kept running even after multiple handovers with different kinds of IP access.

Broadband Provider

- Need:
  - IPv6 application to deploy to home networks.
  - Support issues and reachability to end nodes are very important.
  - IPv4 networks
- Solution:
  - IPv6 in IPv4 tunnels with NAT traversal
  - AAA with permanent addressing for users.
  - Prefix delegation
  - Hexago Migration Broker
  - TSP client in either home gateway or in end node.

Broadband with TSP Tunnel Broker

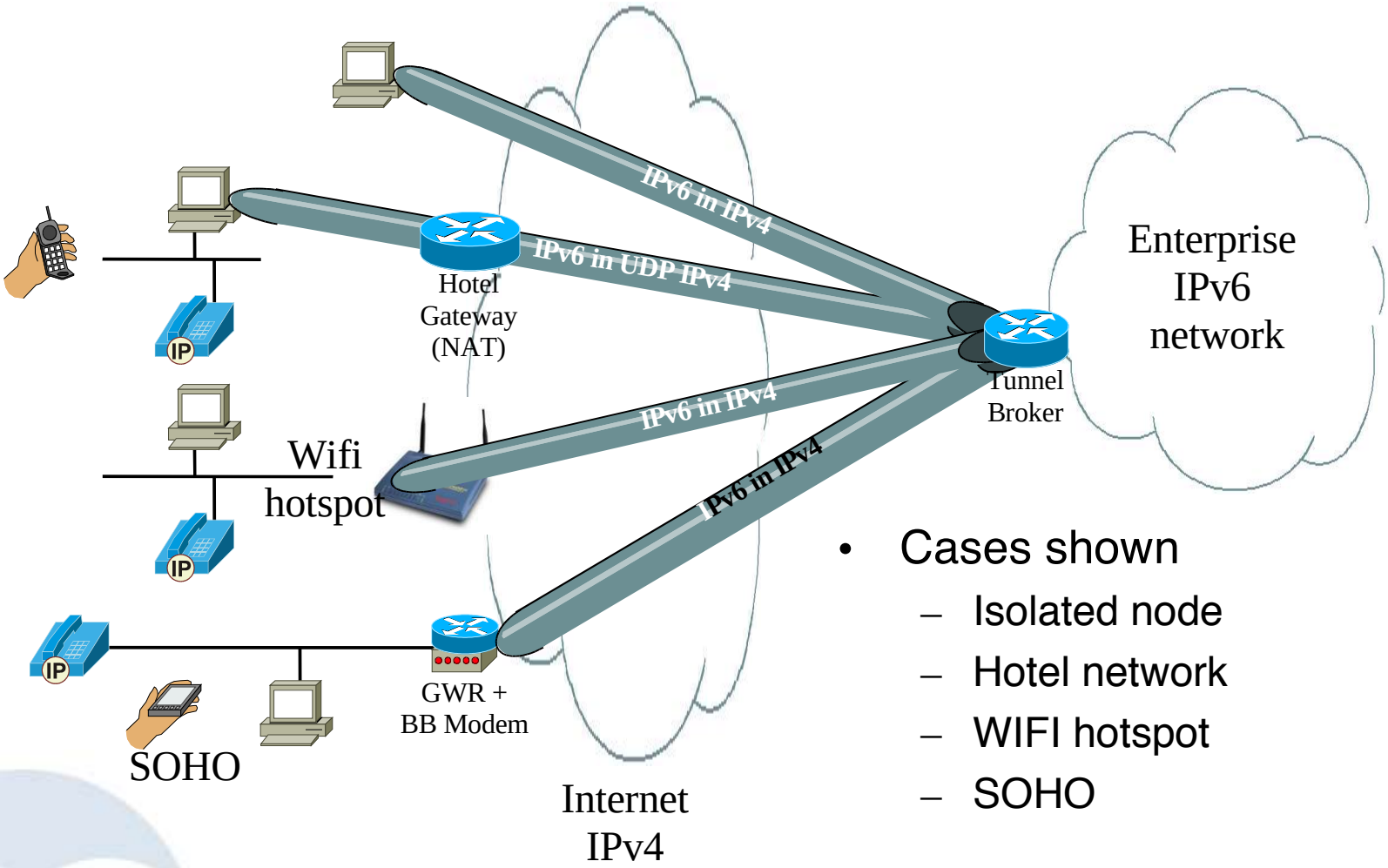


- Cases shown
  - Host tunnel
  - Host tunnel behind GWR (NATv4)
  - GWR tunnel
  - GWR-BB tunnel

Enterprise Remote Access

- Enterprise has:
  - An IPv6 network
  - Employees: travelling, remote offices, soho, mobile.
- Needs a way for employees to access the enterprise IPv6 network (VPN-like scenario)
  - NAT are used in all access networks (wifi hotspots, hotel networks, etc...)
- TSP tunnel broker:
  - NAT traversal
  - AAA for user authentication
  - Prefix delegation if mobile/home network
  - Mobility

Enterprise Remote Access Scenario



- Cases shown
  - Isolated node
  - Hotel network
  - WIFI hotspot
  - SOHO

Conclusion

- IPv6 solves today issues
- Multiple link and IP versions requires ubiquitous IP
- Deployment blocks: application, OS, network.
- Incremental deployment enables low upfront cost and early service availability.
- TSP Tunnel Broker is a technology for incremental deployment and ubiquitous IP.
- Customer case studies

References

- Hexago: http://www.hexago.com
- IPv6 Tunnel Broker: RFC 3053
-
- North American IPv6 Task Force: http://www.nav6tf.org
- IPv6Forum: http://www.ipv6forum.com
- Moonv6: http://www.moonv6.org
-

Hexago

- Founded after 6 years of R&D in IPv6, spinoff of Viagénie.
- IPv6 deployment solutions company
- Flagship product: Migration Broker
  - Responding to customer needs
  - Implements the TSP tunnel broker
  - Manage thousands of IPv6 in IPv4 tunnels
  - NAT-Traversal with automatic discovery
  - AAA
  - Secure and managed IPv6 deployment
  - Industry standard CLI. Easy to configure.
  - Low-cost and fast deployment of IPv6
  - IPv4 in IPv6 tunnelling for IPv6-only backbones
- Involved in IETF, IPv6Forum, North American V6 Task force
- Customers: Providers, Enterprise, Military, R&E. Worldwide.
- http://www.freenet6.net. Free IPv6 service using the Migration Broker. Available since Jan 1999!