Network Station Manager Version 2 Release 1

The Boot Process

Network Station Education
IBM NCD
August 1999

Objectives/Summary

- **Provide a high-level overview of the Network Station boot process**
  - What are the basic Network Station Components?
  - How does the Network Station obtain it's operational software?
  - What are the different methods of booting?
  - How does a Network Station locate a boot server?
  - What files need to be downloaded?
  - What is the sequence of events?
  - What are Boot servers and Application servers?

Notes

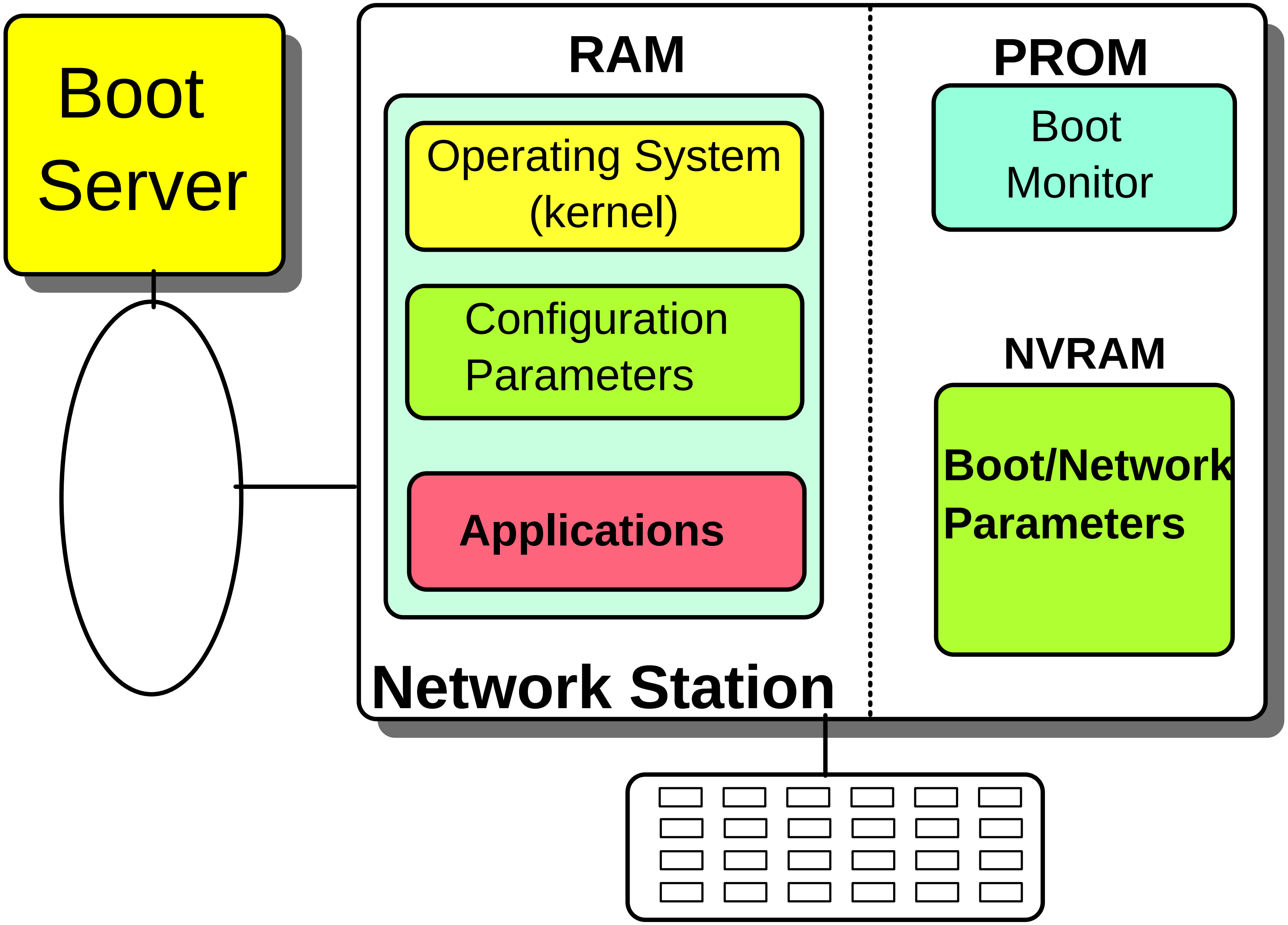
The objective of this presentation is to provide a high-level overview of the Network Station boot process. This is meant mainly for those who have not been exposed to this topic before and who are unfamiliar with a thin client or Network Station.

This presentation has not changed much since the last version because the concepts really have not changed. There are just a few slight differences and maybe a few new charts, but most of the charts are the same.

We take a look at the basic Network Station components and the steps that are required for a station to become operational.

Many of these individual components or processes are covered in a lot more details, when necessary, in other presentations on this CD or in the supplied redbooks and product publications.

Network Station Components



Notes

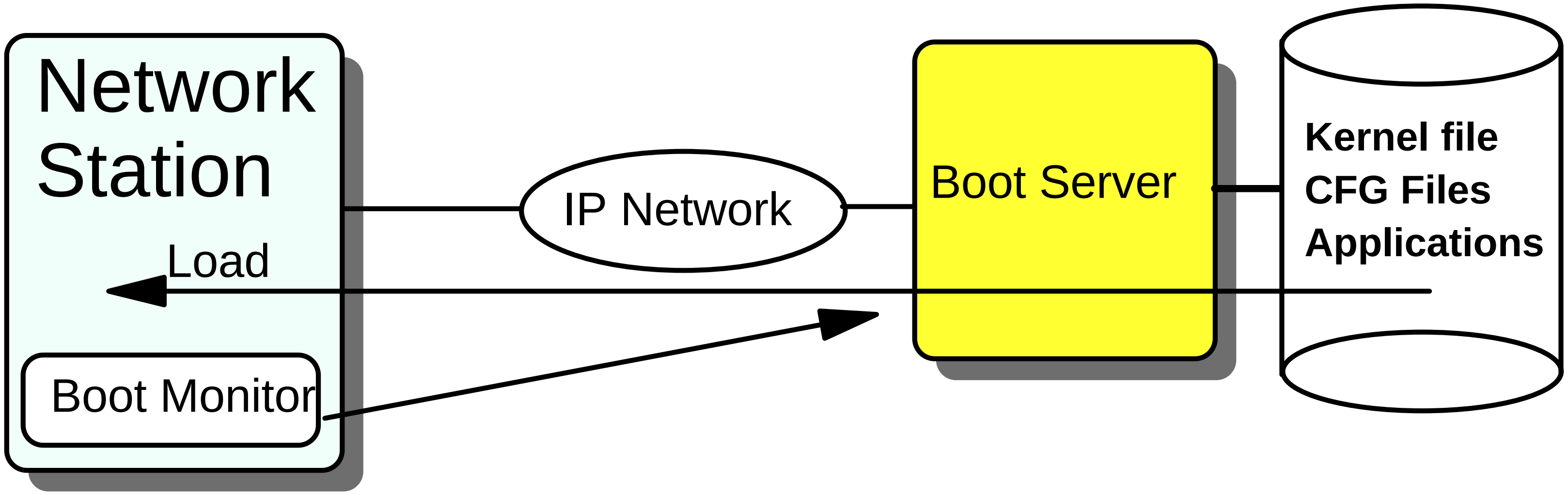
This chart illustrates the basic Network Station components.

- The Boot prom contains a copy of the boot monitor, which is the essential component required to get the station started in its boot process

- The nonvolatile RAM (NVRAM) is used to store some of the configuration parameters that are to be retained between power offs and power ons of the station.

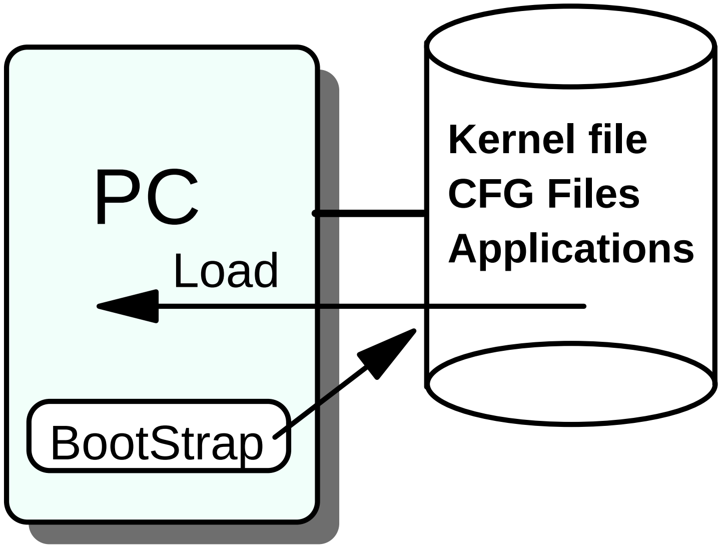
- Then comes the RAM, that contains
  - the operating system that has been downloaded from a server o the network
  - additional configuration parameters that are downloaded from servers on the network
  - applications, also downloaded from a server, as they are started by a user

Traditional PC vs Network Station Boot



- **For a PC, the boot process involves loading files from a local disk**

- **For a Network Station, the boot process involves loading files from a remote disk**



Notes

The process of starting a Network Station is really not very different from starting a PC.

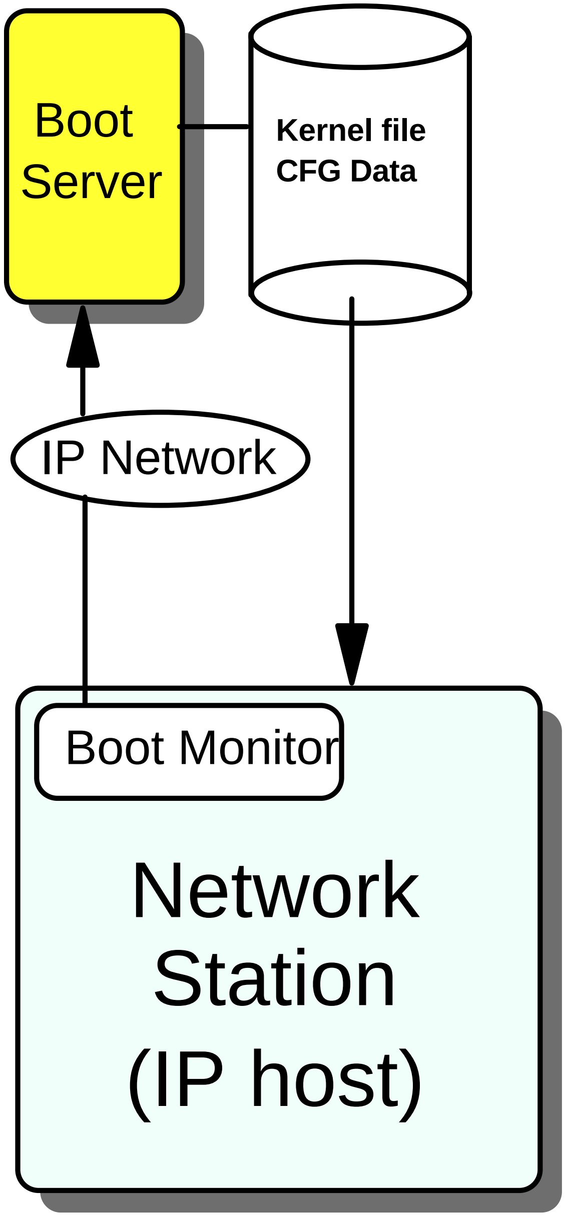
This chart illustrates the differences and similarities. In the bottom right hand corner, when a PC is powered on, a small piece of code called a bootstrap, located on a local disk, is executed and knows to load an operating system from the local disk.

On a Network Station, the equivalent of the bootstrap code is the boot monitor code, and instead of residing on a local drive, it resides in a PROM chip.

When the boot monitor code is given control, it fetches an operating system, but instead of loading it from a local disk, it fetches it from a remote disk. What that means is that the boot monitor code must be a little more sophisticated than a bootstrap code because it needs to be able to connect to a server over a network before it can fetch an operating system, but the generic function and concept is basically the same.

Network Station Initialization Phases

- **Four Phases**
  - Power-on Self Tests (**POST**)
  - **Boot**
    - Locate a boot server
    - Download an Operating System (kernel)
  - **Customization**
    - Download Terminal Configuration data
  - User **Logon**
    - Validate the user
    - Download user and group specific configuration data



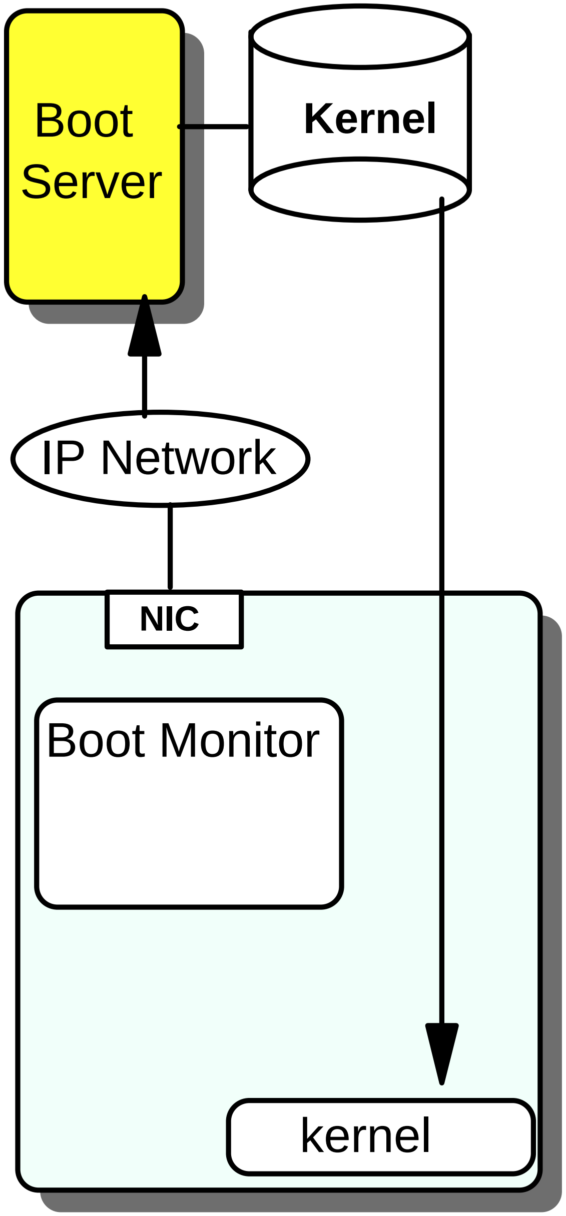
Notes

The network station's initialization process can be broken down into four phases:

- The Power-on Self Tests (POST) phase that verifies all the internal circuitry
- The boot phase which locates a boot server and download an Operating System (kernel)
- The customization phase that download Terminal Configuration data
- The user login phase that validates the user and download user and group specific configuration data

What is the Boot Monitor (Boot Code)?

- A Program that resides permanently in the Network Station's nonvolatile memory (NVRAM)
- Is given control after the Power-On Self tests have completed
- Its responsibilities are to:
  - Open the network interface card (Token-Ring or Ethernet adapter)
  - Locate a Boot server
  - Contact the boot server to get its operating system (kernel)
  - Hand over control to the kernel and remove itself from memory



Notes

The boot monitor is a program that resides permanently in the Network Station's nonvolatile memory (NVRAM) and that is given control after the Power-On Self tests have completed.

Its main responsibilities are to:

- Open the network interface card
- Locate a Boot server
- Contact the boot server to get its operating system (kernel)
- Hand over control to the kernel and remove itself from memory

If its process is interrupted after the Power on self tests are completed (by using the ESC key), it also presents a graphical interface that allows an administrator to enter configuration parameters into NVRAM, as well as to perform problem determination tasks if necessary.

How to Locate Servers?

- **Extract the configuration data from the local NVRAM. This data includes:**
  - **It's own IP address**
  - **The IP address of a boot server**
  - **The address of a gateway**
  - **The Protocol to use, etc.**
- **Send a broadcast on the network to find a DHCP or a BOOTP server that will supply this same configuration data**
  - This is the PREFERRED method
  - DHCP is preferred over BOOTP (more flexible)

Notes

How does the station initially locate a server?

There are a couple of methods that can be used:

- If the administrator has used the boot monitor's interactive configuration interface to enter configuration data in NVRAM, the station can be directed to read its data from NVRAM. THis is why this is called an NVRAM boot.

- Or the station can be directed (this is also an NVRAM parameter) to issue a broadcast on the network looking for a DHCP server that will provide it with the same configuration information that the administrator would enter in NVRAM .

This second method is the preferred and recommended method because it is a lot more flexible and lends itself to centralized management of a network of stations.

User LOGON

- User login panel is displayed
- Login client contacts the Network Station Login Daemon on the authentication server
- User must be part of NSMUser group on the authentication server
- Triggers the choice of user and group preferences
  - For desktop appearance such as background color, or launchbar icons
  - For automatic startup of applications

Notes

Next is the user login phase that starts with the display of a panel so that the user can enter a user name and password.

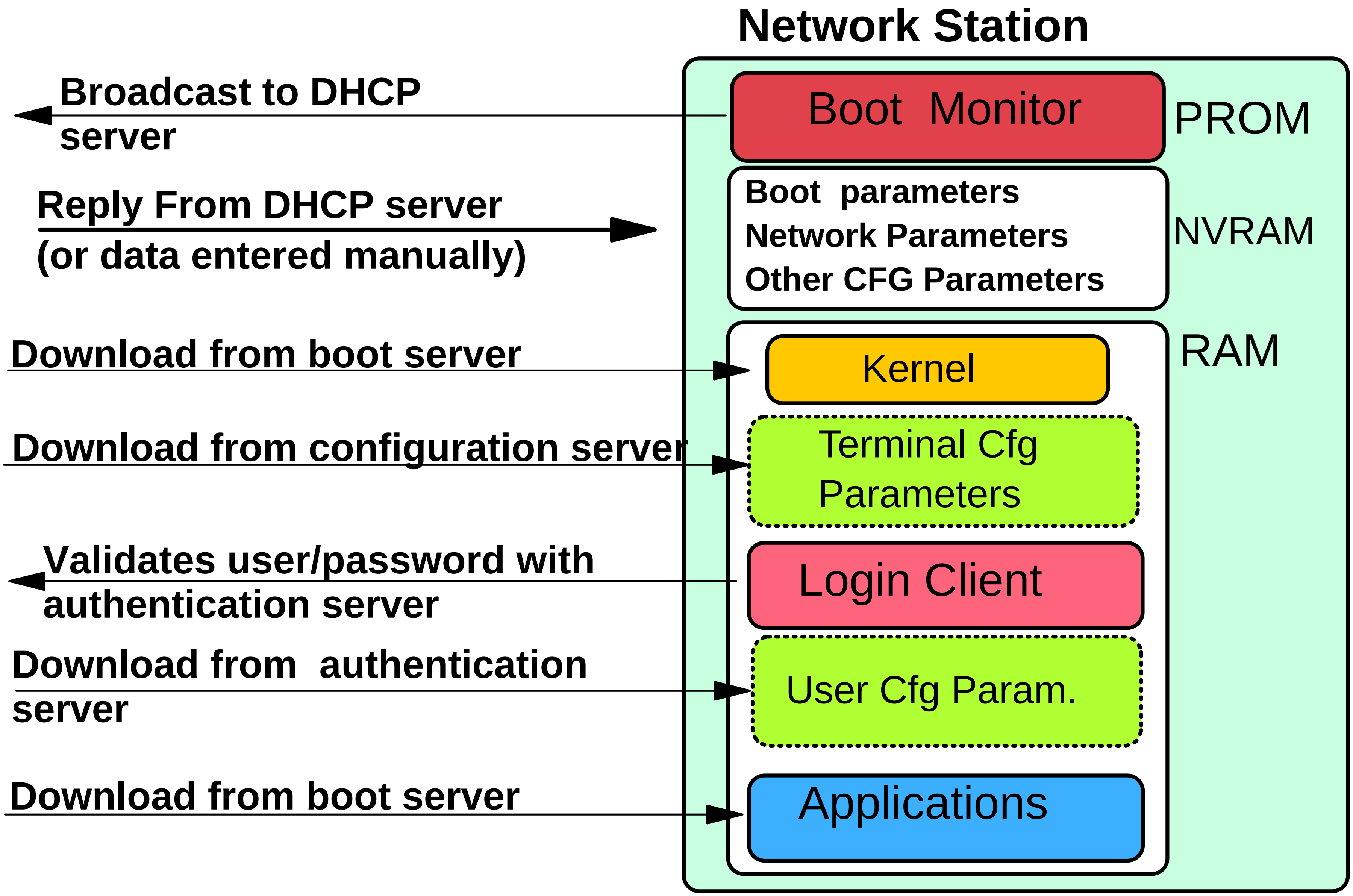
There are exceptions to this process when the station is configured to operate in kiosk mode. See the kiosk presentation for more details.

Once the user name and password is entered, the login client on the station contacts the Network Station Login Daemon on an authentication server.

Note that the user must be part of NSMUser group on the authentication server to be allowed to login.

Once the user is known, this triggers the choice of user and group preferences for desktop appearance such as background color, or launchbar icons and for automatic startup of applications.

Summary - Boot Sequence



Network Station

Broadcast to DHCP server

Reply From DHCP server (or data entered manually)

Download from boot server

Download from configuration server

Validates user/password with authentication server

Download from authentication server

Download from boot server

Boot Monitor

PROM

Boot parameters
Network Parameters
Other CFG Parameters

NVRAM

RAM

Kernel

Terminal Cfg Parameters

Login Client

User Cfg Param.

Applications

Notes

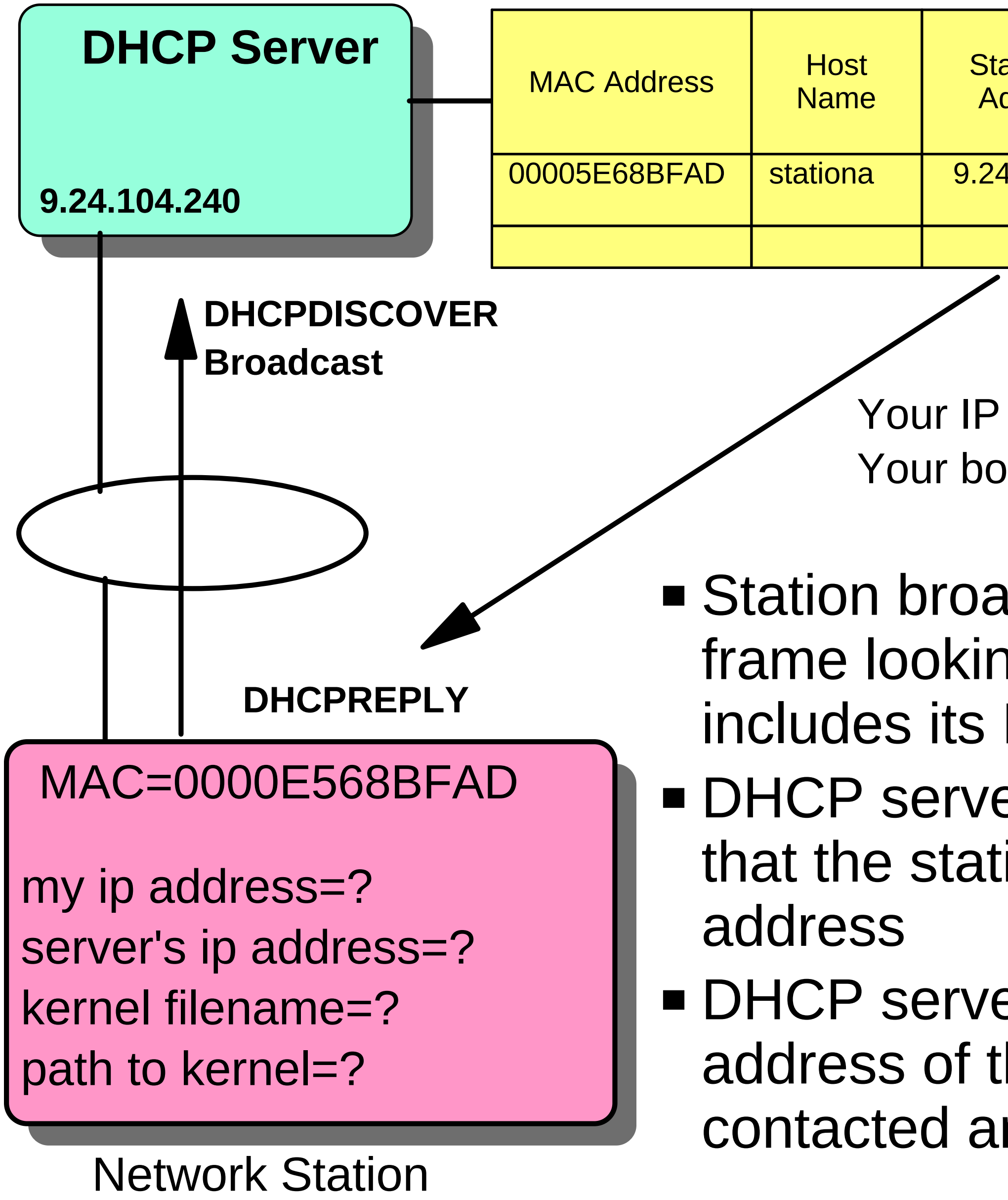
This summarizes and recaps the boot process in a simplified fashion.

- The boot monitor finds a DHCP server and obtains required configuration data from that server.
- If DHCP is not used, the same data was entered manually by an administrator in the station's NVRAM
- Using this configuration data, the station contacts a boot server and downloads its operating system
- It then obtains additional terminal configuration data from a configuration server
- The login client then validates the user with an authentication server and user specific configuration data is downloaded from that server
- Applications are finally downloaded from a boot server either as they are autostarted or as the user requests them.

Example - Locate a Server Using DHCP

DHCP CONFIGURATION FILE

MAC Address	Host Name	Station IP Address	Boot Server IP Address	Kernel Path	Kernel File
00005E68BFAD	stationa	9.24.104.189	9.24.104.178	/prodbase /x86/	kernel. 2800



Your IP address is 9.24.104.189
Your boot server is 9.24.104.178, etc.

- Station broadcasts a DHCP DISCOVER frame looking for a DHCP server. It includes its MAC address as identification.
- DHCP server replies with the IP address that the station should use for its own address
- DHCP server also replies with the IP address of the boot server that should be contacted and the path to the kernel

Notes

This is an overview of the process in the case where DHCP is used.

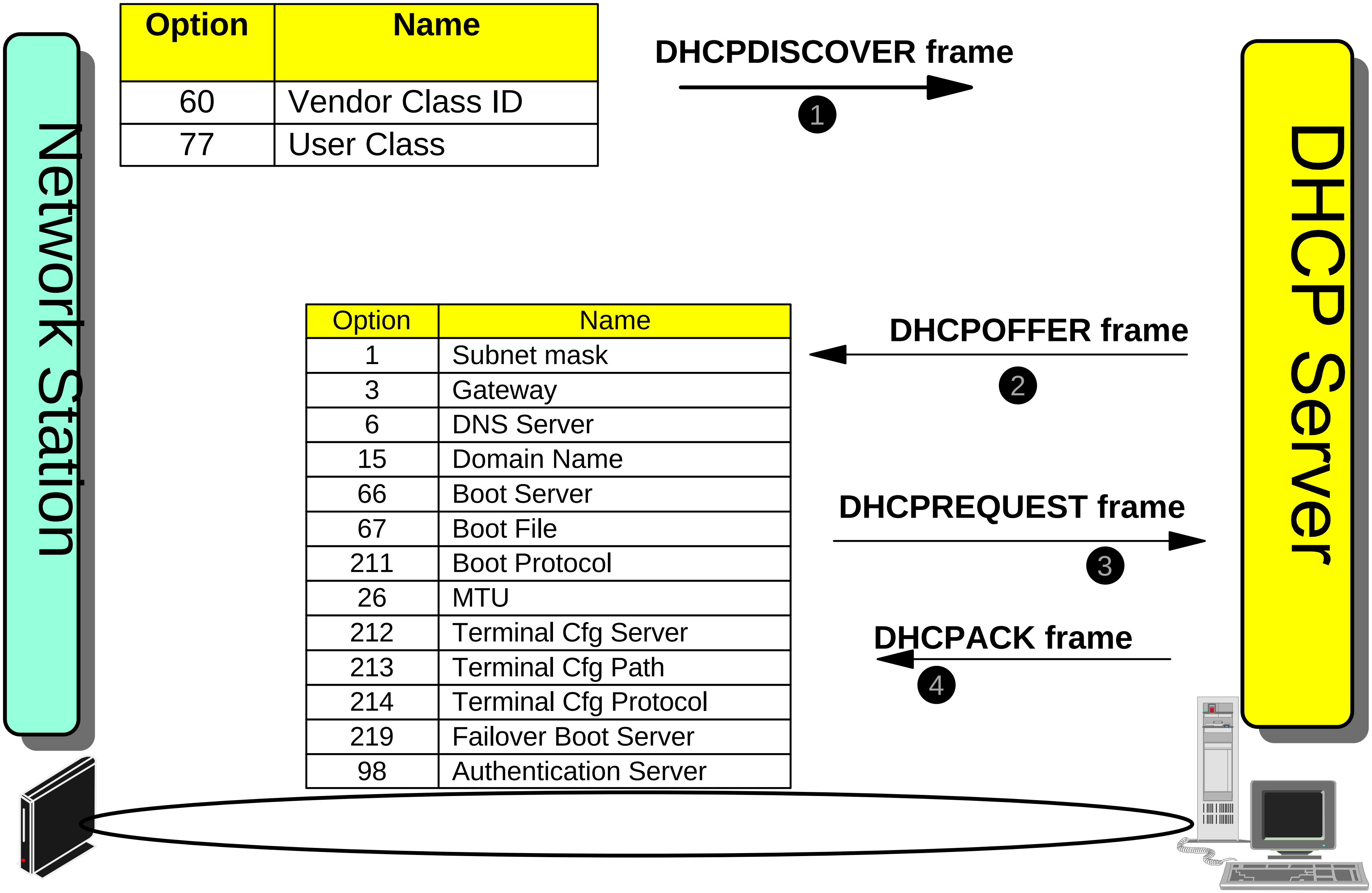
The station (a DHCP client) issues a DHCPDISCOVER broadcast, looking for a DHCP server that can respond with the type of configuration data that it needs. In the frame that it sends, the station includes its MAC address as an identifier.

Dependent on how it is configured, the DHCP server may or may not have a record that identifies this client specifically. In this example, it does have a client record, and that record indicates the IP address that is reserved for that client (in this case, 9.24.104.189).

The DHCP server replies to the client, giving it the IP address that it should use but also the address of the boot server that it should contact and the name and location of the kernel file that it should download.

There are a few other pieces of information also sent, such as the subnet mask, gateway address, etc. that provides the station with all the data it needs to proceed with its boot process and download its operating system.

DHCP Options Request



Option	Name
60	Vendor Class ID
77	User Class

Option	Name
1	Subnet mask
3	Gateway
6	DNS Server
15	Domain Name
66	Boot Server
67	Boot File
211	Boot Protocol
26	MTU
212	Terminal Cfg Server
213	Terminal Cfg Path
214	Terminal Cfg Protocol
219	Failover Boot Server
98	Authentication Server

Network Station

DHCP Server

DHCPDISCOVER frame 1

DHCPOFFER frame 2

DHCPREQUEST frame 3

DHCPACK frame 4

Notes

Without entering into too many details, here is another look at some of the exchanges that takes place between the station and the DHCP server.

It is important to note, especially for a Network Station as we will see in a moment, the a Network Station has the ability to use DHCP classes.

In the DHCPDISCOVER frame that the station broadcasts initially, it can also include, in addition to its MAC address, a vendor class and a user class that further identifies this particular client.

When the DHCP server initially responds with an offer (2), there are lots of options that can be included, as listed here in this diagram. All of these are those typically used by a Network Station.

The station then sends a DHCP request to indicate its acceptance of the offer after which the server confirms it with a DHCP acknowledge.

DHCP Options Used by the Network Station

Option Number	Name	R3 Boot Code	V2R1 Boot Code	NVRAM
1*	Subnet mask	Y	Y	Y
3*	Gateway	Y	Y	Y
6*	Domain Name Server	Y	Y	Y
15*	Domain Name	Y	Y	Y
66*	Boot Server (or LOCAL)	Y	Y	Y
67*	Boot File (or MCF)	Y	Y	Y
211*	Boot Protocol	Y	Y	Y
26	Max Transmission Unit (MTU)	N	Y	Y
212	Terminal Config Server	Y	Y	Y
213	Terminal Config Path	Y	Y	Y
214	Terminal Config Protocol	Y	Y	Y
219	Failover Boot Server	N	Y	Y
98	Authentication Server	N	Y	Y

* = Required

Notes

This chart lists the options commonly used by the Network Station.

As opposed to regular PCs which typically only require an IP address and subnet mask and possibly a few other, a Network Station, in addition to those, also requires the addresses of the different servers that it needs to contact in order to get its kernel and its configuration files.

This chart also identifies the DHCP options that are new with V2R1. Those are:

- The MTU size
- An alternate address for the boot server in case the first server is not available
- An authentication server address

If you are unfamiliar with these different servers, please review the Archictecture, Planning and Design and the Separaration of servers presentations.

Vendor and User Class

- **Vendor Class ID (DHCP Option 60)**
  - Used by DHCP Clients to identify their vendor type and configuration
  - Server responds with option 43 that may contain an encapsulated string of information that the client must parse
  - Example: The Network Station Vendor Class can be
    - IBM Network Station (for Series 100, 300 and 1000)
    - IBM Network Station X86 (for Series 2200 and 2800)

- **User Class (DHCP Option 77)**
  - Used by DHCP Clients to identify their category of user or application
  - Server responds with a set of options corresponding to the user class (if DHCP server supports classes)
  - Example: The User Class is "IBMNSM 2.0.0" for an 8361-100 (Series 100 Ethernet 8MB Network Station)

Notes

These options are useful in the case of a Network Station, and even more so now that we have different models and families of Network Stations.

The Vendor Class ID (DHCP Option 60) is used by DHCP Clients to identify their vendor type and configuration. The server responds with option 43 that may contain an encapsulated string of information that the client must parse.

For example: The Network Station Vendor Class can be IBM Network Station (for Series 100, 300 and 1000) or IBM Network Station X86 (for Series 2200 and 2800)

Even more important is the user class (DHCP Option 77) because it allows clients to identify themselves more precisely. The server responds with a set of options corresponding to the user class (if the DHCP server supports classes). For example, the User Class is "IBMNSM 2.0.0" for an 8361-100 (Series 100 Ethernet 8MB Network Station).

Network Station User Class

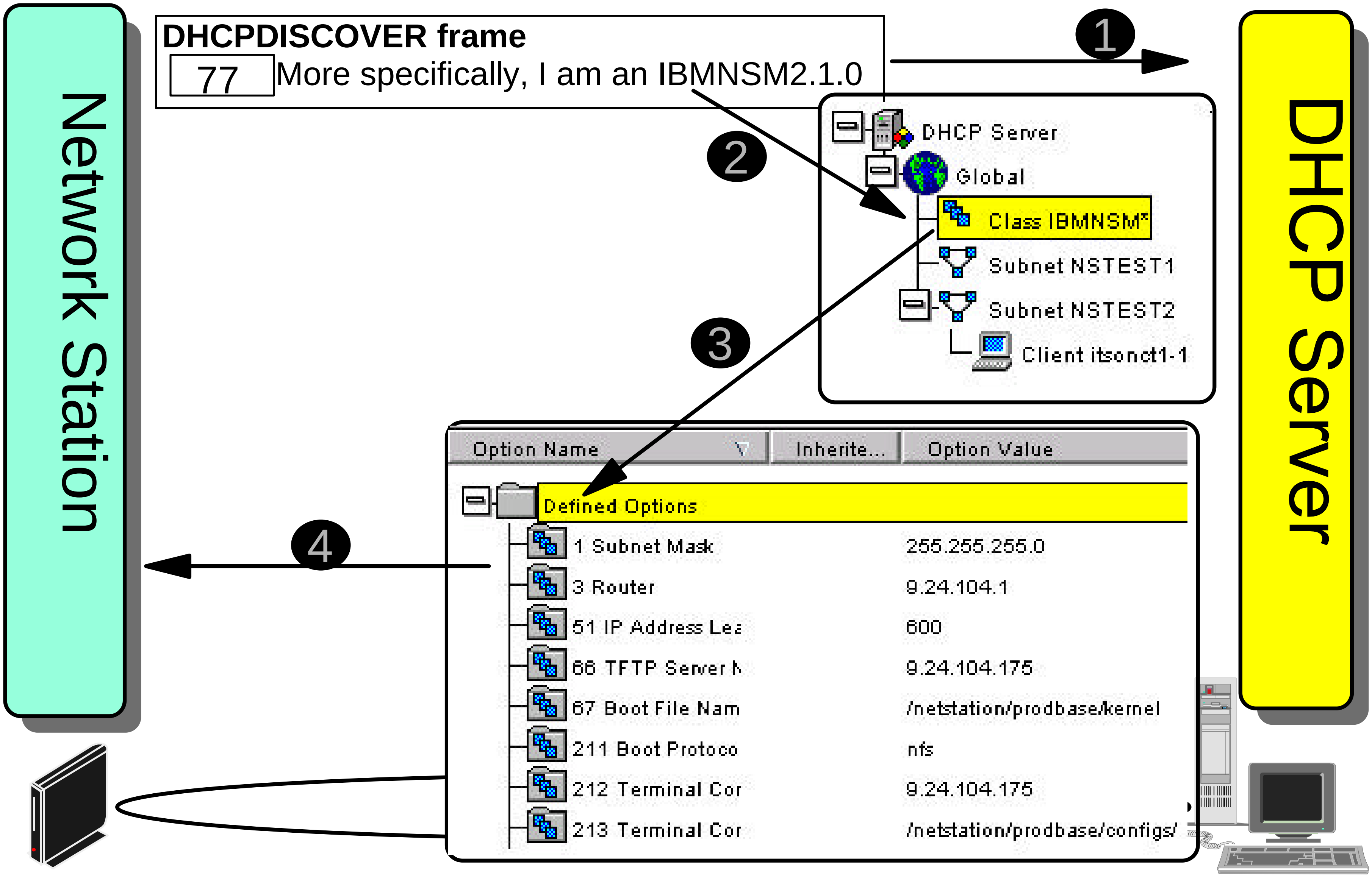
IBM Network Station Model	Description	User Class
8361-100	Series 100 - Ethernet - 8 MB	IBMNSM 2.0.0
8361-200	Series 100 - Token-Ring - 8 MB	IBMNSM 2.1.0
8361-110	Series 300 - Ethernet - 16 MB	IBMNSM 1.0.0
8361-210	Series 300 - Token-Ring - 16 MB	IBMNSM 1.1.0
8361-341	Series 300 - Twinax - 1 MB	IBMNSM 3.4.1
8361-A22	Series 1000/32 MB-TRN	IBMNSM A.2.0
8361-A23	Series 1000/64 MB -TRN	IBMNSM A.2.0
8361-A52	Series 1000/32 MB - ETH	IBMNSM A.5.0
8361-A53	Series 1000/64 MB - ETH	IBMNSM A.5.0
8363-Exx	Series 2200 - Ethernet	8363-EXX
8363-Txx	Series 2200 - Token-ring	8363-TXX
8364-Exx	Series 2800 - Ethernet	8364-EXX
8364-Txx	Series 2800 - Token-Ring	8364-TXX

Notes

This chart lists the user class that correspond to each model of the Network Station.

Let's take a look at how this can work.

User Class Configuration - DHCP Server



Option Name	Inherite...	Option Value
Defined Options		
1 Subnet Mask		255.255.255.0
3 Router		9.24.104.1
51 IP Address Lea		600
66 TFTP Server N		9.24.104.175
67 Boot File Nam		/netstation/prodbase/kernel
211 Boot Protoco		nfs
212 Terminal Cor		9.24.104.175
213 Terminal Cor		/netstation/prodbase/configs/

Notes

In this example, the station sends in a DHCP discover frame (in 1) to request service from the DHCP server.

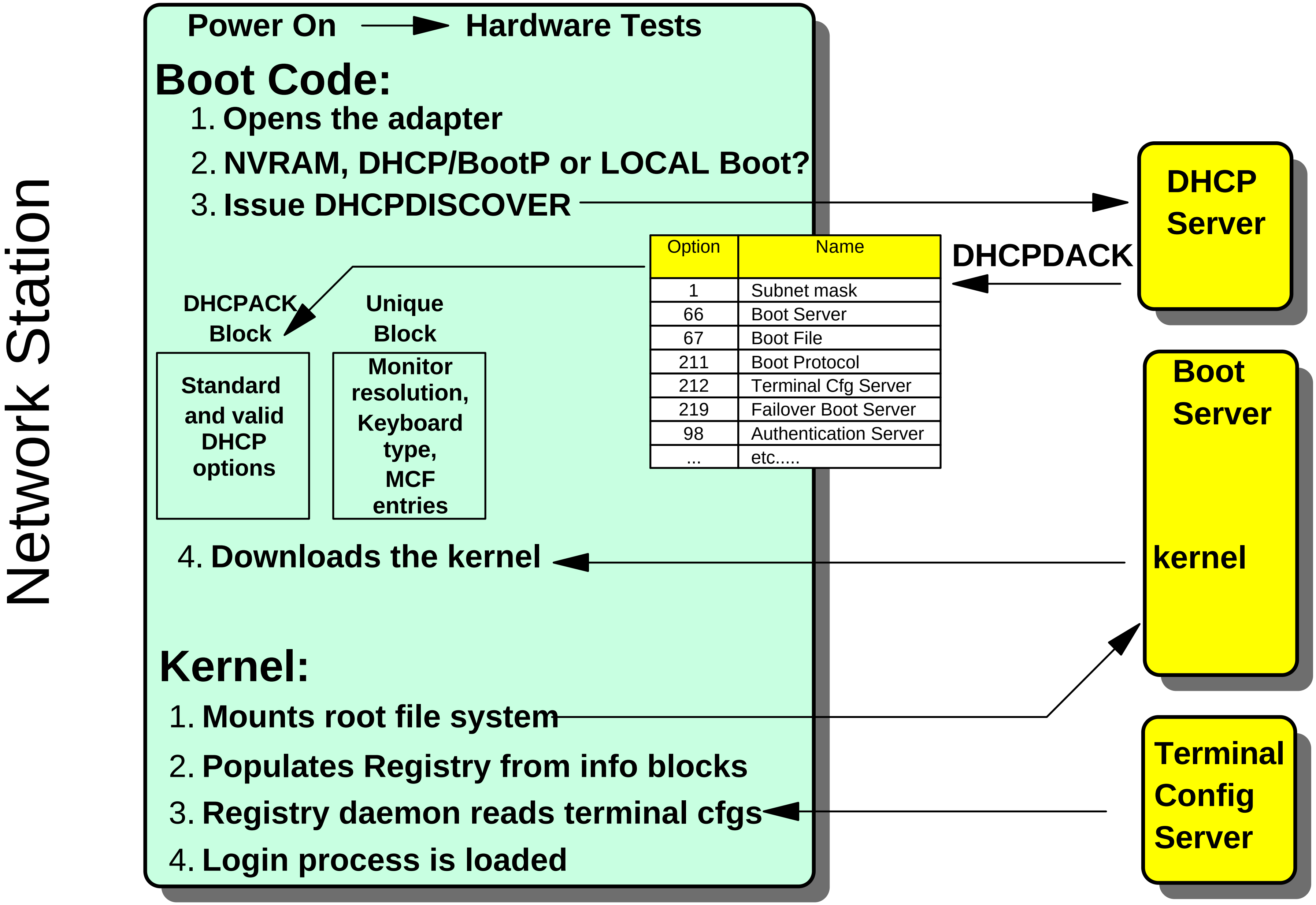
As part of that frame, it identifies itself (in 2) as belonging to the class IBMNSM2.1.0 which tells us that this a Series 100 Token ring 8MB station.

Notice that the DHCP server is configured with a class called IBMNSM* which actually includes all of the PPC models of the Network Station, so this particular client fits that particular class.

In (3), we see the DHCP options that are configured as part of that IBMNSM* class.

The frame that is returned to the client in (4) therefore contains all of the options for that class whereas these options would not be sent to a client that did not identify itself with a class.

Boot Flows



Network Station

Power On → Hardware Tests

Boot Code:

1. Opens the adapter
2. NVRAM, DHCP/BootP or LOCAL Boot?
3. Issue DHCPDISCOVER

DHCPACK Block

Standard and valid DHCP options

Unique Block

Monitor resolution, Keyboard type, MCF entries

Option	Name
1	Subnet mask
66	Boot Server
67	Boot File
211	Boot Protocol
212	Terminal Cfg Server
219	Failover Boot Server
98	Authentication Server
...	etc.....

4. Downloads the kernel

Kernel:

1. Mounts root file system
2. Populates Registry from info blocks
3. Registry daemon reads terminal cfgs
4. Login process is loaded

Notes

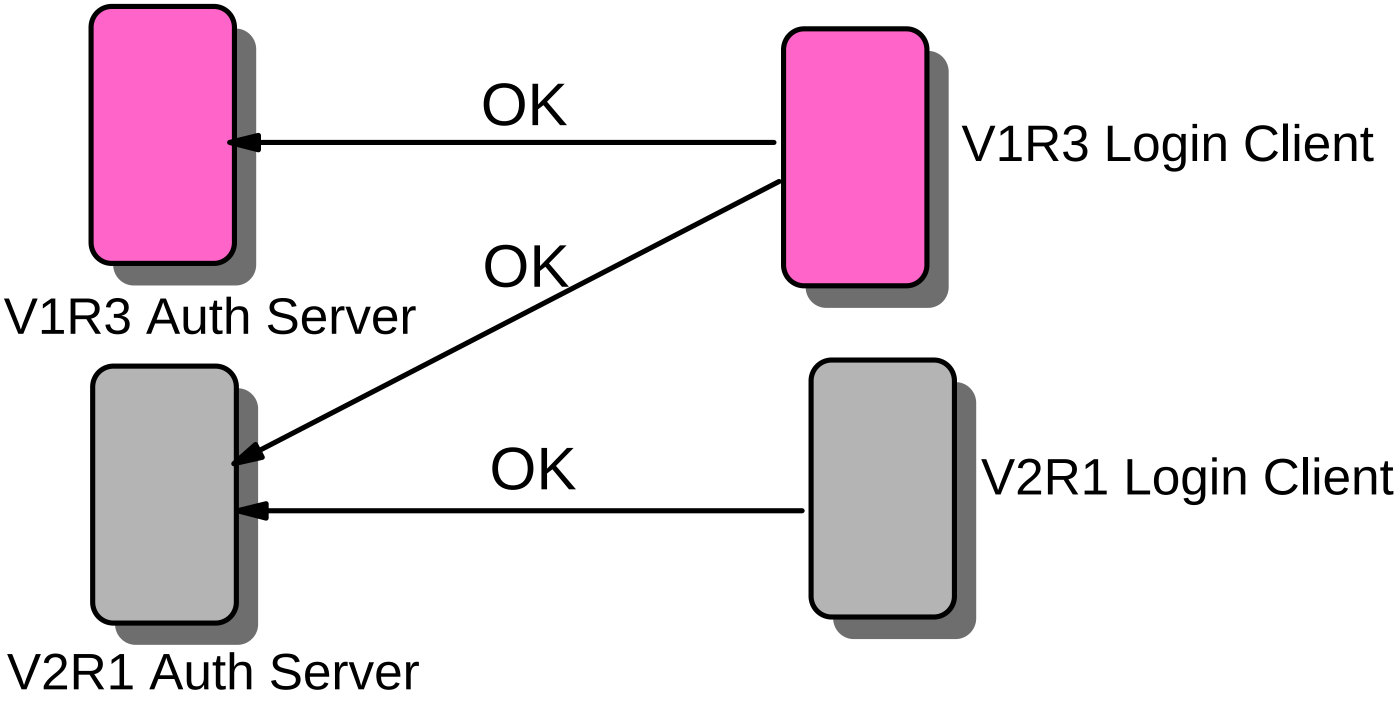
What happens after the client receives these options?

This chart sort of summarizes the boot flow process from the beginning, that is:

- The station is powered on
- The POST tests complete
- The adapter is opened
- The NVRAM config is read to see if the data is there or if it should find a DHCP server
- If DHCP, it sends a broadcast and receives a set of configuration options
- These options are stored in a control block in memory
- The client fetches its operating system from a boot server
- The Registry daemon reads the control blocks to get all the configuration information and populates the registry with that info
- Thge registry daemon then reads the terminal configuration files from the configuration server and populates the registry with that additional information
- The login process is then started, which will display a login panel to the user.

Roaming

- Roaming is the ability to select an authentication server other than the default authentication server
- A V2R1 client cannot use a V1R3 level authentication server but a V1R3 client can use a V2R1 authentication server.



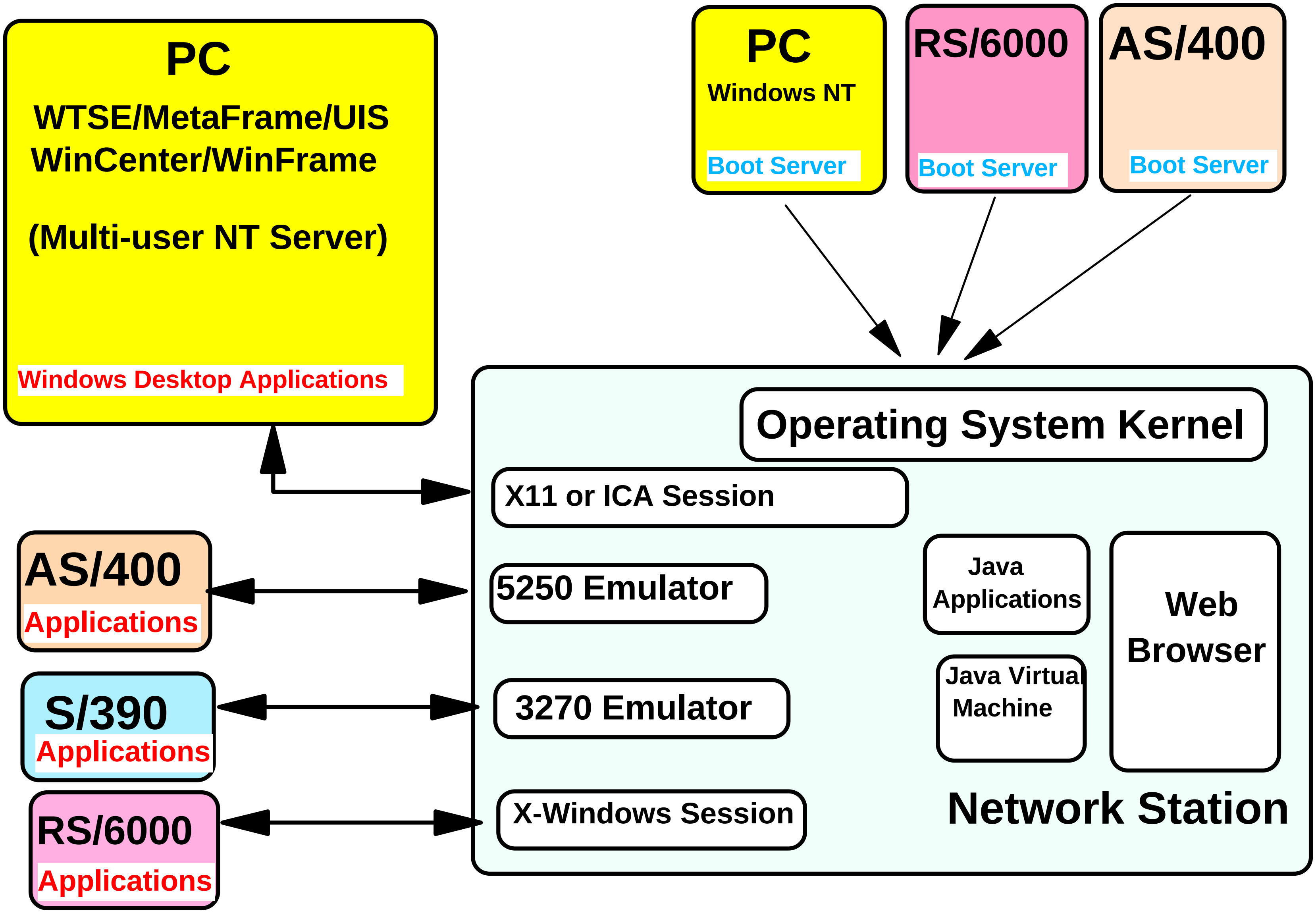
Notes

When the login panel is displayed, the user can use the roam button in order to select an authentication server other than the default server.

Since we can now have both V1R3 and V2R1 servers in the same network, one must realize that a V1R3 client can login to either a V1R3 server or V2R1 server, but that a V2R1 client can only login to a V2R1 authentication server.

When a V2R1 system coexists with a V1R3 system on the same machine, it is the V2R1 Network Station Login Daemon which is active since it can handle both types of clients.

Boot Servers vs Application Servers



PC

WTSE/MetaFrame/UIS
WinCenter/WinFrame

(Multi-user NT Server)

Windows Desktop Applications

PC
Windows NT
Boot Server

RS/6000
Boot Server

AS/400
Boot Server

AS/400
Applications

S/390
Applications

RS/6000
Applications

Operating System Kernel

X11 or ICA Session

5250 Emulator

3270 Emulator

X-Windows Session

Java
Applications

Java Virtual
Machine

Web
Browser

Network Station

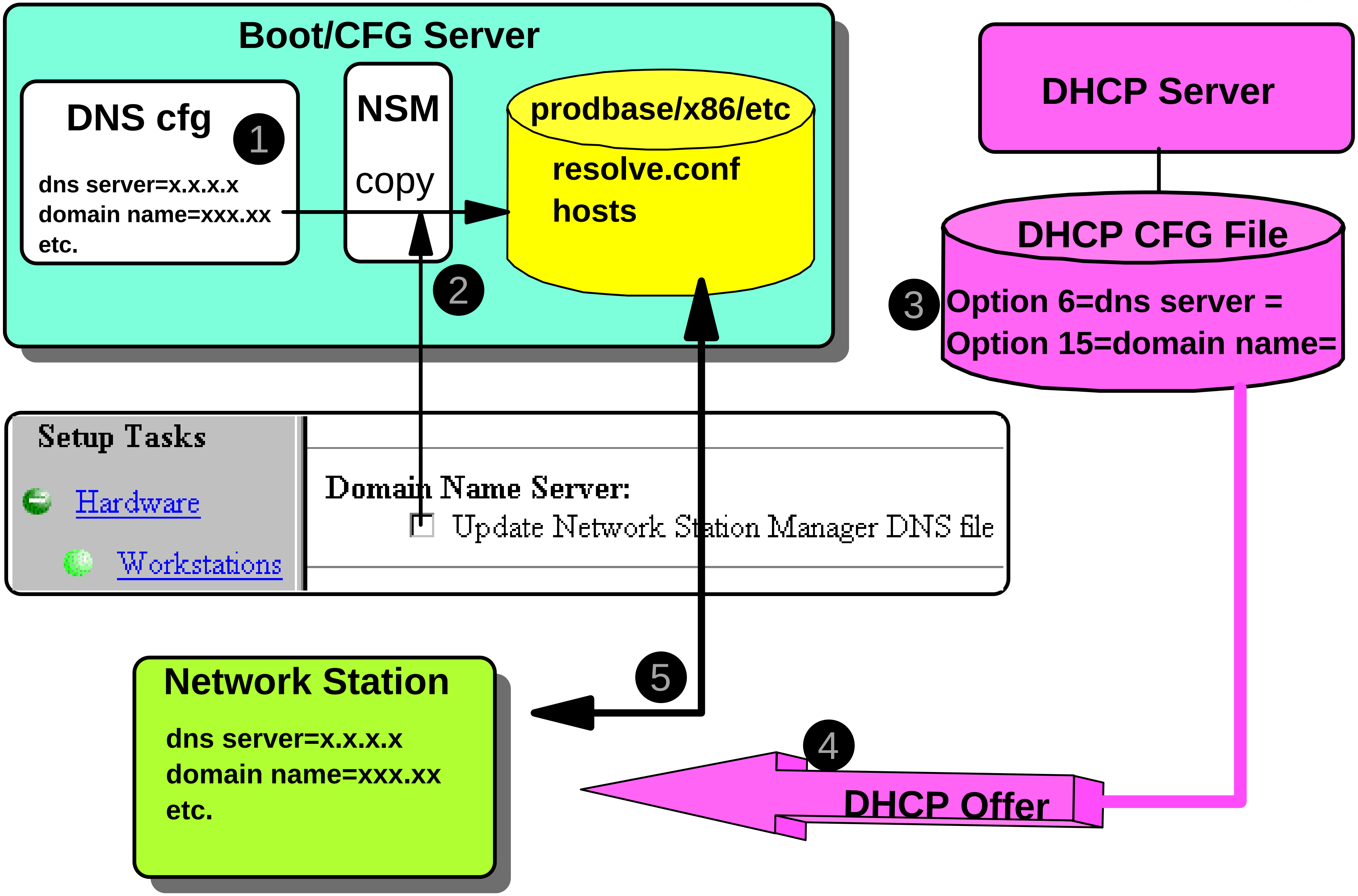
Notes

This chart is a reminder that there is a distinction between boot servers (or configuration servers or authentication servers) that are used during the boot process in order to provide a station with the code and data that it needs to become operational, and the servers that are accessed by applications executing on the station once it is up and running.

The three servers in the top right hand corner of the chart represent these servers, which we have labeled generically as boot servers. The three platforms available for V2R1 are the AS/400, AIX and Windows NT platforms.

On the left hand side of the chart are numerous application servers that are typically or commonly used by the native applications on the station.

How does a Station Get its DNS Info?



Notes

On the boot or authentication server, the normal TCP/IP configuration already exists and has DNS information such as the domain name and one or more domain name servers (1).

In Network Station Manager in the setup task Hardware=>Workstation=>Domain Name Server, the user can click on Update Network Station Manager DNS file. This causes NSM to update the .../prodbase/x86/etc/hosts and .../prodbase/x86/etc/resolv.conf files with the same DNS information that is present on the server (2).

The same DNS configuration information can also be entered by the administrator into the DHCP server's configuration files for those stations that use DHCP (3).

So how does a Network Station then retrieve the DNS information it requires in order to operate?

If the station boots using DHCP and the DHCP server transmits the required options that contain the DNS information (4), then this is the way that the station learns about its DNS information.

If the station boots using NVRAM, or does not have the required DHCP options, the kernel retrieves this information from the /etc/hosts and /etc/resolv.conf files on the server through the file system(5).

Where To Go For More Information?

- Main Web Site
  - www.ibm.com/nc
- Current Network Station Redbook
  - SG24-5844 Network Station Manager V2R1 Guide
- Previous Network Station Redbooks
  - SG24-5187 AS/400 - Techniques for Deployment in a WAN
  - SG24-5221 Windows NT - NSM Release 3
  - SG24-5212 Printing
  - SG24-2127 Windows NT/WinCenter
  - SG24-4954 S/390, SG24-2016 RS/6000, SG24-2153 AS/400
- Product Publications
  - SC41-0684 Installing NSM for AS/400
  - SC41-0685 Installing NSM for RS/6000
  - SC41-0688 Installing NSM for Windows NT
  - SC41-0690 Using NSM
  - IBM Network Station Advanced Information (On the Web Site)

Notes

A lot more information is available from these different sources.

In addition to the current (in draft redbook for V2R1 and the product publications, we list also all previous redbooks, for V1R3, since many networks may still have a mix of V1R3 and V2R1 systems.