



# IPv6 Integration in Federal Government



**Adopting a Phased Approach for Seamless Integration  
and Maximum ROI**

# Preparing for IPv6 integration

## Questions to ask before you begin

- Should we attempt to fully transition to IPv6 all at once, or integrate in phases?
- What is the best approach to ensure applications can co-exist on IPv4 and IPv6?
- How can we take advantage of new IPv6 features, such as peer-to-peer communications and auto-configuration?
- How can we ensure security for both IPv4 and IPv6 during the transition?



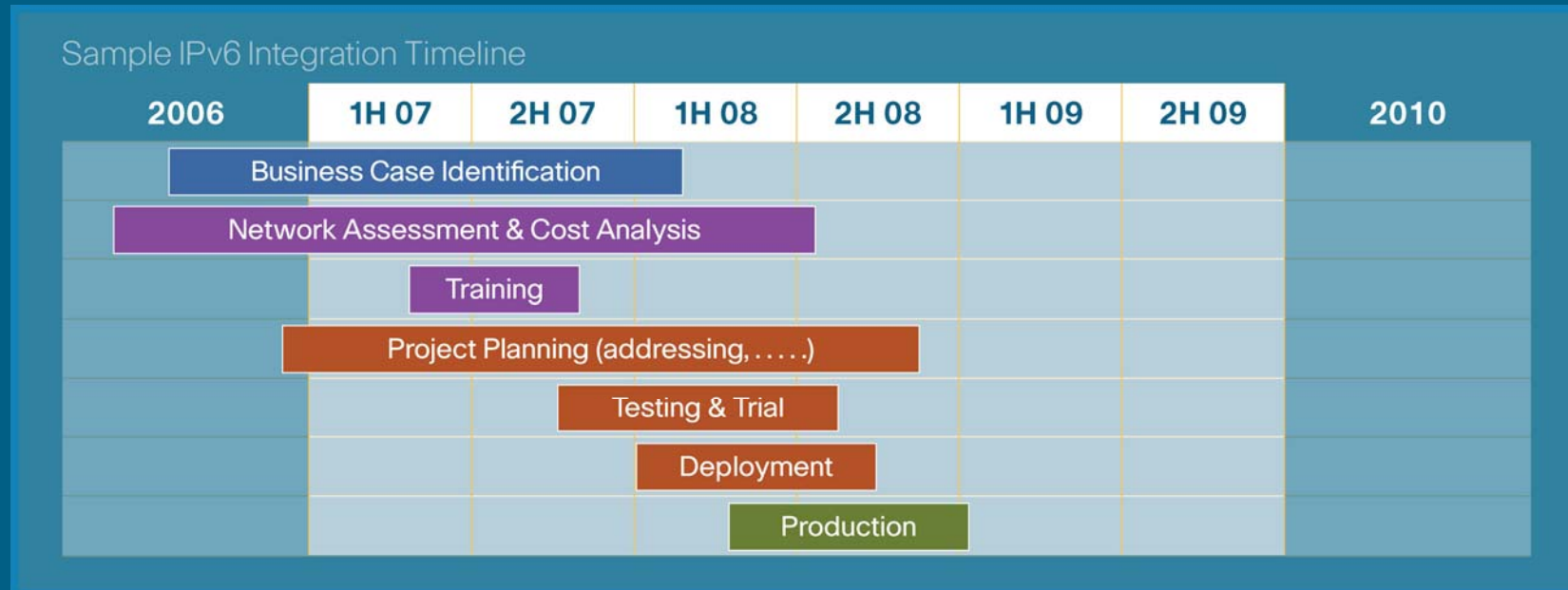
# A phased approach to IPv6 success

## 4 steps to a smooth implementation

- Test the IPv6 integration in network infrastructure and applications in a lab environment
- Conduct a pilot production deployment for one or more campus LAN segments, or the WAN
- Expand the geographic reach of IPv6 by deploying it more broadly in the LAN/WAN environment and using it for Internet connectivity
- Adopt new applications, such as peer-to-peer communications and autodiscovery, that can enhance government applications and services.

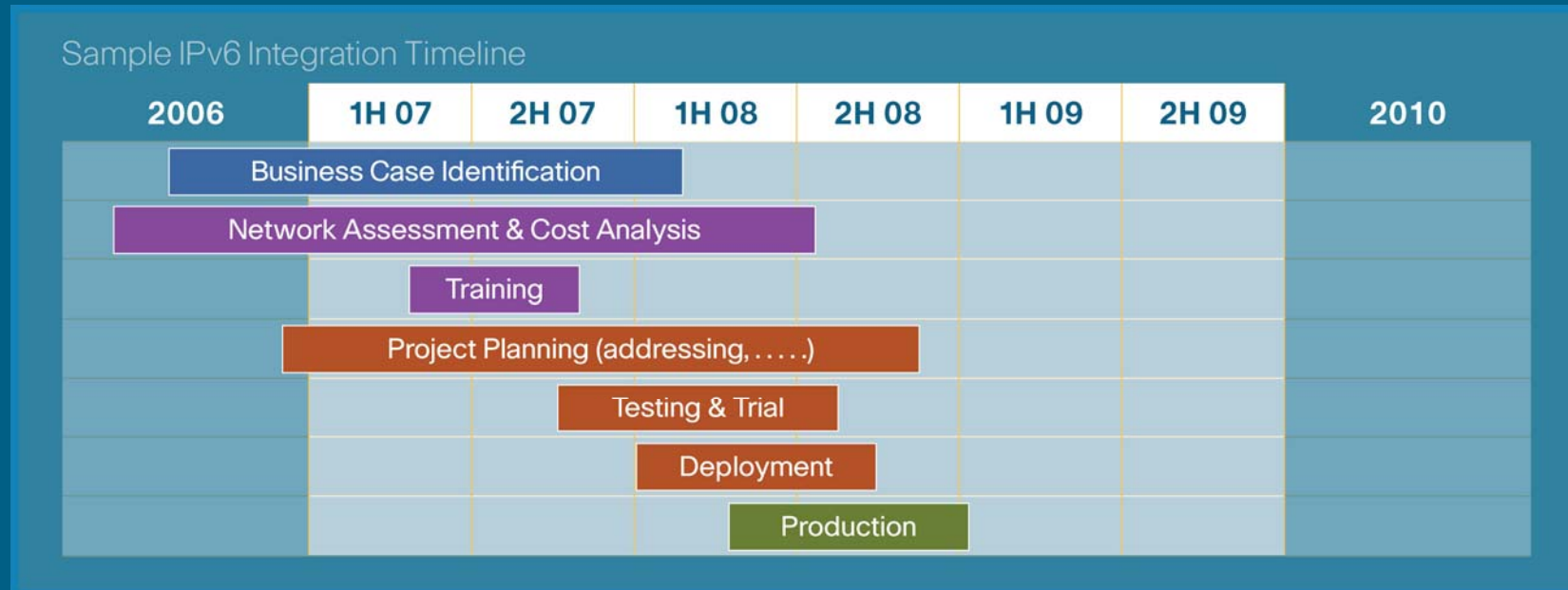


# Planning for a successful IPv6 integration



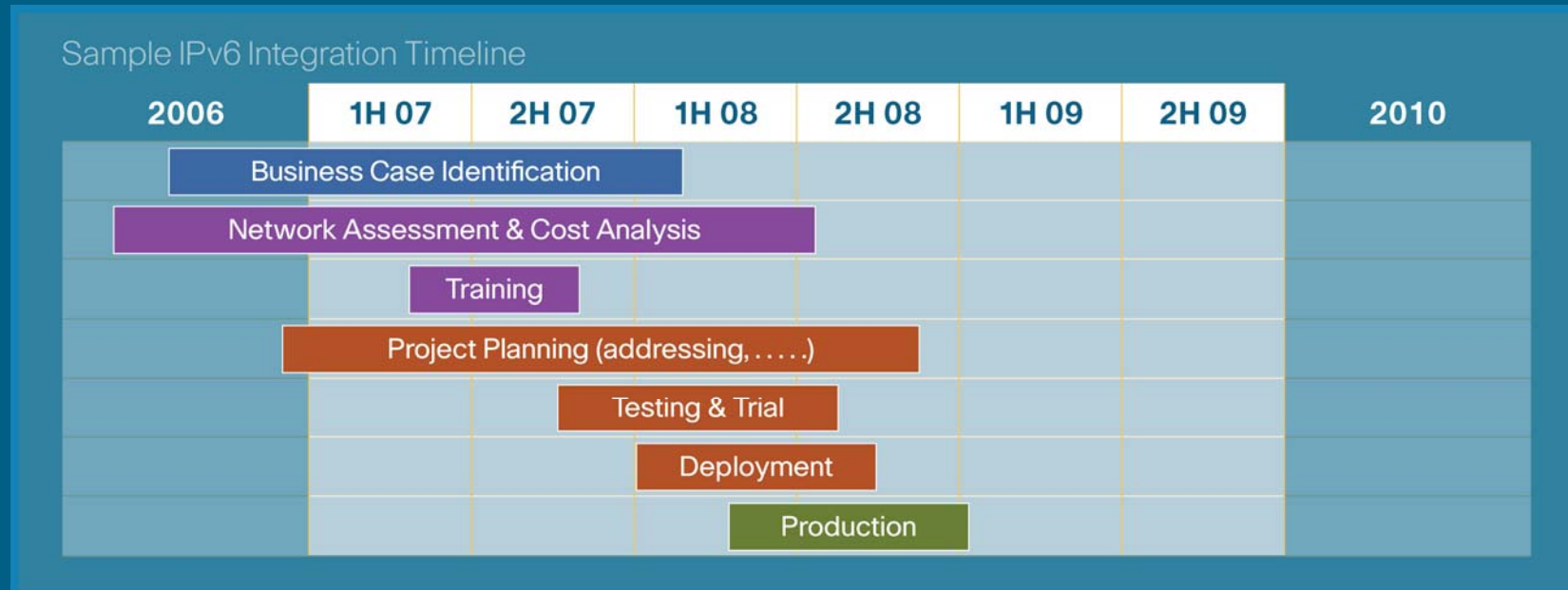
- **Step 1** - View your agency's operation in a network-centric world

# Planning for a successful IPv6 integration



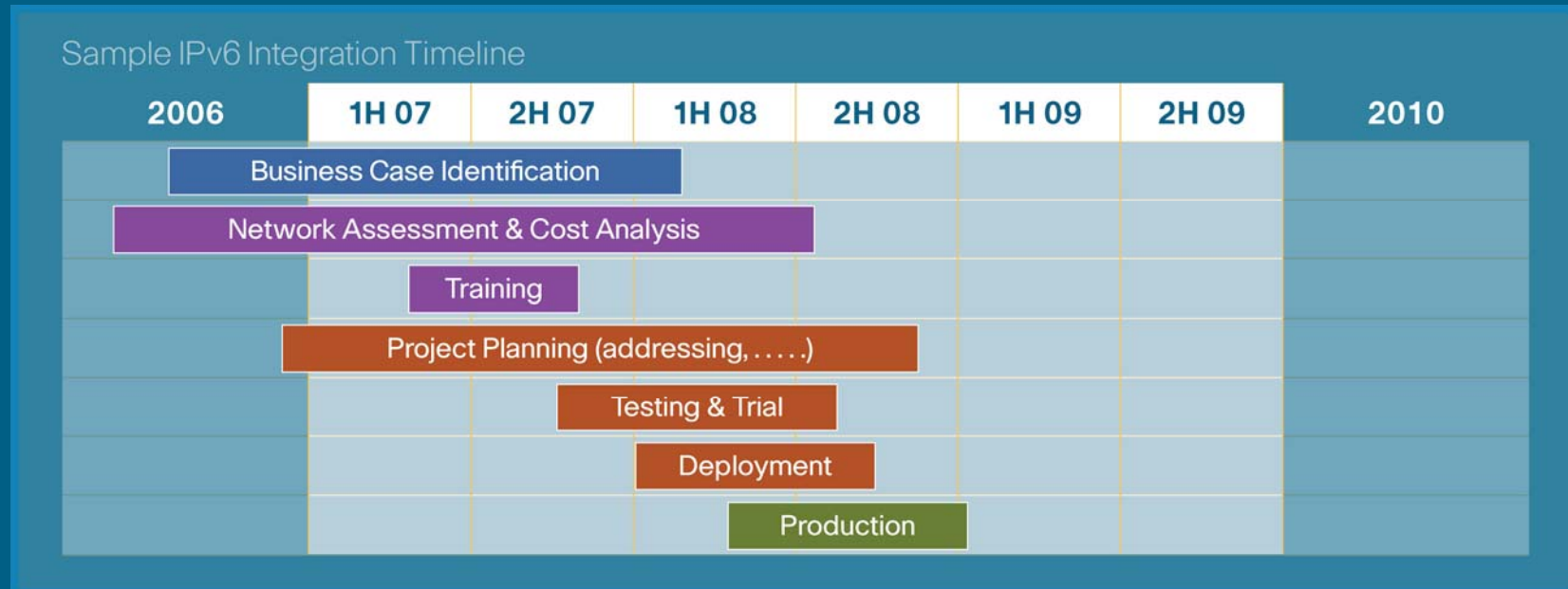
- **Step 2** - Establish goals, a critical path, and general timelines

# Planning for a successful IPv6 integration



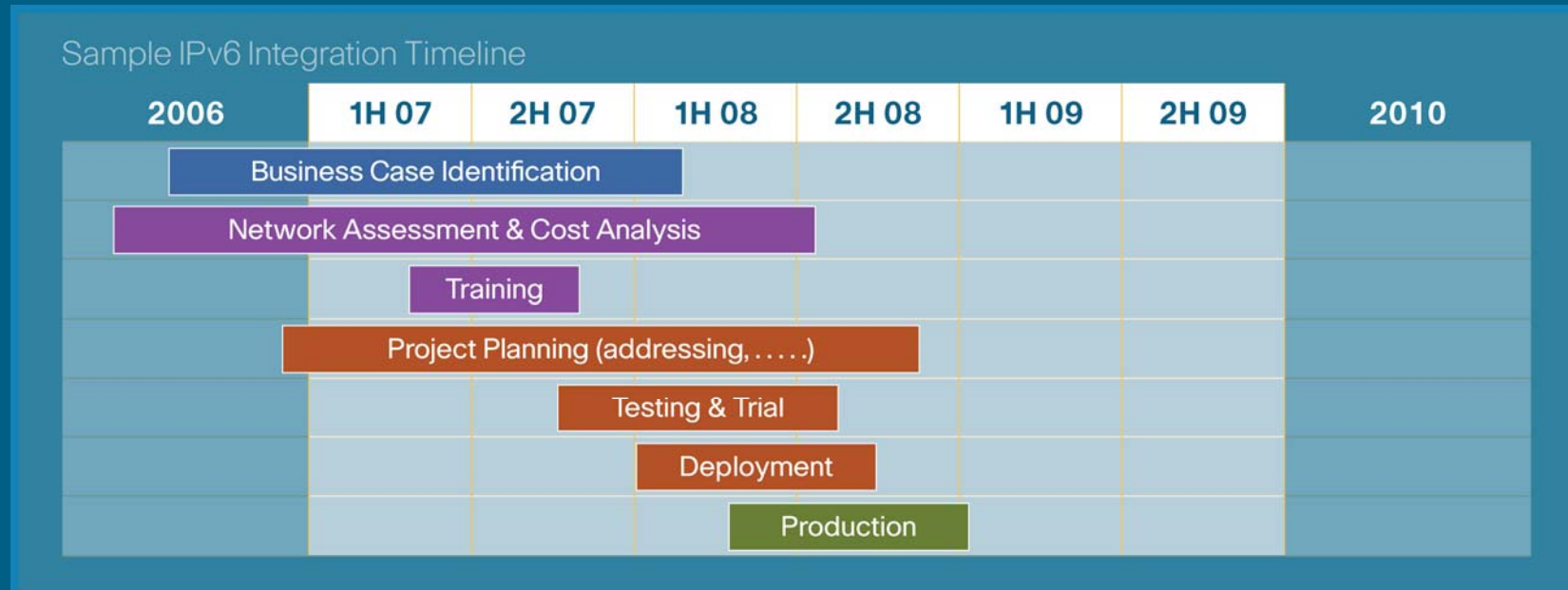
- **Step 3** - Create an IPv6 training strategy and plan

# Planning for a successful IPv6 integration



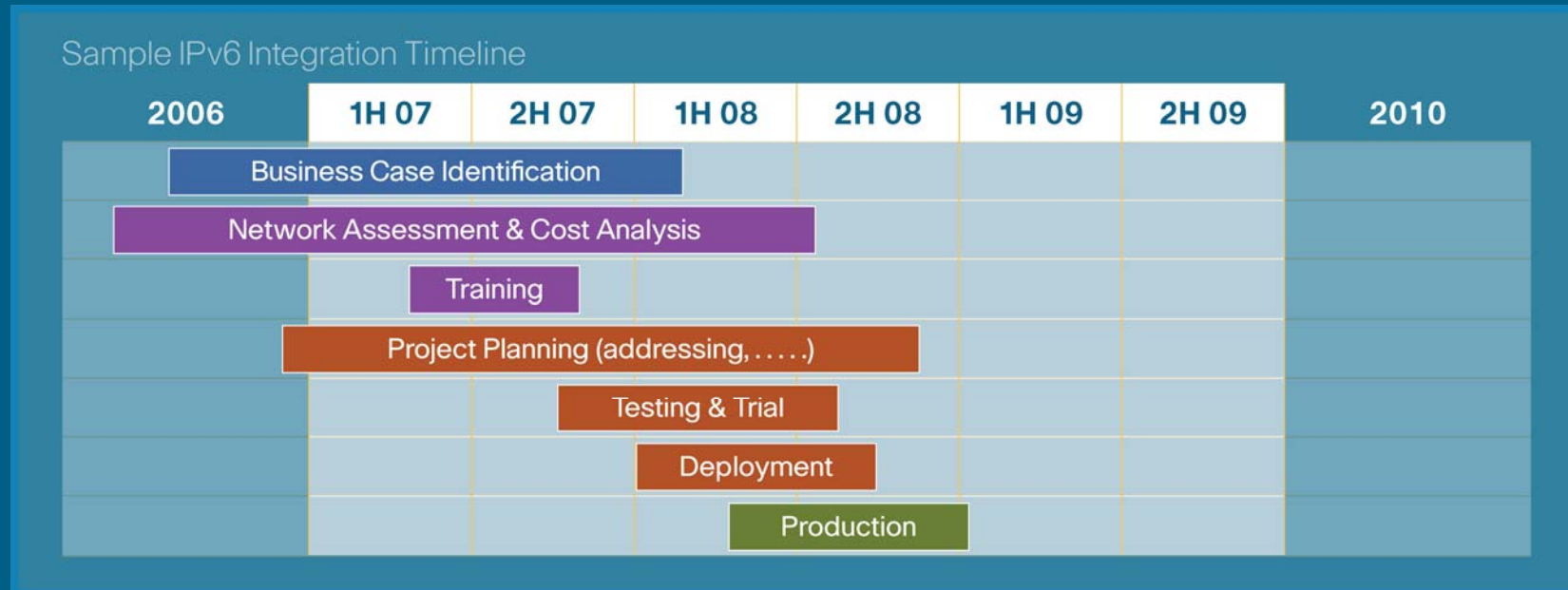
- **Step 4 - Obtain an IPv6 prefix**

# Planning for a successful IPv6 integration



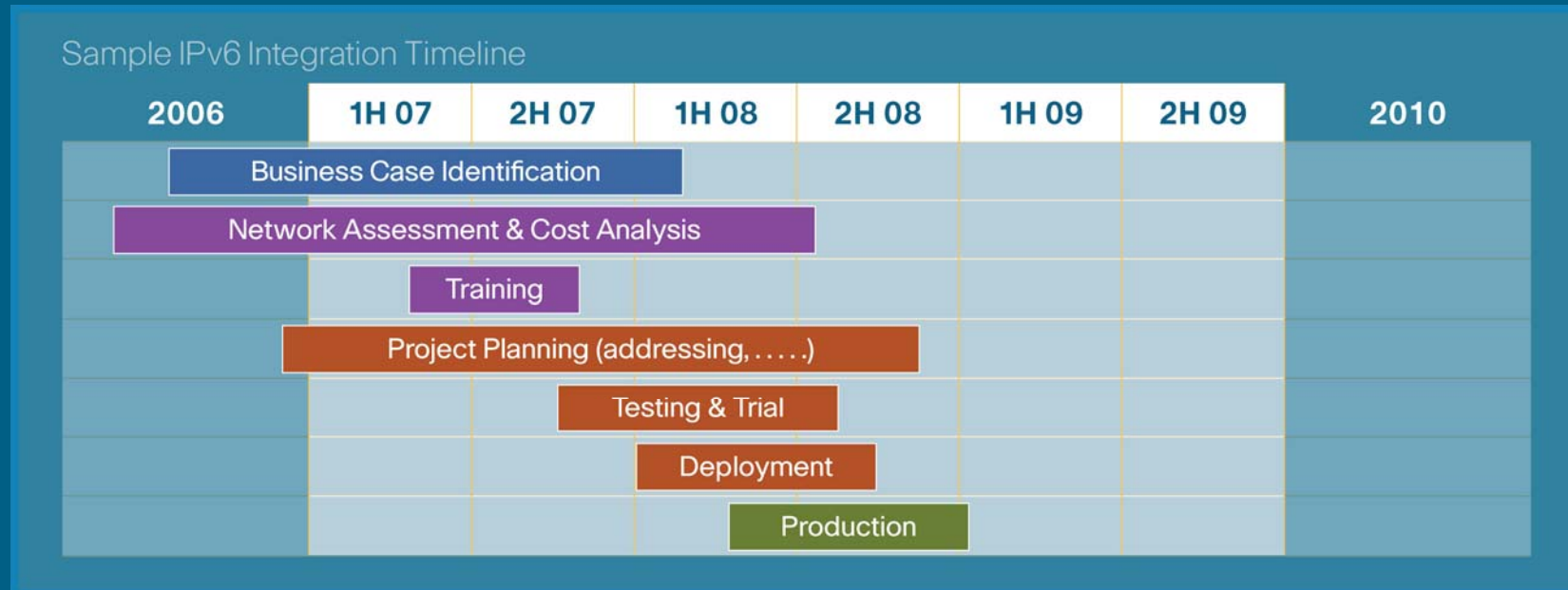
- **Step 5** - Develop an addressing plan and corresponding network architecture

# Planning for a successful IPv6 integration



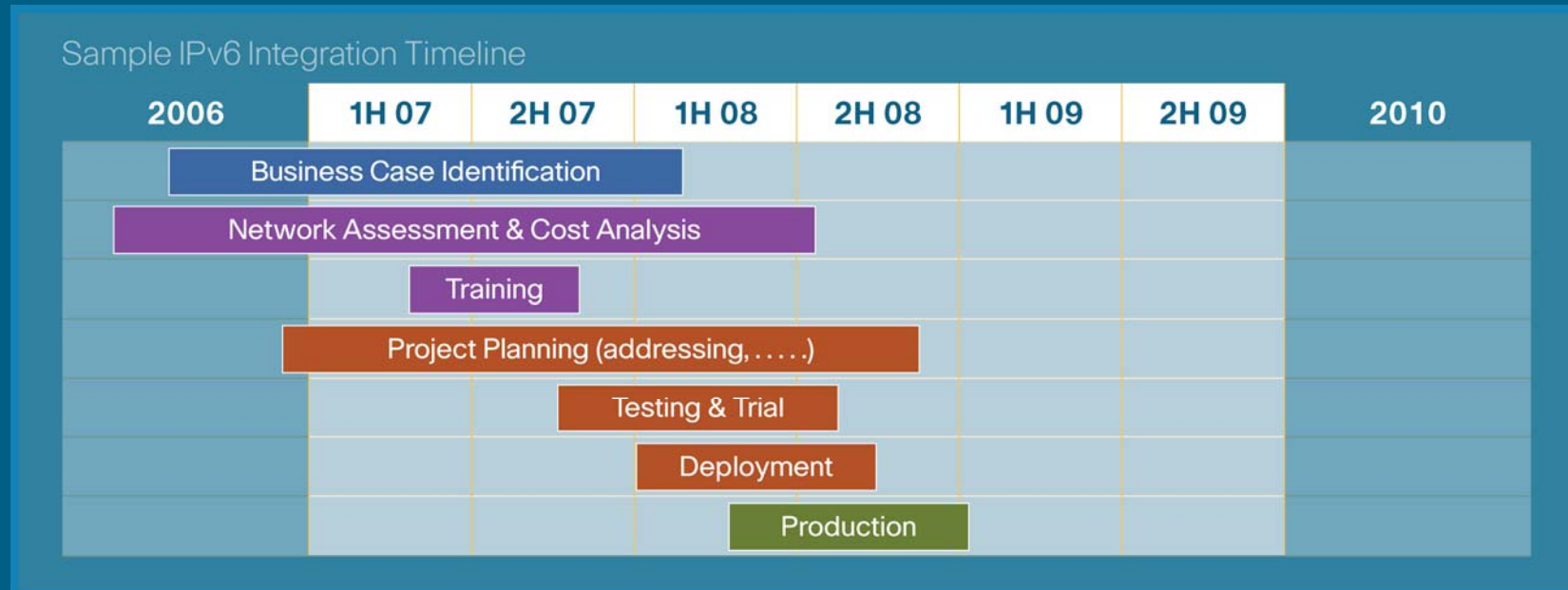
- **Step 6** - Assess IT equipment and identify steps needed to integrate IPv6

# Planning for a successful IPv6 integration



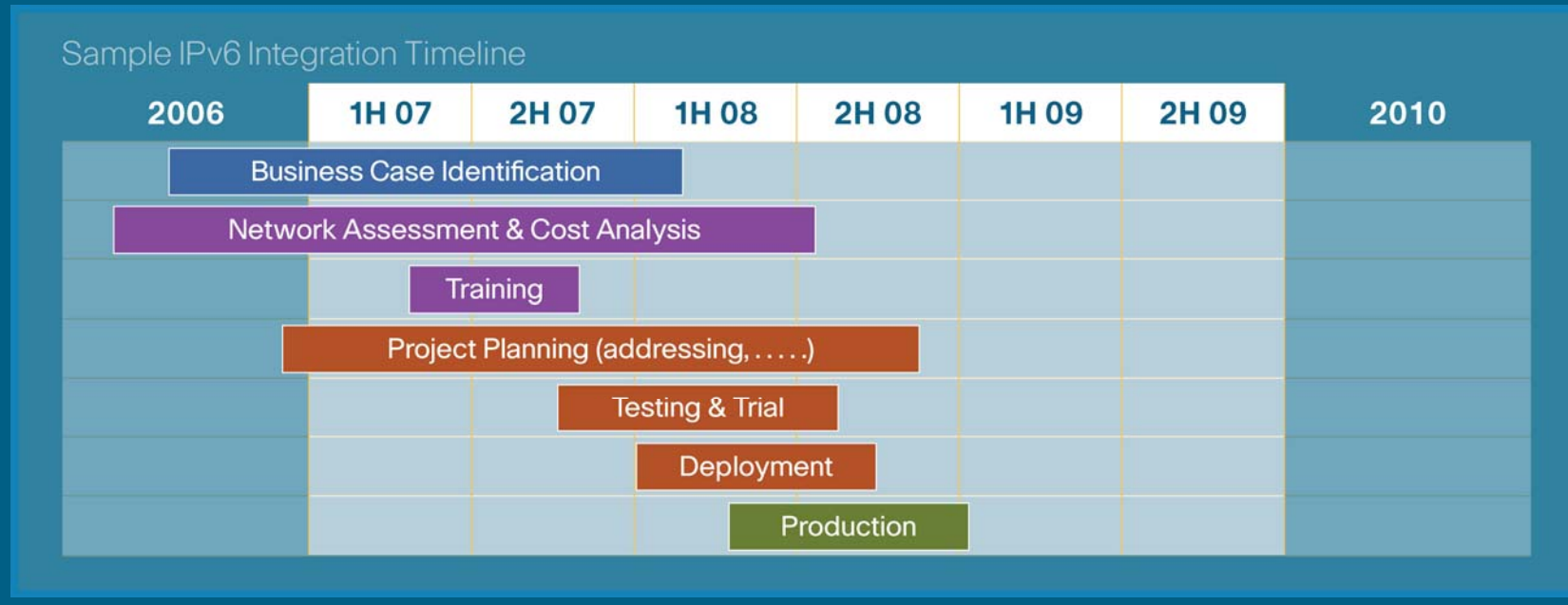
- **Step 7** - Develop an IPv6 procurement strategy and policy

# Planning for a successful IPv6 integration



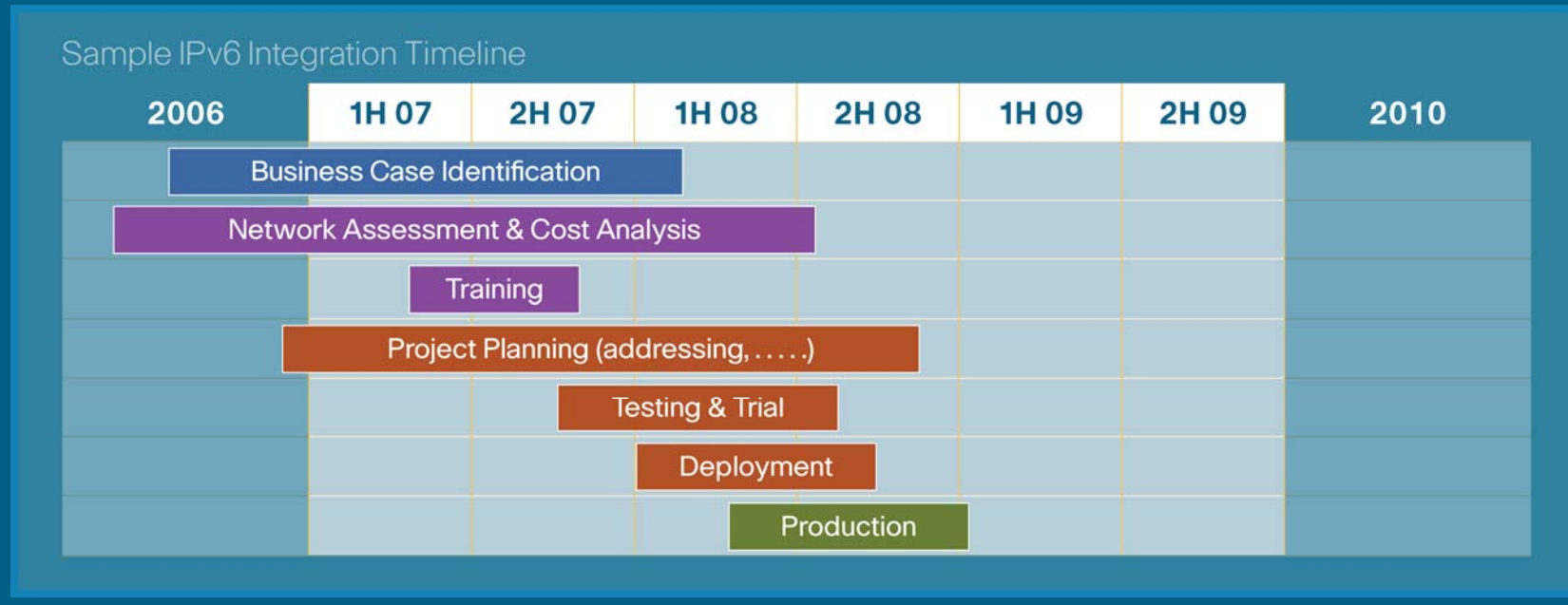
- **Step 8** - For each host on the network, identify its operating system and applications to determine if any hardware and software upgrades are required and schedule them to coincide with the usual hardware lifecycle process.

# Planning for a successful IPv6 integration



- **Step 9** - Adapt the agency's existing IPv4 security policies to include new considerations for IPv6.

# Planning for a successful IPv6 integration



- **Step 10** - Consider applications and systems that will likely not be modified in the foreseeable future in the overall integration strategy if they will communicate over the new IPv6 network.

# A Phased Approach

Stepping toward a successful implementation

## Phase 1: Integrate IPv6 into Infrastructure

- Assess networking equipment, perform any needed upgrades, and then set up in selected locations
- Register for an IPv6 prefix
- Plan IP addressing and policies for autoconfiguration
- Add minimum IPv6 support to critical networking services
- Connect to the IPv6 Internet
- Secure IPv6 access
- Monitor IPv6 traffic on an ongoing basis



# A Phased Approach

Stepping toward a successful implementation

## Phase 2: Operate Selected Applications over IPv6

- Assess host and server operating systems and applications
- Update or configure operating systems and applications to operate over IPv6
- Configure naming services to make selected applications available over IPv6
- Begin operating and monitoring applications over IPv6
- Secure IPv6 on hosts
- Deploy new applications and services that operate over IPv6

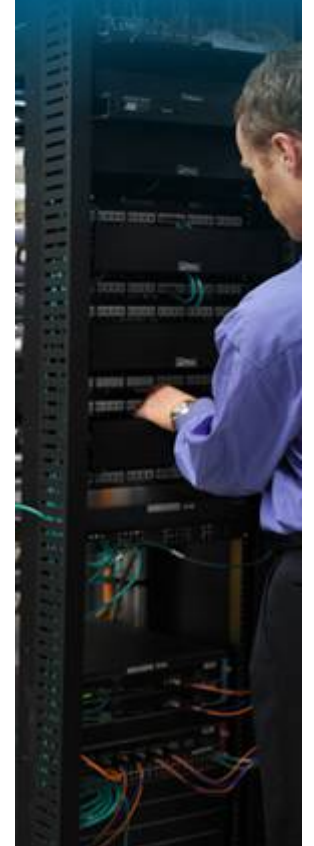


# A Phased Approach

Stepping toward a successful implementation

## Phase 3: Move to Production

- Complete the IPv6 deployment throughout the infrastructure
- Finalize upgrades to operating systems on hosts and servers
- Ensure that management applications are fully operational over IPv6
- Verify that the data center is fully operational for IPv6
- Upgrade specific solutions to IPv6, such as IP Telephony



# Integrating IPv6 into the Network

## The need for peaceful IPv4-IPv6 coexistence

- Agencies cannot disrupt the delivery of mission-critical government services over the existing network.
- Agencies can migrate applications and services to IPv6 over time, which is less expensive and less disruptive than upgrading and testing all applications at once.
- It might not be possible to add IPv6 support to older applications
- Upgrading or replacing old but stable operating systems, or platforms used for dedicated applications, might not provide value.
- Agency staff needs to receive training on IPv6, which takes time.

# Integrating IPv6 into the Network

## Selecting an Option for Co-Existence

- Each agency must determine its own “best approach” for dual-stack networking depending on mission goals, environment, and progress with IPv6 integration.
- Transition steps can include the use of IPv6-over-IPv4 tunnels, native IPv4 and IPv6 over dedicated data links, and IPv6 over Multiprotocol Label Switching (MPLS) backbones.
- Integrating older systems that will not be upgraded to IPv6 can be accomplished using translation mechanisms, including Network Address Translation - Protocol Translation (NAT-PT).

# Integrating IPv6 into the Network

## Assess Network Devices

Before changing any network devices, conduct a detailed inventory that includes hardware type, memory size, software release and licensing, and configuration parameters.

Router Status	Cost
IPv6 compliant and currently running IPv6	None
IPv6 compliant but needs to be configured for IPv6	IT staff time
Requires software upgrade for IPv6 compliance	Software and IT staff time
Requires hardware upgrade to support software upgrade	Hardware, software and IT staff time
Legacy platform: cannot be upgraded to support IPv6 and must be replaced	Hardware, software and IT staff time
Will not be upgraded due to planned discontinuation	None

# Integrating IPv6 into the Network

Take a Phased Approach to Infrastructure Integration

## Phase 1: Test IPv6 in a lab environment

- Reveals potential disruptions and security risks
- Include the network hardware and software features targeted for IPv6 integration, as well as the first applications to operate over IPv6.
- Provides valuable experience and determines any necessary modifications to technology plan or schedule.



# Integrating IPv6 into the Network

Take a Phased Approach to Infrastructure Integration

## Phase 2: Initiate pilot deployment

- Set up routers and switches to process IPv6 traffic.
- Configure the LAN to transport the agency's IPv6 prefixes to production host computers, printers, and other devices.
- Ensure the security architecture is configured to handle both IPv4 and IPv6.
- Set up DNS and DHCP servers to handle IPv6 queries.
- Configure the Network Management System (NMS) to monitor the IPv6 network.



# Integrating IPv6 into the Network

Take a Phased Approach to Infrastructure Integration

## Phase 3: Evaluate advanced features

- Investigate how to improve the design and delivery of applications and services using IPv6 features such as mobility, security, Quality of Service (QoS), and multicast.
- Explore the use of features that are improved in IPv6, such as Mobile IP, and incorporate them in new services.



# Integrating IPv6 into the Network

Take a Phased Approach to Infrastructure Integration

## Phase 4: Plan and provision addresses

- Practically unlimited address space in IPv6 allows agencies to design a network architecture that matches the organizational structure
- Build a solid addressing scheme that will address the agency's growth and application plans.
- Use address aggregation to ensure scalability
- Consider ways the Interior Gateway Protocol (IGP) will aggregate the addresses.



# Moving Applications to an IPv6 Environment

- Assess all servers, desktops, laptops, and workstations to determine what they need to support IPv6.
- Test all applications in the lab to verify that they can operate over IPv6 before they are released into production. Configure them to use IPv6 transport if it is available and IPv4 if it is not.
- Begin upgrading IPv6-ready applications to support IPv6 and installing new IPv6 applications.
- After IPv6-enabling existing applications, consider developing new applications that take advantage of new features in IPv6 to help meet mission objectives.

# Integrating IPv6 into Operations

## Commonly Used Management Tools that Work in a Dual-Stack Environment

Type of Tool	Examples
Traffic Monitoring	Management Information Base (MIB) for IPv6, NetFlow IPv6 records, IPv6 Service Level Agreement (SLA)
Network Services	DHCPv6 Server and Relay, Domain Name Server (DNS), Network Time Protocol (NTP)
Network Management Systems	Network management Applications specific to the IPv6 environment such as an IPv6 topology mapping, IPv6 user's tracking
Other Management Applications	Secure Shell (SSH), Simple Network Management Protocol (SNMP), Syslog

# Integrating IPv6 into Operations

## Security considerations

- IPv6 networks face many of the same threats and attacks as IPv4 networks.
- They are face new threats because of IPv6-specific characteristics and the specifics of various integration mechanisms.
- Vendors, including Cisco, are working to offer a full set of security features for IPv6.
- Until an agency's environment is IPv6-only, the IT group can use existing IPv4 security mechanisms that also secure hosts for IPv6.



# Integrating IPv6 into Operations

## Recommended security practices

- Make reconnaissance more difficult through proper address planning for campus switches
- Control management access to the campus switches
- Implement IPv6 traffic policing, on a per-user microflow basis
- Control ingress traffic from the access layer
- Upgrade to IPv6-aware firewalls
- Monitor and control all transition mechanisms



# Learn more about...

- **Cisco IPv6 technology:** [www.cisco.com/ipv6](http://www.cisco.com/ipv6)
- **Other agency's experiences integrating IPv6:** [blogs.technet.com/ipv6](http://blogs.technet.com/ipv6)
- **Cisco IOS Software for various Cisco switches and routers:**  
[www.cisco.com/en/US/products/sw/iosswrel/ps5187/products\\_configuration\\_guide\\_chapter09186a00801d65ed.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_configuration_guide_chapter09186a00801d65ed.html)
- **Deploying IPv6 in campus networks:**  
[www.cisco.com/application/pdf/en/us/guest/netso/ns107/c649/ccmigration\\_09186a00807753a6.pdf](http://www.cisco.com/application/pdf/en/us/guest/netso/ns107/c649/ccmigration_09186a00807753a6.pdf)
- **Products that have received IPv6 Special Interoperability Certification:**  
<http://jitc.fhu.disa.mil/apl/ipv6.html>
- **Certification activities:**
  - Joint Interoperability Test Command: <http://jitc.fhu.disa.mil/apl/ipv6.html>
  - National Institute of Standards and Technology IPv6 Profile Paper:  
<http://www.antd.nist.gov/usgv6-v1-draft.pdf>
  - IPv6 Ready Logo Program: <http://www.ipv6ready.org/frames.html>
- **IPv6 in general**
  - <http://www.6diss.org/>
  - <http://go6.net/>
  - <http://www.ipv6forum.com/>
  - <http://www.ietf.org/html.charters/v6ops-charter.html>

