IPv6 Migration Issues

Nalini Elkins

Inside Products, Inc.

Inside Products, Inc.
(831) 659-8360
www.insidethestack.com
sales@insidethestack.com

Agenda

- IPv6 planning and migration has lagged at Fortune 500 companies. Yet at some, labs are being set up, address planning and security issues are being explored. How did they do it?
- What are the issues when your organization is one of the pillars of our economic system? Conversion on this scale requires the concerted change of many moving parts. You may liken it to the conversion of one currency system to another!
- Today we will discuss potential strategies and the decisions which need to be made based on work with Fortune 500 companies in the financial and health care sectors.

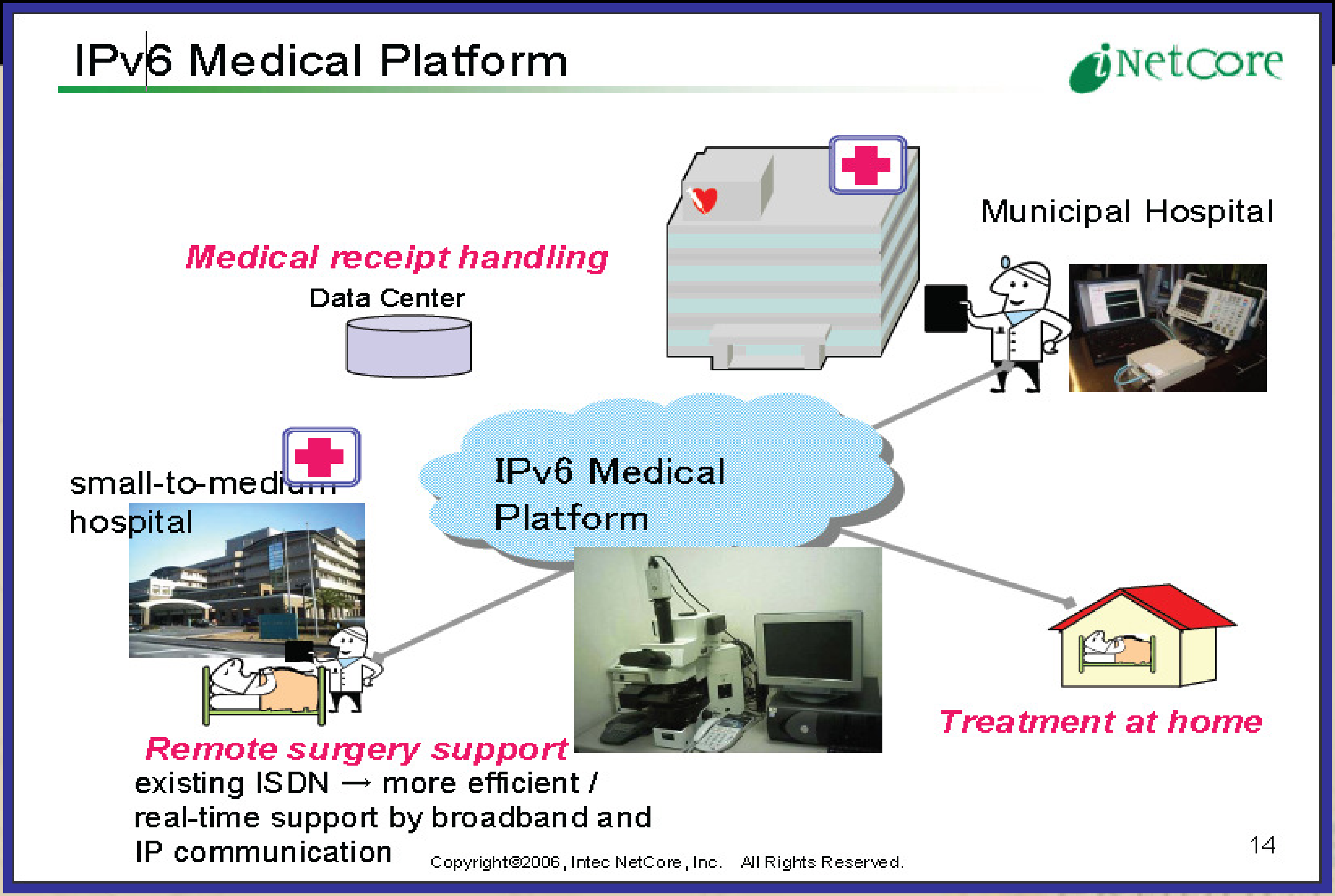
How to Start a Migration Project

- Technical people see the need, management does not. How do we even get a project started?

- Sell based on future needs:
  - Mobility,
  - Sensors,
  - Remaining competitive

- Sell based on possible government mandate
- Sell based on fear – being caught blindsided

Why IPv6?



IPv6 Medical Platform

iNetCore

Municipal Hospital

Medical receipt handling

Data Center

small-to-medium hospital

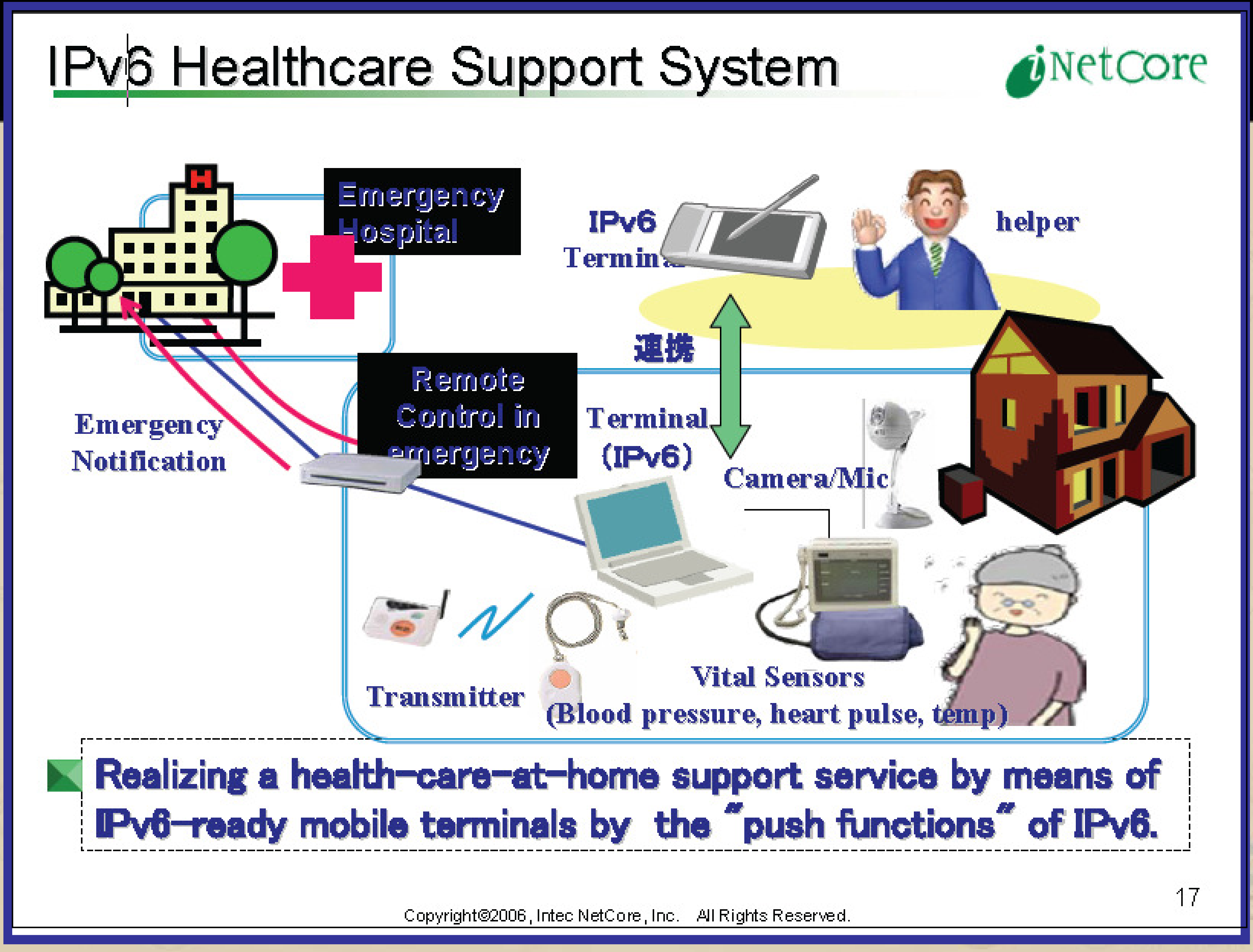
IPv6 Medical Platform

Treatment at home

Remote surgery support

existing ISDN → more efficient / real-time support by broadband and IP communication

And More…

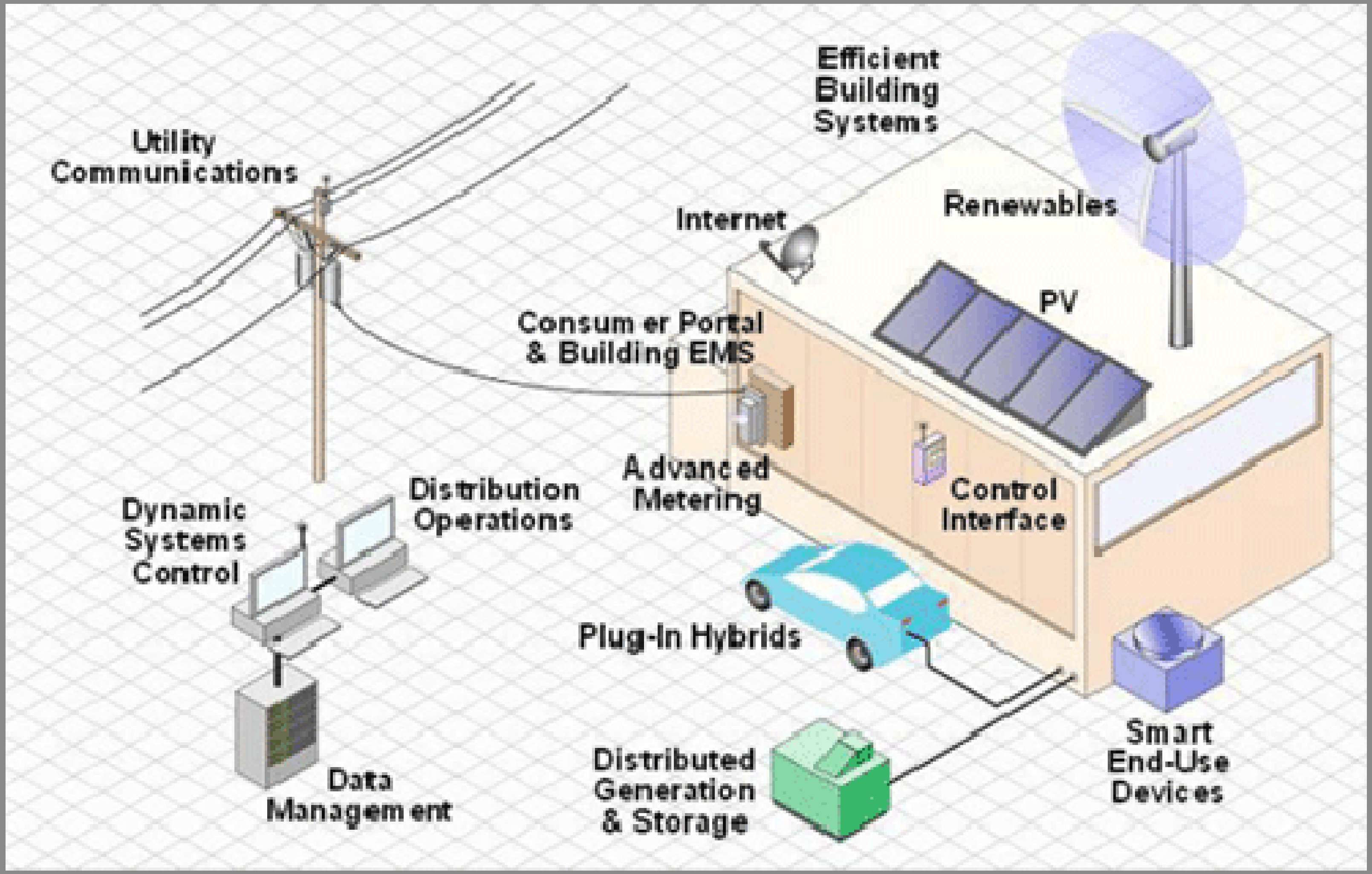


IPv6 Healthcare Support System

iNetCore

- Realizing a health-care-at-home support service by means of IPv6-ready mobile terminals by the “push functions” of IPv6.

Smart Grid


Efficient Building Systems
Utility Communications
Renewables
Internet
PV
Consum er Portal & Building EMS
Advanced Metering
Control Interface
Distribution Operations
Dynamic Systems Control
Plug-In Hybrids
Smart End-Use Devic es
Distributed Generation & Storage
Data Managem ent

Oh, oh. They Bought It.

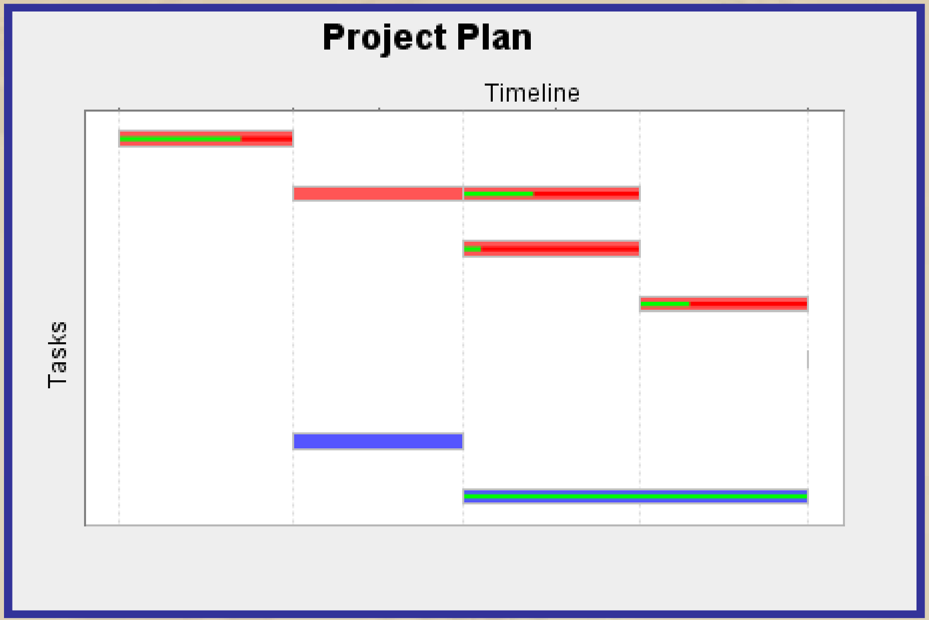
- OK, you have approval to proceed. Now what?
- Huge ship. Turning radius is very large

- Many groups need to be involved (security, applications, network hardware, systems, operations, help desk, vendors.)
- Lights out data centers / automated operations
- Team approach is imperative.

What is this team going to do?

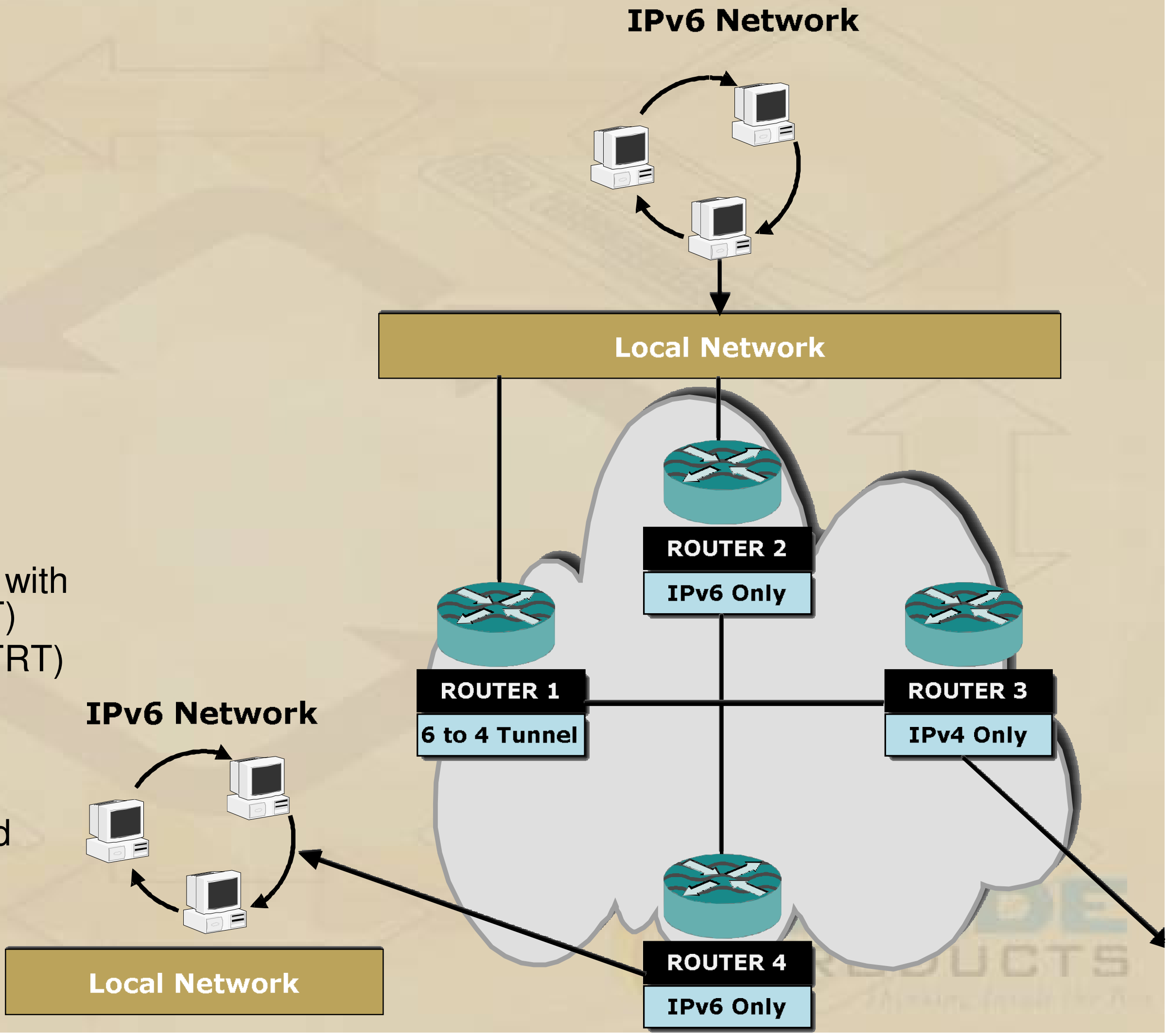
- A roadmap for implementation.
- Timelines and schedules.

- Tasks to be done
  - IPv6 Address Allocation
  - IPv6 Addressing Plan
  - Impact on IPv4 Communications
  - Impact on Applications
  - Types of IPv4/IPv6 Communications
  - Impact on SLAs
  - IPv6 Security
  - Network Services Supported (DNS, DHCP)
  - Campus Networks
  - New IPv6 Capabilities (e.g., mobility, sensors)



Develop Strategy

- How do we actually migrate?
  - Dual stack?
  - Tunneling?
  - Proxies?
  - Translation?
- Direct connection – 6 to 6
- Tunneling
  - 6 to 4 tunnels
  - Teredo
  - Automatic tunnels (ISATAP)
  - Manual
  - GRE (with IPSec)
- Translation
  - Network Address Translation with Protocol Translation (NAT-PT)
  - Transport Relay Translator (TRT)
  - Bump in the Stack (BIS)
  - Bump in the API (BIA)
- Many, many choices.
- Need to develop some policies and standards.



Set Up a Lab!

- Now, that the rubber meets the road, we see that we need some real world experience.
- Classes just won’t do.
- Without hands-on experience, we just won’t know what we are doing.
- We need to have a lab!

Sample Strategy

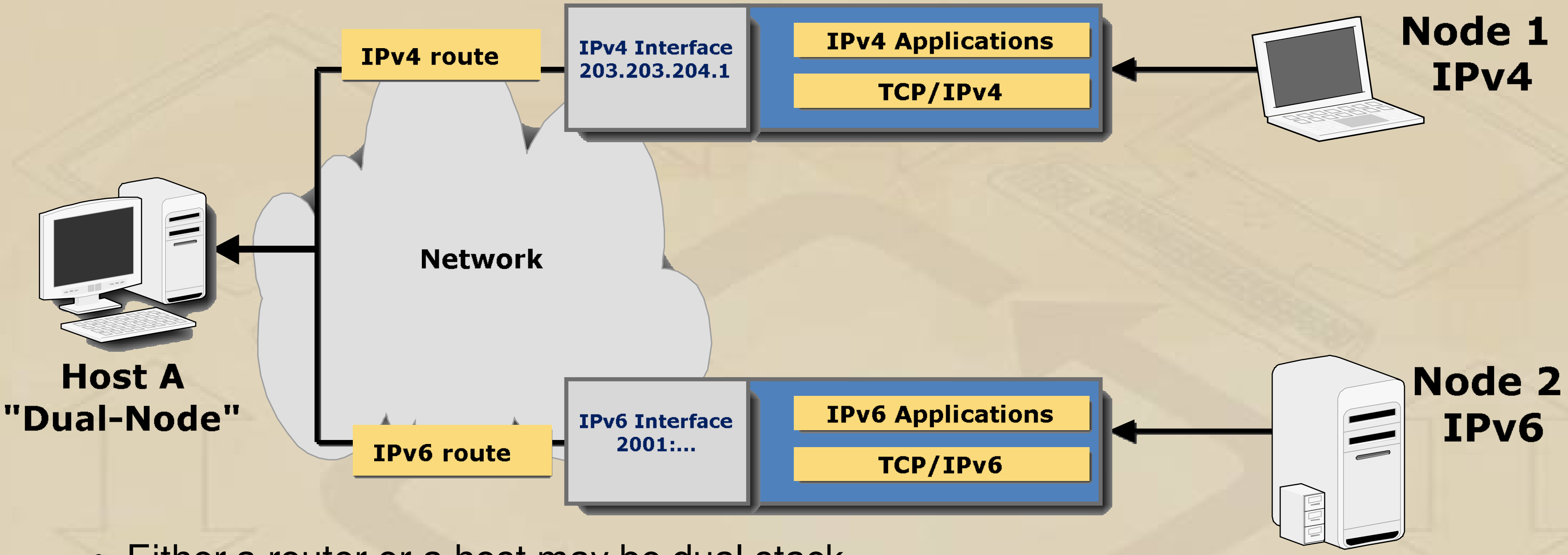
- First, let’s assume that we can’t convert the entire network to IPv6 in one shot – so then, dual stack mode and tunneling must be used. How do these work?

- Let’s examine two potential scenarios for the architecture:
  - Option 1: Backbone becomes IPv6
  - Option 2: Regions, connections or tributaries convert to IPv6 or external government agency or business partner wants IPv6 access. Core backbone remains IPv4.

Architecture under IPv6
Option 1: Backbone Converted

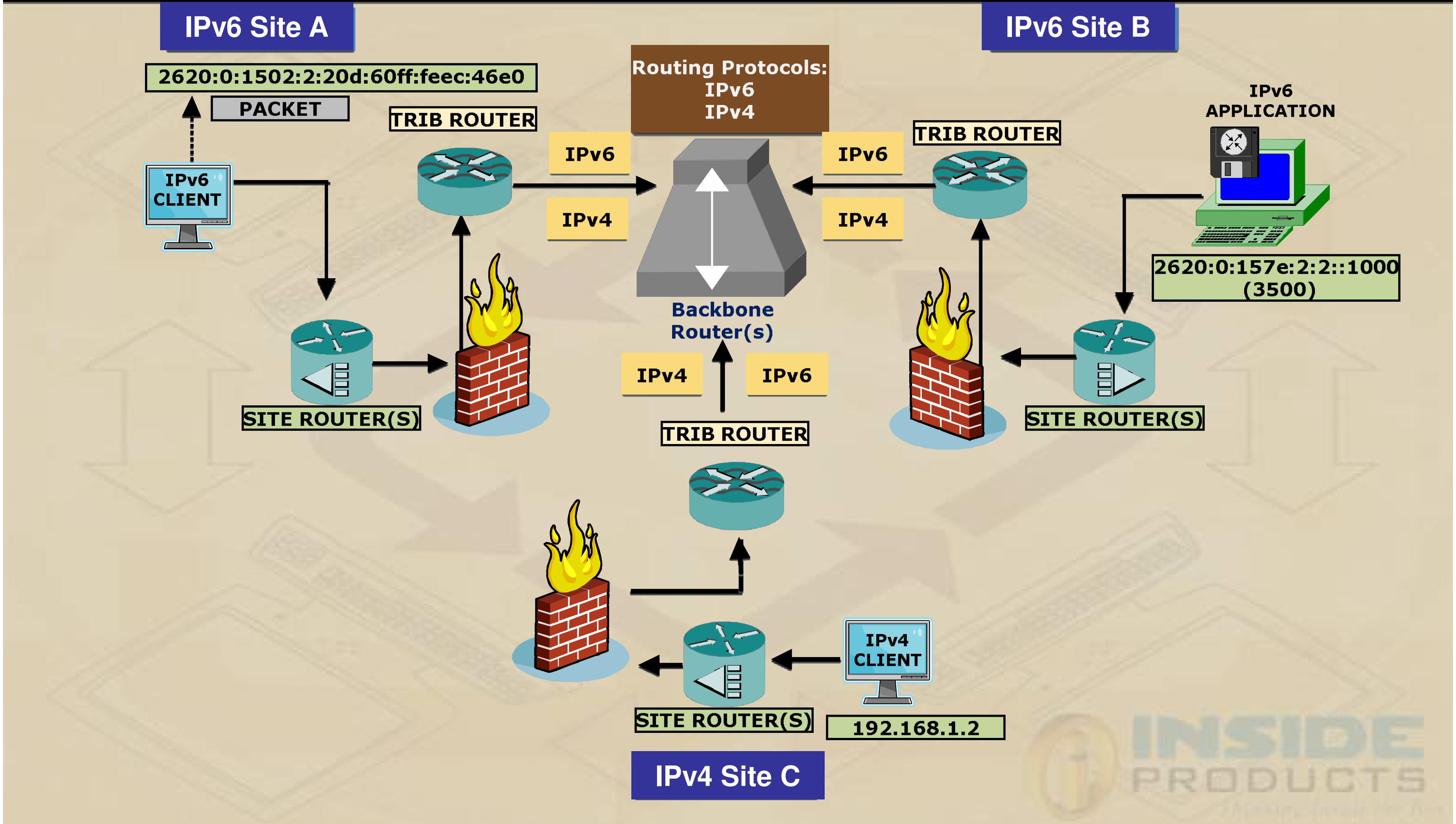
- In this option, the core backbone is converted to dual stack (IPv4 and IPv6) and the servers and tributaries remain at IPv4.
- As each server or region converts to IPv6, their packets can travel natively via IPv6.
- The backbone routers will have both IPv4 and IPv6 routes.
- The IPv6 packet will go across the backbone as IPv6.
- The IPv4 packet will be sent as IPv4.

Dual Stack Mode



- Either a router or a host may be dual stack.
- A dual stack node can run both an IPv4 and IPv6 TCP/IP stack.
- This can be useful during the transition period as not all applications may be converted to IPv6.
- Such nodes can send and receive both IPv4 and IPv6 packets. This is a very common implementation and will be the first step for most, if not all, devices migrating to IPv6.

Dual Stack Backbone



IPv6 Site A

2620:0:1502:2:20d:60ff:feec:46e0

PACKET

IPv6 CLIENT

TRIB ROUTER

SITE ROUTER(S)

Routing Protocols:
IPv6
IPv4

IPv6

IPv4

IPv6

IPv4

Backbone Router(s)

IPv4

IPv6

TRIB ROUTER

IPv6 Site B

TRIB ROUTER

IPv6 APPLICATION

2620:0:157e:2:2::1000 (3500)

SITE ROUTER(S)

IPv4 CLIENT

SITE ROUTER(S)

192.168.1.2

IPv4 Site C

Option 1: Backbone Converted to IPv6: Pros

- Conversion to IPv6 has begun. This approach could provide a starting point for IPv6. This method ‘should’ be transparent to the end users.
- No applications need to be converted. This approach is network only. The applications remain untouched. It is likely that application conversion will be one of the most difficult and time-consuming areas.
- Fewer pieces of equipment need to be converted. In this approach, only the backbone or core routers need to be converted.
- Network operations and systems support groups will gain experience with IPv6. One of the biggest hurdles to the IPv6 migration is the knowledge of the new IPv6 protocols.

Option 1: Backbone Converted to IPv6: Cons

- As with any migration, there are risks involved. The risks may be described as follows:

- **If there is a problem, many users may be affected.**

  A phased approach to migrate a few users at a time may be a good idea. With adequate testing, many flaws should be uncovered before implementation. Still, as each group of clients is added, there may be configuration issues.

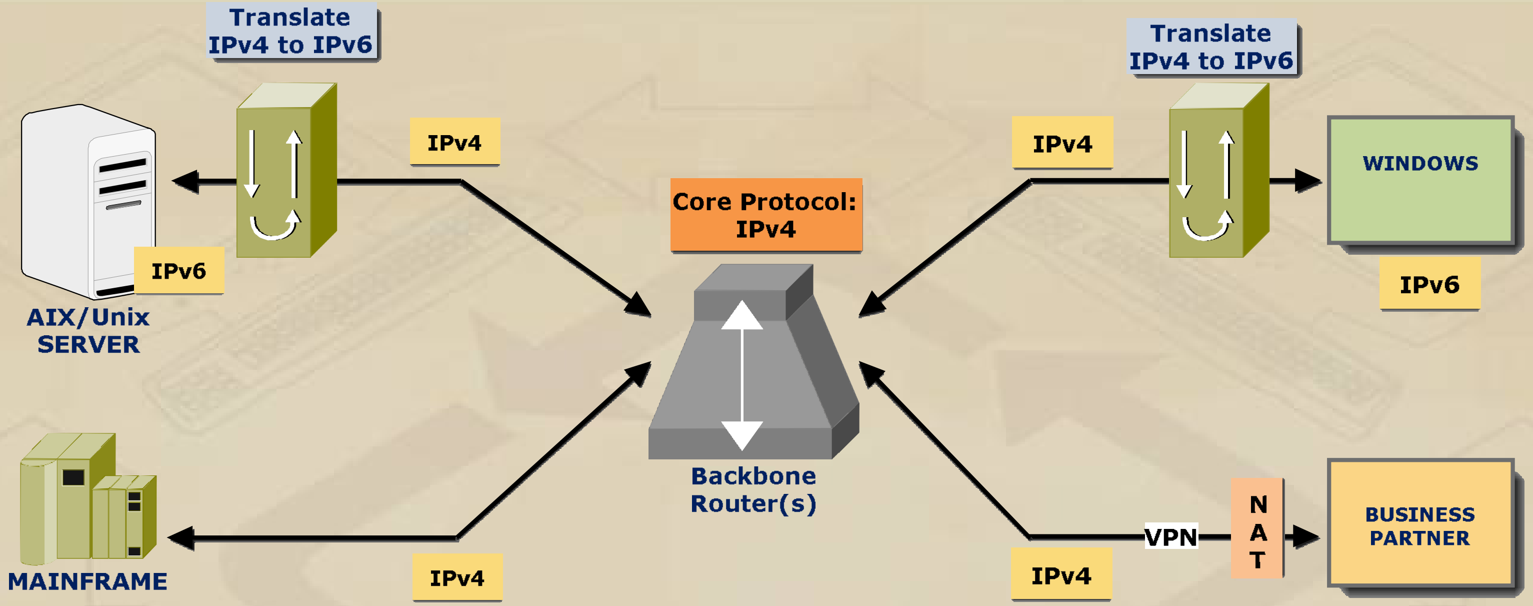
- **What happens if the path or route fails?**

  As in IPv4, routing should recover from failures. But, the IPv6 routing protocols have not been tested as thoroughly as the IPv4 routing protocols. It is unclear how quickly convergence will occur, if routing loops will be created or if the routing tables will fail to be properly managed.

- **It may take longer for the transactions to complete.**

  Extra overhead is imposed on the routers and backbone links because of multiple IPv4 and IPv6 routes. The routers doing the conversion may become bottlenecks.

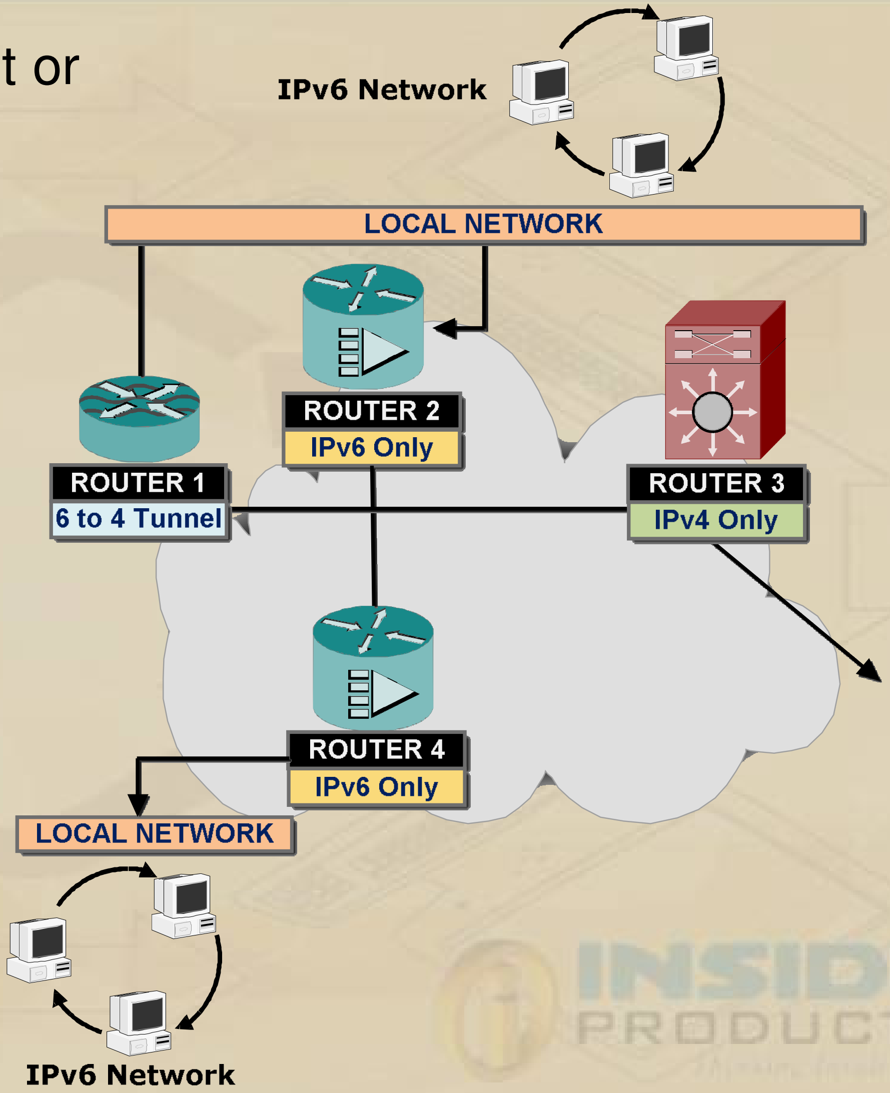
Option 2: Boundary Converts to IPv6



- In this option, the core remains at IPv4.
- In this scenario, an application at a remote server or government agency must be accessed via IPv6.
- Or IPv6 ACLs are wanted to provide a security function not provided by IPv4 ACLs.
- Network only access via IPv6 does not seem reasonable.
- A tunnel or translation gateway must be provided. The options include: static tunnels, 6to4 dynamic tunnels, GRE tunnels or IPv6 proxies.
- The remote routers will perform conversion of packets from IPv6 to IPv4. The IPv4 packet will go across the network and be converted to IPv6 at the receiving end.

Boundary Connectivity

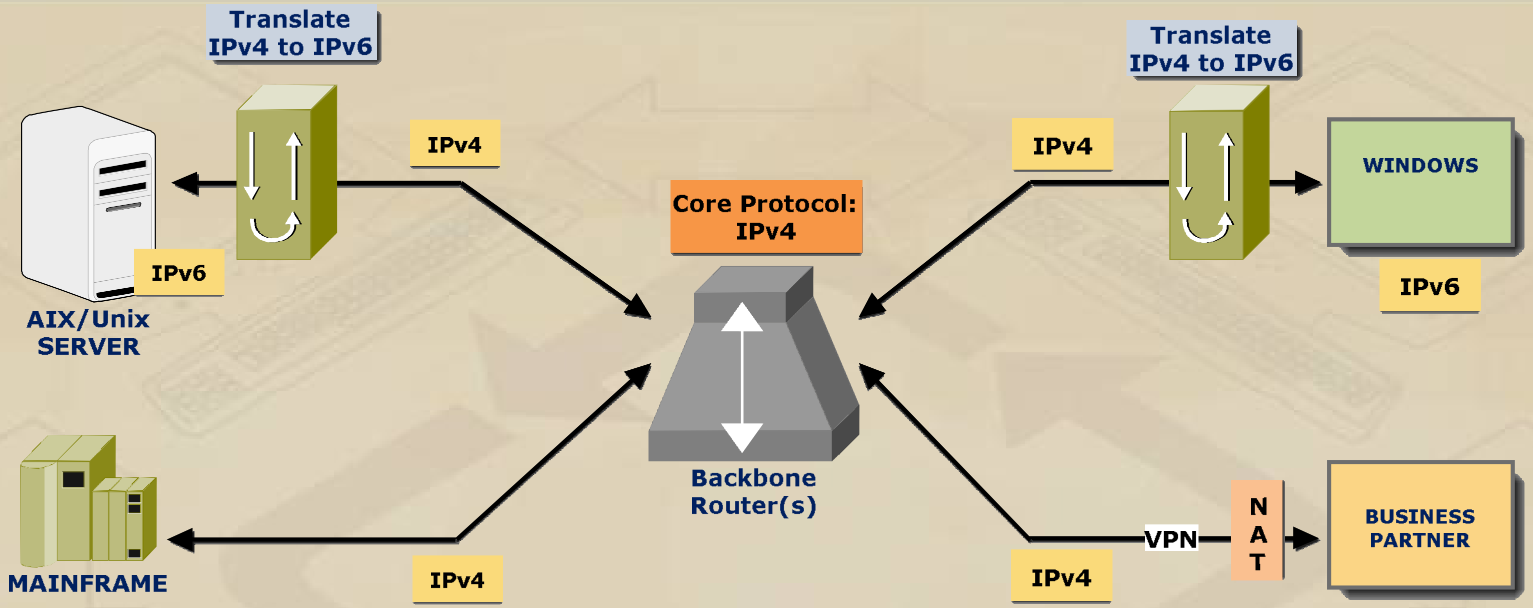
- How do we get out to the internet or over the IPv4 network?
- Direct connection – 6 to 6
- Tunneling
  - 6 to 4 tunnels
  - Teredo
  - Automatic tunnels
  - Pseudo tunneling interface
  - GRE
- Translation – NAT-PT
- Proxies



Option 2: Boundary Converts to IPv6

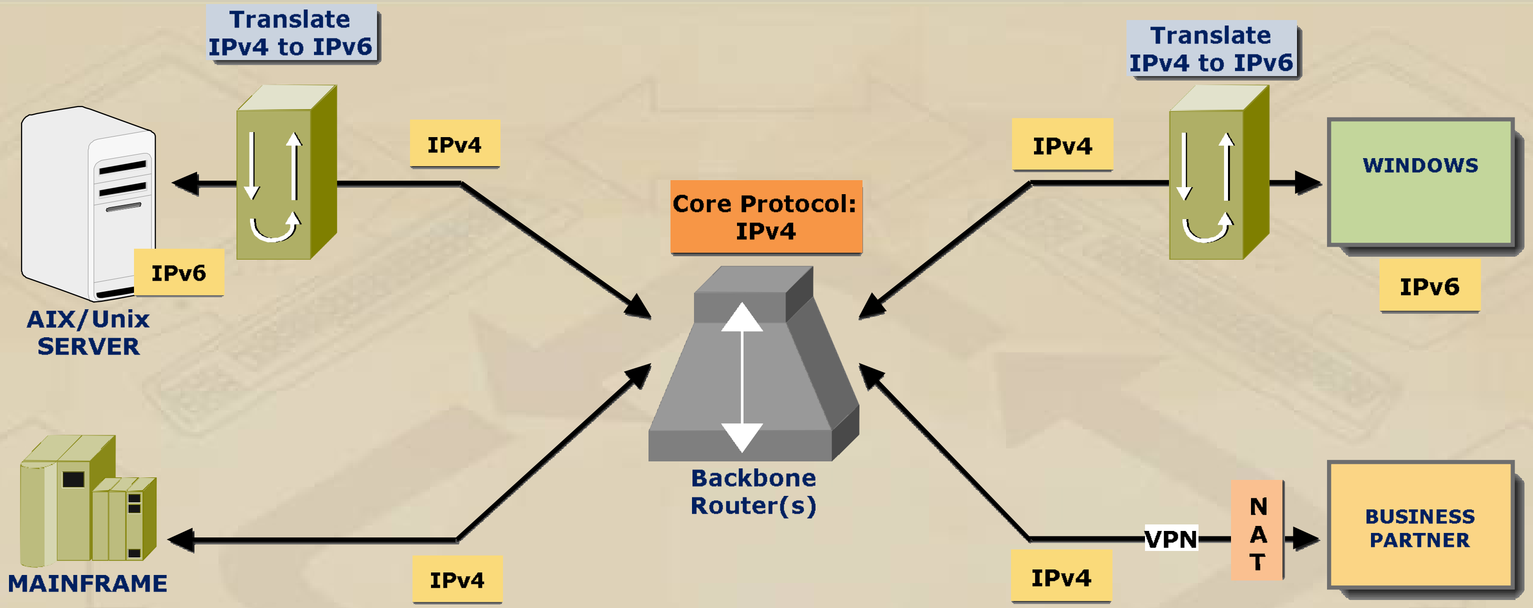
- What this means is that all backbone routers remain at IPv4 and routing is done via IPv4.
- All routers at the remote sites connect to the backbone routers with IPv4.
- The backbone routers will advertise IPv4 routes.
- Any region or remote site which wishes to use IPv6 will do so by tunneling or a translation gateway at the router at the remote site.
- Any such router needs to be upgraded to be dual stack and configured to do tunneling or translation.
- Policies for a standard method for tunneling, translation and ACLs should be put in place.

Option 2: Boundary Converts to IPv6: Pros



- Conversion to IPv6 has begun. This approach could provide a starting point for IPv6.
- If only a few applications are done initially, then hopefully there should not be many problems.
- Fewer pieces of equipment need to be converted – initially. In this approach, only some remote routers need to be converted. The routers at the backbone can remain untouched. As many regions convert, this 'Pro' will change to a 'Con' because many routers will need to be converted.
- Network support staff will gain experience with IPv6. One of the biggest hurdles to the IPv6 migration is the knowledge of the new IPv6 protocols.

Option 2: Boundary Converts to IPv6: Pros



- Routing is less complex. The routing in the backbone will be more straightforward. IPv4 routes will be used throughout the network. No consideration is needed of whether to route via IPv4 or IPv6
- No change to backbone routers. They will carry only tunneled traffic. The load on the backbone routers should be less also because they do not need to be responsible for creating tunnels.
- DNS can remain IPv4.

Option 2: Boundary Converted to IPv6: Cons

- **Scalability of tunneling**

  Scalability of tunneling with a lot of traffic is an issue. If many applications and many remote sites start doing tunnels, then overhead will be added to both network traffic and the routers due to tunneling. Tunneling adds at least 20 bytes to each packet.

- **Many pieces of equipment need to be converted**

  As time goes on and as many remote sites convert, many routers will need to be converted.

- **Network Support is blindsided**

  Actually, a remote site could tunnel IPv6 traffic within IPv4 packets today.   Often, network operations and the firewalls do not detect this.

- **Security problems**

  Firewalls at the remote / central sites may not be able to block packets appropriately or may inappropriately block packets which have embedded protocols.

Summary

- We have examined two potential scenarios for the architecture:
  - Option 1: Backbone becomes IPv6
  - Option 2: Regions, connections or tributaries convert to IPv6 or external government agency or business partner wants IPv6 access. Core backbone remains IPv4.

- Next step is to examine what has to be done to convert the following:
  - Routers
  - Plan connections
  - Applications
  - Addressing
  - DNS / DHCP
  - Security and IDS / IPS
  - Firewalls
  - Network Management Tools

IPv6 Business Information Exchange

www.insidethestack.com/ipv6businessinfo.html

Free service provided by Inside Products

- The goal is to facilitate exchange of technical information about IPv6 that is needed to actually implement IPv6 in large corporate networks. If there are facilities that are not yet provided by the IPv6 protocol and we see a need for such facilities, we may approach the IETF or other bodies for clarification or enhancements.

- Meetings will be held quarterly.