



Cisco Networking Integration with the Citrix ICA Protocol

CITRIX SYSTEMS, INC.

Cisco, the marketshare leader in networking equipment, software, and services, has identified Citrix, the global leader in access infrastructure solutions, and its customers as populating a significant share of the Cisco customer base. As such, a number of Citrix-related capabilities have been built into the Cisco Internetwork Operating System (Cisco IOS®) that is available for Cisco® routers. Beginning March 2004, new configuration options are available for prioritizing the Citrix® ICA® protocol at Layer 6/Presentation using the latest version of Network-Based Application Recognition (NBAR). This can often be done based on existing Cisco hardware. Of course, upgrading software is required as discussed in the *NBAR Support of Citrix ICA Packet Priorities* section; however, as with all IOS and PDLM upgrades, there is no charge for doing so.

These capabilities will be the subject of this white paper, with the intent of providing both Citrix MetaFrame® Presentation Server and network administrators with more information with the goal of creating a better understand of the following:

- Business drivers and needs
- Technical
 - Options and solutions
 - Citrix tests and related sample configuration

MetaFrame XP® Presentation Server 1.0, Feature Release 3, and MetaFrame Presentation Server 3.0 were used as the basis for this white paper.

Feature or nomenclature differences that impact the networking discussion are detailed where appropriate.

2	Business Drivers and Needs
2	User Requirements
2	Service-Level Agreements (SLAs)
3	Overview of MetaFrame Presentation Server Networking
3	TCP Ports
3	Core MetaFrame Presentation Server Components
4	ICA Traffic Flows
5	Technical Options
5	Business Priorities
5	LANs
6	WANs
7	Technical Solutions
7	Layer 3: Prioritize Traffic Based on IP Addresses
7	Layer 4: Prioritize Traffic Based on TCP Port
8	Layer 6: Prioritize Traffic Based on ICA Virtual Channel, Including Cisco Network-Based Application Recognition
9	NBAR Tests
9	Environment
10	Test Methodology
12	Test Results
12	Citrix Considerations
13	Router Configuration
14	Conclusions
14	NBAR Support of Citrix ICA Priority Packet Priorities
14	NBAR Original Support by Published Application
15	Notice

Business Drivers and Needs

Since user requirements and service-level agreements (SLAs) are typically the highest concern for administrators of both the network and MetaFrame Presentation Servers, this section focuses on those business drivers and needs.

USER REQUIREMENTS

Addressing user satisfaction and access to MetaFrame Presentation Server-based applications is typically based on business requirements and can be classified as indicated below:

Environment	Example	Acceptability of Downtime
Mission-critical	Medical: Patient records	None
Power user	Financial: Accounts payable database	Minimal
Standard user	Marketing: E-mail	Varies

These environment types will be used later in this document with respect to defining the criticality of the ICA traffic flows and the user experience.

SERVICE-LEVEL AGREEMENTS (SLAS)

Service providers, as well as some internal IT departments, typically have defined specific metrics based on service availability and response times. These service level agreements (SLAs) primarily serve as a means of defining expectations and are often tied to penalties and/or bonuses.

Examples of SLA metrics include:

- Time to address issues at each support tier
- Time to report or resolve user issues
- Service availability uptime

Citrix deployments that include SLAs are usually based on the availability of MetaFrame Presentation Server-based applications. As such, service requirements are commonly based on 100% or near 100% application availability during business hours.

To support high availability, administrators should consider the following:

- Deploying a sufficient number of servers such that failure of one server or a small percentage of servers will not impact the environment
- Regular maintenance windows to address hardware and software requirements
- A laboratory environment and related procedures that ensure thorough testing processes prior to production deployment
- Prioritizing ICA and related traffic such that network bottlenecks are prevented

Of these items, the latter will be considered within subsequent sections in order to address ICA traffic prioritization within Cisco network environments.

Overview of MetaFrame Presentation Server Networking

This section provides a basic overview of the networking requirements of MetaFrame Presentation Server, including TCP ports, core MetaFrame Presentation Server components, and ICA and associated traffic flows.

TCP PORTS

The following TCP ports are used by default within MetaFrame Presentation Server environments. All Citrix port numbers may be modified, and instructions for doing so are included within the MetaFrame Presentation Server 3.0 Administrator's Guide.

Purpose	Environment	Default Port Number
ICA	Inbound to server	TCP 1494
Citrix XML Service	All	TCP 80
SSL	Optional	TCP 443
IMA Service	Inbound (server to server)	TCP 2512
IMA Service (data store)	Outbound (server to data store server)	TCP 2512
Management Console/ Presentation Server Console*	All (The console name was changed between versions.)	TCP 2513
SQL Server, Oracle, or DB2 databases	All	TCP 139, 523, or 1433
Session Reliability	MetaFrame Presentation Server 3.0	TCP 2598
License Server	MetaFrame Presentation Server 3.0	TCP 27000

CORE METAFRAME PRESENTATION SERVER COMPONENTS

The core MetaFrame Presentation Server software and hardware components can be defined as:

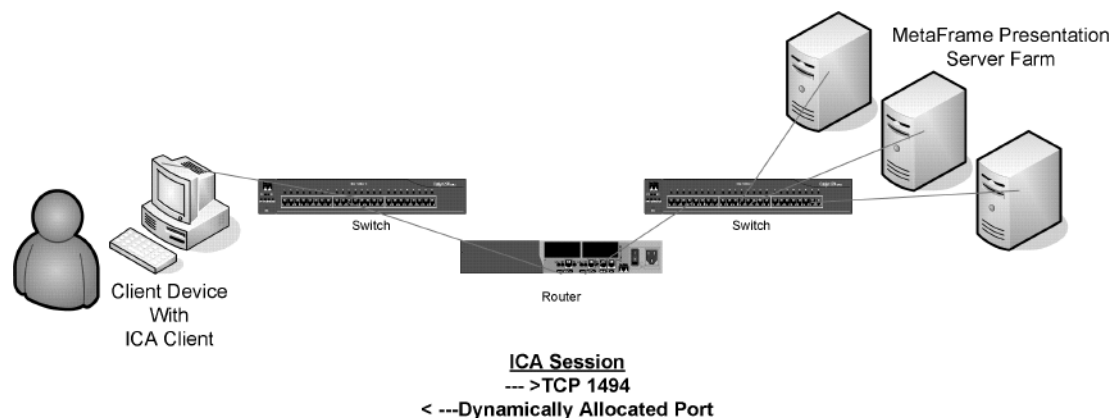
MetaFrame Presentation Server: This is the server that hosts Microsoft® Terminal Services and MetaFrame Presentation Server software, creating a multi-user environment for accessing applications.

Client Device: This is the hardware and associated operating system used to access the MetaFrame Presentation Server.

ICA Client software: This Citrix-provided software is loaded onto the client device so that it can communicate with the MetaFrame Presentation Server.

ICA Session: This is the session that occurs between the client device and the MetaFrame Presentation Server by means of the ICA Client software.

These communications are depicted as follows:



Regardless of whether web interface for MetaFrame Presentation Server or the Program Neighborhood® Agent are added into the environment, application access occurs directly between the client device and the MetaFrame Presentation Server. Web interface acts as a front-end access point for displaying icons for applications, and the ICA session functions exactly the same from a networking perspective no matter which interface is used. The Program Neighborhood Agent allows Windows 32-bit clients to access the application list from the “Start→Programs” menu.

When secure gateway is added to the environment, user sessions are secured and proxied. User sessions are secured via SSL or TLS to the secure gateway server that is located in the DMZ; however, an in-depth discussion of secure gateway and related functionality is beyond the scope of this document.

ICA TRAFFIC FLOWS

According to the MetaFrame Presentation Server 3.0 Administrator's Guide, Citrix ICA (Independent Computing Architecture), is defined as “The architecture that MetaFrame Presentation Server uses to separate an application's logic from its user interface. With ICA, only the keystrokes, mouse clicks, and screen updates pass between the client and server on the network, while 100% of the application's logic executes on the server.”

ICA traffic flows from the client device to the MetaFrame Presentation Server over TCP port 1494. Each ICA session then creates and uses a dynamically allocated TCP port for communications from the server to the client device. The ICA protocol functions on the Presentation layer of the OSI model, which is Layer 6. Within the ICA protocol, virtual channels are used to designate the various functionalities, such as client drive mappings, video, keyboard strokes, etc. Please see the *Citrix Considerations* section for a list of some sample ICA virtual channels and the default prioritization of each.

Layer 3 (IP) and Layer 4 (TCP) functionality of the ICA protocol can easily be viewed by using Microsoft Network Monitor or other network analysis tools. The following example shows two distinct ICA sessions from the same client device (172.16.30.11) to the same MetaFrame Presentation Server (172.16.10.189). Notice that the TCP port used for traffic from the server to the client varies, whereas the port from the client to the server is always TCP port 1494.

Timestamp	Source MAC Address	Destination MAC Address	Type	Protocol	Source IP aAddress	Destination IP Address	Source Port	Dest. Port
13:9:10:239	00:08:02:45:4C:1A	00:04:DD:5F:A7:61	IP	TCP>ICA	172.16.10.189	172.16.30.11	1494	3215
13:9:10:255	00:04:DD:5F:A7:61	00:08:02:45:4C:1A	IP	TCP>ICA	172.16.30.11	172.16.10.189	3215	1494

Timestamp	Source MAC Address	Destination MAC Address	Type	Protocol	Source IP Address	Destination IP Address	Source Port	Dest. Port
17:46:53:126	00:08:02:45:4C:1A	00:04:DD:5F:A7:61	IP	TCP>ICA	172.16.10.189	172.16.30.11	1494	3379
17:46:53:314	00:04:DD:5F:A7:61	00:08:02:45:4C:1A	IP	TCP>ICA	172.16.30.11	172.16.10.189	3379	1494

Although other ports are used to support MetaFrame Presentation Server-related traffic as indicated in the *TCP Ports* section, the most critical traffic from the user perspective is the ICA session itself. As such, the remainder of this document focuses on ICA traffic flows only and the impact on user sessions.

Technical Options

In order to address user requirements and the network aspects of SLAs, administrators need to consider business priorities in relation to the technical options, and this section focuses on these.

BUSINESS PRIORITIES

Administrators of networks and MetaFrame Presentation Servers typically have the following priorities:

- Provide the best user experience
- Use the least administrative overhead
- Incur the lowest cost

LANs

Ensuring a quality user experience across LANs, *e.g.*, within a headquarters building, can be provided at a reasonable cost and typically with minimal additional administrative overhead.

The following table depicts the client device and server connections most commonly seen by Citrix Consulting:

Computer Device	Connection Speed	Network Device
Client	10 or 100 Mbps	Hub or switch
Server	100 Mbps or 1000 Mbps	Switch

Within the data centers of most large enterprise environments, Layer 3 switches — *i.e.*, switches such as the Cisco 6500 series that include a router module and are based on a backplane that can support a significant amount of traffic — are deployed. These networking devices provide substantial throughput, so there is rarely a need to consider the network impact of ICA sessions that traverse LANs in order to ensure that latency or dropped connections do not impact users.

Options

Using the headquarters example from above, if the MetaFrame Presentation Servers are located within the same building as the users, LAN issues related to ICA traffic will be minimal or non-existent. Any issues that are presented are typically addressed by upgrading the LAN infrastructure and thus no other options will be required.

WANS

ICA sessions from remote locations require some type of remote connection, most typically a WAN. WAN connections introduce significant costs and a variety of additional variables, including:

- One or more service providers
- Various types of networking equipment and related configurations
- Contractually required and optional bandwidth throughput, *e.g.*, frame relay CIR and burst
- Remote locations that may have little or no administrative support

Options

When enterprises are faced with business decisions regarding additional bandwidth requirements, the basic options are:

- Lease additional bandwidth
- Prioritize traffic types

Since WAN links are commonly the largest portion of an IT department budget, typically the less palatable solution is to lease additional bandwidth, especially over international links. Provisioning international links is not only a process that takes several months or longer, but also may be prohibitively expensive. However, both nationally and globally, the cost for WAN circuits continues to decrease, so this option should be considered where appropriate.

Network traffic prioritization or Quality of Service (QoS) requires administrative expertise. For example, based on the ICA session traffic flows described in the *ICA Traffic Flows* section, an administrator seeking to prioritize ICA traffic may inadvertently apply the configuration only to TCP port 1494, without the full understanding regarding the corresponding return traffic and the need to prioritize it. Such a configuration would not be optimal and consequently would not provide the desired solution. In all cases, testing should be performed to ensure the desired results.

When considering giving priority to more important traffic types, such as ICA sessions, administrators need to remember that no additional bandwidth becomes available as a result of prioritizing network traffic; instead, traffic with low or no prioritization traverses the network more slowly or may be dropped when over-saturation of the network occurs. For example, consider a call center environment where business-critical applications are housed on MetaFrame Presentation Servers and all ICA traffic is deemed the highest priority. Within this enterprise, call center agents are permitted to browse the internet when not taking calls. In this case, there are no business repercussions to slow or dropped packets traversing TCP port 80. Thus, HTTP traffic can be sacrificed at the expense of ICA traffic, and instituting QoS is a sound business decision. However, in such a situation, the Citrix XML Service should be designated on a port other than 80 to ensure that the initial browsing required to support user connections is not likewise de-prioritized.

Technical Solutions

Based on the discussion in the previous section, if QoS is deemed the best business decision, there are several solutions on Cisco routers that should be considered:

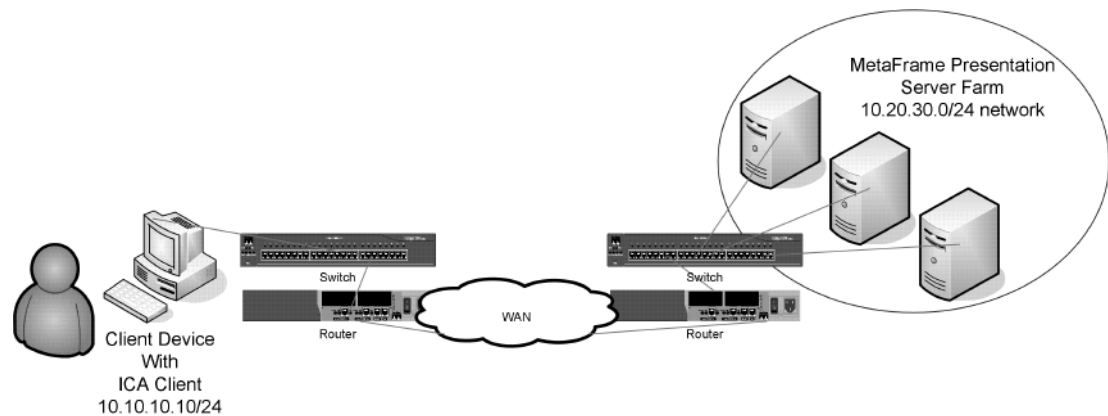
- Layer 3: Prioritize traffic based on IP address
- Layer 4: Prioritize traffic based on TCP port
- Layer 6: Prioritize traffic based on ICA virtual channel, including Network-Based Application Recognition

Each of these solutions will be discussed within this section.

LAYER 3: PRIORITIZE TRAFFIC BASED ON IP ADDRESSES

If all MetaFrame Presentation Servers are located within the same subnet, all traffic going in and out of that subnet can be prioritized based on the IP addresses. This is the simplest type of traffic prioritization to implement from an administrative standpoint, and can be done by means of access lists.

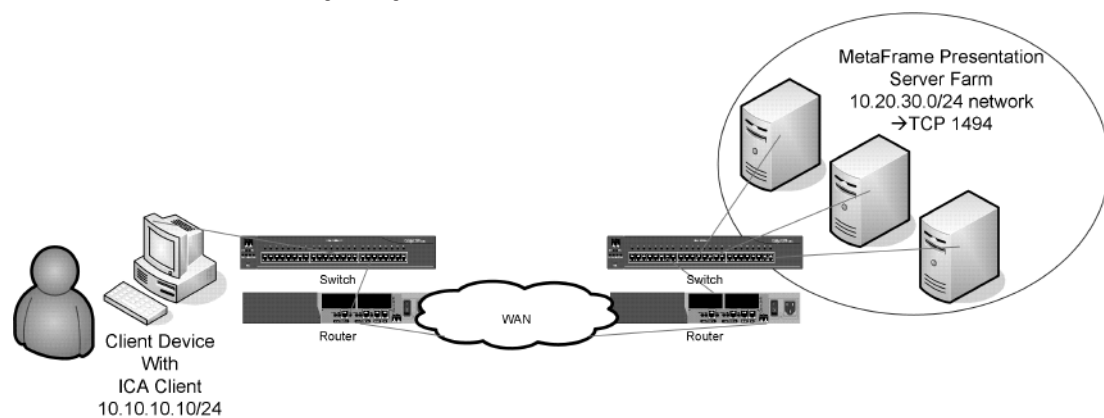
In the diagram shown below, all of the MetaFrame Presentation Servers are located in the 10.20.30.0/24 network, so prioritizing inbound and outbound traffic based on that subnet would be sufficient. Of course, if any other servers were located in that subnet, that traffic would likewise be prioritized; thus, when this type of prioritization is utilized, only the MetaFrame Presentation Servers and other required servers should be co-located within this subnet.



LAYER 4: PRIORITIZE TRAFFIC BASED ON TCP PORT

As stated in the *ICA Traffic Flows* section, ICA communications flow from the client device to the MetaFrame Presentation Server via TCP port 1494, so prioritizing this traffic presents no technical difficulties. If prioritizing inbound network traffic is the only requirement and/or if outbound communications from the server to the client device can be prioritized via the IP subnet address of the client or servers, this is a satisfactory solution. However, in most cases, the former solution, *i.e.*, prioritizing only TCP port 1494, will not yield the desired results, whereas the latter solution considers both inbound and outbound traffic and may be appropriate within some environments.

In the diagram shown below, traffic inbound to the MetaFrame Presentation Server can be prioritized based on TCP port 1494. Because outbound ICA traffic traverses the network based on a dynamically allocated port, it is not possible to designate and prioritize traffic based on TCP port number. However, similar to the previous example relating to prioritization based on Layer 3 addressing, the subnet where the MetaFrame Presentation Servers are located could serve as the distinguishing factor.



LAYER 6: PRIORITIZE TRAFFIC BASED ON ICA VIRTUAL CHANNEL, INCLUDING CISCO NETWORK-BASED APPLICATION RECOGNITION

Prioritization of the ICA virtual channels may be desired when a specific virtual channel, such as client printer mapping, needs higher precedence than that which is granted by default. For example, if the environment consists of large number of small office/home office users that have heavy printing requirements, it may be necessary to prioritize print traffic to ensure that their locally attached client printers receive high prioritization.

Cisco Network-Based Application Recognition (NBAR) was enhanced in March 2004 to identify Citrix ICA packet priorities. Previously, NBAR support of Citrix traffic was based on specific applications and required that session sharing be disabled.

NBAR Support of Citrix ICA Packet Priorities

Beginning with the release of the NBAR `citrix_ica` Packet Data Language Module (PDLM) release 1.0 in March 2004, support for classification based on ICA priority packet tagging was added. This allows an ICA virtual channel to serve as the priority differentiator, in addition to the existing support for classification based on published applications. Importantly, this `citrix_ica` PDLM can be uploaded to existing Cisco routers running versions of Cisco IOS software that support NBAR; a software reload is not required. Going forward, this support is also included natively in Cisco IOS software releases subsequent to 12.3(7)T, which was released in March 2004.

Tests performed by Citrix Engineering and the corresponding results relating to this new release of Cisco NBAR are detailed in the *NBAR Tests* section. Please note that classification based on ICA priority packet tagging augments the existing support for application classification; it is not a substitute for it. Both methods are important and can be used together.

Original NBAR Support of Citrix Traffic

The original version of NBAR support of Citrix traffic, which is still available, automatically assumes TCP port 1494 and UDP port 1604 is used for ICA traffic and enables a network administrator to identify and classify network traffic based on Citrix published applications, thus further defining prioritization.

This earlier NBAR support of Citrix traffic is effective where published applications exist; MetaFrame Presentation Server environments that publish the desktop use the same session parameters and therefore cannot be differentiated. Further, the application would need to be published in non-session-sharing mode in order to differentiate based on the application name. Session sharing enables users to share existing ICA sessions to support subsequent applications that are hosted on the same MetaFrame Presentation Server as the original session.

To disable session sharing, the MetaFrame administrator must modify the registry within each MetaFrame Presentation Server. Specifically, within the following path: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\WFSHELL\TWI, the following value must be added: Name: SeamlessFlags; Data type: DWORD; Data value: 1

In general, disabling session sharing will not have a negative impact on the servers; however, it may have an impact depending on the applications served. For example, if the server were hosting Microsoft Office, users would open a new session for each application launched. Thus, Word may be launched from one server, Excel from another, and PowerPoint® from yet another. Therefore, the login script processing, file shares, print shares, user profiles, and drive mappings would all be duplicated unnecessarily. Disabling session sharing will, however, require slightly more resources, and in large MetaFrame Presentation Server farms, this may have a greater impact. Disabling session sharing is required in order to enable the original version of NBAR support to differentiate the applications with the granularity required.

To confirm the port numbers in use by the router from privileged mode or to confirm which version of NBAR is in use, the following can be used:

```
RouterA#show ip nbar port-map citrix
Port-map citrix udp 1604
Port-map citrix tcp 1494
```

As stated previously, the requirement for client-side browsing via UDP port 1604 became optional after the release of MetaFrame 1.8 Feature Release 1.

To modify or redefine the port numbers in use by the router for port-map citrix, the following can be configured:

```
RouterA(config)#ip nbar port-map citrix tcp [up to 16 port numbers]
RouterA(config)#ip nbar port-map citrix udp [up to 16 port numbers]
```

In addition, the router should be configured as follows:

```
RouterA(config)#class-map citrix
RouterA(config-cmap)#match protocol citrix app [app name]
```

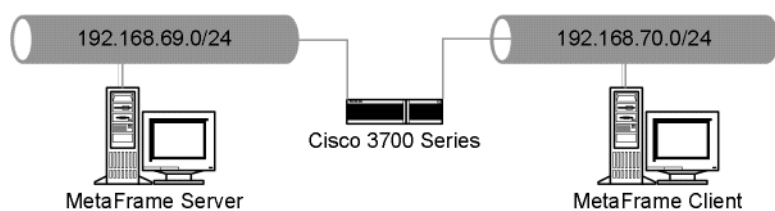
Please note that the above commands and configurations are only applicable to the original Cisco NBAR functionality.

NBAR Tests

Citrix tested the latest Cisco Network-Based Application Recognition in March 2004. The tests were based on the Cisco IOS version 12.3(4)T and the citrix_ica Packet Data Language Module (PDLM) release 1.0. The results of these tests are outlined within this section.

ENVIRONMENT

The Cisco 3700 Series router was configured used to test the latest version of the Cisco NBAR ICA PDLM as of April 2004. The network diagram tested is shown below:



The router was configured to connect the two isolated subnets and then modifications were made to the pre-configured citrix policy-map and service-policies. The citrix policy-map was configured to be used as input for both network segments. For a complete router configuration, please refer to the *Router Configuration* section later in the document.

No additional configurations were made to the MetaFrame Presentation Servers or the ICA Clients; the MetaFrame default configuration was used to set ICA packet priorities for the test. For more information on the Citrix configuration, see the *Citrix Considerations* section later in the document.

TEST METHODOLOGY

To verify all four levels of Citrix ICA priority bits could be successfully identified, the following policy map was created:

```

policy-map citrix
  class citrix0
    set dscp cs4
  class citrix1
    set dscp cs1
  class citrix2
    set dscp cs2
  class citrix3
    set dscp cs3

```

Setting the priorities for all the bits in one map allowed the test iteration to be run once and provide verification that all packets with priority bits were successfully set by the router. Using CS4 for the citrix0 class allowed the ICA priority packets to be easily distinguished from the un-prioritized packets, which would usually have a priority of 0. In a normal deployment, the citrix0 class would have a dscp of cs0 and was modified purely for testing purposes.

Microsoft Network Monitor was installed on both network segments to capture the packets and allow manual inspection of the DSCP bits and the ICA priority bits at the packet level. Using the following chart, the captured packets were verified to have the correct values for both their DSCP and ICA priority bytes.

Citrix Priority Setting	Hexadecimal Value of ICA High Order Data Length Byte	DSCP Setting (Decimal)	Hexadecimal Value of IP Precedence Byte
0	00-05	CS4 (40)	08-09
1	40-45	CS1 (8)	02-03
2	80-85	CS2 (16)	04-05
3	C0-C5	CS3 (24)	06-07

In addition to manual packet inspection, the “show policy-map interface” command was used to verify that the router was correctly classifying the number of ICA packets sent.

Each iteration of the test consisted of the following steps:

1. Launch a connection from Program Neighborhood
2. Login to the server
3. Generate text in a file
4. Save a file to the mapped client drive
5. Print the file to the mapped client printer
6. Logoff

These steps generate ICA traffic across several virtual channels causing packets to be generated in all four of the priority levels. The above test iteration was then performed for each of the following configurations. The test results are shown in the table along with the configuration.

Configuration	Test Results
MetaFrame XP for Windows with Feature Release 3	Pass
MetaFrame Presentation Server for Windows 3.0	Pass
ICA Client version 7.0	Pass
ICA Client version 8.0	Pass
Custom ICA Connections	Pass
Published Applications	Pass
Published Desktop	Pass
Anonymous Users	Pass
Compression on/off	Pass
Seamless/Non-seamless	Pass
Non-standard ICA Port	Pass
Basic Encryption	Pass
Encryption*	Fail

**The PDLM does not support this feature at this time, but the results are nonetheless included here.*

As stated in the *Layer 6: Prioritize ICA Traffic via Virtual Channels* section, the original version of NBAR classified UDP port 1604 traffic. Use of this UDP port is not required for client-side browsing for MetaFrame 1.8 with Feature Release 1 or higher and corresponding ICA Clients. Thus, in most cases, the requirement for UDP port 1604 is no longer necessary, since newer versions of the ICA Client locate the MetaFrame Presentation Servers via the Citrix XML Service, which typically shares TCP port 80 with HTTP.

For the non-standard ICA port test, the MetaFrame Presentation Server was configured to accept incoming ICA requests on TCP port 1495, and the following line was added to the router configuration:

```
ip nbar port-map citrix tcp 1495
```

TEST RESULTS

The Cisco NBAR Citrix PDLM operates as expected in a Citrix MetaFrame Presentation Server environment. Please note the following:

- ICA Clients using encryption other than basic will not have their packets classified.
- ICA browsing protocol (UDP port 1604) traffic is not classified.

UDP port 1604 traffic was used to support ICA browsing, primarily with MetaFrame 1.8 and older. Although ICA browsing over UDP port 1604 can be used with MetaFrame Presentation Server 1.0 and 3.0 to support older ICA Client versions, it is uncommon.

CITRIX CONSIDERATIONS

The minimum requirements to allow ICA packet prioritization are listed below.

- MetaFrame 1.8 with Feature Release 1
- MetaFrame XP for Windows with Feature Release 1
- ICA Client version 6.20.985 or later
- TCP/IP protocol

Packet priorities are assigned based on the virtual channel data contained in the packet. If a packet contains data from more than one virtual channel, then the packet is assigned the priority of the highest virtual channel data. The table below identifies the four levels of ICA packet priorities and lists some of the virtual channels associated with that priority by default.

Priority	ICA Bits (Decimal)	Sample Virtual Channels
High	00 (0)	Video, mouse and keyboard screen updates
Medium	01 (1)	Program Neighborhood, clipboard, audio mapping and license management
Low	10 (2)	Client COM port mapping, client drive mapping
Background	11 (3)	Auto Client Update, client printer mapping and OEM Channels.

The administrator can change the ICA packet priorities by modifying the registry on the MetaFrame Presentation Server. For more information on configuring ICA packet priorities, download the Citrix ICA Priority Packet Tagging

article available at the Citrix Support website
(http://support.citrix.com/servlet/KbServlet/download/23-102-7625/ICA_Priority_Packet_Tagging.pdf).

ROUTER CONFIGURATION

```
!  
version 12.3  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname pet-3745  
!  
boot-start-marker  
boot system flash:c3745-jsx-mz.123-4.T3  
boot-end-marker  
!  
!  
no aaa new-model  
ip subnet-zero  
!  
ip nbar pdlm flash:citrix_ica4.pdlm  
!  
no ip domain lookup  
!  
ip cef  
!  
class-map match-any citrix1  
  match protocol citrix ica-tag "1"  
class-map match-any citrix0  
  match protocol citrix ica-tag "0"  
class-map match-any citrix3  
  match protocol citrix ica-tag "3"  
class-map match-any citrix2  
  match protocol citrix ica-tag "2"  
class-map match-any dscp1  
  match ip dscp 1  
!  
!  
policy-map citrix  
  class citrix0  
    set dscp cs4  
  class citrix2  
    set dscp cs2  
  class citrix3  
    set dscp cs3  
  class citrix1  
    set dscp cs1  
policy-map dscp1  
  class dscp1  
    set dscp default  
!  
!  
interface FastEthernet0/0  
  no ip address  
  duplex auto  
  speed auto  
!  
interface FastEthernet0/1  
  no ip address  
  shutdown  
  duplex auto  
  speed auto  
!  
interface FastEthernet1/0  
  ip address 192.168.69.1  
  255.255.255.0  
  service-policy input citrix  
  service-policy output dscp1  
  speed 100  
  half-duplex  
!  
interface Serial1/0  
  no ip address  
  shutdown  
  clockrate 2000000  
!  
interface FastEthernet1/1  
  ip address 192.168.70.1  
  255.255.255.0  
  service-policy input citrix  
  service-policy output dscp1  
  speed 100  
  half-duplex  
!  
interface Serial1/1  
  no ip address  
  shutdown  
  clockrate 2000000
```

```
!  
interface Serial1/2  
  no ip address  
  shutdown  
  clockrate 2000000  
!  
interface Serial1/3  
  no ip address  
  shutdown  
  clockrate 2000000  
!  
interface Hssi2/0  
  no ip address  
  shutdown  
  serial restart-delay 0  
!  
interface GigabitEthernet3/0  
  no ip address  
  shutdown  
  speed 1000  
  media-type gbic  
  negotiation auto  
!  
ip http server  
ip classless  
!  
control-plane  
!  
gatekeeper  
  shutdown  
!  
line con 0  
  exec-timeout 0 0  
line aux 0  
line vty 0 4  
  login  
!  
!  
end
```

Notice

The information in this publication is subject to change without notice.

THIS PUBLICATION IS PROVIDED "AS IS" WITHOUT WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. CITRIX SYSTEMS, INC. ("CITRIX"), SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN, NOR FOR DIRECT, INCIDENTAL, CONSEQUENTIAL OR ANY OTHER DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS PUBLICATION, EVEN IF CITRIX HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE.

This publication contains information protected by copyright. Except for internal distribution, no part of this publication may be photocopied or reproduced in any form without prior written consent from Citrix.

The exclusive warranty for Citrix products, if any, is stated in the product documentation accompanying such products. Citrix does not warrant products other than its own.

Version History

1.0

Jo Harder, Citrix Corporate Consulting

June 2004

The following individuals contributed to this document:

Jo Harder, Citrix Corporate Consulting

Paul Wilson, Brad Pederson, and Rick Braddy, Citrix Engineering

Tom Craig and Josh Drachman, Citrix Corporate Development

Tim McSweeney and Clyde Layton, Cisco Systems



Citrix Consulting

About Citrix: Citrix Systems, Inc. (Nasdaq:CTXS) is the global leader in access infrastructure solutions and the most trusted name in enterprise access. Citrix software enables people in businesses, government agencies, and educational institutions to securely, easily and instantly access the on-demand enterprise, from anywhere, anytime, using any device, over any connection. Nearly 50 million people in more than 120,000 organizations rely on the Citrix MetaFrame Access Suite to do their jobs. Citrix customers include 100% of the *Fortune* 100 companies, 99% of the *Fortune* 500, and 92% of the *Fortune* Global 500. Based in Fort Lauderdale, Florida, Citrix has offices in 26 countries, and more than 7,000 channel and alliance partners in more than 100 countries. For more information visit www.citrix.com.

Citrix Worldwide

WORLDWIDE HEADQUARTERS

Citrix Systems, Inc.

851 West Cypress Creek Road
Fort Lauderdale, FL 33309 USA
Tel: +1 (800) 393 1888
Tel: +1 (954) 267 3000

EUROPEAN HEADQUARTERS

Citrix Systems International GmbH

Rheinweg 9
8200 Schaffhausen
Switzerland
Tel: +41 (52) 635 7700

ASIA PACIFIC HEADQUARTERS

Citrix Systems Hong Kong Ltd.

Suite 3201, 32nd Floor
One International Finance Centre
1 Harbour View Street
Central
Hong Kong
Tel: +852 2100 5000

CITRIX ONLINE DIVISION

5385 Hollister Avenue
Santa Barbara, CA 93111
Tel: +1 (805) 690 6400

www.citrix.com