Migrating Industrial Ethernet IPv4 Network to IPv6
A Phased Approach to IPv6 Transition

Technical Track

www.odva.org
Industrial IPv4 Network

- Enterprise Network
- DMZ
- Supervisory Network
- Control System Network
- Remote Facility/Vendor
- Wireless Field Network

Key Components:
- Internet
- Cloud Systems
- Web Server
- App Server
- SCADA
- Historian
- Database
- HMI
- IEDs/PLCs
- Historian
- VPN
- 6TiSCH

© 2014 ODVA, Inc. All rights reserved.
Why Migrate to IPv6

- Bigger address space
- Efficient routing and packet processing
- Directed data flows
- Simplified network configuration
- Support for new services
- Conforming IPv6 implementation must support IPSec
There’re some common IPv6 transition mechanisms that can be used for migrating Industrial Network...
Dual-Stack Endpoints
NAT64 and DNS64

① What the IPv6 address of “foo.example.com”?
② What the IPv4 address of “foo.example.com”?
③ It's 192.0.2.26.
④ It's 64:ff9b::c00:21a.
⑤ Packet is sent to 64:ff9b::c00:21a.
⑥ Packet is translated with src=192.0.2.1 and dst=192.0.2.26.
MAP (Mapping Address + Port)
The combination of NAT64 and Dual-Stack Endpoints is the main transition strategy for Industrial Network.
IPv6 Migration Strategy and Stages

Stage 1
- Migrating from IPv4-only network to dual-stack network
  - IPv4-only and IPv6-only nodes co-exist on the same network
  - No dual-stack support is required on endpoints
  - Intelligence is in the network

Stage 2
- Migrating IPv4-only endpoints to IPv6
  - No dual-stack support is required on endpoints
  - NAT64 is used for communication between IPv4 and IPv6 endpoints

Stage 3
- Migrating from dual-stack network to IPv6-only network
  - All network endpoints support IPv6
  - IPv4 is no longer needed on the network

Time
- Stage 1: 2 – 3 years
- Stage 2: 5 – 15 years
- Stage 3: 1 – 2 years
Why We’re Taking this Approach?

Minimize network topology change

Simplify upgrading process

Endpoint upgrade is independent from network change

Protect investment on existing machine endpoints for longer period
Stage 1 – Migrate IPv4-Only Network to Dual-Stack Network
Instead of transforming the entire Enterprise and Control network to dual-stack in one single motion, it’s better to take a phased approach...
Wireless Field Network is Driving IPv6 Adoption
Stage 1 Objectives

- Build intelligent network that supports both IPv4 and IPv6 endpoints
- Preserve existing network topology and protect existing network investment
- Separate network migration completely from IPv6 upgrade on endpoints
What’s Need to be Done for Stage 1

- Replace regular layer-3 routers and gateways with **NAT64-capable devices** via HW and/or SW upgrade.

- Replace IPv4 DNS servers with **DNS64 servers**.

- Install DHCPv6 servers to **serve stateful DHCP requests**.

- Use a **central NMS** to manage all NAT64 gateways and DNS64 servers and ensure **consistent configuration across all systems**.
NAT64 will be used to facilitate the communications between IPv4 and IPv6 hosts in all three stages. It’s supported by NAT64 gateway and NAT64 DNS server, and completely transparent to endpoints.
**NAT64 Configuration**

**Configure NAT64 Gateway**
- All layer-3 routers and gateways should support NAT64.
- A separate IPv4 address pool should be configured for each NAT64 gateway to facilitate translation.
- To allow IPv4 clients access IPv6 servers, the same static address mappings must be created on NAT64 gateways for IPv6 servers.
- Routing must be configured properly for IPv4 and IPv6 networks to ensure correct path for translated traffic.

**Configure DNS64 Server**
- The DNS64 server must support dual-stack and serve DNS requests from both IPv4 and IPv6 endpoints.
- Every A record should have a corresponding AAAA record with translated address, and vice versa (this mapping may be generated dynamically).
- Configuration on DNS64 servers must be consistent with NAT64 gateways.
Stage 2 – Migrate IPv4-only Endpoints to IPv6
Stage 2 Objectives

Support each endpoint to upgrade to IPv6 independently

Allow different software and hardware products to be upgraded independently
What’s Need to be Done for Stage 2

- Upgrade servers, employee desktops, laptops, and important IT assets to IPv6
- Upgrade HMI, Historian, and other assets on the Supervisory network to IPv6
- Upgrade PLCs, Drives, and other I/O devices to IPv6
Communication Scenarios in Stage 2

- IPv6-only Host accesses IPv4 Server
- IPv4-only Host accesses IPv6 Server
- Remote IPv4-only Host accesses local IPv6 server via VPN
Scenario 1 – IPv6-only Host accesses IPv4 Historian (Stateful NAT64 Translation)

- Acquire Destination IP
  - IPv6 host queries “historian.example.com”
  - DNS server finds the A record of 192.0.2.26.
  - DNS64 server translates A record to AAAA record and returns 64:ff9b::c00:21a.

- Contact Destination
  - Host sends first packet to 64:ff9b::c00:21a.
  - Packet is routed to the default IPv6 gateway, which is the NAT64 gateway.
  - NAT64 gateway re-encapsulates payload in IPv4 packet with the destination IP address of 192.0.2.26 and the source IP address of its own (192.0.2.1).
  - NAT64 gateway sends the IPv4 packet to historian.

- Handle Return Traffic
  - Historian accepts request and sends back IPv4 response to NAT64 gateway.
  - NAT64 gateway re-encapsulates payload in IPv6 packet with the destination IP address of the host and source IP address of 64:ff9b::c00:21a.

Return AAAA record of 64:ff9b::c00:21a for “historian.example.com”
Scenario 2 – IPv4-only Host accesses IPv6 Server (Stateless NAT64 Translation)

- **Configure static address mapping on NAT64 gateway and DNS64 server**
  - Map **192.0.2.1**/110 to **2001:db8:12**/110
  - Create A record of **192.0.2.1** for "pop3.example.com"

- **Acquire Destination IP**
  - IPv4 host queries "pop3.example.com"
  - DNS server returns the A record of **192.0.2.1**.

- **Contact Destination**
  - Host sends first POP3 TCP packet to **192.0.2.1**.
  - Packet is routed to the default IPv4 gateway, which is the NAT64 gateway.
  - NAT64 gateway re-encapsulates payload in IPv6 packet with the destination IP address of **2001:db8:12** and the source IP address of **64.ff9b::c00:21a**.
  - NAT64 gateway sends the IPv6 packet to the mail server.

- **Handle Return Traffic**
  - Mail server accepts request and sends back IPv6 response to NAT64 gateway.
  - NAT64 gateway re-encapsulates payload in IPv4 packet with the destination IP address of the host (**192.0.2.26**) and source IP address of **192.0.2.1**.

Translate pop3 traffic with destination IPv4 address **192.0.2.1** to **2001:db8:12** and vice versa

Return A record of **192.0.2.1** for "pop3.example.com"
Scenario 3 – Remote IPv4-only Host accesses IPv6 Server across VPN

- Remote VPN gateway establishes IPSec VPN tunnel with the local VPN gateway on the Supervisory Network, which also happens to be the NAT64 gateway.

- Configure static address mapping on NAT64 gateway and DNS64 server
  - Map 192.0.2.61 to 2001:db8:66
  - Create A record of 192.0.2.61 for “hmi.example.com”

- Acquire Destination IP
  - Remote IPv4 host queries “hmi.example.com”. Request is sent over VPN to the DNS64 server on Supervisor Network.
  - DNS server returns the A record of 192.0.2.61.

- Contact Destination
  - Remote host sends TCP packet to 192.0.2.61.
  - Packet is tunneled to the VPN + NAT64 gateway.
  - NAT64 gateway decrypts packet and re-encapsulates payload in IPv6 packet with the destination IP address of 2001:db8:66 and the source IP address of 64:ff9b::c00:21a.
  - NAT64 gateway sends the IPv6 packet to the IPv6 HMI.

- Handle Return Traffic
  - HMI accepts request and sends back IPv6 response to NAT64 gateway.
  - NAT64 gateway re-encapsulates payload in IPv4 packet with the destination IP address of the host (10.10.1.126) and source IP address of 192.0.2.61. Packet is encrypted and sent to the remote VPN gateway.
Issues and Challenges for Stage 2

Dependencies on the IPv4 Infrastructure
- Using IPv4 address as device and service identifiers
- Always assume a four-byte IP address
- Rely on the broadcast and multicast functions of IPv4

IPv4 Address Embedded in Control Protocols
- For example, the ListIdentity response message in EtherNet/IP protocol contains the IP address of the responding device
- Ring protocols (e.g. DLR) may embed IP address as part of the payload.
- The EtherNet/IP configuration objects may contain IP address definitions

IPv4-based Management Tools and Utilities
- Existing network and automation management tools present IPv4-based management interfaces
• Industrial protocols need to re-designed to work with IPv6.

• Management tools must be upgraded to support IPv6.

• Control systems that are engaged in the same control loop (e.g. using the same protocols) should be upgraded together to avoid any issues with NAT64.

• I/O devices on the same Ring topology must be upgraded together.
Stage 3 – Migrate Dual-Stack Network to IPv6-Only Network
Stage 3 Objectives

- Support smooth transition to full IPv6-only network
- Allow different network segments to be migrated independently
What’s Need to be Done for Stage 3

- Selectively disable NAT64 functionality on NAT64 gateways and DNS64 servers and test drive IPv6-only network.
- Create small IPv6 pockets by replacing NAT64 gateways with regular IPv6 gateways. Merge small IPv6 pockets into bigger IPv6 subnets.
- Remove all IPv4 infrastructure assets (e.g. gateway, DNS server, DHCP server, ... etc). And then celebrate!
NAT64 is a complex technology. Here’s a list of challenges we’ve solved and you need to know...
Common NAT64 Problems

- Smaller IP Path MTU on IPv6 Network
- Optional UDP Checksum on IPv4 Network
- IPv4 and IPv6 Fragments
- Unnecessary Translation for Dual-Stack Endpoints
- Different Endpoints on the Same Layer-2 Network
- Special Protocols
- IP Multicast
- Broken IPSec VPN
- The IP Path MTU (Maximum Transmission Unit) on IPv6 network is smaller due to larger IPv6 header.
- To avoid fragmenting translated payload on IPv6 network, the IP Path MTU on IPv4 network should be set at a lower value (e.g. 1460).
- If not possible to configure the MTU on IPv4 endpoints, NAT64 gateways must participate in Path MTU Discovery and notify IPv4 endpoints of the new MTU value.
- NAT64 gateways must be able to fragment big IPv4 datagrams that exceed MTU on IPv6 network.

Solution to "Smaller IP Path MTU on IPv6 Network"
Solution to “Optional UDP Checksum on IPv4 Network”

- NAT64 gateway must recalculate TCP and UDP checksums, which is typically done by calculating the difference between the two different pseudo-headers.
- UDP checksum is mandatory on IPv6 network, but is optional in IPv4.
- NAT64 gateway must recalculate UDP checksum using the entire payload data when it receives an UDP datagram with zero checksum.
- If the zero-checksum UDP datagram is also a fragment, NAT64 gateway must reassemble the UDP datagram before recalculating the checksum. If the fragments arrive out of order, the UDP datagram may end up being dropped.
• **IPv6 fragments are handled end-to-end. IPv6 router shall never fragment an IPv6 datagram.**

• **If IP fragments arrive in order, NAT64 gateway will translate fragments as they arrive. States will be maintained on the gateway to translate following fragments.**

• **If IP fragments arrive out of order, NAT64 gateway queues fragments until the first fragment arrives, at which time translation will be done for queued fragments as well.**

**Solution to “IPv4 and IPv6 Fragments”**
• Some endpoints may support dual-stack, though not required.
• To talk to another endpoint, the dual-stack host needs to know whether to use IPv4 or IPv6. If wrong stack is chosen, unnecessary translation may occur.
• To solve this problem, separate DNS servers (independent from DNS64 server) should be configured for IPv4 and IPv6 network independently. The host should always use the stack on which a valid DNS record was returned.
• The host should send the query on IPv6 network first. If a valid AAAA record is returned on IPv6 network, the host must not send the DNS query on IPv4 network. If for some reason the host receives valid DNS records on both networks (e.g. timeout the first query too quickly), it’s up to the host to decide which stack to use for talking to the other endpoint.

Solution to “Unnecessary Translation for Dual-Stack Endpoints”
Both IPv4 and IPv6 endpoints may be on the same layer-2 network (e.g. same VLAN and connected by same switches).

NAT64 gateway must be able to perform translation on any physical or logical interface, and must handle the scenario where source and destination endpoints are connected to the same physical or logical port.

IPv4 and IPv6 endpoints should be grouped into separate layer-2 networks whenever is possible.
• Some protocols embed IP addresses in the protocol payload, e.g. FTP, RTSP, PPTP, SIP, EtherNet/IP... etc.
• You shall only install NAT64 gateways that support ALG (Application Level Gateway) functionality for these protocols.
• If the NAT gateway doesn’t support the required ALGs, to avoid service disruption, client and server endpoints using these protocols should be migrated to IPv6 at the same time.
• Some protocols use IP multicast for communications, e.g. EtherNet/IP. In order to forward such multicast traffic across the NAT64 boundary, NAT64 gateway must be able to translate between IPv4 and IPv6 multicast packets.

• NAT64 gateway should maintain the one-to-one mappings between IPv4 and IPv6 multicast addresses. The mapping entries can be manually configured or hard-coded.

• NAT64 gateway must be able to function as a MLD or IGMP proxy on each network interface, and translate MLD and IGMP messages accordingly.

• Because multicast IP address is embedded in the Explicit CIP message setting up the multicast exchange, NAT64 gateway must implement the CIG ALG that is capable of translating IP address contained in such messages.

• When SSM (Source-Specific Multicast) was specified by an endpoint, NAT64 gateway should translate the source IP address of the multicast if it knows the mapping; otherwise, NAT64 gateway will have to drop the source in the translated messages. Note that when the IGMP version on the IPv4 network is not 3, all SSM information from MLD will be lost in translation.

• In a CIP environment, if the installed NAT64 gateway cannot meet the requirements of translating CIP multicast packets, you should disable multicast on EtherNet/IP CIP endpoints.

Solution to "IP Multicast"
• **IPSec AH and IPSec ESP in Tunnel Mode breaks** because it protects the outer IP header.

• **A single IPSec ESP session in Transport Mode generally works** across NAT64 gateway. Multiple sessions between an endpoint and the NAT64 gateway may not work because PAT cannot be performed on IPSec ESP. You should install NAT gateways that support IPSec pass-through if you need to pass IPSec VPN traffic through the gateways.

• **NAT-T negotiation or IPSec-over-UDP** (i.e. NAT-T without negotiation) should be always enabled for all IPSec endpoints.

**Solution to “Broken IPSec VPN”**
There’re some **NAT64** challenges that are specific to the Industrial Control Network...
Industrial Specific NAT64 Problems

- Ring Topology
- Large Complex Layer-2 Network
- Time Synchronization
- Real-Time and Deterministic Performance
• Some ring protocols (e.g. DLR) embed IP address in the payload. Such protocol will need updates to support IPv6 addresses.
• Due to the nature of ring topology, traffic may go either direction on the ring. When there’re multiple exits, traffic may go in and out of the ring through different gateway devices.
• The ring exit/gateway must not be a layer-3 device, hence not a NAT64 gateway.

Solution to “Ring Topology”
Solution to “Large Complex Layer-2 Network”

- IPv4 endpoints on large layer-2 network may be upgraded to IPv6 at different times.
- Complex layer-2 control network makes communication between IPv4 and IPv6 hosts difficult. While it’s possible for the same NAT64 gateway to handle the translation “hairpin” style, such deployment may run into problem on a large complex network.
- If problem does occur, NAT64 gateways need to be installed to partition the complex layer-2 network.
• Timing is a critical aspect of Industrial Control Systems.
• Typically PTP (Precision Time Protocol or IEEE1588) is used to synchronize time on the control network at a very fine level.
• Layer-2 PTP should always be used (i.e. directly over Ethernet) instead of over UDP to avoid any potential problems with NAT64.

Solution to “Time Synchronization”
• The communication between control systems needs to be real-time and deterministic.
• NAT64 implementation needs to minimize the forwarding delay possibly by offloading actual translation to hardware.
• To meet the deterministic requirement, the same technique used on the IPv4 network needs to be carried over to the IPv6 network (e.g. IEEE TSN). NAT64 gateway must be able to handle those signaling protocols and participate in the actual scheduling operation should it be on the actual packet path.
Intelligent Network is the key to IPv6 migration...