

Networking Issues Affecting

Citrix® MetaFrame Environments

White Paper

Date Revised:

April 2003 – Version 3.04

Prepared by:

Jo Harder, Senior Architect

E-mail: jo.harder@citrix.com



Table Of Contents

1.	Overview and Intended Audience	1
2.	Servers Supporting the MetaFrame Environment	2
2.1	<i>MetaFrame Presentation Servers</i>	2
2.1.1	Effects of Audio	2
2.2	<i>MetaFrame XP Data Store</i>	2
2.3	<i>Zone Data Collector</i>	3
2.4	<i>MetaFrame Web Interface, Secure Gateway and Related Servers</i>	3
2.5	<i>File Servers</i>	3
2.5.1	Profiles	3
2.5.2	Home Directory	4
2.5.3	Novell File and Print Servers	4
2.6	<i>Terminal Services License Server</i>	4
2.6.1	Network Traffic Generated by Terminal Services Licensing Server	5
3.	Layer 2: NIC Configuration and Settings	6
3.1	<i>Duplex and Speed</i>	6
3.1.1	NICs	6
3.2	<i>Protocols</i>	6
3.3	<i>Multiple NICs</i>	6
3.3.1	NIC Teaming	7
3.3.2	Failover	8
3.3.3	BackUp NICs	8
3.3.4	Multi-Homed MetaFrame Servers	8
4.	Layer 2: Switch Configuration and Settings	10
4.1	<i>Layer 2 and 3 Switch Technologies</i>	10
4.2	<i>Configuration of a Switch Ports</i>	10
5.	Layer 2: WANs and Remote Access	12
5.1	<i>WAN Connectivity</i>	12
5.2	<i>ICA Session Monitoring and Control</i>	12
5.3	<i>Complex Caching and Encapsulation</i>	12
5.4	<i>Queuing/Quality of Service (QoS)</i>	13
5.4.1	First-In, First-Out (FIFO)	13
5.4.2	Weighted Fair Queuing (WFQ)	14
5.4.3	Priority Queuing	14
5.4.4	Custom Queuing	14
5.4.5	Network-Based Application Recognition	15
5.5	<i>Firewalls</i>	16
5.6	<i>Web Interface</i>	17
5.7	<i>Secure Gateway</i>	17
5.8	<i>VPN</i>	17
5.9	<i>Dial-Up Directly to the MetaFrame Server</i>	17
5.10	<i>RAS</i>	17
5.11	<i>Network Security</i>	18
6.	Layer 3: IP Addressing	19
6.1	<i>Minimizing Broadcast Traffic</i>	19
6.1.1	Subnetting and Variable-Length Subnet Masks (VLSM)	19
6.1.2	Virtual LANs	20
6.1.3	Subnets and Zones	20
7.	Layer 3: Routers	21

7.1	Layer 3 Routing	21
7.2	Routers	21
7.3	Windows 2000 Routing	21
8.	Layer 4: TCP Ports	22
8.1	TCP Port Numbers	22
8.1.1	ICA TCP Port Number	22
8.1.2	Citrix XML Service Port Number	22
8.1.3	SSL Port	23
8.1.4	MetaFrame XP Port Numbers	23
8.1.5	Database Port Numbers	23
9.	MetaFrame Server Network Environment	24
9.1	Inside Static Network Address Translation (NAT) and Port Address Translation (PAT)	24
9.1.1	NAT Using ALTADDR on MetaFrame Servers	24
9.1.2	Static Inside NAT and PAT on Routers and Firewalls	24
9.2	Static vs. DHCP-Assigned TCP/IP Address	25
9.3	Permission to Monitor Over the Network	25
10.	Network-Related MetaFrame Features and Associated Implications	26
10.1	SpeedScreen	26
10.2	Disk Caching and Data Compression	26
10.3	Printer Bandwidth Throttling	26
10.4	Client Mapping Settings	26
10.5	Printer Creation	27
11.	Network Impact of Citrix Add-On Products	28
11.1	Load Manager	28
11.2	Resource Manager	28
11.3	Installation Manager	28
11.3.1	Application(s)	29
11.4	Network Manager/SNMP	29
12.	General Network Topics	30
12.1	WINS and DNS for Name Resolution	30
12.1.1	ICA Browsing with MetaFrame XP	30
12.2	Windows 2000 Services	30
12.2.1	Citrix XML Service	31
12.2.2	IMA Service	31
12.2.3	Secure Gateway Service	31
13.	ICA Client	32
13.1	ICA Client Versions	32
13.1.1	Program Neighborhood ICA Client Configuration	33
13.1.2	Web-Based ICA Client	33
13.1.3	PN Agent ICA Client	33
13.2	Client Login Scripts	33
13.3	Network Protocols	34
14.	Most Commonly Overlooked Network Issues	35
14.1	Proper Configuration of Subnets	35
14.1.1	Class C	35
14.1.2	Variable-Length Subnet Mask (VLSM)	35
14.2	TCP 1494 (or other configured ICA port) Not Open	35
14.3	TCP 2512 or 2513 Not Open	35
15.	Windows Operating System Troubleshooting Tools and Tips	36
15.1	Computer to Computer	36

15.1.1	Finding the Router(s)	36
15.2	<i>Performance/System Monitor</i>	36
15.3	<i>Network Monitor</i>	37
15.4	<i>Registry Settings</i>	38
16.	Router (Cisco®) Troubleshooting Tools and Tips	39
16.1	<i>Switch and Router Access Privileges</i>	39
16.2	<i>Network</i>	39
16.2.1	Ping	39
16.2.2	Trace	40
16.2.3	Telnet	40
16.2.4	Switch Errors	40
16.2.5	Token Ring	41
16.3	<i>Access Lists</i>	41
17.	Appendix A – TCP/IP Subnetting	42
17.1	<i>TCP/IP Subnetting and Variable-Length Subnet Masks (VLSM)</i>	42
17.2	<i>Private IP Addresses</i>	45
18.	Appendix B – OSI Model	46
18.1	<i>OSI Model Basics</i>	46

1. Overview and Intended Audience

Designing the network to adequately support Citrix® MetaFrame XP Presentation Server requires a number of technical considerations. This white paper addresses specific issues that should be considered when planning the network environment, as well as a number of processes and methods that can be used on an ongoing basis to determine whether an existing environment has been implemented optimally and thus maximizes existing network bandwidth.

This white paper peripherally addresses:

- Microsoft® Windows 2000 operating system but also contains references to environments that co-exist with Novell® File and Print Servers.
- Cisco® networking equipment, since this is the single leading equipment manufacturer found in most premises networking environments where Citrix MetaFrame is used.

This document is targeted toward:

- Citrix Certified Administrators (CCA) or equivalent that are also Microsoft Certified Systems Engineers (MCSE) or equivalent.
- Cisco® Certified Network Administrators (CCNA) or equivalent that support MetaFrame environments.

Wherever possible, best practices or examples are included and should not be construed as optimal settings for every Citrix MetaFrame environment. In particular, Microsoft Windows registry settings and Cisco router and switch configuration settings are referenced. For more information regarding Cisco router privileges, please see [Cisco Router Access Privileges](#). Please note that there are two levels of access to the commands:

- User or Unprivileged Mode
 - read-only mode;
 - commonly used to view switch or router status;
 - indicated with the > symbol.
- Privileged Mode
 - full-control mode wherein configuration settings can be changed;
 - usually reserved for network administrators;
 - indicated with the # symbol.

It is assumed that the reader has a good understanding of TCP/IP version 4 since the fundamentals of TCP/IP will not be addressed. It is also assumed that TCP/IP is the primary or only protocol deployed in the Citrix MetaFrame environment. TCP/IP version 6 will not be addressed since its implementation is not widespread.

Special thanks to the following Citrites: Trevor Davis, Rob Ruzicka, Jay Tomlin, Jeff Reed, Anatoliy Panasyuk, and Henry Collins for their contributions and review of this white paper.

For more information regarding the networking concepts discussed herein, please see <http://www.citrix.com>, <http://www.microsoft.com>, or <http://www.cisco.com>.

Windows® 2000 is a registered trademark of Microsoft.

Cisco® is a registered trademark of Cisco Systems.

2. Servers Supporting the MetaFrame Environment

A number of different servers comprise the MetaFrame environment. This section discusses not only the MetaFrame presentation servers, but also the other related servers that are commonly found in MetaFrame implementations.

It is common to have servers supporting various functionality requirements in the MetaFrame environment. The specific number and type of servers depends on the specific environment. It is critical that MetaFrame servers are configured so as to minimize latency and maximize throughput, e.g., all MetaFrame servers should reside on the same subnet, whether connected by physical switch or Virtual LAN.

2.1 MetaFrame Presentation Servers

MetaFrame presentation servers are servers that host applications for users. MetaFrame servers should be member servers, not domain controllers. Since domain controllers are peers and support a great deal of network traffic, this additional load would have a negative impact a server's ability to serve applications to users. Thus, it is strongly suggested that MetaFrame servers not support both domain controller and application server functionality.

MetaFrame applications servers should not host BackOffice applications, such as SQL Server or Exchange Server. Such would put too much of a strain on the server.

MetaFrame servers typically are grouped into server farms that mainly are based on published applications. User data and profiles should not be stored on the MetaFrame presentation servers since this would generate additional network traffic and increase latency, as well as introduce inconsistencies for files or profiles that have the same name on different servers.

2.1.1 Effects of Audio

Applications that include audio requirements will add from 16 Kbps (low) to 1.3 Mbps (high) of bandwidth to the ICA session. This is in addition to the approximately 20 Kbps of bandwidth required for each ICA session.

If audio is not required it should be set to low or turned off completely. If audio is required, its impact on the network should be evaluated to ensure that adequate bandwidth exists. If the audio level must be set to low or medium because of bandwidth issues, this should be tested to ensure that a reduced audio setting still provides the level of quality that is acceptable to end users.

2.2 MetaFrame XP Data Store

MetaFrame XP introduced the Data Store, which is a centralized database that persistently stores information about MetaFrame XP. The Data Store is a critical component within MetaFrame XP, and access to the Data Store cannot be interrupted for more than 96 hours without adversely affecting the server farm. MetaFrame XP servers communicate with the Data Store via the IMA Service.

Most MetaFrame XP traffic consists of reads from the Data Store. When changes are made on the MetaFrame XP servers, such as adding print drivers or published applications, these modifications create additional network traffic as these changes are written to the Data Store and communicated to the other MetaFrame XP servers. Please see the *MetaFrame XP Advanced Concepts Guide* for specific details regarding the network traffic that is generated.

A significant network impact relates to print drivers, so it is recommended that only the minimum required of printers be installed and replicated. The Universal Print Driver can minimize the number of print drivers required. The number of MetaFrame XP servers in the server farm and the number of applications also have an impact, but it is minimal in comparison to the number of print drivers.

2.3 Zone Data Collector

In all but very small MetaFrame environments, it is likely that a single server will be dedicated as a Primary Zone Data Collector (ZDC). The ZDC acts as a centralized information hub for the other servers as it relates to published applications, load balancing, and other data. ZDC functionality is not resource intensive but may be network intensive. Wherever possible, two NICs should be teamed as discussed in the [NIC teaming](#) section. Please see the *MetaFrame XP Advanced Concepts Guide* for specific details regarding the network traffic that is generated.

2.4 MetaFrame Web Interface, Secure Gateway and Related Servers

While the resource requirements of the Web Interface (formerly NFuse Classic), Secure Gateway (formerly Citrix Secure Gateway), Secure Gateway Proxy, and Secure Ticket Authority functionality are minimal, the networking requirements should be carefully considered. In all cases, an individual server that supports any of the aforementioned functionalities should not be a single point of failure from a resource or network perspective.

Because the servers supporting the Web Interface, Secure Gateway, Secure Gateway Proxy, and Secure Ticket Authority functionality are responsible for initiating and maintaining ICA sessions, it is strongly recommended that the NICs on these servers be teamed so as to improve throughput and enable failover, as discussed in [NIC Teaming](#) section.

Secure Gateway and Web Interface servers are usually placed in the demilitarized zone (DMZ), i.e., between two logical firewalls. Some enterprises use one physical firewall device that has a DMZ interface, whereas others may deploy several firewall devices to create multiple DMZs. Firewall devices can include a router with firewall software, a firewall blade within a large Layer 3 switch (such as the Cisco 6500), or a firewall device with multiple interfaces.

The Secure Gateway and Web Interface servers require digital certificates, which are accessed by default on TCP port 443. In order to allow external access, this port must be opened on the external firewall interface. This is usually done by means of either an access list or conduit.

2.5 File Servers

Most environments consist of one or more file servers which host user data and profiles, and which may also function as print servers. Storage Area Network (SAN) and Network Attached Storage (NAS) solutions are also becoming widely used.

Whether user data and profiles are stored on the same file server or two different servers, it is recommended that these servers be peer nodes in the same subnet as the MetaFrame servers. Otherwise, the user will need to traverse another network and thus experience additional latency when initially logging on and/or when accessing application data.

Because file and print servers are subject to heavy traffic, it may be optimal to configure these servers with more than one NIC as indicated in the [NIC Teaming](#) section to avoid creating a bottleneck. Ensuring that the NIC is not a bottleneck will minimize the latency that the users experience during logon and printing. Further, eliminating or minimizing router hops between the users and the file and print servers will increase the speed of access.

2.5.1 Profiles

Terminal Services profiles are generally stored on a file server. Of course, large roaming profiles take a long time to load. Roaming profiles enable the user to personalize settings; however, during initial logon, the user may experience additional latency when roaming profiles are used. Mandatory profiles are smaller and load much faster. Ensuring high availability and high bandwidth access to the file and print server(s) may decrease or minimize the latency associated with accessing the roaming profile.

Especially in task-oriented environments, such as a call center, the impact of a large number of users logging into the MetaFrame server farm at the same time should be carefully considered and mandatory profiles should be used where possible. When mandatory profiles are used, these may be stored on each MetaFrame server so that user logon time is minimal. If this configuration is used, the administrator should ensure that the mandatory profile stored on each MetaFrame server is an exact duplicate.

2.5.2 Home Directory

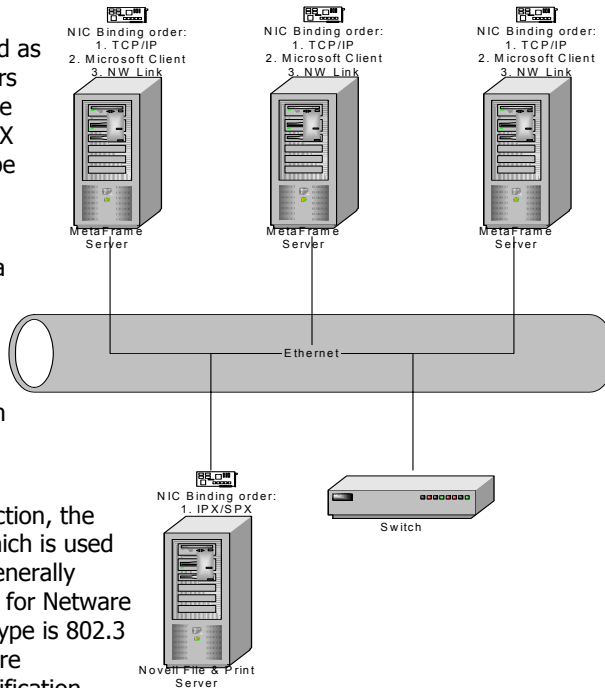
Under Windows 2000, if the Terminal Services user home directory is left blank, it will default to the same location as the Terminal Services user profile. This may or may not be the desirable result.

Pointing the home directory to a separate share point is recommended to avoid resource contention. If this directory has a high number of users, this excessive network traffic may result in additional latency for the user. Wherever possible, a distinct physical drive or SAN/NAS technology should be used to ensure resource availability.

2.5.3 Novell File and Print Servers

In some Windows MetaFrame environments, Novell servers are used as file and print servers. If Novell servers running IPX co-exist in the MetaFrame environment, it is critical that both IPX be enabled and that the frame type be configured correctly.

The most common configuration for a MetaFrame server farm supported by a Novell File and Print server(s) is as shown. Typically, the MetaFrame servers support TCP/IP as well as NWLink, Microsoft's version of IPX/SPX.



If the frame type is set for auto-detection, the default frame type is 802.2 (Sap), which is used for NetWare 3.12 and above. This generally works fine for all networks; however, for Netware 3.11 and below, the required frame type is 802.3 (Novell-ether). If both frame types are required concurrently, a registry modification is necessary (HKLM\System\Current Control Set\Services\NwlinkIPX\Parameters\Adapters\ID). Of course, the registry should be backed up prior to making changes. Dissimilar frame types will not permit traffic to traverse the network and will likely cause network issues.

2.6 Terminal Services License Server

When running Citrix MetaFrame on a Windows 2000 server (regardless as to whether Active Directory has been enabled), it is important to note that Terminal Services requires a license server which stores and tracks Client Access License (CAL) data. Thus, the MetaFrame servers must be able to connect to an activated Windows 2000 Terminal Services license server before Terminal Services licenses are issued. From a network perspective, it is advantageous for this license server to be located in the same subnet as the MetaFrame servers.

In Windows NT 4.0 domains, the domain license server can be installed on any server. In Windows 2000 mixed or native domains, the Terminal Services license server must be installed on a domain controller. Thus, the designated domain controller will support both Active Directory and

Terminal Services licensing. The Terminal Services license server should be logically located near the MetaFrame servers so that subnet traversal and network traffic is minimized.

2.6.1 Network Traffic Generated by Terminal Services Licensing Server

If the Terminal Services/Citrix MetaFrame server does not have the license server identified in Active Directory or the registry, the Windows 2000 Terminal Services/Citrix MetaFrame server polls the domain and Windows 2000 Active Directory (if enabled) in search of a License Server. These checks result in negligible network traffic.

To mitigate this traffic, identify one or more Terminal Services Licensing servers within Active Directory. By doing so, not only will the Licensing server(s) be identified properly, but also more than one Licensing server can be identified.

Active Directory will automatically recognize a Terminal Services Licensing server if it is installed as an Enterprise mode Terminal Services Licensing server by an individual with Enterprise administrator rights. Please note that the default installation for Terminal Services Licensing is the Domain mode, not Enterprise mode.

A less favorable alternative is to modify the registry in each Windows 2000 Terminal Services/Citrix MetaFrame server such that each points directly to the Windows 2000 Terminal Services Licensing server. Of course, the registry should be backed up prior to making changes. It is important to note that only one Terminal Services License Server can be designated in the registry. Further, if the Terminal Services Licensing server is changed and the registry of each server is not modified accordingly, Terminal Services licensing will fail after the temporary licenses expire 90 days later.

To select a specific license server, locate the following path in the registry:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TermService\Parameters

Add the following value:

- Name: DefaultLicenseServer
- Data type: REG_SZ
- Data value: ServerName
- Substitute the name of the appropriate license server for ServerName

Having a backup of the license server data is critical. License server backups should be done regularly and must include:

- System State data
- Lserver directory (by default located in %windir%\system32\Lserver)

For more information regarding Windows 2000 Terminal Services licensing, please see http://www.microsoft.com/windows2000/en/server/help/default.asp?url=/WINDOWS2000/en/server/help/ts_lice_c_015.htm.

3. Layer 2: NIC Configuration and Settings

Network Interface Card (NIC) configuration and settings must be properly designated to ensure maximum throughput for the MetaFrame environment.

3.1 Duplex and Speed

Both switch ports and NICs commonly default to autosensing the speed and duplex.

3.1.1 NICs

All known 10/100 or 100/1000 NICs default to autosensing the speed and duplex setting of the attached device. Autosensing identifies the highest speed and duplex that can be transmitted. For example, for a 10/100 environment, this is based on the following order: 100BaseTX full duplex, 100BaseT4 half duplex, 100Base TX half duplex, 10BaseT full duplex, and, lastly, 10BaseT half duplex.

Although Gigabit Ethernet NICs have come down in price and are now commonly shipped with new servers, the throughput associated with 1000 Mbps speed is rarely required for MetaFrame servers. NICs capable of supporting 100 Mbps speed should suffice without issue, although these should be teamed as recommended below for redundancy purposes.

The speed and duplex settings should be manually configured. Not only does autosensing introduce some latency, but sometimes the resulting setting is not optimal. Further, if the settings between the NIC and switch port are not the same, the result will be dropped frames.

When connecting to a switch, it is recommended that the NIC(s) be manually configured for full duplex and the fastest common speed for maximum throughput. If connecting to a hub, then the NIC(s) should be manually configured for half-duplex and the fastest common speed; this is required to ensure that collisions do not occur. Please note that connecting MetaFrame servers to hubs is not recommended in any size environment; switches should always be used.

When updating hardware drivers, it is a good practice to reconfirm that the full duplex and speed settings are maintained. It is possible that new NIC drivers will overwrite configured settings, in which case the default autosensing will once again be used.

3.2 Protocols

Having several protocols bound to the NIC could cause unwanted latencies within a MetaFrame environment, so it is recommended that any unnecessary protocols be removed. Protocol binding order is important to make sure that data is sent from the most commonly used protocol first, since each protocol is attempted sequentially. Since most MetaFrame environments utilize TCP/IP as the primary protocol, it is suggested that the MetaFrame server binding order should be the following:

- TCP/IP
- Client for Microsoft Networks
- NWLink or IPX/SPX (if present)

3.3 Multiple NICs

Having two or more NICs present in a MetaFrame server is common. These may be configured for NIC teaming/Cisco EtherChannel support, failover, and/or multi-homing. Of these, NIC teaming is considered a best practice, and multi-homing is discouraged since it is frequently not configured correctly and may create security holes. Multiple NIC options are discussed in the order of most desirable to least desirable configurations.

3.3.1 NIC Teaming

There are several NIC teaming technologies available today from switch vendors. Cisco uses the term "Fast EtherChannel." Various switch vendors use various terms, and these may or may not provide the same exact functionality.

Cisco Fast EtherChannel is a failover and load-distribution technology wherein the same MAC address or IP address is bound to two or four Fast Ethernet or Gigabit Ethernet NICs, providing parallel links. This translates into high bandwidth, load sharing, and redundancy. Citrix MetaFrame supports this technology, and it is considered a best practice where feasible.

It is unlikely that more than two Fast EtherChannel links will be required per MetaFrame server. The primary purpose for using EtherChannel is to ensure redundancy in the event of a NIC or switch port failure; network bandwidth and load requirements in a well-running environment are generally not higher than a single full-duplex FastEthernet NIC can support. In addition to the basic redundancy provided by the virtual interface created during EtherChannel teaming, EtherChannel does improve on the load capacity of the NIC by providing double (in the case of two NICs) or quadruple (in the case of four NICs) the throughput of one NIC.

EtherChannel is sometimes configured improperly, causing the optimization goals expected to instead create a multitude of network issues. All switch ports must belong to the same [Virtual LAN](#) or subnet. The same speed and duplex settings must be available and configured on both the switch port and the NIC. Further, Cisco IOS version 12 or higher should be used.

When configuring the switch to support EtherChannel, the port group can be created automatically using Port Aggregation Protocol or by manual configuration. The latter is recommended to create a port group for the switch ports that will correspond to the teamed NICs. This exact command for creating a port group varies according to the switch model. For example, the network administrator would configure EtherChannel using the following command on each of the switch ports to be aggregated:

```
2900B(config-if)#port group [#] distribution [source|destination]
```

If source is chosen as the distribution method, then all blocks of incoming packets from the same source will traverse through the same port. This is the default and is recommended. If destination is chosen as the distribution method, then all incoming packets are forwarded based only on the destination.

Contiguous ports must be used for EtherChannel connections on some stackable Cisco switches. Thus, in a Cisco environment where this is required, on a 12-port switch, bundle the connections into ports 1-4, 5-8, or 9-12; on a 24-port switch, it is best to bundle the connections into ports 1-8, 9-16, or 17-24. On the larger non-stackable Cisco switches, such as the 6500 series, EtherChannel ports should be spread across blades to provide higher redundancy.

Use of EtherChannel technology requires support from the server hardware vendor, NIC vendor, and layer-2 switch vendor. As of September 2002, Cisco supports NICs from the following vendors: Adaptec, Auspex, Compaq, Hewlett-Packard, Intel, Phobos, Sun Microsystems, and ZNYX.

When using the Compaq drivers, the most up-to-date teaming driver as of December 2002 is CP002710.exe, which installs Compaq driver version 7.11.711.1. Use Add/Remove Programs to load the teaming driver; failure to do so may cause the NIC teaming to appear to be configured but not actually do so. After the teaming driver is loaded, each NIC should be manually set to the maximum speed and full duplex. Then, the NICs should be selected and Team should be chosen. Lastly, the Teaming Controls should be set to Load Balancing and Switch-Assisted Load Balancing. Load balancing can be achieved via MAC address or IP address. Using the MAC address for load balancing is advantageous since it is performed at layer 2, which is the same OSI layer where the switch resides. Teaming by IP address is not recommended since IP address can change and are dependent

upon server configuration and MAC address. After configuring NIC teaming, reboot if necessary and reset the TCP/IP address of the single newly teamed virtual NIC; failure to do so will likely result in the NIC defaulting to a 169.254.x.x address, which will not communicate properly with the server farm.

To avoid issues with Spanning Tree, either the switch ports connected to the MetaFrame server NICs could be disabled from participating in Spanning Tree or PortFast should be used. The latter is recommended. PortFast enables switch ports that will not participate in Spanning Tree to connect to the network in less than one second by entering the "forwarding" state. Thus, the 50-second Spanning Tree process is minimized.

To configure a Cisco 2900 switch for PortFast, the following should be configured for each switch port that connects to a MetaFrame server NIC that is using EtherChannel teaming.

```
2900B(config-if)#spanning-tree portfast
```

When using the Intel NICs, the PROSet II drivers provide the functionality needed for NIC teaming. With Windows 2000, PROSet II needs to be installed as a separate component in addition to the Intel PRO drivers. To configure teaming, right click the desired NIC within the PROSet II configuration screen and follow the wizard. The same options discussed above for the Compaq NICs are presented.

It is very important that servers be updated with the latest NIC drivers and that the NIC settings be rechecked after updating NIC drivers. New NIC drivers may override previously configured settings. Of course, specific instructions from your network vendor should be followed explicitly.

3.3.2 Failover

Failover implies that only one NIC will be active at any given time and that the secondary NIC will only automatically be activated if the primary fails. While failover does provide redundancy, it does not provide the additional throughput nor load distribution that is available with NIC teaming. In environments where the switch will not support connecting teamed NICs to different blades, failover is considered the best option.

The process of failing over to the secondary NIC introduces a slight delay of less than 0.5 seconds during the transition. When tested in a laboratory environment, this delay was not enough to drop active ICA sessions.

3.3.3 BackUp NICs

Although it is highly unlikely that a NIC failure will occur, a single NIC may represent a single point of failure in a MetaFrame environment. Thus, where NIC teaming is not selected because of a lack of available switch ports or other reason, a second NIC card installed in each server can be used as a backup.

If the second NIC is used as a backup, Windows 2000 will usually automatically detect it as part of the Plug 'n Play process; however, the TCP/IP settings should be configured and then disabled under Device Manager. Of course, should the primary NIC fail, then the backup NIC should be manually enabled and connected to the switch port, thus ensuring users' continued access to applications.

3.3.4 Multi-Homed MetaFrame Servers

A multi-homed server is one that contains two or more NICs with different IP addresses that are usually connected to different subnets. The most common reason for multi-homing a MetaFrame server is to connect directly to a database server, file server, or other data source that is located on another subnet.

When connected to two or more subnets, the MetaFrame server will communicate directly with these subnets. By going directly to a subnet, the security associated with the router interface(s) is

circumvented and security holes may be created. Multi-homing MetaFrame servers is not recommended for security reasons.

Enabling multi-homing on a MetaFrame server for the purpose of creating a direct connection from the MetaFrame server to one or more additional networks may introduce undesired latency and unwanted results if not configured properly. Beginning with MetaFrame XP with Feature Release 1, multi-homing is supported for TCP/IP only if is configured as specified within the *Citrix MetaFrame XP Advanced Concepts Guide*. To properly multi-home a MetaFrame server, only one NIC should contain a default gateway address. If any additional NICs require access to IP addresses on another subnet that is not accessible, a static route should be configured; a default gateway should not be configured for any additional NIC(s).

4. Layer 2: Switch Configuration and Settings

Proper configuration of the switch ports enables MetaFrame traffic to traverse the network. This may include

4.1 Layer 2 and 3 Switch Technologies

Using Layer 2 switch FastEthernet connections ensures that each MetaFrame server is its own collision domain. The only frames that all clients within the same subnet see are broadcasts.

Each interface should be set to full duplex and the fastest common speed as described in the [NIC Teaming](#) section. Thus, each server's inherent bandwidth is doubled and contention for the switch port is eliminated. This also eliminates the potential for collisions.

Layer 3 switches provide Layer 2 switch functionality but also includes a routing module so that data can traverse subnets via the same physical device. Layer 3 switches are more efficient because they "route once, switch many."

4.2 Configuration of a Switch Ports

When setting the switch port to support full duplex, it is important to ensure that the corresponding NIC to which it is connected is likewise configured for full duplex on the specific port. If this is not done, then the Layer 2 switch may not provide full-duplex functionality, the setting may essentially be overridden, frames may be dropped, and/or disparate network connection speeds may result in network latency or other issues. The most common result is dropped frames. Further, the speed should match the fastest common NIC speed capability.

For example, on a Cisco access-layer switch, if the layer-2 switch port is FastEthernet, then the default is Auto, signifying that the port auto-negotiates the duplex setting (full vs. half duplex) as well as speed (10 vs. 100). Setting the switch port to Full implies that only full-duplex communications will occur. Although this reduces CPU resources associated with auto-negotiation, it also requires that the NIC be set to full duplex in order to guarantee full duplex communications. If a NIC is replaced or a previously configured full-duplex NIC is modified, then it is possible that communications with the switch may not occur correctly; in this case, the Layer 2 switch port will be expecting full-duplex transmissions and the NIC may providing another type of transmission. It is likely that frames will be dropped when mismatches in duplexing and/or speed are present.

Similarly, with network cabling, the lowest common denominator or the weakest link will dictate the speed of the connection. Using a 10 Mbps switch port or Category 3 patch cord will force a maximum speed of 10 Mbps, no matter what other speed settings are configured. Hubs are layer 1 devices which only transport signals and are not configurable; hubs require half-duplex setting. As stated earlier, hubs are not recommended for networking MetaFrame servers. For a review of the [OSI model](#), please see Appendix B.

Connectivity options for the various Ethernet speeds are as follows. Please note that Gigabit half duplex is generally not an option.

This NIC Setting:	Should be used for this device:
10 Mbps Half Duplex	10 Mbps hub
100 Mbps Half Duplex	100 Mbps hub
10 Mbps Full Duplex	10 Mbps switch port set to Full Duplex
100 Mbps Full Duplex (recommended)	100 Mbps switch port set to Full Duplex
1000 Mbps Full Duplex	1000 Mbps switch port set to Full Duplex

On a Cisco 1900, 2900, or 3500 series switch, to configure the Layer 2 switch port for full duplex, the network administrator would use the following command from the interface in privileged mode:

```
2900A(config-if)#duplex full
2900A(config-if)#speed 100
```

As part of this process, the network administrator may also wish to configure a permanent MAC address to a specific Layer 2 switch port associated with each MetaFrame server. The advantage of a permanent address is that it never ages out, meaning that the switch never has to learn or relearn the MAC address association because it remains permanent in the Content Addressable Memory (CAM) of the switch. The disadvantage is that if a NIC is replaced, it will not be able to communicate with the switch since the switch is expecting traffic from another previously identified MAC address; the MetaFrame server will therefore not be able to communicate with the switch port.

On a Cisco 2900 series switch, to configure the permanent MAC address association, the network administrator would use the following commands in privileged mode:

```
2900A(config)#mac-address-table permanent [MAC Address] [port]
```

Please note that Citrix Technical Support does not support the configuration of the switch and MAC address; please contact your switch manufacturer.

5. Layer 2: WANs and Remote Access

Users frequently connect to MetaFrame servers over WAN connections. This section discusses RAS, VPN, Web Interface, and Secure Gateway as mechanisms for connectivity, as well as general WAN issues. Mechanisms for maximizing WAN bandwidth are also discussed.

5.1 WAN Connectivity

The most common reason for dropped MetaFrame sessions is insufficient bandwidth across WAN links. MetaFrame sessions should be estimated at an average minimum of 20 Kbps of bandwidth unless application-specific testing indicates otherwise. If sufficient bandwidth is not available, it is likely that the user experience will be poor, including dropped sessions.

Particularly as it relates to satellite connections and wireless wide-area networks, consistency of the connection is important; dropped frames are not conducive to consistent ICA connections. If a user connection is dropped, the Version 6.00 and higher ICA Clients will automatically attempt to reconnect the user connection.

When architecting or diagnosing network issues within a MetaFrame environment supporting a large number of users, not only should 20 Kbps per user be allocated, but also additional capacity must be allocated for ICA session printing, non-MetaFrame traffic, and general overhead, e.g., routing protocol broadcasts or multicasts, routing decisions, and ICMP traffic as applicable.

In particular, misunderstandings regarding frame relay links should be investigated. When contracting for frame relay service from a provider, two metrics are used: CIR and Burst. CIR, or Committed Information Rate, signifies the contracted bandwidth, whereas Burst signifies additional throughput that will be provided if and when available. Since the service provider is only required to provide the CIR throughput contracted, the administrator should plan accordingly.

According to Cisco, every switch, router, and distance of approximately 100 miles each increase latency by as much as 1 millisecond. Unfortunately, it is impossible to estimate the maximum latency that will be acceptable to users due to variations in the applications, WAN links, and user tolerance.

5.2 ICA Session Monitoring and Control

On <http://www.citrix.com/cdn>, Citrix has made available the ICA Session Monitoring and Control Software Development Kit (SMC SDK). This developer's kit exposes APIs that can be used to create applications to control many network-related facets of ICA sessions.

The SMC Console is an example of the SMC SDK and can be loaded on any MetaFrame server with Feature Release 2 and above. This tool provides a rudimentary means of testing and troubleshooting applications based on bandwidth requirements, latency, virtual channels, and other network-related capabilities.

5.3 Complex Caching and Encapsulation

Complex caching and encapsulation implies network appliances that use patented caching technologies that transparently maximize network bandwidth. This technology inherently includes numerous ICA-related features. While the ICA protocol caches on a per-session basis, both Expand Networks (<http://www.expand.com>) and Peribit (<http://www.peribit.com>) take it one step further by caching unchanged portions of the screen for multiple sessions based on the entire site. Thus, if users typically access one or few applications, it is likely that many of the screen bitmaps are housed on the proprietary network device closest to the clients. Further, both Expand and Peribit encapsulate multiple ICA packets so that fewer large packets traverse the WAN link instead of many small packets.

5.4 Queuing/Quality of Service (QoS)

Quality of Service implies a queuing policy that prioritizes specific packet types as they traverse through the router. QoS is most commonly implemented for WAN connections because LANs typically have abundant bandwidth available. QoS solutions are offered by Cisco and other router vendors. In addition, Packeteer (<http://www.packeteer.com>), and Sitara (<http://www.sitara.com>) offer additional QoS offerings. The solutions offered by Packeteer and Sitara require additional hardware. These solutions allow the administrator to monitor traffic traversing the network and the apply policies depending on the prioritization desired.

Cisco routers are discussed in detail within this paper because most MetaFrame installations already employ Cisco routers. Packeteer and/or Sitara products may provide optimal QoS solutions. Both companies are Citrix Business Alliance partners and their solutions should be investigated as appropriate.

On Cisco routers, the commonly available QoS types are: first in/first out (FIFO), weighted fair queuing (WFQ), priority queuing, custom queuing, and, most recently, network-based application recognition (NBAR). Weighted fair queuing is the default on WAN links at E1 (2.048 Mbps) or slower, and First In/First Out is the default on all WAN and LAN links above E1 speed. Most recently, Cisco has also added class-based weighted fair queuing and low-latency queuing; however, these new technologies are very complex and are beyond the scope of this document. As further defined below, these alternatives allow the network administrator to very specifically define the type(s) of packets to be prioritized.

The most common Cisco QoS types and associated characteristics are:

Parameters/Method	Weighted Fair Queuing	Priority Queuing	Custom Queuing
Queue Basis	None	4 queues	16 queues
How Serviced	Low volume traffic prioritized	High priority queue prioritized	Round robin
Where Used	WAN links < 2 Mbps	WAN or LAN	WAN or LAN
How configured	Default	Manual	Manual

Especially in MetaFrame environments in which users are accessing the server farm over congested WAN links, QoS alternatives will provide performance benefits for ICA traffic. If ICA packets are consistently dropped as they traverse the network, it is not unlikely for the user session to likewise be disconnected. For example, if one user in a remote office is transferring a very large file that consumes all available bandwidth and this transfer receives preference over ICA traffic, another user that is using MetaFrame will likely experience a dropped connection.

MetaFrame traffic is very small (approximately 20 Kbps), but it is critical that the packets arrive without delay or retransmission wherever possible. Although one feature of MetaFrame is that it will reconnect a user to his previous session (depending on the timeout setting), the user experience will likely not be positive if frequent reconnections are required.

Although the political climate in many companies dictates that QoS is not implemented in any fashion, it is strongly recommended that both the benefits of QoS and its implications be reviewed in detail.

5.4.1 First-In, First-Out (FIFO)

First-in, first-out simply implies that packets are processed sequentially, with no concern for prioritization. This is the default for LANs and WANs above 2.048 Mbps.

5.4.2 Weighted Fair Queuing (WFQ)

Weighted fair queuing is a dynamic prioritization algorithm and is the Cisco default on all interfaces supporting WAN speeds below 2.048 Mbps (E1). It is a method of prioritizing delay-sensitive packets, thus disallowing high-volume traffic from consuming all available network bandwidth.

WFQ sorts traffic into conversations based on source and destination addresses or ports, frame relay connection, and QoS and then ascertains that each conversation fairly shares the network bandwidth. Low-volume traffic is given priority over high-volume traffic, and this ensures that each concurrent session has balanced use of the available bandwidth.

WAN interfaces operating at speeds greater than 2.048 Mbps are not available for weighted fair queuing; Ethernet interfaces cannot use WFQ.

5.4.3 Priority Queuing

Priority Queuing allows you to set up a priority on a particular protocol and port number. It is straightforward in that anytime a router receives a packet with that protocol and port number, it is given high, medium, normal, or low priority, in that specific order. All high traffic flows first, then all medium traffic, and so on.

By using priority queuing, however, other non-prioritized protocols or port traffic may not be given the opportunity to transmit traffic and/or be limited if there is significant amount of higher priority traffic passing through the router. For example, during periods of prioritized large file transfer traffic, there may not be sufficient network bandwidth for ICA traffic, an FTP session, or non-ICA print job.

Priority queuing is not difficult to configure. To configure priority queuing, the network administrator needs to create a priority queuing list, assign a default queue for all other traffic, and then assign the priority list number to an interface. Optionally, an [access list](#) can be used to define incoming traffic for prioritization, and the priority queue size can be modified, however the latter is not recommended and may cause packets to be dropped.

As an example, to set TCP 1494 and UDP 1604 to high status and all other traffic to normal, the network administrator in privileged mode could enter the following:

```
RouterA(config)#priority-list 1 protocol ip high tcp 1494
RouterA(config)#priority-list 1 protocol ip high udp 1604
RouterA(config)#priority-list 1 default normal
RouterA(config)#int s0
RouterA(config-if)#priority-group 1
```

In privileged mode, the network administrator can confirm the priority queuing settings by entering "show queueing priority". Note the spelling of queueing in this case. Sample output from this configuration is as follows:

```
RouterA#show queueing priority
Current DLCI priority queue configuration:
Current priority queue configuration:
List           Queue           Args
1              high            protocol ip      tcp port 1494
1              high            protocol ip      udp port 1604
```

5.4.4 Custom Queuing

Custom Queuing allows a finite number of bytes of each specified class of traffic to be transmitted by the router. It provides the ability to set up 16 different queues that act in a round robin format. This is similar to the methodology behind 802.5 token ring in that each queue can transmit traffic. However, the size of each queue can be set to an unequal number of bytes so as to allow one or more types of traffic to transmit a higher or lower number of bytes.

The router processes packets sequentially in a round robin format. The administrator sets the byte length for a specific queue so that multiple packets from the same protocol are transmitted up to the total allocation. If there are no packets in the queue to be processed or the queue is only partially full, the router does not remain idle at that queue; it moves on to the next queue in sequence and begins servicing it. This is considered a better alternative than Priority Queuing due to its level of customization but is more complex to configure.

The process for configuring Custom Queuing is as follows:

- Set custom queue filtering for a protocol or interface
- Assign a default custom queue
- Configure the maximum number of bytes per queue
- Assign the custom queue list to an interface

As an example, the network administrator in privileged mode may wish to allocate five times (5x) as much bandwidth to TCP 1494 and UDP 1604 (in queue 1) as compared to all other network traffic (in queue 2) and could enter the following:

```
RouterA(config)#queue-list 1 protocol ip 1 tcp 1494
RouterA(config)#queue-list 1 protocol ip 1 udp 1604
RouterA(config)#queue-list 1 default 2
RouterA(config)#queue-list 1 queue 1 byte-count 30000
RouterA(config)#queue-list 1 queue 2 byte-count 6000
RouterA(config)#int s0
RouterA(config-if)#custom-queue-list 1
```

In privileged mode, the network administrator can confirm the priority queuing settings by entering "show queueing custom". Note the spelling of queueing in this case. Sample output from this configuration is as follows:

```
RouterA#show queueing custom
Current custom queue configuration:
List      Queue      Args
1         2          default
1         1          protocol ip      tcp port 1494
1         1          protocol ip      udp port 1604
1         1          byte-count 30000
1         2          byte-count 6000
```

5.4.5 Network-Based Application Recognition

Beginning with the Cisco IOS 12.1(2)E, Network-Based Application Recognition (NBAR) was enabled for Citrix ICA traffic. NBAR 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.

NBAR is only effective where published applications exist; MetaFrame environments that publish the desktop use the same session parameters and therefore cannot be differentiated. Further, the application would need to be published in seamless, non-session sharing mode in order to differentiate based on the application name. Configuring NBAR is complex and should only be done by experienced network administrators.

To disable session sharing, the MetaFrame administrator must modify the registry in each Windows 2000 Terminal Services/Citrix MetaFrame server. In general, disabling session sharing will not have a negative impact on the MetaFrame servers; however, it may have an impact depending on the applications served. For example, if the client were hosting Microsoft Office through NFuse, the users would open a new environment for each application launched. 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 server farms, this may have a greater impact. Disabling session sharing will enable NBAR to differentiate the applications with the granularity required. Of course, the registry should be backed up prior to making changes.

To disable session sharing, locate the following path in the registry:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\WFSHELL\TWI

Add the following value:

- Name: SeamlessFlags
- Data type: DWORD
- Data value: 1

To confirm the port numbers in use by the router from privileged mode, the following can be used:

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

Please note that UDP port 1604 is not used by MetaFrame XP by default. It can be invoked for backwards compatibility with older ICA clients.

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]
```

Thus, IP QoS classification can be applied to the specific MetaFrame application, not merely the TCP ports that are used to traverse the network.

5.5 Firewalls

To enable access to environments with MetaFrame XP behind a firewall without Secure Gateway or Web Interface, access via the Citrix XML service (default is TCP port 80) should be enabled. The Citrix XML Service is a Windows service that provides a means of encapsulating ICA browsing traffic within HTTP. Optionally, beginning with Citrix MetaFrame XP Feature Release 1, digital certificates were supported on MetaFrame servers. Thus, Secure Socket Layer (SSL) relay service can provide additional security as it traverses TCP port 443. To use SSL, a certificate is required for each MetaFrame XP Feature Release 1 or higher server. Unless Secure Gateway is deployed, it is necessary to open TCP port 1494 on the firewall so that external users may access internal MetaFrame servers, thus allowing ICA traffic to traverse the network. Of course, if the default ports are modified, the renamed ports should be substituted. For specific port requirements, see [TCP Port Numbers](#).

In previous versions of MetaFrame, it was necessary for clients to communicate with MetaFrame servers via UDP port 1604. MetaFrame XP no longer has this requirement unless it is specifically enabled, such as when Version 4.00 and older ICA Client versions are still in use.

Firewalls can be configured to block Java applets and/or ActiveX controls. For example, the Java ICA client is a Java applet that runs in the browser. This should be considered if the ICA Java client

and/or ActiveX control (web client) will be implemented. The firewall configuration should be thoroughly tested to ensure that client connections are permitted and can run as expected.

Wherever possible, it is recommended that the external users be explicitly permitted in the firewall configuration as an extra measure of security. Depending on the firewall software, external users can generally be identified by source TCP/IP address or network. This helps ensure that unauthorized users do not gain access to the MetaFrame server farm. Auditing should also be deployed if the firewall resources can support it.

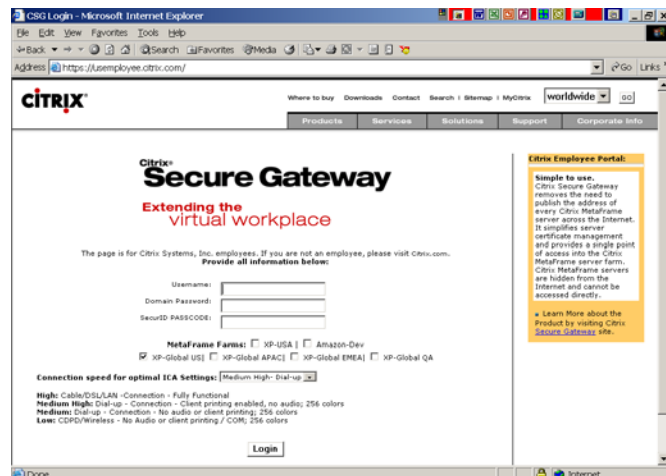
5.6 Web Interface

Web Interface, formerly known as NFuse Classic, dynamically provides application icons to users based on permissions so that users may access their applications. Web Interface may be deployed within the DMZ, but by doing so without the use of Secure Gateway, TCP port 1494 must be opened on the external firewall interface. Web Interface can include a digital certificate; however, when this level of security is desired, Secure Gateway is generally deployed.

A minimal amount of network traffic is generated when clients access the Web Interface web site. The interaction with the MetaFrame server farm is based on generating the client's list of published applications and then connectivity to the specific MetaFrame server(s) that will host the application(s). The session connection to the MetaFrame server(s) uses the same ICA protocol bandwidth as the traditional Citrix Program Neighborhood or Remote Application Manager.

5.7 Secure Gateway

Since its introduction in December 2001, Secure Gateway has been used as an easy-to-use access method from a standard web page. This add-on product requires a digital certificate, and users gain access the MetaFrame server farm securely via SSL or TLS, which is done over TCP port 443 by default. The user connection is proxied, and information such as MetaFrame server IP address remains hidden.



5.8 VPN

VPN connections use a DSL or other internet connection to then create a virtual tunnel into the corporate network. Since the public Internet is the means of access, security is critical to ensure that the MetaFrame servers being accessed are not compromised. Some type of encryption is suggested, the strongest being 3DES. Network bandwidth requirements will increase slightly as a result of using high encryption, and users may experience some additional latency as a result of high encryption. Thus, the critical issue of latency versus security must be considered and evaluated.

5.9 Dial-Up Directly to the MetaFrame Server

Although generally used only in very small MetaFrame environments, it is possible to access the MetaFrame server farm by dial-up connection directly via modem to a MetaFrame server. Using one or more Telephone API (TAPI) modems installed in the MetaFrame server, the modem(s) can be configured as Async connections. In Citrix Connection Configuration, modem connection(s) will show as Async and may need to be configured accordingly.

5.10 RAS

A Remote Access Server (RAS) is typically used for dial-in connections. RAS connections are point-to-point and asynchronous, i.e., the user dials directly into the RAS server. RAS does not typically

add a significant amount of overhead and presents no hindrance to using MetaFrame since typically only 20 Kbps is required and most RAS connections are in the 40 Kbps to 50 Kbps range. A minimum connection of 28.8 Kbps is recommended to access and adequately maintain a MetaFrame session.

5.11 Network Security

Security requirements must be weighed against any the latency impact associated with additional authentication, encapsulation, encryption, and/or other security measures. Network security presents many challenges that are beyond the intended scope of this document.

6. Layer 3: IP Addressing

6.1 Minimizing Broadcast Traffic

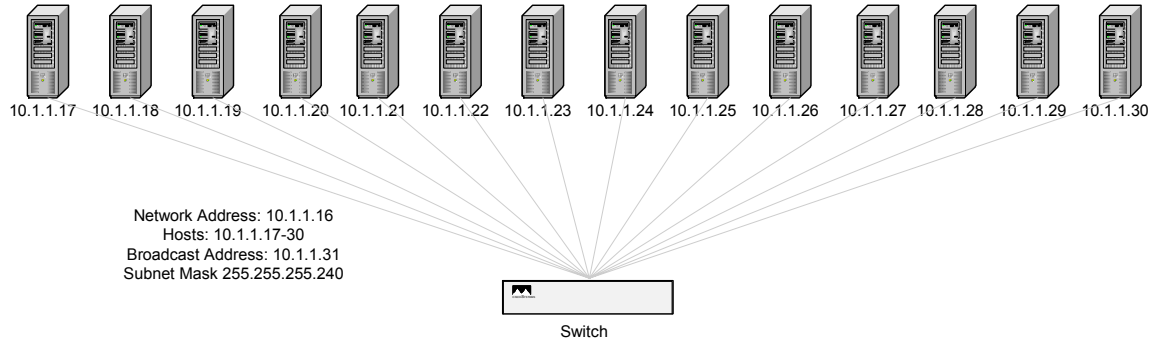
IP addressing encompasses the IP identification of the server. To minimize cross-network broadcast traffic, two technologies are commonly used: subnetting and virtual LAN. These are discussed below.

6.1.1 Subnetting and Variable-Length Subnet Masks (VLSM)

In a standard networking environment, when a broadcast is received on a subnet, each host acknowledges the packet, although only the host(s) with the destination IP address and corresponding MAC address respond.

Subnetting creates smaller broadcast domains. Subnetting the network wherein the MetaFrame servers are located is an excellent method of ensuring that both network broadcasts and network traffic are minimized. If the number of hosts within the network is minimized by subnetting, only the packets that are actually destined for the segmented group MetaFrame servers will reach that subnet. Please see [Appendix A](#) for more detailed information regarding allowable variable-length subnet mask configurations.

For example, if the MetaFrame environment consists of a total of 14 servers, including 12 MetaFrame servers, one file/print server, and a Terminal Services license server, using static TCP/IP addresses such as 10.1.1.17 through 10.1.1.30 with subnet mask 255.255.255.240 or /28 would keep network traffic segmented just amongst the MetaFrame related servers. In this case, the network address is 10.1.1.16 and the broadcast address is 10.1.1.31. However, if additional servers were to be added to the network, the subnet mask would need to be modified, since the /28 subnet mask only supports 14 hosts.



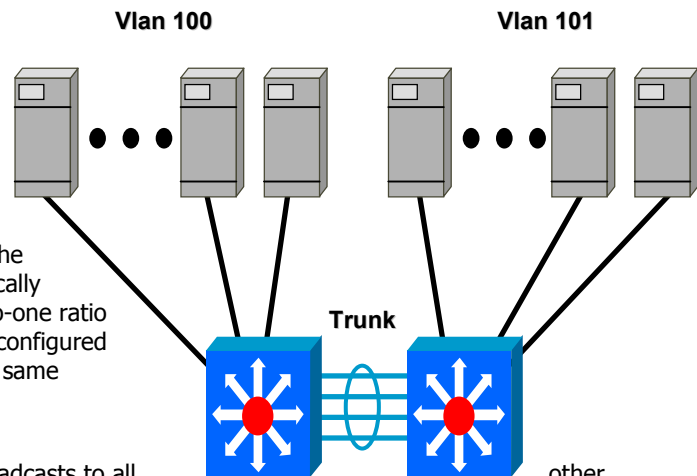
If two additional MetaFrame servers were to be added to the MetaFrame segment, modifying the subnet mask to be 255.255.255.224 or /27 would allow 30 hosts per subnet. If the router does allow use of the first and last IP range within a subnet (on Cisco routers, this is implemented via the "ip subnet-zero" command), then only that only the subnet mask would need to be modified and the additional servers could be allocated TCP/IP addresses with lower numbers in the last octet without issue. In this case, only the subnet mask of the static IP configuration of the 14 servers existing in the current MetaFrame environment would need to be modified, and the two additional MetaFrame servers would need to be designated with lower TCP/IP addresses, e.g., 10.1.1.2/27 and 10.1.1.3/27. If using an older router or operating system that does not utilize the first and last IP range within a subnet, then, for example, all servers in the subnet would need to be modified to use static TCP/IP addresses, e.g., 10.1.1.33 through 10.1.1.62. In this case, the network address becomes 10.1.1.32 and the broadcast address becomes 10.1.1.63. Static TCP/IP addresses 10.1.1.49 through 10.1.1.62 would then be available for growth.

If the two additional MetaFrame servers had been assigned the sequential TCP/IP addresses of the original segment without the modifications discussed above, the resulting addresses would have equated to the network broadcast address of the original network (10.1.1.31) and the TCP/IP network address of the subsequent yet unknown network (10.1.1.32). This would generate network instability, broadcast, undesirable network traffic, and other potential problems and should be avoided.

Proper design and ongoing review of the network segmentation is strongly recommended for the health of the MetaFrame environment. Citrix Consulting Services frequently finds that undesirable network broadcasts and bottlenecks are the result of improper network subnetting.

6.1.2 Virtual LANs

A virtual LAN (VLAN) is a Layer 2 switching technology used to create segmented broadcast domains. Switch ports are configured so as to designate each port or MAC address as part of a specific VLAN. Either the physical switch port is statically assigned to the VLAN or the MAC address of the server can be dynamically assigned to the VLAN. Generally, a one-to-one ratio exists between a VLAN and a subnet. All configured devices in each VLAN are members of the same broadcast domain.



Instead of propagating multicasts and broadcasts to all ports on one or more switches, only the port(s) logically defined as being within the same VLAN receive the multicasts or broadcasts. This is dictated by the source port and IP address. It is becoming more popular to use Layer 3 switches to support VLAN technology for separating smaller subnets, with reliance on more complex and expensive routers only for inter-LAN traffic.

When the VLAN spans multiple switches, trunk links are used to extend the VLAN from one switch to another. For flavors of Ethernet, either Cisco's proprietary Inter-Switch Link (ISL) protocol or the IEEE standard 802.1q frame tagging are used for inter-trunk link communications. When network traffic needs to cross from one VLAN to another, Layer 3 routing functionality is required.

MetaFrame servers can benefit greatly by being associated with the same subnet and VLAN. If MetaFrame servers are not physically co-located and plugged into the same switch, VLAN technology may provide the best solution since this technology allows the MetaFrame servers to logically reside on the same subnet. This may be particularly useful for a backup server farm or operations center that is located elsewhere.

6.1.3 Subnets and Zones

The architecture of MetaFrame XP allows for the placement of servers into zones, which are generally defined by the physical location. Technically, MetaFrame servers in the same farm may reside within different subnets, although this will create additional load on the network and associated router(s) that transport the traffic.

If all the MetaFrame servers are in one physical location, then a single zone is most likely the best architecture. Where possible, the single zone should reside within a single VLAN and/or subnet to minimize network traffic. Additionally, other MetaFrame-related servers, such as the Data Store database server, should be co-located in that subnet if possible.

7. Layer 3: Routers

Ensuring that network traffic is minimized and that all router settings are optimized ensures that packets traverse the network most efficiently.

7.1 Layer 3 Routing

Layer 3 of the [OSI Model](#), Network, consists of:

- **Routing:** Determining where and how to send a packet, as well as transporting it
- **Switching:** Actually transporting the packet from one subnet to the subsequent subnet

7.2 Routers

Enterprise-grade routers should be used to support LAN and WAN traffic. Cisco networking equipment has been referenced within this white paper because it is market share leader and commonly found within most MetaFrame environments; however, a business decision should be made regarding routers from any vendor that can effectively support the required routing needs.

7.3 Windows 2000 Routing

Windows 2000 includes the Routing and Remote Access Service (RRAS), and these routing capabilities are discouraged even for small, non-complex Layer 3 routing environments. Windows 2000 routing provides capabilities for DHCP relay agent, Network Address Translation (NAT), Routing Information Protocol (RIP) versions 1 and 2, and Open Shortest Path First (OSPF).

Traditional routers provide not only routing but also security features. Thus, it is strongly suggested that an RRAS server not be placed into the MetaFrame environment.

8. Layer 4: TCP Ports

A number of TCP ports are used for MetaFrame-related traffic, as defined within this section.

8.1 TCP Port Numbers

A number of TCP port numbers are used for MetaFrame traffic and are modifiable as indicated below:

Purpose	Environment	Port number	Modifiable
ICA	All	TCP 1494	Yes
Citrix XML Service	MetaFrame XP	TCP 80 (HTTP default generally chosen)	Yes
SSL	MetaFrame XP with Feature Release 1 and above (optional), Secure Gateway 2.0, and Web Interface 2.0 (optional)	TCP 443	Yes, although very uncommon
MetaFrame XP IMA	MetaFrame XP (inbound - server to server)	TCP 2512	Yes
MetaFrame XP DS	MetaFrame XP (outbound – server to data store server)	TCP 2512	Yes
MetaFrame XP CMC	MetaFrame XP (CMC to host server)	TCP 2513	Yes, with FR1 and higher
SQL Server, Oracle, or DB2 databases	MetaFrame XP	TCP 139, 523, or 1433	As required by database

In addition, if RDP is used for testing, the TCP port 3389 should be enabled.

Prior to changing any modifiable ports, it is recommended that "netstat -a" be issued from the command prompt to list the TCP ports in use. Any unused port between 0 and 65535 may be used, although it is recommended that an unused port number above 1023 be used for this purpose.

8.1.1 ICA TCP Port Number

The default TCP port 1494 is used for inbound traffic to the MetaFrame servers. Outbound traffic is via a dynamically chosen TCP port number. To configure the inbound TCP/IP port number used by the ICA protocol on the MetaFrame server, modify as follows:

- At the command prompt, type ICAPORT /port:x, where x is the new port number.

The server then must be rebooted and the ICA-tcp listener port must be reset.

This process must be repeated on every Citrix MetaFrame server in the environment and the administrator must also modify every Citrix ICA Client that will connect to that server. To ensure that this change is performed uniformly on all servers and clients, it is suggested that some type of batch file or script be used.

8.1.2 Citrix XML Service Port Number

Citrix XML service and Web Interface can be configured to use any port number between 0 and 65535; however, the default and most common configuration is to share port TCP 80 (HTTP) for this purpose. The ISAPI .dll file used with Web Interface allows TCP port 80 to be shared with the web server.

To change the XML Service port number, first stop the Citrix XML Service (Control Panel→Administrative Tools→Services) and then close the Services window. At a command prompt, type `ctxmlss /u` to unload the Citrix XML Service from memory. Type `ctxmlss /rx`, where *x* is the number of the port you want to use. For example, `ctxmlss /r8080` forces the Citrix XML Service to use TCP/IP port 8080. Then restart the Citrix XML Service in the Control Panel.

Important: If you change the XML Service port on one MetaFrame server, you must repeat the change on all other MetaFrame servers in the farm in order for the ticketing feature of Web Interface or NFuse Classic to function. Note also that any MetaFrame server providing XML data to Web Interface or NFuse Classic should have network connectivity to the XML service port on all other MetaFrame servers in the farm.

If using access lists on the router, be sure to add this port number to the router's access list, so that the Citrix XML traffic will traverse the network appropriately. See the [Access List](#) section for further information.

8.1.3 SSL Port

When installing Microsoft Internet Information Server (IIS) 5.0, whether as part of an initial installation or as an add-on component, TCP port 443 is the default for SSL connections. This port number is also the default on routers and firewalls. If Secure Gateway is deployed, then the default TCP port 443 (or other defined port) must be open on the routers and/or firewalls.

8.1.4 MetaFrame XP Port Numbers

The default TCP ports 2512 and 2513 are used for MetaFrame XP traffic. To configure the TCP/IP port number used by the IMA protocol on the MetaFrame server, modify as follows:

- At the command prompt, type `IMAPORT /set {IMA:<num> | DS:<num> | CMC:<num>}`

See chart above for default port numbers. This process modifies the port number on the local machine only.

See the *MetaFrame XP Administrator's Guide* for more detailed instructions.

8.1.5 Database Port Numbers

Please see documentation from the specific database vendor in order to determine whether the port number is modifiable, and if so, how it should be done.

9. MetaFrame Server Network Environment

Modifications to IP addresses and TCP port numbers can be made to optimize the network environment. However, these modifications should be performed with caution, and proper configuration is critical. For more information regarding the Citrix commands and port numbers shown below, please see the *MetaFrame XP Administrator's Guide* and *MetaFrame XP Advanced Concepts Guide* available at <http://www.citrix.com/support>.

9.1 Inside Static Network Address Translation (NAT) and Port Address Translation (PAT)

Static inside translations, i.e., one-to-one IP and/or port mappings of TCP/IP nodes, are frequently implemented on firewalls and/or routers to hide the internal identification of MetaFrame servers. Addressing these security concerns is especially important for environments that do not use Secure Gateway. Secure Gateway acts as a proxy server and thus hides the identity of MetaFrame servers.

Static NAT, i.e., mapping one IP address to another, is supported on MetaFrame XP servers by using the ALTADDR command. Although the default ICA port can be altered using the ICAPORT command, this results in altering the port number, not translating it.

9.1.1 NAT Using ALTADDR on MetaFrame Servers

Network Address Translation on MetaFrame servers involves mapping one specific IP address to another specific IP address. This is most commonly implemented to allow an internal MetaFrame server with an internal IP address (such as 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16) to map to an external IP address. This can be implemented on MetaFrame servers by using the ALTADDR command. The ALTADDR utility is used to configure each MetaFrame server to return the external IP address to Citrix ICA Clients. A unique alternate address must be specified for *each* server in a server farm.

To set an alternate address for a Citrix server:

- At a command prompt, type ALTADDR /set x.x.x.x, where x is the external IP address for the Citrix MetaFrame server.

To set up an alternate address for a multi-homed Citrix server:

- At the command prompt, type ALTADDR /set [internal IP] [external IP]

Although it is technically possible to modify both the IP address and the port number of the MetaFrame server with the ALTADDR command, Citrix Technical Support does not support use of this command for static PAT addressing. Further, this may not function correctly within a native-mode MetaFrame XP server farm. The ICAPORT command should be used to modify the port number of a MetaFrame server.

NFuse 1.7 or later can support PAT deployments without any changes needed on the MetaFrame servers.

9.1.2 Static Inside NAT and PAT on Routers and Firewalls

More commonly, static inside NAT and PAT mappings are configured on routers and/or firewalls. The rules applied to the router and/or firewall enable the network administrator to maintain higher level of security, such as including IP addresses that are permitted to access a network node. Further, auditing can be implemented to track any non-authorized attempts at accessing the MetaFrame servers.

Implementing NAT and PAT is complex and should be thoroughly tested. Please consult your network vendor documentation.

9.2 Static vs. DHCP-Assigned TCP/IP Address

TCP/IP addresses can be statically configured or reserved within DHCP. Using a static TCP/IP address is recommended for Windows 2000 Terminal Services/Citrix MetaFrame servers. Static addresses ensure networking stability and reduce the traffic associated with contacting a DHCP server. Further, static addresses will not cause issues if a NIC is replaced.

Alternatively, IP addresses may be manually reserved in the DHCP server by indicating the MAC address. This works well in environments where the assignment of IP addresses is not centralized; the DHCP server can serve as a main point of reference for all administrators. If the NIC is replaced or the MAC address is renamed, however, DHCP will need to be updated or the IP assignment will not work correctly.

If the TCP/IP addresses assigned to MetaFrame servers are DHCP reserved addresses and if a segregated IP subnet is used for these MetaFrame servers, then it is necessary to install a DHCP relay agent within the subnet hosting the MetaFrame servers. This is because it will be necessary to transfer messages between the DHCP clients, i.e., the MetaFrame servers, and the DHCP server, which is located on another subnet. On Cisco routers, the `ip helper-address` command defaults to forwarding not only DHCP (UDP ports 67 and 68), but also the UDP traffic associated with Time (port 37), TACACS (port 49), DNS (port 53), TFTP (port 69), and NetBIOS (ports 137 and 138) traffic. In privileged mode, the administrator will enter the following:

```
2621A(config-if)#ip helper-address 10.10.10.9
```

Variations of the IP helper command can be used to ignore some or all of the redirection of these UDP ports, as well as add other UDP ports. Please see the Cisco documentation for more information.

If for any reason the TCP/IP address(es) of the MetaFrame server(s) are duplicated via DHCP or any other means throughout the network, a multitude of networking problems will arise.

9.3 Permission to Monitor Over the Network

In a MetaFrame environment, it may be necessary to monitor user activity from time to time to resolve network or other issues. To ensure that the user is aware that network monitoring or shadowing may be occurring without his/her explicit knowledge, it is important from a legality standpoint that the user see a banner advising such upon login and that the user agree to these terms before accessing the corporate network and associated resources. The details of the verbiage to be shown should be determined by corporate legal counsel. In Windows 2000, this can easily be accomplished by customizing Group Policies or by invoking a logon script. In any event, the user should be shown a modal dialog box and forced to click "OK" in order to proceed.

MetaFrame XP optionally adds a "You are being shadowed" window to inform the user that shadowing is occurring.

10. Network-Related MetaFrame Features and Associated Implications

MetaFrame includes a number of customizable features that affect network bandwidth requirements and/or perceived network performance. For more information regarding these features, please see the *MetaFrame XP Administrator's Guide*.

10.1 SpeedScreen

SpeedScreen technology allows users to see their mouse and keyboard input on the screen prior to that input actually being communicated with the MetaFrame server. The screen output is visual only and is an estimation as to how the output will look based on communication with the MetaFrame server. SpeedScreen is most notable across WAN links and can be configured within the SpeedScreen Latency Reduction Manager screen.

Citrix has introduced several versions of SpeedScreen. Most notably, in MetaFrame XP Feature Release 3, SpeedScreen Browser Acceleration was introduced. This optional feature uses ICA Session Monitoring and Control (SMC) in the background to automatically determine when images should be compressed based on the bandwidth available on the WAN link.

10.2 Disk Caching and Data Compression

Disk caching reduces the amount of data sent over the communications link to the ICA client by storing frequently used application images locally on the client device. Thus, performance is increased because locally cached data is not retransmitted. This is a standard feature of the ICA protocol and saves on network bandwidth, while enabling users to physically see images such as icons and bitmaps faster.

Data compression minimizes the amount of data that is transferred at the expense of processor resources to compress and decompress the data. Data compression can increase performance if bandwidth is limited but processor resources are readily available.

10.3 Printer Bandwidth Throttling

With MetaFrame XP, access to the printing virtual channel for printer bandwidth throttling is possible. Modifying this setting in accordance with the available bandwidth allows MetaFrame Administrators to balance the ICA session requirements with printing requirements. Administrators can use the printing virtual channel to determine how much of the available bandwidth will be allocated for printing. For example, administrators responsible for environments that require heavy printing over slow WAN links may wish to prioritize ICA sessions and decrease the importance of the print jobs.

10.4 Client Mapping Settings

MetaFrame XP includes six client mapping settings that can be administered by either Policies or the Citrix Connection Configuration→Client Settings screen. The former controls the entire farm, whereas the latter controls individual servers. As part of the logon process, any Client Mapping setting not explicitly disabled is established. Depending on the specific Client Mapping and ICA session activity, additional data corresponding to any mappings not explicitly disabled will traverse the network.

By disabling unneeded client mapping(s), responsiveness will improve because the enabled virtual channels do not need to share the bandwidth with the virtual channels that have been disabled. For example, for ICA clients where the clipboard mapping feature is not disabled, each time data is copied to or pasted from the remote (MetaFrame) session clipboard, there is corresponding communication with the client local clipboard via the client clipboard virtual channel. This communication could degrade the perceived performance of the session, especially over low bandwidth connections.

Frequently, Windows Client Printer Mapping, Client Drive Mapping, and/or Client Audio Mapping are not utilized and should be considered for disablement. Of course, each environment is unique and disabling mappings should be carefully considered.

10.5 Printer Creation

Beginning with MetaFrame XP Feature Release 2, published applications could be configured so that printers are created in parallel with launching the application, instead of being done serially. Since users rarely have the need to print immediately, the printer creation process occurs while or after the application is presented to the user, resulting in a more expeditious application display. This feature does not have an impact on the network resources.

11. Network Impact of Citrix Add-On Products

MetaFrame XPa includes Load Manager, whereas MetaFrame XPe includes Load Manager, Resource Manager, Installation Manager, and Network Manager.

11.1 Load Manager

With Load Manager, the MetaFrame server load data is forwarded to the Zone Data Collector (ZDC), which uses this data to determine the least-busy server. The criteria for load balancing can be established by the administrator within the Management Console. Each server has a numeric load level that is determined based on current usage and calculated using a proprietary algorithm. The user is then connected to the server with the lightest load.

The resulting network traffic is negligible; however, the ZDC must be readily able to accept the load data from the farm servers and provide a quick response to embryonic ICA client connection requests.

11.2 Resource Manager

Resource Manager is an excellent tool for monitoring the health of the MetaFrame servers, including NIC(s). RM enables the administrator to receive e-mail messages and pager messages, which have minimal impact on the network. RM monitors the MetaFrame server every 15 seconds by default, and a negligible effect on the network will be experienced since much of the data is stored on the local server.

RM requires that a Farm Metric Server be established, which is usually the Zone Data Collector. The Farm Metric Server (FMS) collects and summarizes farm-wide metrics. All servers in the farm communicate with the FMS. This is an additional reason for establishing a dedicated Zone Data Collector/Farm Metric Server that does not host user applications.

Server data is maintained on the local MetaFrame server and then uploaded to a Database Connection Server daily at midnight by default, a time when network communications are likely at a minimum. However, if backups or other network-intensive activities are also occurring on affected subnets at this same time, the time should be modified.

The Farm Metric Server and the Database Connection Server should be co-located on the same subnet so as not to create additional traffic by traversing subnets. In addition, the summary database server should be housed on the same subnet whenever possible.

11.3 Installation Manager

Installation Manager deploys applications simultaneously to MetaFrame servers, and deployment of applications will heavily impact the network. Thus, it is suggested that deployment packages be deployed after general business hours.

Each target server individually pulls the data from the file server or other location where the installation package is stored. Thus, it is strongly recommended that the file server support two switched FastEthernet connections and that each is hard coded for 100 Mbps speed and full duplex. If IM is used for large software deployments on a frequent basis, a switched Gigabit Ethernet connection may be considered on the file server. As discussed in the [NIC](#) section, the NIC and switch port must be configured for the correct speed and duplex.

Installation Manager allows for target MetaFrame servers to be grouped, which will reduce the impact on the network. In a large environment, grouping the servers into subsets and deploying packages to one subset at a time ensures that the additional network traffic associated with the

deployment will be a fraction of the entire MetaFrame server farm. LM allows deployments to be scheduled for nights or weekends, when the impact of additional network traffic is likely to be less.

If deploying an application over a WAN link, consider the size and timing of the application in order to ensure that regular user activities are not impacted. If MetaFrame servers are located at various locations, it may be advantageous to copy the package to a remote file server then deploy to remote MetaFrame servers.

11.3.1 Application(s)

If an application encodes the MAC or IP address of the server during the packaging process, using IM to roll out the application may not function correctly. Applications to be deployed via IM should be fully tested in a lab environment prior to deployment.

11.4 Network Manager/SNMP

Network Manager includes Management Information Bases (MIBs) that enable monitoring the MetaFrame servers from an Simple Network Management Protocol (SNMP) management console. SNMP generates a negligible amount of additional traffic on UDP port 162. It is important that the community name and SNMP trap destinations are established correctly.

12. General Network Topics

12.1 WINS and DNS for Name Resolution

WINS is used to resolve NetBIOS names, e.g., CITRIX1. DNS name format is somewhat different, e.g., CITRIX1.company.com. When loading the Windows 2000 operating system, it is strongly recommended that the NetBIOS server name and DNS server name be exactly the same. If these names are identical, this will make it easier to troubleshoot networking issues because the reference will be the same.

In standard Windows 2000 environments, WINS is optional; however, many applications that will run in the MetaFrame environment continue to depend on WINS to resolve NetBIOS names.

If WINS lookup is enabled on the Windows 2000 DNS server, then WINS is used as a secondary method for name resolution. If the name cannot be resolved by either DNS or WINS, only then will a broadcast occur. Both forward and reverse lookups are supported by Microsoft Windows 2000 DNS.

If DNS and WINS are unable to resolve NetBIOS names, network broadcasting will be used, which will add unnecessary network traffic. For redundancy and to ensure high availability, it is recommended that at least two WINS servers be available for NetBIOS name resolution and that these be configured for the push (changes) and pull (time interval) replication appropriate for the network, i.e., during non-peak hours. Likewise, two DNS servers should be available for redundancy and high availability.

Within DHCP, WINS (Option 046 - WINS/NBT node type) should be configured as hybrid node, i.e., 0x8. Hybrid dictates that first P-node (point-to-point communications) will be attempted before B-node (broadcast).

12.1.1 ICA Browsing with MetaFrame XP

With MetaFrame XP and the full Program Neighborhood client, when an ICA client is browsing for applications, the client attempts to resolve the DNS prefix "ica" if no server is otherwise specified. Thus, a host record can be configured to automatically map this name to one or more MetaFrame XP server IP addresses.

Beginning with MetaFrame XP Feature Release 1, DNS Address Resolution became available. This capability allows a MetaFrame XP server to respond with its Fully Qualified Domain Name (FQDN) instead of its IP address. This may result in additional network overhead.

12.2 Windows 2000 Services

MetaFrame XP server farms depend on the Independent Management Architecture (IMA) service, as well as the Citrix XML Service. Each of these respective services is listed on the Windows Services screen and can be stopped, started, or restarted as necessary.

If the "IIS Port Sharing" feature is chosen during MetaFrame installation, the Citrix XML Service does not appear in the services control panel because it is delivered by IIS instead of cctxmlss.exe.

Secure Gateway Service is a service that is required on Secure Gateway servers so that they may support the associated functionality.

In order to ensure that that a failure of any of these services does not cause a MetaFrame server to cease functioning, these services should be set to automatically restart upon failure.

12.2.1 Citrix XML Service

All MetaFrame servers must use the same TCP port number for the Citrix XML Service. When ICA clients use TCP+HTTP, the Citrix XML Service data is encapsulated within HTTP and transported on default TCP port 80, unless configured otherwise. The Citrix XML Service is also used to support communications with Web Interface.

12.2.2 IMA Service

The IMA Service is responsible for communications between MetaFrame XP servers, as well as the Data Store. When invoking the Citrix Management Console (CMC), whether on a MetaFrame server Win32 client, or the Citrix Web Console (which became available with MetaFrame XP Feature Release 1), communications take place using the IMA service over TCP/IP.

12.2.3 Secure Gateway Service

The Secure Gateway service functions as an Internet gateway between ICA Clients and a MetaFrame server farm. It is only present on the Secure Gateway server.

13. ICA Client

How the client device is configured and accesses the MetaFrame server farm can have an affect on the user's experience. This section discusses the various ICA Client versions that are available, as well as configuration options. Since the Win32 ICA Client is the most popular of all those offered, it is focused upon in this section.

13.1 ICA Client Versions

Citrix supports ICA clients for almost any type of client device for MetaFrame server access. For a full list of the ICA clients offered, see <http://www.citrix.com/download>. The Java ICA Client is growing in popularity since it is a Java applet that runs within a browser and is based on a zero footprint. However, Java applets must not be disabled on the firewall in order to function properly.

Whenever possible, it is recommended that the most recent version of the ICA Client be installed on the client device. ICA clients can be distributed via the Web-based client installation available within Web Interface or the ICA Client Updated included in MetaFrame XP; however, the former is generally faster. Distributing updated ICA clients via an automated method ensures that clients are uniform and that the newest capabilities are supported.

Distributing the ICA client via the web-based ICA client deployment will impact your web server and associated network bandwidth since this is a large file that is being pushed out to each user. If a large number of users are accessing the Web Interface web site for the first time, whether internally or externally, this will generate a tremendous amount of network traffic. Depending on the web server settings and bandwidth available, this may impact or even block other users from accessing the Web Interface web site.

MetaFrame XP Feature Release 2 and the Version 6.30 ICA Clients associated with that release made significant improvements in bandwidth efficiency by using a much bigger TCP window and more buffers. Bandwidth requirements dropped by as much as 50% for some specific tasks.

For the Windows 32-bit ICA client, there are three versions available for Version 6.30.1051:

- Full Program Neighborhood ("ica32") – full functionality.
- Web Version ("ica32t") – contains only the essential ICA client functionality to support Web Interface connectivity.
- Program Neighborhood Agent ("ica32a") – contains only the essential ICA client functionality to present icon(s) symbolize application(s) on the user's desktop but are actually MetaFrame-hosted application(s); MetaFrame XP with Feature Release 1 or higher is required.

As a comparison, the "ica32" file is approximately 3.2 MB in size, the "ica32a" file is approximately 2.8 MB in size, and the "ica32t" file is approximately 1.9 MB in size. The minimal ICA client required to support the desired functionality should be used.

For the Version 7.00 Windows 32-bit ICA Client, the wficac.cab is being introduced. It is approximately 1.0 MB in size and is much like the "ica32t" version but without the following features so that an even smaller download can be achieved:

- Zero Latency
- 128-bit SecureICA
- Universal Print Driver
- Font manager
- Client audio mapping
- Client COM port mapping
- Netscape plug-in
- Auto client update

13.1.1 Program Neighborhood ICA Client Configuration

With MetaFrame XP, the ability to eliminate UDP 1604 client browsing has been enabled by default. When using the Version 6.00 and newer ICA clients, selecting TCP/IP+HTTP as the Server Location/Network Protocol on the ICA client enables communication without the use of UDP port 1604. This setting uses Citrix XML data encapsulated in HTTP packets, which the client sends via port 80 by default, thus eliminating the client's use of UDP port 1604 broadcasts to locate MetaFrame servers.

Beginning with MetaFrame XP Feature Release 1 in combination with Version 6.20 and newer ICA clients, communications can take place via Secure Socket Layer (SSL) running on TCP port 443 by default. Thus, SSL + HTTPS should be used.

For clients using Program Neighborhood, in the Server Location/Address List box, specifying the Data Collector's IP address, MetaFrame server name, or DNS alias in the Primary Server Group box minimizes browse traffic. However, if the specified server listed in the Primary Server Group is unavailable, the ICA client will not resort to auto-locating but will instead be unable to find the MetaFrame server farm. Thus, it is also a good practice to include the IP address or MetaFrame server name for a second MetaFrame server under the Backup 1.

The full Program Neighborhood client is being deployed less and less frequently within many enterprises since the web client and PN Agent client became available.

13.1.2 Web-Based ICA Client

A feature of Web Interface is web-based ICA client installation. When the user connects to the Web Interface site, upon successfully logging in, the server will automatically sense that the Win32 or Win16 client does not have the ICA client installed. It will automatically determine the appropriate ICA client to be downloaded and can then proceed with the download. The "ica32t" client, which is a scaled-down version of the ICA client that does not include Program Neighborhood and other features of the standard ICA client, is best used for this purpose.

13.1.3 PN Agent ICA Client

The PN Agent version of the ICA Client enables users to access applications from their Start→Programs menu, much like if the programs were installed locally. PN Agent uses Web Interface as the behind-the-scenes mechanism for accessing applications. Thus, Web Interface is a required component of this type of deployment.

13.2 Client Login Scripts

In particular, the client login scripts are typically not well controlled in many large MetaFrame environments and subsequently have a negative impact on the user logon process. Login scripts are often used to modify specific settings for groups or individuals, so that modifications can be made without affecting the user's current environment as defined by his/her roaming profile. However, these must be properly designed and implemented.

While the use of login scripts is fully supported in a MetaFrame environment, it is unfortunate yet common to see multiple or lengthy login scripts, which results in additional user login time. The resulting slow login time may cause the user to perceive that consistent network or server latency issues are present.

Login scripts should be reviewed periodically to determine if unnecessary parameters could be identified or other steps that would enable faster processing realized. For example, in Windows 2000, the use of Windows Script Host or VB Scripting is becoming more common based on execution time alone.

Further, since login scripts are generally extracted from a centralized file server, it is critical that access to that file server be readily available. If, for example, a large number of call center agents log in between 7:58 and 8:00 AM every morning, the file server, its NIC, and the network will be taxed and the login process will be very slow.

13.3 Network Protocols

If only TCP/IP is required for the ICA client machines to access the MetaFrame servers, then this should be the only or primary protocol installed. Network protocol binding order affects client devices, since each protocol will be attempted sequentially until a network connection is completed.

Since most ICA clients utilize TCP/IP as the primary protocol, it is suggested that the binding order be configured as follows:

- TCP/IP
- Microsoft Client Network
- NWLink or IPX/SPX (if present)

14. Most Commonly Overlooked Network Issues

The most common issues associated with designing and maximizing the network infrastructure are:

- Improperly Configured Subnets
- TCP 1494 (or other configured ICA port) not open

14.1 Proper Configuration of Subnets

Proper configuration of the subnet where MetaFrame servers will be located is critical to the success of the MetaFrame environment. Not only must the initial subnet or Variable-Length Subnet Mask (VLSM) be configured correctly, but all future adds, moves, and changes to the servers within the MetaFrame environment must be revisited from a subnetting perspective.

14.1.1 Class C

In many MetaFrame environments, a single Class C (255.255.255.0 or /24) subnet is allocated, which allows for up to 254 host IP addresses. This simple subnetting configuration can provide many benefits from an architectural standpoint if only MetaFrame server traffic is permitted on the subnet and the number of servers is planned or permitted to grow.

For MetaFrame XP environments, the Data Collector process is completely different. Tests have been run with nearly 1,000 MetaFrame servers supported within one zone by a Zone Data Collector without issue. According to Cisco, enterprise subnets should have no more than 1,000 IP nodes.

Thus, a full Class C or perhaps even a subnetted Class B configuration would be appropriate for most environments. Please see [Appendix A TCP/IP Subnetting](#) for more information regarding the proper configuration of subnets.

14.1.2 Variable-Length Subnet Mask (VLSM)

Variable-Length Subnet Mask (VLSM) technology provides for a method for modifying the standard number of hosts and subnets allocated to standard Class A, Class B, and Class C addresses. Please see [Appendix A TCP/IP Subnetting](#) for more information regarding the proper configuration of subnets.

14.2 TCP 1494 (or other configured ICA port) Not Open

MetaFrame traffic requires TCP port 1494 (or other configured ICA port) to be open, so that ICA traffic may traverse the network. The default TCP port 1494 is used for inbound traffic to the MetaFrame servers. Outbound traffic is via a dynamically chosen TCP port number. If the ICA port is changed and/or router configurations are changed, it is critical that ICA traffic is not blocked by the router or firewall. Please see the [ICA TCP Port Number](#) section for more information regarding changing the standard ICA port from TCP 1494 to another port number.

Particularly in networks where all or some ports above 1023 are blocked for security reasons, opening the ICA ports, i.e., TCP port 1494 (if TCP/IP+HTTP is not being used) will enable MetaFrame traffic to flow. On the router, this is commonly done via an access list. Please see the [Access Lists](#) section for more information and an example.

14.3 TCP 2512 or 2513 Not Open

MetaFrame XP uses TCP port 2512 for the IMA Service, which supports server-to-server communications, including communications with the Data Store. MetaFrame XP uses TCP port 2513 for supporting the Citrix Management Console communications with the host server. This becomes particularly important where a zone spans different physical locations that have ports blocked by a firewall or router. Although both of these port numbers can be modified with Feature Release 1, it is essential that network communications can flow between servers effectively via the default or modified port numbers.

15. Windows Operating System Troubleshooting Tools and Tips

The information below is based on standard utilities included with the Microsoft Windows operating system.

Please note that when using ping, tracert, or other similar utilities, if Internet Control Message Protocol (ICMP) packets are disabled on the receiving device, the resulting "request timed out" message may represent an incomplete picture of the current health of the network. Some network administrators disable ICMP packets, particularly on external routers.

15.1 Computer to Computer

From a computer within the same subnet, try each of the following:

Command	Desired Result
Ping (IP Address)	4 sent/4 received packets with 0% loss
Ping (Server Name)	4 sent/4 received packets with 0% loss (Note: if ping <i>IP address</i> is successful but ping <i>server name</i> is not, this indicates an issue with server name resolution and can likely be traced to DNS or WINS.)
Tracert	Up to 30 hops with time (in milliseconds) statistics
Pathping	Ping and tracert data with additional statistics (only available with Windows 2000)
Telnet 1494 (or other designated ICA port)	Connection and an "ICA sounder"
Telnet 80 (HTTP port)	Connection (any typing should show an HTTP error)

15.1.1 Finding the Router(s)

In order to find the IP address of the router(s), tracert or pathping should be used to identify the router hops. Each IP address listed signifies a router interface that the traffic must traverse.

A large number of router hops likely signifies network latency and should be discussed with the network administrator. The ICA protocol does not do well in a latent environment and will likely result in lost packets and dropped sessions.

15.2 Performance/System Monitor

Windows 2000 System Monitor, previously known as Performance Monitor, can provide a variety of monitoring counters for a single server. Beginning with MetaFrame XP Feature Release 2, over 60 counters were added under the objects Citrix IMA networking, Citrix MetaFrame XP, and ICA Session. Please note that Secure Gateway and the Secure Ticket Authority also have specific counters related to that specialized functionality.

In particular, the following objects are useful in identifying network issues:

Object	Validity	Counters
Citrix IMA Networking	All (2 total)	As applicable
Citrix MetaFrame XP	All (19 total)	As applicable
ICA Session	All (45 total)	As applicable
IP	All – may wish to focus on sent or received only	As applicable
Network Interface	All – may wish to focus on sent or received only	Choose instance for specific NIC and all applicable counters
TCP	All – may wish to focus on sent	As applicable

	or received only	
Terminal Services	All – may wish to focus on Active sessions only	Active, Inactive, and Total Sessions
Terminal Services Session	All – may wish to focus on input or output only	As applicable

In addition to the monitoring capabilities available, Performance Alerts can be enabled to send a network message, start performance data log, and/or run a program. Based on reaching a set threshold, this will trigger the programmed alert so that corrective or monitoring activities can begin immediately.

Performance Alerts are especially useful when the MetaFrame server(s) resources reach any of the following:

Object	Counter	Parameter
Network Interface	Packets Outbound Discarded	>0
Network Interface	Packets Outbound Errors	>0
Network Interface	Packets Received Discarded	>0
Network Interface	Packets Received Errors	>0
Terminal Services Session	Input Errors	>0
Terminal Services Session	Input Timeouts	>0
Terminal Services Session	Input Transport Errors	>0
Terminal Services Session	Output Errors	>0
Terminal Services Session	Output Timeouts	>0
Terminal Services Session	Output Transport Errors	>0
Terminal Services Session	Total Errors	>0
Terminal Services Session	Total Timeouts	>0
TCP	Connections Reset	>0
TCP	Segments Retransmitted	>0

15.3 Network Monitor

Network Monitor is an effective tool for viewing and dissecting network traffic as sent and received by a host. These frames comprise source and destination address, protocol headers, and the data itself. Network Monitor is an especially useful tool when two or more MetaFrame server(s) and/or ICA Client(s) are communicating sporadically or otherwise cannot communicate.

On Windows servers, Network Monitor is not installed by default but instead must be installed through Add/Remove Programs→Windows Components→ Management and Monitoring Tools.

The standard version of Network Monitor included in Windows 2000 is for a single server only; if monitoring several servers is desired, more sophisticated hardware and/or software may be required, e.g., Microsoft Systems Management Server (SMS) or a network sniffer. If using SMS and various instances of Network Monitor, the Network Monitor driver must be installed on remote server(s) or client(s) by installing this optional component to the Properties for the specific LAN connection.

When opening Network Monitor, be aware that the network to be monitored is dependent upon the NIC chosen. If more than one NIC is installed, a separate instance of Network Monitor should be opened to view and/or capture the statistics listed below.

These fields in particular affect the MetaFrame environment and should be viewed and/or captured using Network Monitor. These are:

Window	Identifier	Optimized Output
Graph	Network Utilization	Lower is better
Graph	Network Broadcasts	Should be minimal
Total Stats	Network Statistics: # of Frames	Lower is better
Total Stats	Network Statistics: # of Broadcasts	Should be none or minimal
Total Stats	Network Statistics: # of Frames Dropped	Should be none or minimal
Total Stats	Per Second Statistics: % Network Utilization	Lower is better
Total Stats	Per Second Statistics: # of Broadcasts/second	Should be none or minimal
Total Stats	Network Card (MAC) Statistics: # of Broadcasts	Should be none or minimal
Total Stats	Network Card (MAC Error) Statistics: CRC Errors	Should be none or minimal
Total Stats	Network Card (MAC Error) Statistics: # Frames Dropped (No Buffers)	Should be none or minimal
Total Stats	Network Card (MAC Error) Statistics: # Frames Dropped (Hardware)	Should be none or minimal
Station Stats	Broadcasts Sent	Should be none or minimal

In particular, what is sometimes perceived as a network problem is actually a NIC issue that can be easily determined based on the Network Card parameters shown above.

Network Monitor enables data capture or what is commonly referred to as a "trace." When configuring the Capture Filter, it may be useful to eliminate protocols and/or network address types that are not related to the issue being investigated. A Network Monitor trace typically returns a tremendous amount of data and requires a correspondingly large capture buffer. If all data is captured as part of the Network Monitor trace, then the data also can be filtered later.

If the Network Monitor trace does not yield data which is helpful in resolving issues wherein MetaFrame server(s) and/or ICA Clients cannot communicate, an incident can be opened with Citrix Technical Support so that the Network Monitor trace can be analyzed by an Escalation Engineer.

15.4 Registry Settings

There are some registry settings, such as ICAEnableKeepAlive and TCPMaxDataRetransmissions, that have an effect on the keepalive time or data retries of a packet. In MetaFrame XP FR3, this can be turned on from within the Management Console. A keepalive is essentially a "Can you hear me now?" type of message to confirm that the connection is still active. Although making changes to such registry settings can have an effect on the MetaFrame servers, it is recommended that the root of the problem, i.e., the WAN bandwidth or configuration, be reviewed in depth prior to manually adjusting these or other similar registry settings.

Enabling the ICA keepalive can sometimes prevent user sessions from being disconnected by firewalls that view an ICA or SSL session as inactive after a fixed time interval.

If network congestion or improper configuration is causing the ICA packets to time out or otherwise not traverse the network timely, manually adjusting keepalive time or data retries may have other undesirable implications. These types of issues should be addressed at the network level and/or tested in a laboratory environment.

16. Router (Cisco®) Troubleshooting Tools and Tips

Viewing some details of the router configuration may assist in determining the root cause of network issues.

Please note that when using ping, trace, or other similar utilities, if Internet Control Message Protocol (ICMP) packets are disabled on the receiving device, the resulting "request timed out" message may represent an incomplete picture of the current health of the network. Some network administrators disable ICMP packets, particularly on external routers.

16.1 Switch and Router Access Privileges

Cisco switches and routers have both user mode and privileged mode access. With standard mode user privileges, some router and switch configuration settings can be viewed in a read-only mode. It is commonly used to view switch or router status and is indicated by a > symbol. Standard mode does not allow for any configuration changes; configuration changes can only be done in privileged mode. Typically, privileged mode access is closely guarded and used only by the network administrator(s) since configuration changes affecting the entire network can be made under this mode. Privileged mode is indicated with a # symbol and generally requires a password.

If the network administrator will grant the MetaFrame administrator standard mode user privileges via Telnet, this will assist the MetaFrame Administrator with access to read-only data and assist with minor troubleshooting as necessary.

Standard mode can be accessed via Telnet (At Start→Run, type Telnet). However, using Telnet to access a router using standard mode should be minimized since many routers default to only five Telnet connections (0 through 4).

Standard mode access appears with the router or switch name followed by a greater than sign as follows:

```
RouterA>
```

Privileged mode access appears with the router or switch name followed by a number symbol as follows:

```
RouterA#
```

In order to use any of the commands shown below via Telnet, standard mode user privileges and Telnet login and password are required.

16.2 Network

When using the IP tools below on a router or switch, either the IP address or the server name can be identified. The server name can only be used if it has been manually configured on the router. For information regarding locating the router IP addresses within the network, please see [Finding the Router\(s\)](#).

16.2.1 Ping

Example of Ping:

```
RouterB>ping 10.2.1.2
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.2.1.2, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

16.2.2 Trace

Example of Traceroute (please note that the router command is traceroute not tracert!):

```
RouterB>traceroute ip 10.2.1.2
Type escape sequence to abort.
Tracing the route to 10.2.1.2

 0  16 msec 16 msec 16 msec
 1  10.2.1.2 36 msec 28 msec *
```

16.2.3 Telnet

On a Cisco 2900 series switch, an IP address must be configured for the switch in order to telnet into it, as well as to gather basic information. By using the following command in user mode, basic switch information can be garnered:

```
2900A>show ip
```

As an example, possible results of this command are:

```
IP Address: 10.10.10.3
Subnet Mask: 255.255.255.0
Default Gateway: 10.10.10.1
Management VLAN: 1
Domain Name: name
Name Server: 10.10.10.1
HTTP Server: Enabled
HTTP Port: 80
RIP: Enabled
```

For example, knowing that HTTP is enabled on port 80 may assist with researching a TCP/IP addressing or NFuse-related issue.

Example of Telnet from router:

```
RouterC>telnet 172.16.40.2
Trying 172.16.40.2 ... Open

User Access Verification

Password:
```

Example of Telnet from router to test utilization of name resolution:

```
RouterA>telnet RouterC
Trying 172.16.40.2 ... Open

User Access Verification

Password:
```

Example of use of the word Telnet being optional:

```
RouterC>172.16.40.2
Trying 172.16.40.2 ... Open

User Access Verification

Password:
```

16.2.4 Switch Errors

To determine if receive errors, transmit errors, and security violations are occurring on the switch, the "show usage exception" command can be used. All errors recorded are based on the entire time that the switch has been operational and reloading or resetting the switch will cause all columns to

default to zero. It may be beneficial to baseline the errors to determine when the errors occurred. An example of "show usage exception" and the desired results are as follows:

```
2900A>show usage exception
      Receive      Transmit      Security
      Errors      Errors      Violations
-----
 1 :           0           0           0
 2 :           0           0           0
 3 :           0           0           0
 4 :           0           0           0
 5 :           0           0           0
 6 :           0           0           0
 7 :           0           0           0
 8 :           0           0           0
 9 :           0           0           0
10 :           0           0           0
11 :           0           0           0
12 :           0           0           0

AUI:           0           0           0
 A :           0           0           0
 B :           0           0           0
```

16.2.5 Token Ring

Ensuring that the ring speed is properly set will enable token ring traffic to traverse the network. For example, the network administrator in privileged mode could use the commands shown below to reset the ring speed for the token ring network to 16 Mbps and to enable the interface:

```
RouterA(config)#int to0
RouterA(config-if)#ring-speed 16
```

16.3 Access Lists

An access list is a packet filtering technique that controls the type(s) of data specifically permitted or denied at the router level. Creating and applying an access list to an interface causes the router to analyze every packet that crosses in the specified direction and take the prescribed action. At the end of each access list is an explicit deny, so all traffic not specifically permitted will be denied. Specific access list numbers can be applied as a variable within most QoS methods.

To ensure that each of the ports specified in the [TCP Port Numbers](#) section is opened, it is recommended that an extended IP access list, i.e., specifying source IP, destination IP, protocol, and/or port number, be created and an extended IP access list number between 100 and 199 be used.

For example, to allow the ports specified in the aforementioned section to traverse through the router, the network administrator in privileged mode could create the following access list and apply on interface e0:

```
RouterA(config)#access-list 110 permit tcp any any eq 1494
RouterA(config)#access-list 110 permit tcp any any eq 80
RouterA(config)#access-list 110 permit tcp any any eq 443
RouterA(config)#access-list 110 permit tcp any any eq 2512
RouterA(config)#access-list 110 permit tcp any any eq 2513
RouterA(config)#int e0
RouterA(config-if)#ip access-group 110 [in|out]
```

17. Appendix A – TCP/IP Subnetting

17.1 TCP/IP Subnetting and Variable-Length Subnet Masks (VLSM)

When subnetting, the first address in a subnet is the IP address for the entire subnet and the last address is the broadcast address for that subnet. All addresses in between represent valid hosts in that subnet. Routers only use network and broadcast addresses for the subnet to route packets; host addresses have little importance to the router except as the specific source or destination.

Cisco operating systems prior to 12.0 did not allow for the first possible subnet (subnet address range beginning with 0) and the last possible subnet (subnet address range ending with 255) to be used because such would imply all 0s or all 1s in the address. On these older operating systems, the command "ip subnet-zero" would need to be manually configured on the router. Cisco IOS 12.0 and higher implements "ip subnet-zero" as the default, thus allowing for the first possible subnet and last possible subnet to be used without additional manual configuration. For example:

```
2621(config)#ip subnet-zero
```

Note that not all vendor equipment supports the use of "ip subnet-zero" as described here and that this needs to be considered when devising IP subnetting.

Subnet Mask Octet Value	Number of Subnet Bits	Max. # of Valid Subnets	# of Valid Hosts Class C	# of Valid Hosts Class B	Subnet Address Range (Network/Valid Host Addresses/Broadcast)
128	1	2	2	32,766	0/1-126/127* 128/129-254/255*
192	2	4	62	16,382	0/1-63/64* 64/65-126/127 128/129-190/191 192/193-254/255*
224	3	8	30	8,190	0/1-30/31* 32/33-62/63 64/65-94/95 96/97-126/127 128/129-158/159 160/161-190/191 192/193-222/223 224/225-254/255*
240	4	16	14	4,094	0/1-14/15* 16/17-30/31 32/33-46/47 48/49-62/63 64/65-78/79 80/81-94/95 96/97-110/111 112/113-126/127 128/129-143/143 144/145-158/159 160/161-174/175

					176/177-190/191 192/193-206/207 208/209-222/223 224/225-238/239 240/241-254/255*
248	5	32	6	2,046	0/1-6/7* 8/9-14/15 16/17-22/23 24/25-30/31 32/33-38/39 40/41-46/47 48/49-54/55 56/57-62/63 64/65-70/71 72/73-78/79 80/81-86/87 88/89-94/95 96/97-102/103 104/105-110/111 112/113-118/119 120/121-126/127 128/129-134/135 136/137-142/143 144/145-150/151 152/153-158/159 160/161-166/167 168/169-174/175 176/177-182/183 184/185-190/191 192/193-198/199 200/201-206/207 208/209-214/215 216/217-222/223 224/225-230/231 232/233-238/239 240/241-246/247 248/249-254/255*
252	6	64	2	1,022	0/1-2/3* 4/5-6/7 8/9-10/11 12/13-14/15 16/17-18/19 20/21-22/23 24/25-26/27 28/29-30/31 32/33-34/35

					36/37-38/39
					40/41-42/43
					44/45-46/47
					48/49-50/51
					52/53-54/55
					56/57-58/59
					60/61-62/63
					64/65-66/67
					68/69-70/71
					72/73-74/75
					76/77-78/79
					80/81-82/83
					84/85-86/87
					88/89-90/91
					92/93-94/95
					96/97-98/99
					100/101-102/103
					104/105-106/107
					108/109-110/111
					112/113-114/115
					116/117-118/119
					120/121-122/123
					124/125-126/127
					128/129-130/131
					132/133-134/135
					136/137-138/139
					140/141-142/143
					144/145-146/147
					148/149-150/151
					152/153-154/155
					156/157-158/159
					160/161-162/163
					164/165-166/167
					168/169-170/171
					172/173-174/175
					176/177-178/179
					180/181-182/183
					184/185-186/187
					188/189-190/191
					192/193-194/195
					196/197-198/199
					200/201-202/203
					204/205-206/207
					208/209-210/211
					212/213-214/215
					216/217-218/219

					220/221-222/223 224/225-226/227 228/229-230/231 232/233-234/235 236/237-238/239 240/241-242/243 244/245-246/247 248/249-250/251 252/253-254/255*
254	7	128		510	
255	8			254	

*Requires the use of "ip subnet-zero" or similar command in order to allow for the first and last subnet to be used.

17.2 Private IP Addresses

IP addresses which may not be used on the public Internet are:

- 10.x.x.x/8
- 172.16.x.x/12
- 192.168.x.x/16

For security reasons, it is recommended that a private IP address be assigned to MetaFrame servers so that they are not directly accessible from the Internet.

18. Appendix B – OSI Model

18.1 OSI Model Basics

The Open System Interconnection (OSI) model is a seven-layer architectural standard for networks. A basic overview is provided here as a reference only.

Layer	Protocol Data Unit	Functionality	Examples
Application		Program-to-program communications such as file, print, database and other application services	WWW, E-Mail Gateways
Presentation		Data conversion, compression, decompression, encryption, decryption	ICA
Session		Creating, managing, and tearing down communications sessions by using simplex, half-duplex, and full-duplex modes	RPC, X Windows
Transport	Segment	Segments and reassembles data into a data stream; end-to-end data transport services; port numbers	TCP, UDP, SPX
Network	Packet	Routes data packets	IP, Routers
Data Link	Frame	Contains Logical Layer Control (LLC – flow control and timing) and Media Access Control (MAC – physical address)	NICs, Bridges, Switches, VLANs
Physical	Bit	Sends and receives bits	Cabling, Hubs