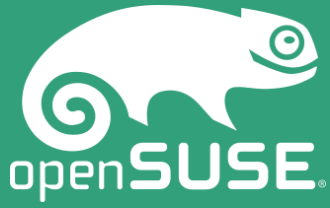


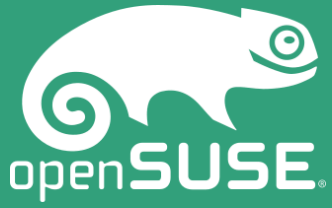

# Network Boot in a Zero-Trust Environment with UEFI

## Using SUSE & UEFI to Configure HTTPS Boot

**Brian Richardson**
**Intel Corporation**

**Director, Firmware Ecosystem Engagements**


**@intel_brian**



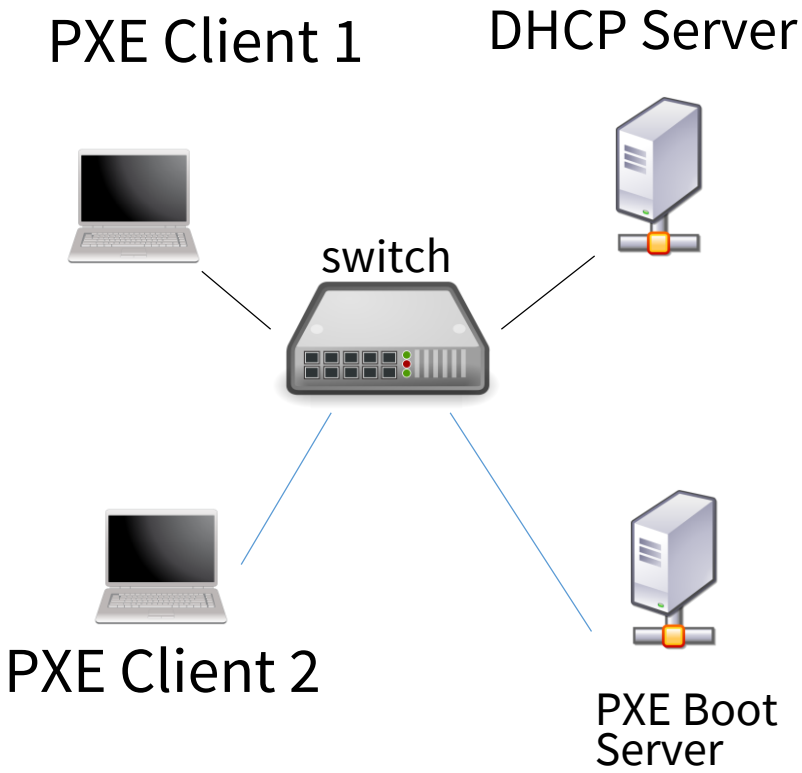

# Agenda

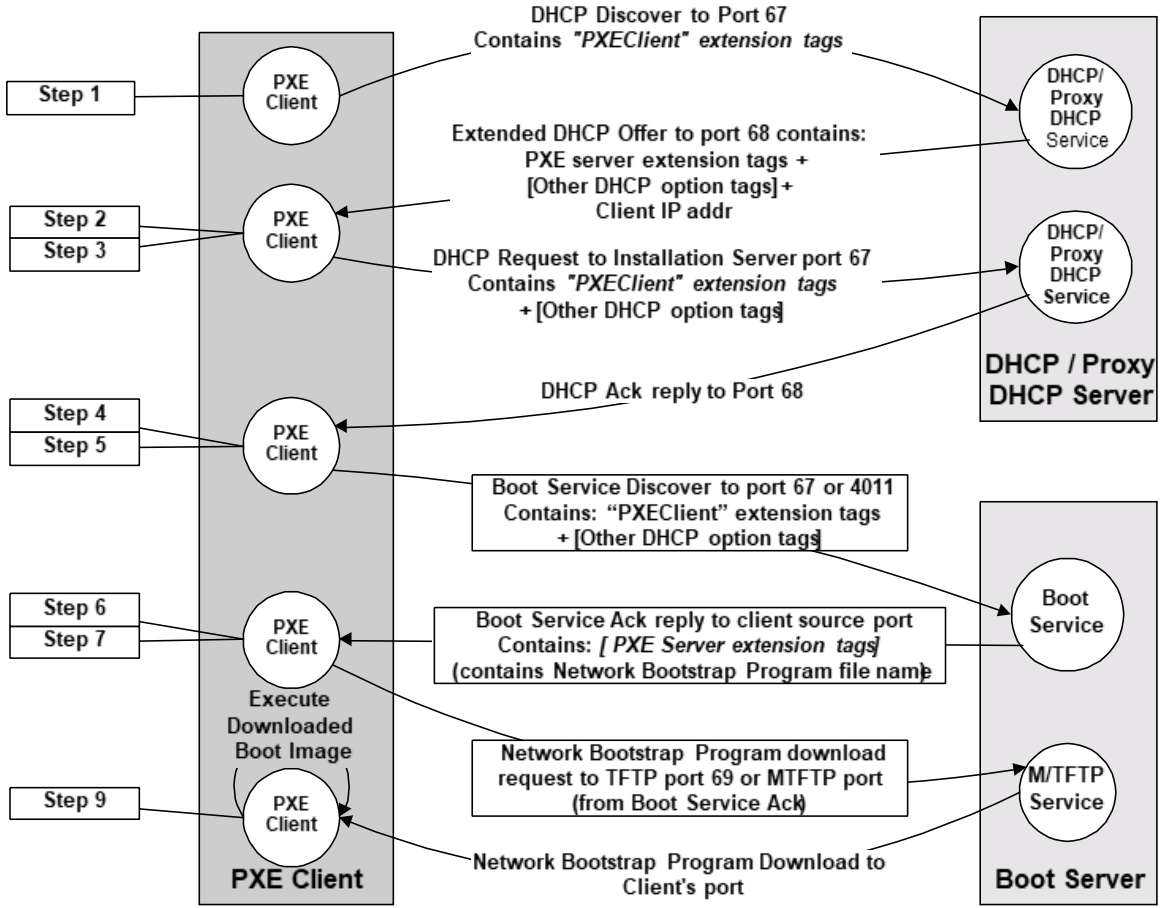
- Current State of Network Boot
- Limitations with the Legacy Model
- Modernizing Network Boot
- Use Cases for HTTP(S) Boot
- Call to Action

# Current State of Network Boot

- Network client is Booted to a server on a local network.
- Boot based on Pre-Boot Execution Environment or PXE (defined by Wired for Management or WfM in the 1990's).
- Architecture is based on the 16-bit Basic Input/Output System (BIOS).
- Requires a network controller to provide a low-level driver based on the Universal Network Device Interface (UNDI) format.

# PXE Boot


PXE Client 1
DHCP Server
switch
PXE Client 2
PXE Boot Server


Step 1
Step 2
Step 3
Step 4
Step 5
Step 6
Step 7
Step 9
PXE Client
PXE Client
PXE Client
PXE Client
Execute Downloaded Boot Image
PXE Client
PXE Client
DHCP Discover to Port 67
Contains "PXEClient" extension tags
Extended DHCP Offer to port 68 contains:
PXE server extension tags +
[Other DHCP option tags] +
Client IP addr
DHCP Request to Installation Server port 67
Contains "PXEClient" extension tags
+ [Other DHCP option tags]
DHCP Ack reply to Port 68
Boot Service Discover to port 67 or 4011
Contains: "PXEClient" extension tags
+ [Other DHCP option tags]
Boot Service Ack reply to client source port
Contains: [ PXE Server extension tags]
(contains Network Bootstrap Program file name)
Network Bootstrap Program download
request to TFTP port 69 or MTFTP port
(from Boot Service Ack)
Network Bootstrap Program Download to
Client's port
DHCP/ Proxy DHCP Service
DHCP/ Proxy DHCP Service
DHCP / Proxy DHCP Server
Boot Service
M/TFTP Service
Boot Server

# Limitations with the Legacy Model

- It doesn’t scale to large networks (limited to IPv4 & UDP).
- Must modify DHCP server to respond to PXE client queries.
- “Intranet”, not “Internet” - PXE server must be on same subnet or forward requests via proxy
- Router/Switch “fast learning spanning tree” may drop UDP packets.
- No security/authentication in PXE design.
- The first PXE server that responds will service the client (cannot specify server).

# Limitations with the Legacy Model

Legacy PXE is not designed for a “zero trust” network environment…
*“Zero Trust is a security concept centered on the belief that organizations should not automatically trust anything inside or outside its perimeters and instead must verify anything and everything trying to connect to its systems before granting access.”*
– *CSO Online, Jan 2018*

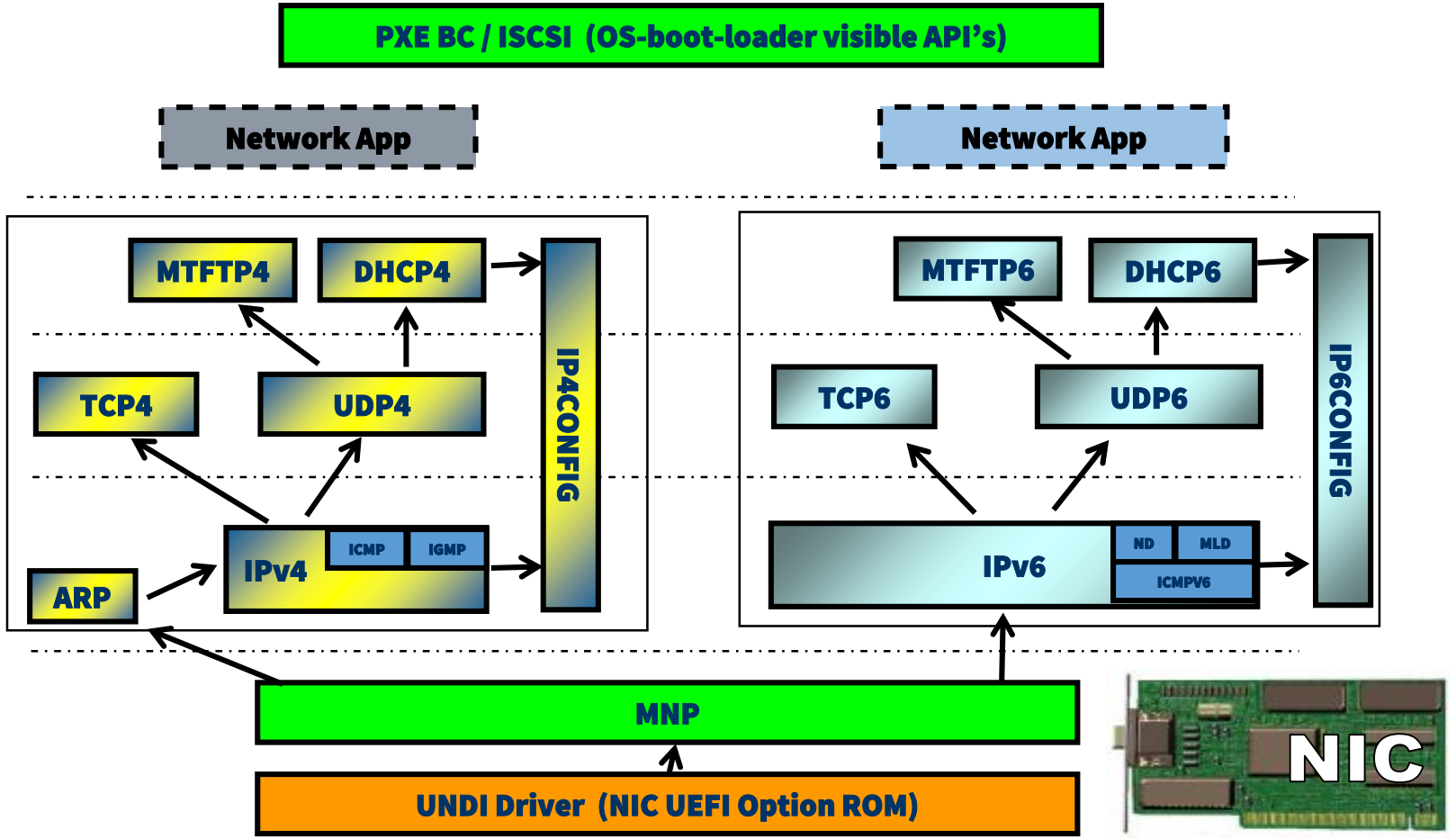
- Router/Sw… …g spanning tree” may drop UDP packets.
- No security/authentication in PXE design.
- The first PXE server that responds will service the client (cannot specify server).

# Modernizing Network Boot

The Unified Extensible Firmware Interface (UEFI) Specification introduces a number of improvements over the Legacy BIOS PXE.

- UEFI Networking Model.
- UEFI Network Boot via PXE.
- UEFI Secure Boot.
- UEFI Network Boot via HTTP/HTTPS.

# UEFI 2.3.1+ Networking Model: IPv4 and IPv6



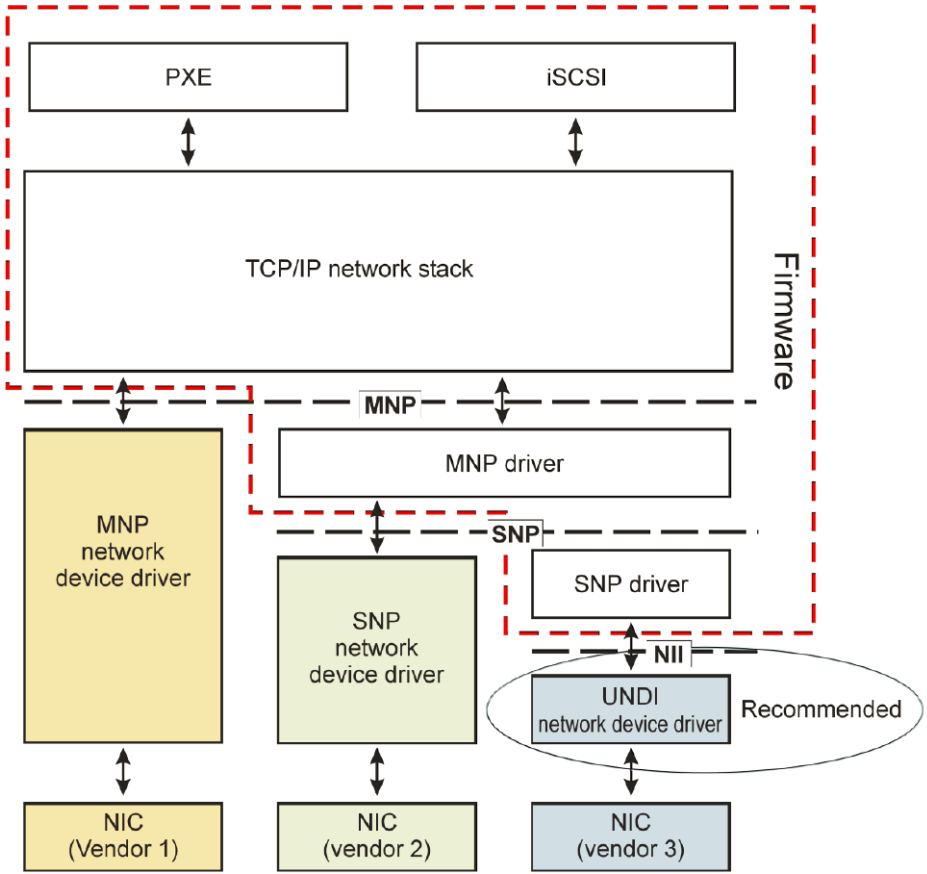
# UEFI 2.3.1+ Network Stack (PXE and iSCSI)

**Application**

**Transport**

**Internet**

**Network Interface**



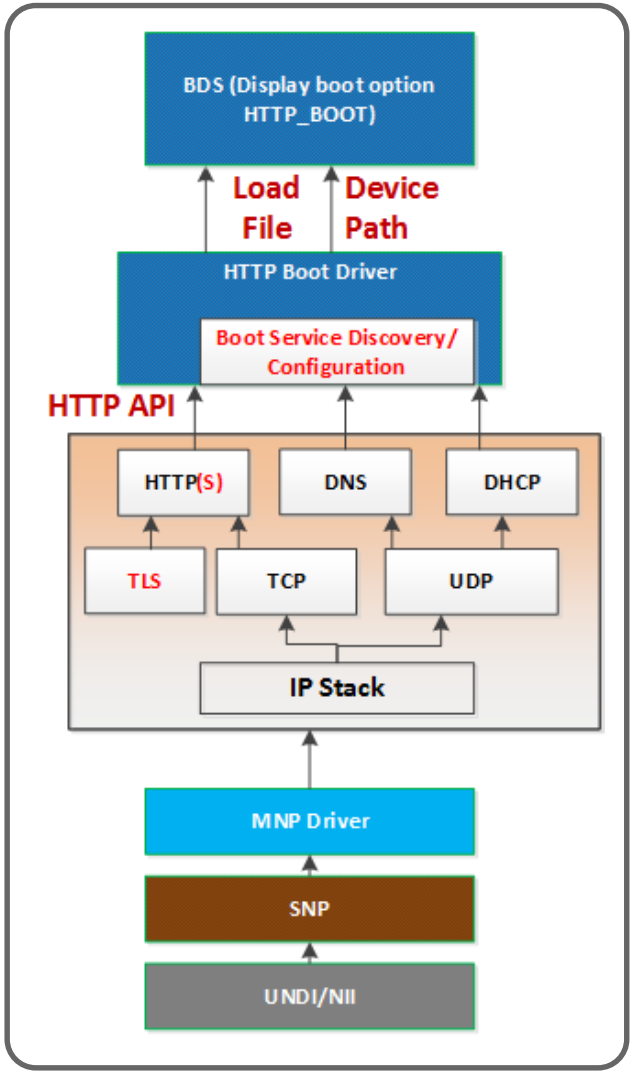
# UEFI Network Boot via PXE

- UEFI Network Boot was initially based on the PXE model.
- Added IPV6 & iSCSI/TCP features to existing IPv4 services.
- UEFI Secure Boot can provide a layer of authentication for PXE (signed bootloader, verified by certificates on client firmware).
- However… *none of the PXE limitations listed earlier are resolved by UEFI because they're part of PXE architecture (unencrypted traffic via UDP).*

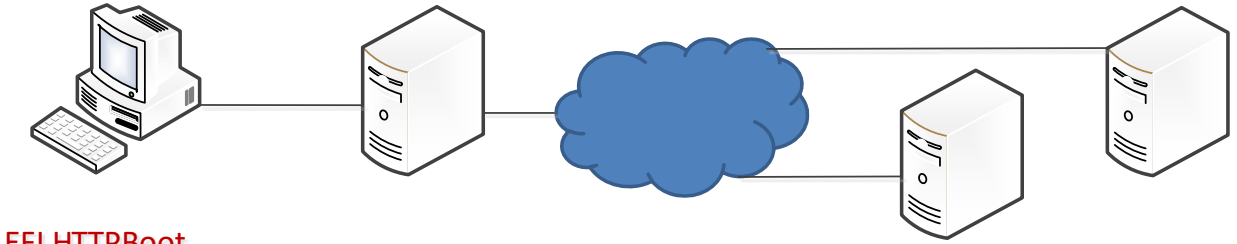
# UEFI 2.5 HTTP(S) Boot from URL/filename

| Driver | Library |
|---|---|
| HTTP Boot Driver<br>HTTP Driver<br>HTTP Utilities Driver<br>TLS Driver | HTTP Library<br>TlsLib Library<br>OpenslTlsLib Library |

- **Flexible Network Deployment**
- **Home Environment Support**
- **Corporate Environment Support**



# HTTP(S) Boot Flow



EFI HTTPBoot Client

DHCP Server

DNS Server

HTTP(S) Server

DHCP: address config

DNS: Host name resolution

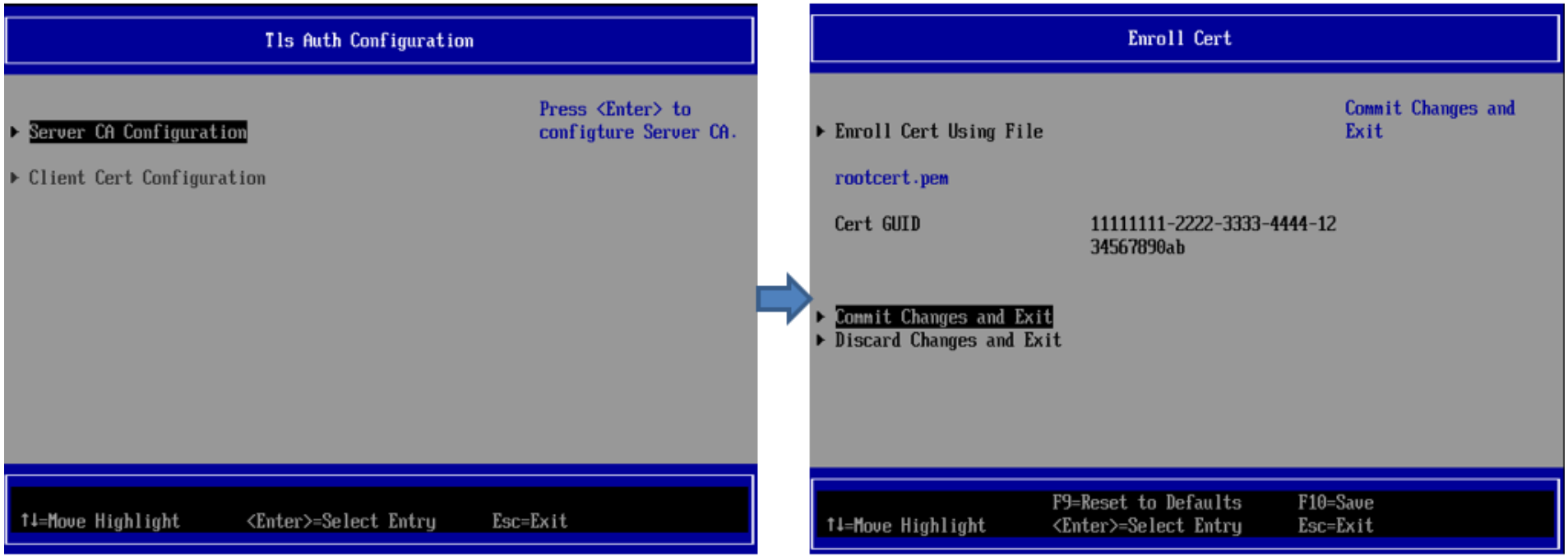
HTTP: 1). Get NBP file size 2). Download NBP file

Booted!

# HTTP(S) Boot via UEFI Firmware

- Boot file URL, using IP address or DNS (i.e. www.xyz.com/bootme.efi).
- Works on any network topology supporting TCP & HTTP(S).
- Supports IPv4/IPv6, not limited to a single subnet.
- Supports UEFI Secure Boot for additional verification.
- HTTPS only allows URLs that can be verified via client certificates.
- Combine with RAMDisk to download package to local file system.

# Putting the ‘S’ in HTTPS: Enrolling Certificates




Currently, UEFI HTTPS Boot only supports server authentication with an unauthenticated client. This requires enrolling a Server CA certificate (**`rootcert.pem`**) on the Client prior to boot.

*Reference: Getting Started with UEFI HTTPS Boot on EDK II*

# Use Cases for HTTP(S) Boot

- Install/deployment of OS (with default ISO, if using RAMDisk).
- Firmware update without an OS (via UEFI Capsule Update).
- System recovery from LAN or cloud storage.
- Diskless systems boot to OS via HTTPS (blade, thin client, …).

*Use cases are extended beyond traditional “trust boundaries”*

# Distributions that support install via UEFI HTTP(S)

*Can install SUSE or openSUSE from a host server via UEFI HTTPS*

- openSUSE 42.3 - HTTPS
- SUSE SLES 15 - HTTPS
- SUSE SLES 12 SP3 - HTTP (no HTTPS at this time)


# DEMO

# Call to Action

Upgrade from legacy PXE boot to address “zero trust” model

Investigate UEFI Secure Boot & HTTP(S) boot implementations

Review openSUSE documentation for HTTP(S) configuration

# Resources and References

https://github.com/tianocore/tianocore.github.io/wiki/HTTPS-Boot

https://www.tianocore.org/

https://www.uefi.org

Thanks to Harry Hsiung (Intel) for setting up the demo system.

Thanks to Gary Lin and Joey Lee (SUSE) for their work on UEFI support in SUSE/openSUSE and the related HTTP/HTTPS documentation.

# UEFI HTTP(S) Installation Instructions

Setup UEFI HTTPS boot in OVMF (virtual environment)
https://en.opensuse.org/UEFI_HTTPBoot_with_OVMF

Setup UEFI HTTPS for Physical Host Server
https://en.opensuse.org/UEFI_HTTPBoot_Server_Setup

HTTP/HTTPS Boot Getting Started Guide for EDK II
https://legacy.gitbook.com/book/edk2-docs/getting-started-guide-of-edk-ii-http-boot
https://legacy.gitbook.com/book/edk2-docs/getting-started-with-uefi-https-boot-on-edk-ii/

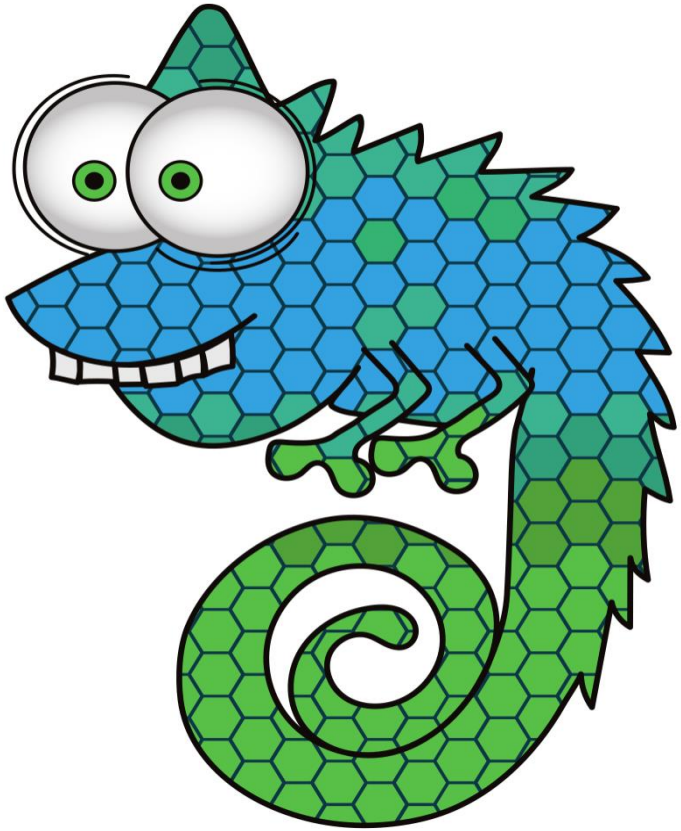
# Information on UEFI Systems with HTTP(S)

Information on HTTP(S) Boot in EDK II
https://github.com/tianocore/tianocore.github.io/wiki/HTTP-Boot
https://github.com/tianocore/tianocore.github.io/wiki/HTTPS-Boot

EDK II Open Virtual Machine Firmware (OVMF)
https://github.com/tianocore/tianocore.github.io/wiki/OVMF

MinnowBoard Max Turbot (support included in firmware images)
https://firmware.intel.com/projects/minnowboard-max

Hewlett Packard Enterprise* Proliant Gen10 servers
https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-a00016376en_us



Join Us at www.opensuse.org

## License



## General Disclaimer



## Credits

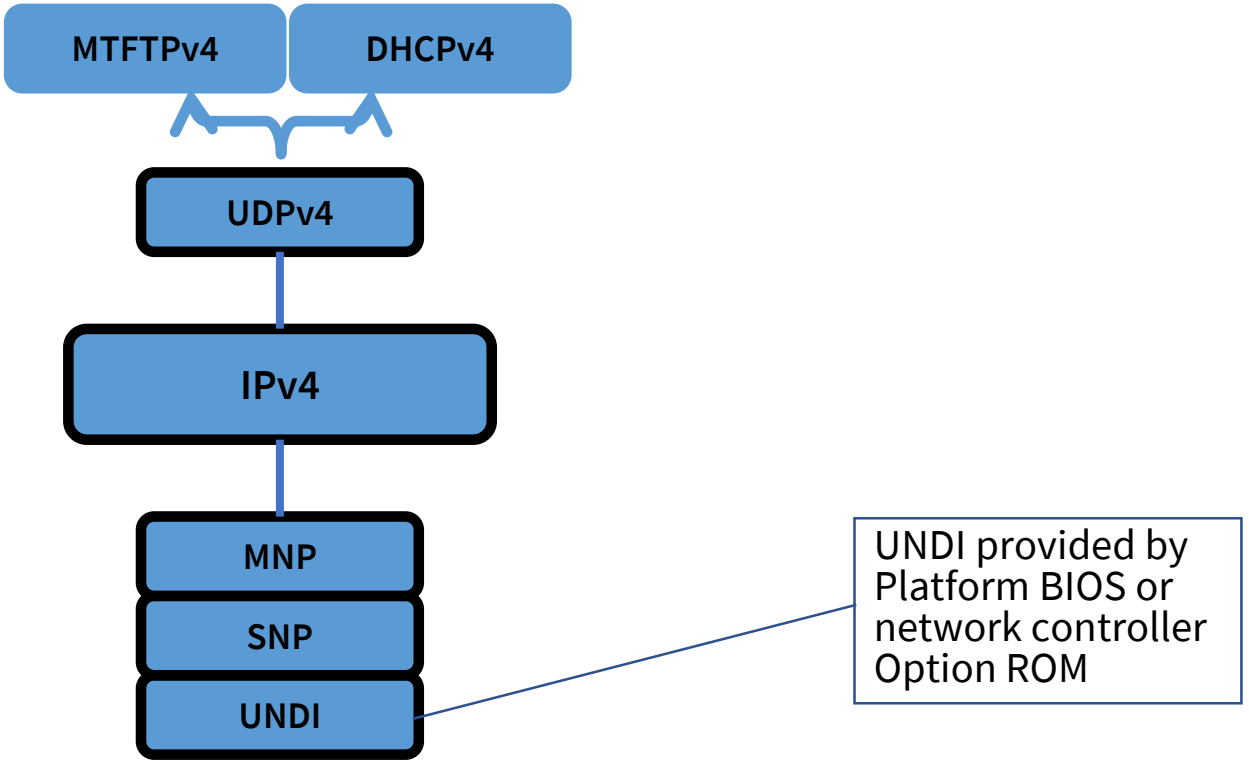
**Template**
Richard Brown
rbrown@opensuse.org

**Design & Inspiration**
openSUSE Design Team
http://opensuse.github.io/branding-guidelines/

# Glossary

- IPv4 - Internet Protocol version 4
- UDP - User Datagram Protocol
- HTTP - Hypertext Transfer Protocol
- HTTPS - Hypertext Transfer Protocol Secure
- ISCSI – Internet Small Computer Systems Interface
- MTFTP – Multicast Trivial File Transfer Protocol
- DHCP – Dynamic Host Configuration Protocol
- TCP – Transmission Control Protocol
- ARP – Address Resolution Protocol
- MNP – Microcom Networking Protocol
- NIC – Network Interface Controller
- SNP – Scalable Networking Pack
- TCP/IP – Transmission Control Protocol/Internet Protocol
- TFTP – Trivial File Transfer Protocol
- TLS – Transport Layer Security
- BDS – Boot Device Selection
- URL – Uniform Resource Locator
- NII – Network Independent Interface
- ISO - International Organization for Standardization

# Backup - Legacy PXE Stack Overview



Unified Extensible Firmware Interface Forum

Member Pages

# Member Event: Spring 2019 UEFI Plugfest

April 8-12, 2019

Embassy Suites by Hilton Seattle Bellevue Bellevue, WA

All UEFI members are welcome to attend testing sessions, technical sessions, and networking events.

For more information go to the events page

To Join UEFI Forum go to the membership page


https://uefi.org/events/