

Configuring PIX to Allow Remote Access to Shared Folders on an NT Domain

Document ID: 18801

Introduction

Before You Begin

Conventions

Prerequisites

Components Used

Configuring Your PIX Software

Network Diagram

Configuring WINS and the PIX Firewall

Verify

Verifying Accessibility Through the PIX Firewall

Troubleshooting Procedure

Troubleshooting Information and Sniffer Trace Example

Related Information

Introduction

This document explains how to configure the Cisco Secure PIX Firewall to allow access to shared folders on an NT domain through the PIX Firewall. You can access the hosts residing in the PIX inside interface by using Windows Networking. You can also log on to the domain with the same configuration. The configuration information in this document covers the Windows NT domain only and does not include Windows 2000 or Active Directory.

Note: An administrator should evaluate the security implications of allowing Windows Networking traffic with respect to any corporate security policies.

Before You Begin

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Prerequisites

This document assumes familiarity with Microsoft and Windows Networking principles. You may want to consult these useful references for further information:

- Windows Networking Design Implementation Guide
- Windows 98 – Logon Browsing and Resource Sharing
- How to Configure a Firewall for Domains and Trusts

This section describes how to configure the PIX to allow the following traffic flow when a user attempts to access a shared folder on the NT domain.

- Before attempting to access the shared folder:

1. The PC attempting access first registers itself using the NetBIOS name service, using source and destination UDP port 137.
 2. It searches for the domain controller for the domain using Netlogon traffic, using source and destination UDP port 138.
- While accessing and closing the folder:
 1. It establishes a Network Basic Input/Output System (NetBIOS) session for accessing the shared folder, using source 1024–65536/TCP and destination 139/TCP.
 2. It terminates the NetBIOS session when finished.

Components Used

Though you can use any hardware and PIX software, this document was developed and tested using the following:

- Cisco PIX Firewall Software Release 6.1(1)

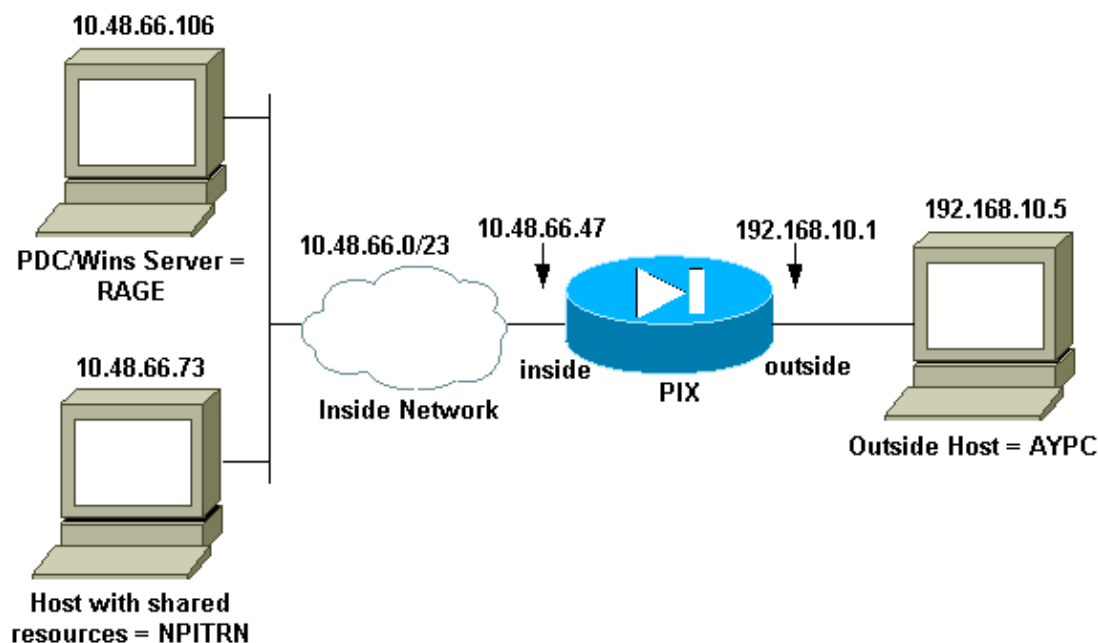
The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

Configuring Your PIX Software

This section describes how to configure the PIX to allow the following traffic flow when a user attempts to access a shared folder on the NT domain.

Network Diagram

This document uses the network setup shown in the diagram below.



This example includes two inside hosts:

- **10.48.66.106** – RAGE, which is both a primary domain controller (PDC) and a Windows Naming Service (WINS) server in this example.

- **10.48.66.73** – NPITRN, which is another host with resources or folders to share.

The host AYPC resides on the outside interface and has an IP address of 192.168.10.5. In this setup, this machine is part of the domain on the inside. However, this does not have to be the case in order to access shared folders. This differs from a domain logon where the machine must belong to the domain or a trust relationship must exist.

For accessing resources or folders through the firewall, you can either use the Universal Naming Convention (UNC), entering **resource_name**, for example; or you can double-click the Network Neighborhood icon.

This example uses a two-interface PIX, but the concept remains the same for any number of interfaces.

Configuring WINS and the PIX Firewall

Use the following steps to configure WINS and the PIX Firewall.

1. Configure WINS and verify accessibility without PIX. (*optional*)

If you have not done so already, configure WINS for NetBIOS name resolution.

In this particular setup, the PDC and WINS are on the same machine. This might be different in your network. The domain name in this setup is TACWEB and the computer name is RAGE. This lab-environment example shows an attempt to access shared folders on RAGE and/or NPITRN. An entry exists for the PDC and the inside host NPITRN in the WINS server.

More details on how to configure WINS are available in the Managing MS WINS Servers chapter of the Windows NT resource kit. If your WINS server is multihomed, you need to configure static mappings for all of the IP addresses and configure appropriate static and access lists in the PIX.

Ensure that the outside clients are configured for WINS name resolution.

2. Configure the PIX Firewall with appropriate statics and conduits/access lists (without NAT).

If your configuration involves Network Address Translation (NAT), please refer to step 3 below. Only relevant portions of the PIX configuration discussed are shown here. For basic PIX configuration details, refer to the Related Information section. Windows Networking uses UDP port 137, UDP port 138 and TCP 139 for various NetBIOS services needed to access folders.

Note: This document uses the PIX **access-list** syntax which was introduced in version 5.0.1; conduits may also be used, but not in conjunction with access lists.

To allow traffic from a lower security interface to high security interface, define access lists on the PIX.

```
pixfirewall(config)# access-list msnet permit tcp any h 10.48.66.106 eq 139
pixfirewall(config)# access-list msnet permit udp any h 10.48.66.106 eq 138
pixfirewall(config)# access-list msnet permit udp any h 10.48.66.106 eq 137
pixfirewall(config)# access-list msnet permit tcp any h 10.48.66.73 eq 139
pixfirewall(config)# access-list msnet permit udp any h 10.48.66.73 eq 138
pixfirewall(config)# access-list msnet permit udp any h 10.48.66.73 eq 137
```

```
pixfirewall(config)# show access-list
access-list msnet permit tcp any host 10.48.66.73 eq 139 (hitcnt=0)
access-list msnet permit udp any host 10.48.66.73 eq netbios-dgm (hitcnt=0)
access-list msnet permit udp any host 10.48.66.73 eq netbios-ns (hitcnt=0)
access-list msnet permit tcp any host 10.48.66.106 eq 139 (hitcnt=0)
access-list msnet permit udp any host 10.48.66.106 eq netbios-dgm (hitcnt=0)
access-list msnet permit udp any host 10.48.66.106 eq netbios-ns (hitcnt=0)
```

As you can see, the PIX replaces the port numbers with well-known service names. You need to open PIX for Windows NetBIOS services, as shown above, for each host on the inside that you want to access remotely. The exception is when you define a network static, which encompasses all the hosts on your inside network and permits the whole subnet to be accessed.

Note: All the resources that you want to access remotely need to have a static IP assignment and may not use Dynamic Host Configuration Protocol (DHCP). Configure the appropriate statics and verify them.

```
pixfirewall(config)# show stat
static (inside,outside) 10.48.66.106 10.48.66.106 netmask 255.255.255.255 0 0
static (inside,outside) 10.48.66.73 10.48.66.73 netmask 255.255.255.255 0 0
```

3. Configure the PIX Firewall with NAT. (if needed)

Note: This section only applies to PIX configurations with NAT involved. If you do not have NAT involved, please check that you have completed step 1 and step 2 above and then proceed to Verifying Accessibility Through the PIX Firewall.

Consider the following two factors when NAT is involved.

- ◆ Configure the WINS server so that it can return both the translated and the internal IP addresses to the WINS client. To do this, select **Internet Group** as the Type option in the Add Static Mappings dialog box of the WINS manager. The user-defined Internet Group option allows you to specify up to 25 addresses for a single name.

When WINS client does NetBIOS name resolution with the WINS server, WINS returns both of the addresses and the client can establish the NetBIOS session with the resource in question.

- ◆ The PIX configuration needs to reflect the appropriate access lists and statics. For example, using the same setup but with NAT involved, the configuration is:

```
static (inside,outside) 192.168.10.50 10.48.66.106 netmask 255.255.255.255 0 0
static (inside,outside) 192.168.10.60 10.48.66.73 netmask 255.255.255.255 0 0
access-list msnet permit tcp any host 192.168.10.50 eq 139
access-list msnet permit udp any host 192.168.10.50 eq netbios-dgm
access-list msnet permit udp any host 192.168.10.50 eq netbios-ns
access-list msnet permit tcp any host 192.168.10.60 eq 139
access-list msnet permit udp any host 192.168.10.60 eq netbios-dgm
access-list msnet permit udp any host 192.168.10.60 eq netbios-ns
access-list msnet permit icmp any any
access-group msnet in interface outside
```

Verify

Verifying Accessibility Through the PIX Firewall

Use the following steps to verify accessibility through the PIX Firewall.

Note: Prior to proceeding with the verification steps, ensure you that are able to ping the inside resources (RAGE and NPITRN hosts in this example) in order to avoid issues related to any basic IP connectivity problems. You can configure an access list or conduit to permit ping and later remove it if your security policy does not permit ping traffic.

1. Turn on debugging on the PIX firewall to see the packet flow.

```
pixfirewall(config)# logging on
```

```
pixfirewall(config)# logging console debug
```

2. Verify the settings using the **show logging** command:

```
pixfirewall(config)# show logging
<snip>
  Console logging: level debugging, 25 messages logged
<snip>
```

```
pixfirewall(config)# show xlate
0 in use, 45 most used
```

3. Attempt to reboot the PC and access the resource using UNC. On the remote computer, select **Start > Find Computer** and type the name of the resource you want to access. In this example, NPITRN is this resource.
4. Reboot the PC on the outside (AYPC in this example). While AYPC boots, we see the following debugs on the PIX. This is expected and part of the overview of packet flow described above.

```
pixfirewall(config)#
609001: Built local-host inside:10.48.66.106
305002: Translation built for gaddr 10.48.66.106 to laddr 10.48.66.106
302005: Built UDP connection for faddr 192.168.10.5/137 gaddr 10.48.66.106/137
laddr 10.48.66.106/137
302005: Built UDP connection for faddr 192.168.10.5/138 gaddr 10.48.66.106/138
laddr 10.48.66.106/138
302001: Built inbound TCP connection 420 for faddr 192.168.10.5/1027
gaddr 10.48.66.106/139 laddr 10.48.66.106/139
302001: Built inbound TCP connection 421 for faddr 192.168.10.5/1032
gaddr 10.48.66.106/139 laddr 10.48.66.106/139
pixfirewall(config)# 302006: Teardown UDP connection for faddr 192.168.10.5/138
gaddr 10.48.66.106/138 laddr 10.48.66.106/138
pixfirewall(config)#show xlate
1 in use, 45 most used
Global 10.48.66.106 Local 10.48.66.106 static
pixfirewall(config)# show conn
3 in use, 12 most used
TCP out 192.168.10.5:1027 in 10.48.66.106:139 idle 0:01:41 Bytes 23514
flags UIOB
TCP out 192.168.10.5:1032 in 10.48.66.106:139 idle 0:02:29 Bytes 1302
flags UIOB
UDP out 192.168.10.5:137 in 10.48.66.106:137 idle 0:00:56 flags
```

Troubleshooting Procedure

Troubleshooting Information and Sniffer Trace Example

The following information is provided to help you troubleshoot and understand your configuration.

Microsoft Networking uses Server Message Block (SMB) protocol for Windows file sharing and print services. For an introduction to SMB, visit [Just what is SMB?](#) .

If you receive The Network Path was Not Found error message dialog when you attempt to access the folder using `\\resource_name`:

- The WINS server might not be responding to the client's request to resolve the NetBIOS name. When this happens, the client retries but if there is no response, it will resort to broadcast on the local segment. Because the PIX blocks broadcasts (this cannot be changed), name resolution will fail. This eventually results in the above error message.

To resolve this issue, check why the WINS server is not responding and fix the WINS server. Try capturing a sniffer trace to see if WINS is responding and if the packet is making its way back to the

client. Fix the issue so that packet reaches the client.

If your WINS server is multihomed, verify static mappings in the WINS manager and verify that static and access lists exist for all IP addresses involved.

A fifteen-frame sample sniffer trace for a working connection is provided below. Use this as a baseline trace while troubleshooting similar issues.

- Frames 1–6 show the name registration process occurring between the client and the WINS server.
- Frames 7–8 show the NetLogon process (the client looking for a DC) between the client and the WINS server.
- Frames 9–11 show TCP session establishment.
- Frame 12–13 show NetBIOS session establishment.
- Frame 14–15 show the start of SMB negotiation and how the process continues and terminates when a user has finished accessing the resource.

Note: Due to space limitations, this sniffer trace has been edited to fit the screen.

```
----- Frame 1 -----
\"Flags \",\"Frame \",\"Delta Time \",\"Destination \",\"Source
\", \"Bytes\", \"Protocol \", \"Summary\"
\" M \", \" 1\", \"0.000.000 \", \"RAGE \", \"AYPC \", \"
92 \", \"WINS\", \" C ID=32860 OP=QUERY NAME=TACWEB<1C>\"
DLC: ----- DLC Header -----
DLC:
DLC: Frame 1 arrived at 12:58:27.6668; frame size is 92 (005C hex) bytes.
DLC: Destination = Station 001083027B34
DLC: Source = Station 005054FEEA31
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: .... ...0 = CE bit - no congestion
IP: Total length = 78 bytes
IP: Identification = 5889
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 128 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = 0C57 (correct)
IP: Source address = [192.168.10.5], AYPC
IP: Destination address = [10.48.66.106], RAGE
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: Source port = 137 (NetBIOS-ns)
UDP: Destination port = 137 (NetBIOS-ns)
UDP: Length = 58
UDP: Checksum = 0F61 (correct)
UDP: [50 byte(s) of data]
UDP:
WINS: ----- WINS Name Service header -----
```

```

WINS:
WINS: ID = 32860
WINS: Flags = 01
WINS: 0... .... = Command
WINS: .000 0... = Query
WINS: .... ..0. = Not truncated
WINS: .... ...1 = Recursion desired
WINS: Flags = 0X
WINS: ...0 .... = Non Verified data NOT acceptable
WINS: Question count = 1, Answer count = 0
WINS: Authority count = 0, Additional record count = 0
WINS:
WINS: Question section:
WINS:     Name = TACWEB<1C>
WINS:     Type = NetBIOS name service (WINS) (NetBIOS name,32)
WINS:     Class = Internet (IN,1)
WINS:
----- Frame 2 -----
\"Flags \",\"Frame \",\"Delta Time  \",\"Destination  \",\"Source
  \",\"Bytes\", \"Protocol  \",\"Summary\"
"    ", "    2", "0.000.582    ", "AYPC    ", "RAGE    ", "
110 ", "WINS", " R ID=32860 STAT=OK "
DLC: ----- DLC Header -----
DLC:
DLC: Frame 2 arrived at 12:58:27.6674; frame size is 110 (006E hex) bytes.
DLC: Destination = Station 005054FEEA31
DLC: Source      = Station 001083027B34
DLC: Ethertype   = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP:     000. .... = routine
IP:     ...0 .... = normal delay
IP:     .... 0... = normal throughput
IP:     .... .0.. = normal reliability
IP:     .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP:     .... ...0 = CE bit - no congestion
IP: Total length   = 96 bytes
IP: Identification = 49634
IP: Flags         = 0X
IP:     .0.. .... = may fragment
IP:     ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live   = 128 seconds/hops
IP: Protocol      = 17 (UDP)
IP: Header checksum = 6163 (correct)
IP: Source address = [10.48.66.106], RAGE
IP: Destination address = [192.168.10.5], AYPC
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: Source port      = 137 (NetBIOS-ns)
UDP: Destination port = 137 (NetBIOS-ns)
UDP: Length          = 76
UDP: Checksum        = A5AB (correct)
UDP: [68 byte(s) of data]
UDP:
WINS: ----- WINS Name Service header -----
WINS:
WINS: ID = 32860
WINS: Flags = 85
WINS: 1... .... = Response
WINS: .... .1.. = Authoritative answer

```



```

UDP: Checksum          = 627C (correct)
UDP: [266 byte(s) of data]
UDP:
NETB: ----- NetBIOS Datagram protocol -----
NETB:
NETB: Type = 17 (Direct_group datagram)
NETB: Flags = 1A
NETB: .... .1. = First packet
NETB: .... ..0 = No more to follow
NETB: Datagram ID = 805A
NETB: Source node = [192.168.10.5], AYPC
NETB: Port = 138
NETB: Total datagram length (including names) = 252
NETB: Packet offset = 0
NETB:      Source NetBIOS name = AYPC<00>
NETB: Destination NetBIOS name = TACWEB<1C>
NETB: Total datagram length (excluding names) = 184
NETB:
SMB: ----- SMB (CIFS) Transaction Command header -----
SMB:
SMB: SMB Constant
SMB: Command          = 25 (Transaction)
SMB: Reserved         = 0
SMB: Flags = 18
SMB: 0... .. = Client Command
SMB: ..0. .... = No Opportunistic file Locking
SMB: ...1 .... = Pathnames are already in canonicalized format
SMB: .... 1... = Pathnames should be treated as caseless
SMB: .... ..0. = Send.No.Ack can not be used as a response
SMB: .... ..0 = Doesn't support Lock&Read, Write&Unlock
SMB: Flags2 = 0003
SMB: 0... .. . .... = STRING type is ASCIIZ
SMB: .0.. .... . .... = DOS style Error code
SMB: ..0. .... . .... = No Paging IO
SMB: ...0 .... . .... = No DFS support
SMB: .... 0... . .... = Client not aware of extended security
SMB: .... .... .0.. . = Don't use message authentication
SMB: .... .... ..1. . = Client supports extended attributes
SMB: .... .... ....1 = Client supports Long file names
SMB: Reserved2(MBZ)   = 000000000000000000000000
SMB: Tree ID          = 0000
SMB: Process ID       = CAFE
SMB: Unauth User ID   = 0000
SMB: Multiplex ID     = 0000
SMB:
SMB: ----- Transaction Header -----
SMB:
SMB: Word count        = 17
SMB: Parameter words   = 00005C0002000000000000200FFFFFFF000000005C005C005C0
00300010000000200
SMB: Byte Count        = 115
SMB: Byte parameters   = 5C4D41494C534C4F545C4E45545C4E544C4F474F4E000012000
000410059005000430000004100590050004300240000005C4D41494C534C4F545C4E45545C47455444
4330343200800000001800000000000010400000000000515000000221A8324C44B14687144060B010
00000...
SMB: Total parameter bytes being sent = 0
SMB: Total data bytes being sent      = 92
SMB: Max number of parameter bytes to return = 2
SMB: Max number of data bytes to return   = 0
SMB: Max number of Setup words to return  = 0
SMB: Reserved(MBZ)                       = 00
SMB: Additional information                = 0002
SMB: ..... 1. = One way transaction
SMB: ..... 0 = Preserve TID
SMB: Timeout to completion                 = Indefinite wait
SMB: Reserved(MBZ)                       = 0000

```

SMB: Number of parameter bytes in this buffer = 0
SMB: Offset from header to parameter bytes = 92
SMB: Number of data bytes in this buffer = 92
SMB: Offset from header to data bytes = 92
SMB: Setup word count = 3
SMB: Reserved(MBZ) = 00
SMB: Setup words = 010000000200
SMB: Byte Count = 115
SMB: Transaction name = \MAILSLOT\NET\NTLOGON
SMB: Data bytes = 120000004100590050004300000041005900500043002400000
05C4D41494C534C4F545C4E45545C474554444330343200800000001800000000000010400000000
000515000000221A8324C44B14687144060B01000000FFFFFFFF

SMB:

SMBMSP: ----- SMB MAILSLOTS Protocol -----

SMBMSP:

SMBMSP: Op code = 1 (Write mail slot)

SMBMSP: Priority of transaction = 0

SMBMSP: Class of service = 2 (Unreliable & broadcast)

SMBMSP: Total size of mail data = 115

SMBMSP: MAILSLOT = "\MAILSLOT\NET\NTLOGON"

SMBMSP:

NETLOGON: ----- SMB NETLOGON Protocol -----

NETLOGON:

NETLOGON: NETLOGON Command = 12 (SAM LOGON Request from client)

NETLOGON: Request Count = 0 (0x0000)

NETLOGON: Unicode Computer Name = AYPC

NETLOGON: Unicode User Name = AYPC\$

NETLOGON: Mailslot Name = "\MAILSLOT\NET\GETDC042"

NETLOGON: Allowable Account control bits = 00000080

NETLOGON:0.. = User account not auto-locked

NETLOGON:0. = User Password will expire

NETLOGON:0 = Not a Server Trust user account

NETLOGON:1..... = Workstation Trust user account

NETLOGON:0..... = Not an Inter-domain Trust user account

NETLOGON:0..... = Not a MNS Logon user account

NETLOGON:0.... = Not a normal user account

NETLOGON:0... = Not a temp duplicate user account

NETLOGON:0.. = User password required

NETLOGON:0. = User Home directory not required

NETLOGON:0 = User account enabled

NETLOGON: Domain SID Size = 24 (0x00000018)

NETLOGON: SID = 000000010400000000000515000000221A8324
C44B146871

NETLOGON:

----- Frame 4 -----

\ "Flags \", \"Frame \", \"Delta Time \", \"Destination \", \"Source

\", \"Bytes \", \"Protocol \", \"Summary \"

" , " 4", "0.000.900", "AYPC", "RAGE", " , "

266 ", "NETLOGON", " SAM Response to SAM LOGON Request"

DLC: ----- DLC Header -----

DLC:

DLC: Frame 4 arrived at 12:58:27.6706; frame size is 266 (010A hex) bytes.

DLC: Destination = Station 005054FEEA31

DLC: Source = Station 001083027B34

DLC: Ethertype = 0800 (IP)

DLC:

IP: ----- IP Header -----

```

IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP:      000. .... = routine
IP:      ...0 .... = normal delay
IP:      .... 0... = normal throughput
IP:      .... .0.. = normal reliability
IP:      .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP:      .... ...0 = CE bit - no congestion
IP: Total length   = 252 bytes
IP: Identification = 49890
IP: Flags          = 0X
IP:      .0.. .... = may fragment
IP:      ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live    = 128 seconds/hops
IP: Protocol        = 17 (UDP)
IP: Header checksum = 5FC7 (correct)
IP: Source address  = [10.48.66.106], RAGE
IP: Destination address = [192.168.10.5], AYPC
IP: No options
IP:

UDP: ----- UDP Header -----
UDP:
UDP: Source port      = 138 (NetBIOS-dgm)
UDP: Destination port = 138 (NetBIOS-dgm)
UDP: Length           = 232
UDP: Checksum         = D678 (correct)
UDP: [224 byte(s) of data]
UDP:

NETB: ----- NetBIOS Datagram protocol -----
NETB:
NETB: Type = 16 (Direct_unique datagram)
NETB: Flags = 1A
NETB: .... ..1. = First packet
NETB: .... ...0 = No more to follow
NETB: Datagram ID = 8FEE
NETB: Source node = [10.48.66.106], RAGE
NETB: Port = 138
NETB: Total datagram length (including names) = 210
NETB: Packet offset = 0
NETB:      Source NetBIOS name = RAGE<00>
NETB: Destination NetBIOS name = AYPC<00>
NETB: Total datagram length (excluding names) = 142
NETB:

SMB: ----- SMB (CIFS) Transaction Command header -----
SMB:
SMB: SMB Constant
SMB: Command          = 25 (Transaction)
SMB: Reserved         = 0
SMB: Flags = 00
SMB: 0... .... = Client Command
SMB: ..0. .... = No Opportunistic file Locking
SMB: ...0 .... = Pathnames are not in canonicalized format
SMB: .... 0... = Pathnames are case sensitive
SMB: .... ..0. = Send.No.Ack can not be used as a response
SMB: .... ...0 = Doesn't support Lock&Read, Write&Unlock
SMB: Flags2 = 0000
SMB: 0... .... ..0... ..0... ..0... ..0... = STRING type is ASCIIZ
SMB: .0.. .... ..0... ..0... ..0... = DOS style Error code
SMB: ..0. .... ..0... ..0... ..0... = No Paging IO
SMB: ...0 .... ..0... ..0... ..0... = No DFS support
SMB: .... 0... ..0... ..0... ..0... = Client not aware of extended security
SMB: .... .... ..0... ..0... ..0... = Don't use message authentication
SMB: .... .... ..0... ..0... ..0... = Client does not support extended attributes
SMB: .... .... ..0... ..0... ..0... = Client does not support Long file names

```

```

SMB: Reserved2(MBZ)      = 000000000000000000000000
SMB: Tree ID             = 0000
SMB: Process ID         = 0000
SMB: Unauth User ID     = 0000
SMB: Multiplex ID       = 0000
SMB:
SMB: ----- Transaction Header -----
SMB:
SMB: Word count          = 17
SMB: Parameter words     = 000032000000000000000000E8030000000000000003200
5C000300010001000200
SMB: Byte Count          = 73
SMB: Byte parameters     = 5C4D41494C534C4F545C4E45545C47455444433034320013
005C005C005200410047004500000041005900500043002400000054004100430057004500420000
0001000000FFFFFFFF
SMB: Total parameter bytes being sent = 0
SMB: Total data bytes being sent      = 50
SMB: Max number of parameter bytes to return = 0
SMB: Max number of data bytes to return   = 0
SMB: Max number of Setup words to return  = 0
SMB: Reserved(MBZ)                       = 00
SMB: Additional information                = 0000
SMB: .....0. = Two way transaction
SMB: .....0 = Preserve TID
SMB: Timeout to completion                = 1000 (Milliseconds)
00:00:01.0(HH:MM:SS.MS)
SMB: Reserved(MBZ)                       = 0000
SMB: Number of parameter bytes in this buffer = 0
SMB: Offset from header to parameter bytes  = 0
SMB: Number of data bytes in this buffer = 50
SMB: Offset from header to data bytes      = 92
SMB: Setup word count = 3
SMB: Reserved(MBZ) = 00
SMB: Setup words = 010001000200
SMB: Byte Count = 73
SMB: Transaction name = \MAILSLOT\NET\GETDC042
SMB: Data bytes = 13005C005C0052004100470045000000410059005000430
02400000540041004300570045004200000001000000FFFFFFFF
SMB:
SMBMSP: ----- SMB MAILSLOTS Protocol -----
SMBMSP:
SMBMSP: Op code = 1 (Write mail slot)
SMBMSP: Priority of transaction = 1
SMBMSP: Class of service = 2 (Unreliable & broadcast)
SMBMSP: Total size of mail data = 73
SMBMSP: MAILSLOT = "\MAILSLOT\NET\GETDC042"
SMBMSP:
NETLOGON: ----- SMB NETLOGON Protocol -----
NETLOGON:
NETLOGON: NETLOGON Command = 13 (SAM Response to SAM LOGON Request)
NETLOGON: Unicode Logon Server = \\RAGE
NETLOGON: Unicode User Name = AYPC$
NETLOGON: Unicode Domain Name = TACWEB
NETLOGON: NT Version = 1 (0x00000001)
NETLOGON: LMNT Token = 0xFFFF
NETLOGON: LM20 Token = 0xFFFF (Lan Manager 2.0 or higher)
NETLOGON:
- - - - - Frame 5 - - - - -
\"Flags \",\"Frame \",\"Delta Time \",\"Destination \",\"Source
 \",\"Bytes\", \"Protocol \",\"Summary\"
"  ", " 5", "1.755.851", "RAGE", "AYPC", "
110 ", "WINS", " C ID=32862 OP=REGISTER NAME=ADMINISTRATOR<03>"
DLC: ----- DLC Header -----
DLC:
DLC: Frame 5 arrived at 12:58:29.4265; frame size is 110 (006E hex) bytes.

```

DLC: Destination = Station 001083027B34
DLC: Source = Station 005054FEEA31
DLC: Ethertype = 0800 (IP)
DLC:

IP: ----- IP Header -----

IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. = routine
IP: ...0 = normal delay
IP: 0... = normal throughput
IP:0.. = normal reliability
IP:0. = ECT bit - transport protocol will ignore the CE bit
IP:0 = CE bit - no congestion
IP: Total length = 96 bytes
IP: Identification = 6913
IP: Flags = 0X
IP: .0.. = may fragment
IP: ..0. = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 128 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = 0845 (correct)
IP: Source address = [192.168.10.5], AYPC
IP: Destination address = [10.48.66.106], RAGE
IP: No options
IP:

UDP: ----- UDP Header -----

UDP:
UDP: Source port = 137 (NetBIOS-ns)
UDP: Destination port = 137 (NetBIOS-ns)
UDP: Length = 76
UDP: Checksum = 3663 (correct)
UDP: [68 byte(s) of data]
UDP:

WINS: ----- WINS Name Service header -----

WINS:
WINS: ID = 32862
WINS: Flags = 29
WINS: 0... = Command
WINS: .010 1... = Registration
WINS:0. = Not truncated
WINS:1 = Recursion desired
WINS: Flags = 0X
WINS: ...0 = Non Verified data NOT acceptable
WINS: Question count = 1, Answer count = 0
WINS: Authority count = 0, Additional record count = 1
WINS:
WINS: Question section:
WINS: Name = ADMINISTRATOR<03>
WINS: Type = NetBIOS name service (WINS) (NetBIOS name,32)
WINS: Class = Internet (IN,1)
WINS:
WINS: Additional record section:
WINS: Name = ADMINISTRATOR<03>
WINS: Type = NetBIOS name service (WINS) (NetBIOS name,32)
WINS: Class = Internet (IN,1)
WINS: Time-to-live = 300000 (seconds)
WINS: Length = 6
WINS: Node flags = 60
WINS: 0... = Unique NetBIOS name
WINS: .11. = H-type node
WINS: Node address = [192.168.10.5], AYPC
WINS:

```

\"Flags \" , \"Frame \" , \"Delta Time \" , \"Destination \" , \"Source
  \" , \"Bytes\" , \"Protocol \" , \"Summary\"
"      " , "      6\" , \"0.001.987 \" , \"AYPC \" , \"RAGE \" , \"
  104 \" , \"WINS\" , \" R ID=32862 STAT=OK \"
DLC: ----- DLC Header -----
      DLC:
      DLC: Frame 6 arrived at 12:58:29.4285; frame size is 104 (0068 hex) bytes.
      DLC: Destination = Station 005054FEEA31
      DLC: Source      = Station 001083027B34
      DLC: Ethertype   = 0800 (IP)
      DLC:
IP: ----- IP Header -----
      IP:
      IP: Version = 4, header length = 20 bytes
      IP: Type of service = 00
      IP:      000. .... = routine
      IP:      ...0 .... = normal delay
      IP:      .... 0... = normal throughput
      IP:      .... .0.. = normal reliability
      IP:      .... ..0. = ECT bit - transport protocol will ignore the CE bit
      IP:      .... ...0 = CE bit - no congestion
      IP: Total length   = 90 bytes
      IP: Identification = 50146
      IP: Flags         = 0X
      IP:      .0.. .... = may fragment
      IP:      ..0. .... = last fragment
      IP: Fragment offset = 0 bytes
      IP: Time to live   = 128 seconds/hops
      IP: Protocol      = 17 (UDP)
      IP: Header checksum = 5F69 (correct)
      IP: Source address  = [10.48.66.106], RAGE
      IP: Destination address = [192.168.10.5], AYPC
      IP: No options
      IP:
UDP: ----- UDP Header -----
      UDP:
      UDP: Source port      = 137 (NetBIOS-ns)
      UDP: Destination port = 137 (NetBIOS-ns)
      UDP: Length          = 70
      UDP: Checksum        = 1CFA (correct)
      UDP: [62 byte(s) of data]
      UDP:
WINS: ----- WINS Name Service header -----
      WINS:
      WINS: ID = 32862
      WINS: Flags = AD
      WINS: 1... .... = Response
      WINS: .... .1.. = Authoritative answer
      WINS: .010 1...  = Registration
      WINS: .... ..0. = Not truncated
      WINS: Flags = 8X
      WINS: ..0. .... = Data NOT verified
      WINS: 1... .... = Recursion available
      WINS: Response code = OK (0)
      WINS: ...0 .... = Unicast packet
      WINS: Question count = 0, Answer count = 1
      WINS: Authority count = 0, Additional record count = 0
      WINS:
      WINS: Answer section:
      WINS:      Name = ADMINISTRATOR<03>
      WINS:      Type = NetBIOS name service (WINS) (NetBIOS name,32)
      WINS:      Class = Internet (IN,1)
      WINS:      Time-to-live = 518400 (seconds)
      WINS:      Length = 6
      WINS: Node flags = 60
      WINS: 0... .... = Unique NetBIOS name

```

WINS: .11. = H-type node
WINS: Node address = [192.168.10.5], AYPC
WINS:

----- Frame 7 -----
\"Flags \",\"Frame \",\"Delta Time \",\"Destination \",\"Source
 \",\"Bytes\", \"Protocol \", \"Summary\"
\" \" \" 7\", \"32.953.258 \" ,\"RAGE \" ,\"AYPC \" ,\"
60 \" ,\"TCP\", \" D=139 S=1037 SYN SEQ=39758 LEN=0 WIN=8192\"

DLC: ----- DLC Header -----

DLC:
DLC: Frame 7 arrived at 12:59:02.3817; frame size is 60 (003C hex) bytes.
DLC: Destination = Station 001083027B34
DLC: Source = Station 005054FEEA31
DLC: Ethertype = 0800 (IP)
DLC:

IP: ----- IP Header -----

IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. = routine
IP: ...0 = normal delay
IP: 0... = normal throughput
IP:0.. = normal reliability
IP:0. = ECT bit - transport protocol will ignore the CE bit
IP:0 = CE bit - no congestion
IP: Total length = 44 bytes
IP: Identification = 7425
IP: Flags = 4X
IP: .1.. = don't fragment
IP: ..0. = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 128 seconds/hops
IP: Protocol = 6 (TCP)
IP: Header checksum = C683 (correct)
IP: Source address = [192.168.10.5], AYPC
IP: Destination address = [10.48.66.106], RAGE
IP: No options
IP:

TCP: ----- TCP header -----

TCP:
TCP: Source port = 1037
TCP: Destination port = 139 (NetBIOS-ssn)
TCP: Initial sequence number = 39758
TCP: Next expected Seq number = 39759
TCP: Data offset = 24 bytes
TCP: Flags = 02
TCP: ..0. = (No urgent pointer)
TCP: ...0 = (No acknowledgment)
TCP: 0... = (No push)
TCP:0.. = (No reset)
TCP:1. = SYN
TCP:0 = (No FIN)
TCP: Window = 8192
TCP: Checksum = 756A (correct)
TCP:
TCP: Options follow
TCP: Maximum segment size = 1380
TCP:

----- Frame 8 -----
\"Flags \",\"Frame \",\"Delta Time \",\"Destination \",\"Source
 \",\"Bytes\", \"Protocol \", \"Summary\"
\" \" \" 8\", \"0.000.138 \" ,\"AYPC \" ,\"RAGE \" ,\"
60 \" ,\"TCP\", \" D=1037 S=139 SYN ACK=39759 SEQ=590101 LEN=0 WIN=8280\"
DLC: ----- DLC Header -----

```

DLC:
DLC: Frame 8 arrived at 12:59:02.3819; frame size is 60 (003C hex) bytes.
DLC: Destination = Station 005054FEEA31
DLC: Source       = Station 001083027B34
DLC: Ethertype    = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP:   000. .... = routine
IP:   ...0 .... = normal delay
IP:   .... 0... = normal throughput
IP:   .... .0.. = normal reliability
IP:   .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP:   .... ...0 = CE bit - no congestion
IP: Total length = 44 bytes
IP: Identification = 50402
IP: Flags         = 4X
IP:   .1.. .... = don't fragment
IP:   ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live   = 128 seconds/hops
IP: Protocol       = 6 (TCP)
IP: Header checksum = 1EA2 (correct)
IP: Source address  = [10.48.66.106], RAGE
IP: Destination address = [192.168.10.5], AYPC
IP: No options
IP:
TCP: ----- TCP header -----
TCP:
TCP: Source port          = 139 (NetBIOS-ssn)
TCP: Destination port    = 1037
TCP: Initial sequence number = 590101
TCP: Next expected Seq number= 590102
TCP: Acknowledgment number = 39759
TCP: Data offset         = 24 bytes
TCP: Flags               = 12
TCP:   ..0. .... = (No urgent pointer)
TCP:   ...1 .... = Acknowledgment
TCP:   .... 0... = (No push)
TCP:   .... .0.. = (No reset)
TCP:   .... ..1. = SYN
TCP:   .... ...0 = (No FIN)
TCP: Window              = 8280
TCP: Checksum            = BF71 (correct)
TCP:
TCP: Options follow
TCP: Maximum segment size = 1460
TCP:
----- Frame 9 -----
\"Flags \",\"Frame \",\"Delta Time \",\"Destination \",\"Source
  \",\"Bytes\", \"Protocol \", \"Summary\"
  \"   \"   \"   \"   \"   \"   \"   \"   \"   \"   \"   \"   \"   \"   \"
  60 \" , \"TCP\", \" D=139 S=1037   ACK=590102 WIN=8280\"
DLC: ----- DLC Header -----
DLC:
DLC: Frame 9 arrived at 12:59:02.3836; frame size is 60 (003C hex) bytes.
DLC: Destination = Station 001083027B34
DLC: Source       = Station 005054FEEA31
DLC: Ethertype    = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes

```

```

IP: Type of service = 00
IP:      000. .... = routine
IP:      ...0 .... = normal delay
IP:      .... 0... = normal throughput
IP:      .... .0.. = normal reliability
IP:      .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP:      .... ...0 = CE bit - no congestion
IP: Total length = 40 bytes
IP: Identification = 7681
IP: Flags = 4X
IP:      .1.. .... = don't fragment
IP:      ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 128 seconds/hops
IP: Protocol = 6 (TCP)
IP: Header checksum = C587 (correct)
IP: Source address = [192.168.10.5], AYPC
IP: Destination address = [10.48.66.106], RAGE
IP: No options
IP:
TCP: ----- TCP header -----
TCP:
TCP: Source port = 1037
TCP: Destination port = 139 (NetBIOS-ssn)
TCP: Sequence number = 39759
TCP: Next expected Seq number= 39759
TCP: Acknowledgment number = 590102
TCP: Data offset = 20 bytes
TCP: Flags = 10
TCP:      ..0. .... = (No urgent pointer)
TCP:      ...1 .... = Acknowledgment
TCP:      .... 0... = (No push)
TCP:      .... .0.. = (No reset)
TCP:      .... ..0. = (No SYN)
TCP:      .... ...0 = (No FIN)
TCP: Window = 8280
TCP: Checksum = D72E (correct)
TCP: No TCP options
TCP:
----- Frame 10 -----
\"Flags \",\"Frame \",\"Delta Time \",\"Destination \",\"Source
  \",\"Bytes\", \"Protocol \",\"Summary\"
  \"  \"  \"  10\", \"0.000.222  \" ,\"RAGE  \" ,\"AYPC  \" ,\"
  126 \" ,\"NETB\", \" D=RAGE<20> S=AYPC<00> Session request\"
DLC: ----- DLC Header -----
DLC:
DLC: Frame 10 arrived at 12:59:02.3839; frame size is 126 (007E hex) bytes.
DLC: Destination = Station 001083027B34
DLC: Source = Station 005054FEAA31
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP:      000. .... = routine
IP:      ...0 .... = normal delay
IP:      .... 0... = normal throughput
IP:      .... .0.. = normal reliability
IP:      .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP:      .... ...0 = CE bit - no congestion
IP: Total length = 112 bytes
IP: Identification = 7937
IP: Flags = 4X
IP:      .1.. .... = don't fragment

```

```

IP:      ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live   = 128 seconds/hops
IP: Protocol       = 6 (TCP)
IP: Header checksum = C43F (correct)
IP: Source address  = [192.168.10.5], AYPC
IP: Destination address = [10.48.66.106], RAGE
IP: No options
IP:
TCP: ----- TCP header -----
TCP:
TCP: Source port           = 1037
TCP: Destination port     = 139 (NetBIOS-ssn)
TCP: Sequence number      = 39759
TCP: Next expected Seq number= 39831
TCP: Acknowledgment number = 590102
TCP: Data offset          = 20 bytes
TCP: Flags                 = 18
TCP:      ..0. .... = (No urgent pointer)
TCP:      ...1 .... = Acknowledgment
TCP:      .... 1... = Push
TCP:      .... .0.. = (No reset)
TCP:      .... ..0. = (No SYN)
TCP:      .... ...0 = (No FIN)
TCP: Window                = 8280
TCP: Checksum              = D120 (correct)
TCP: No TCP options
TCP: [72 Bytes of data]
TCP:
NETB: ----- NetBIOS Session protocol -----
NETB:
NETB: Type = 81 (Session request)
NETB: Flags = 00
NETB: Total session packet length = 68
NETB: Called NetBIOS name = RAGE<20> <server service>
NETB: Calling NetBIOS name = AYPC<00>
NETB:
----- Frame 11 -----
\"Flags \",\"Frame \",\"Delta Time  \",\"Destination  \",\"Source
  \",\"Bytes\", \"Protocol  \",\"Summary\"
"    ", "    11", "0.000.125    ", "AYPC                ", "RAGE                ", "
60 ", "NETB", " Session confirm"
DLC: ----- DLC Header -----
DLC:
DLC: Frame 11 arrived at 12:59:02.3840; frame size is 60 (003C hex) bytes.
DLC: Destination = Station 005054FEEA31
DLC: Source       = Station 001083027B34
DLC: Ethertype    = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP:      000. .... = routine
IP:      ...0 .... = normal delay
IP:      .... 0... = normal throughput
IP:      .... .0.. = normal reliability
IP:      .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP:      .... ...0 = CE bit - no congestion
IP: Total length   = 44 bytes
IP: Identification = 50658
IP: Flags          = 4X
IP:      .1.. .... = don't fragment
IP:      ..0. .... = last fragment
IP: Fragment offset = 0 bytes

```

```

IP: Time to live      = 128 seconds/hops
IP: Protocol          = 6 (TCP)
IP: Header checksum   = 1DA2 (correct)
IP: Source address    = [10.48.66.106], RAGE
IP: Destination address = [192.168.10.5], AYPC
IP: No options
IP:
TCP: ----- TCP header -----
TCP:
TCP: Source port      = 139 (NetBIOS-ssn)
TCP: Destination port = 1037
TCP: Sequence number  = 590102
TCP: Next expected Seq number = 590106
TCP: Acknowledgment number = 39831
TCP: Data offset      = 20 bytes
TCP: Flags            = 18
TCP:      ..0. .... = (No urgent pointer)
TCP:      ...1 .... = Acknowledgment
TCP:      .... 1... = Push
TCP:      .... .0.. = (No reset)
TCP:      .... ..0. = (No SYN)
TCP:      .... ...0 = (No FIN)
TCP: Window          = 8208
TCP: Checksum        = 5522 (correct)
TCP: No TCP options
TCP: [4 Bytes of data]
TCP:
NETB: ----- NetBIOS Session protocol -----
NETB:
NETB: Type = 82 (Positive response)
NETB: Flags = 00
NETB: Total session packet length = 0
NETB:
----- Frame 12 -----
\"Flags \",\"Frame \",\"Delta Time \",\"Destination \",\"Source
  \",\"Bytes\", \"Protocol \",\"Summary\"
"  ", " 12", "0.001.427", "RAGE", "AYPC", "
228 ", "CIFS/SMB", " C Negotiate Protocol Max Dialect Index=7"
DLC: ----- DLC Header -----
DLC:
DLC: Frame 12 arrived at 12:59:02.3854; frame size is 228 (00E4 hex) bytes.
DLC: Destination = Station 001083027B34
DLC: Source      = Station 005054FEEA31
DLC: Ethertype   = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP:      000. .... = routine
IP:      ...0 .... = normal delay
IP:      .... 0... = normal throughput
IP:      .... .0.. = normal reliability
IP:      .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP:      .... ...0 = CE bit - no congestion
IP: Total length = 214 bytes
IP: Identification = 8193
IP: Flags         = 4X
IP:      .1.. .... = don't fragment
IP:      ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live   = 128 seconds/hops
IP: Protocol      = 6 (TCP)
IP: Header checksum = C2D9 (correct)
IP: Source address = [192.168.10.5], AYPC

```

```

IP: Destination address = [10.48.66.106], RAGE
IP: No options
IP:
TCP: ----- TCP header -----
TCP:
TCP: Source port                = 1037
TCP: Destination port          = 139 (NetBIOS-ssn)
TCP: Sequence number           = 39831
TCP: Next expected Seq number = 40005
TCP: Acknowledgment number    = 590106
TCP: Data offset               = 20 bytes
TCP: Flags                     = 18
TCP:      ..0. .... = (No urgent pointer)
TCP:      ...1 .... = Acknowledgment
TCP:      .... 1... = Push
TCP:      .... .0.. = (No reset)
TCP:      .... ..0. = (No SYN)
TCP:      .... ...0 = (No FIN)
TCP: Window                   = 8276
TCP: Checksum                  = DE16 (correct)
TCP: No TCP options
TCP: [174 Bytes of data]
TCP:
NETB: ----- NetBIOS Session protocol -----
NETB:
NETB: Type = 00 (Session data)
NETB: Flags = 00
NETB: Total session packet length = 170
NETB:
SMB: ----- SMB (CIFS) Negotiate Protocol Command header -----
SMB:
SMB: SMB Constant
SMB: Command                = 72 (Negotiate Protocol)
SMB: Reserved                = 0
SMB: Flags = 18
SMB: 0... .... = Client Command
SMB: ..0. .... = No Opportunistic file Locking
SMB: ...1 .... = Pathnames are already in canonicalized format
SMB: .... 1... = Pathnames should be treated as caseless
SMB: .... ..0. = Send.No.Ack can not be used as a response
SMB: .... ...0 = Doesn't support Lock&Read, Write&Unlock      SMB: Flags2 = 0003
SMB: 0... .... ..0. .... = STRING type is ASCIIIZ
SMB: .0.. .... ..0. .... = DOS style Error code
SMB: ..0. .... ..0. .... = No Paging IO
SMB: ...0 .... ..0. .... = No DFS support
SMB: .... 0... ..0. .... = Client not aware of extended security
SMB: .... .... ..0. .... = Don't use message authentication
SMB: .... .... ..1. .... = Client supports extended attributes
SMB: .... .... ..1. .... = Client supports Long file names
SMB: Reserved2(MBZ)         = 000000000000000000000000
SMB: Tree ID                 = 0000
SMB: Process ID              = CAFE
SMB: Unauth User ID         = 0000
SMB: Multiplex ID           = 0000
SMB:
SMB: ----- Negotiate Protocol Header -----
SMB:
SMB: Word count              = 0
SMB: Byte Count             = 135
SMB: Byte parameters        = 025043204E4554574F524B2050524F4752414D20312E300
00258454E495820434F524500024D4943524F534F4654204E4554574F524B5320312E303300024C
414E4D414E312E30000257696E646F777320666F7220576F726B67726F75707320332E316100024
C4D312E3258303032...
SMB: Offered Dialects:
SMB:      0 = PC NETWORK PROGRAM 1.0
SMB:      1 = XENIX CORE

```

SMB: 2 = MICROSOFT NETWORKS 1.03
SMB: 3 = LANMAN1.0
SMB: 4 = Windows for Workgroups 3.1a
SMB: 5 = LM1.2X002
SMB: 6 = LANMAN2.1
SMB: 7 = NT LM 0.12
SMB:

----- Frame 13 -----
\"Flags \",\"Frame \",\"Delta Time \",\"Destination \",\"Source
 \",\"Bytes\", \"Protocol \",\"Summary\"
\" \" \" 13\", \"0.000.286 \" \"AYPC \" \"RAGE \" \"
149 \" \"CIFS/SMB\", \" R Negotiate Protocol (to frame 12) Status= OK Chosen Dialect
Index=7\"

DLC: ----- DLC Header -----

DLC:
DLC: Frame 13 arrived at 12:59:02.3857; frame size is 149 (0095 hex) bytes.
DLC: Destination = Station 005054FEEA31
DLC: Source = Station 001083027B34
DLC: Ethertype = 0800 (IP)
DLC:

IP: ----- IP Header -----

IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. = routine
IP: ...0 = normal delay
IP: 0... = normal throughput
IP:0.. = normal reliability
IP:0. = ECT bit - transport protocol will ignore the CE bit
IP:0 = CE bit - no congestion
IP: Total length = 135 bytes
IP: Identification = 50914
IP: Flags = 4X
IP: .1.. = don't fragment
IP: ..0. = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 128 seconds/hops
IP: Protocol = 6 (TCP)
IP: Header checksum = 1C47 (correct)
IP: Source address = [10.48.66.106], RAGE
IP: Destination address = [192.168.10.5], AYPC
IP: No options
IP:

TCP: ----- TCP header -----

TCP:
TCP: Source port = 139 (NetBIOS-ssn)
TCP: Destination port = 1037
TCP: Sequence number = 590106
TCP: Next expected Seq number= 590201
TCP: Acknowledgment number = 40005
TCP: Data offset = 20 bytes
TCP: Flags = 18
TCP: ..0. = (No urgent pointer)
TCP: ...1 = Acknowledgment
TCP: 1... = Push
TCP:0.. = (No reset)
TCP:0. = (No SYN)
TCP:0 = (No FIN)
TCP: Window = 8034
TCP: Checksum = 1A8D (correct)
TCP: No TCP options
TCP: [95 Bytes of data]
TCP:

NETB: ----- NetBIOS Session protocol -----

NETB:

```

NETB: Type = 00 (Session data)
NETB: Flags = 00
NETB: Total session packet length = 91
NETB:
SMB: ----- SMB (CIFS) Negotiate Protocol Response header -----
SMB:
SMB: Response to frame 12
SMB: SMB Constant
SMB: Command = 72 (Negotiate Protocol)
SMB: Error Class = 0 (Success)
SMB: Reserved(MBZ) = 0
SMB: Status = 0 (OK)
SMB: Flags = 98
SMB: 1... .... = Server Response
SMB: ..0. .... = No Opportunistic file Locking
SMB: ...1 .... = Pathnames are already in canonicalized format
SMB: .... 1... = Pathnames should be treated as caseless
SMB: .... ..0. = Send.No.Ack can not be used as a response
SMB: .... ...0 = Doesn't support Lock&Read, Write&Unlock
SMB: Flags2 = 0003
SMB: 0... .... .. = STRING type is ASCIIZ
SMB: .0.. .... .. = DOS style Error code
SMB: ..0. .... .. = No Paging IO
SMB: ...0 .... .. = No DFS support
SMB: .... 0... .. = Client not aware of extended security
SMB: .... .... ..0.. = Don't use message authentication
SMB: .... .... ....1. = Client supports extended attributes
SMB: .... .... ....1. = Client supports Long file names
SMB: Reserved2(MBZ) = 00000000000000000000000000000000
SMB: Tree ID = 0000
SMB: Process ID = CAFE
SMB: Unauth User ID = 0000
SMB: Multiplex ID = 0000
SMB:
SMB: ----- Negotiate Protocol Header -----
SMB:
SMB: Word count = 17
SMB: Parameter words = 07000332000100041100000000010000000000FD43000070
200231859EC101C4FF08
SMB: Byte Count = 22
SMB: Byte parameters = F8F7053802B9C4435400410043005700450042000000
SMB: Selected Dialect index = 7
SMB: Security mode = X3
SMB: .... 0... = Security Signatures not required
SMB: .... .0.. = Does not support Message Authentication protocol
SMB: .... ..1. = Support Challenge response authentication
SMB: .... ...1 = User level security
SMB: Max pending mpx requests= 50
SMB: Max virtual circuits = 1
SMB: Max Buffer size = 4356
SMB: Max Raw size = 65536
SMB: Session key = 00000000
SMB: Capabilities (LSW) = 43FD
SMB: .1.. .... .. = Supports Large Read&X requests
SMB: ...0 .... .. = Does not support Server DFS
SMB: .... ..1. .... = Supports NT Find
SMB: .... ...1 .... = Supports Lock&Read, Write&Unlock
SMB: .... .... 1... = Level II oplocks supported
SMB: .... .... .1.. = NT 32-bit status codes recognized
SMB: .... .... ..1. .... = Remote APIs via RPC supported
SMB: .... .... ...1 .... = NT 0.12 SMBs supported
SMB: .... .... .... 1... = Large files and 64 bit file offsets supported
SMB: .... .... .... .1.. = Unicode strings recognized
SMB: .... .... .... ..0. = Read/Write Block Multiplexed not supported
SMB: .... .... .... ...1 = Read/Write Block Raw supported
SMB: Capabilities (MSW) = 0000

```

SMB: 0... = Does not support extended security validation
SMB: .0.. = Does not support compressed data transfer
SMB: ..0. = Does not support Bulk Read and Write
SMB: Universal Coordinated Time = 16-Jan-02 11:59:03
SMB: Minutes from UCT = 65476
SMB: Encryption Key Length = 8
SMB: Byte Count = 22
SMB: Encryption Key = F8F7053802B9C443
SMB: Server's Primary Domain = TACWEB
SMB:

----- Frame 14 -----
\"Flags \",\"Frame \",\"Delta Time \",\"Destination \",\"Source
 \",\"Bytes\", \"Protocol \",\"Summary\
\" \" \" 14\", \"0.001.963 \" \"RAGE \" \"AYPC \" \"
230 \" \"CIFFS/SMB\", \" C Tree Connect AndX Path=\\RAGE\\IPC\$, Service=IPC\"
DLC: ----- DLC Header -----

DLC:
DLC: Frame 14 arrived at 12:59:02.3877; frame size is 230 (00E6 hex) bytes.
DLC: Destination = Station 001083027B34
DLC: Source = Station 005054FEEA31
DLC: Ethertype = 0800 (IP)
DLC:

IP: ----- IP Header -----

IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. = routine
IP: ...0 = normal delay
IP: 0... = normal throughput
IP:0.. = normal reliability
IP:0. = ECT bit - transport protocol will ignore the CE bit
IP:0 = CE bit - no congestion
IP: Total length = 216 bytes
IP: Identification = 8449
IP: Flags = 4X
IP: .1.. = don't fragment
IP: ..0. = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 128 seconds/hops
IP: Protocol = 6 (TCP)
IP: Header checksum = C1D7 (correct)
IP: Source address = [192.168.10.5], AYPC
IP: Destination address = [10.48.66.106], RAGE
IP: No options
IP:

TCP: ----- TCP header -----

TCP:
TCP: Source port = 1037
TCP: Destination port = 139 (NetBIOS-ssn)
TCP: Sequence number = 40005
TCP: Next expected Seq number= 40181
TCP: Acknowledgment number = 590201
TCP: Data offset = 20 bytes
TCP: Flags = 18
TCP: ..0. = (No urgent pointer)
TCP: ...1 = Acknowledgment
TCP: 1... = Push
TCP:0.. = (No reset)
TCP:0. = (No SYN)
TCP:0 = (No FIN)
TCP: Window = 8181
TCP: Checksum = B44C (correct)
TCP: No TCP options
TCP: [176 Bytes of data]
TCP:

```

NETB: ----- NetBIOS Session protocol -----
NETB:
NETB: Type = 00 (Session data)
NETB: Flags = 00
NETB: Total session packet length = 172
NETB:
SMB: ----- SMB (CIFS) Setup Account AndX Command header -----
SMB:
SMB: SMB Constant
SMB: Command = 73 (Setup Account AndX)
SMB: Reserved = 0
SMB: Flags = 18
SMB: 0... .... = Client Command
SMB: ..0. .... = No Opportunistic file Locking
SMB: ...1 .... = Pathnames are already in canonicalized format
SMB: .... 1... = Pathnames should be treated as caseless
SMB: .... ..0. = Send.No.Ack can not be used as a response
SMB: .... ...0 = Doesn't support Lock&Read, Write&Unlock
SMB: Flags2 = 8003
SMB: 1... .... ..0. .... = STRING type is UNICODE
SMB: ..0. .... ..0. .... = DOS style Error code
SMB: ...0 .... ..0. .... = No Paging IO
SMB: .... 0... ..0. .... = No DFS support
SMB: .... ..0. .... ..0. .... = Client not aware of extended security
SMB: .... ..0. .... ..0. .... = Don't use message authentication
SMB: .... ..0. .... ..1. .... = Client supports extended attributes
SMB: .... ..0. .... ..1. .... = Client supports Long file names
SMB: Reserved2(MBZ) = 0000A9B9522B700714DC0000
SMB: Tree ID = 0000
SMB: Process ID = CAFE
SMB: Unauth User ID = 0000
SMB: Multiplex ID = 0000
SMB:
SMB: ----- Setup Account AndX Header -----
SMB:
SMB: Word count = 13
SMB: Parameter words = 75008400041132000100000000000100000000000000D
4000000
SMB: Byte Count = 71
SMB: Byte parameters = 0000000000570069006E0064006F007700730020004E0
054002000310033003800310000000000570069006E0064006F007700730020004E0054002000
34002E00300000000000
SMB: AndX command = 75 (Tree Connect AndX)
SMB: AndX reserved(MBZ) = 00
SMB: AndX offset = 0084
SMB: Max buffer size = 4356
SMB: Max mux pending requests= 50
SMB: Number of VC's (0=Only) = 1
SMB: Session Key = 00000000
SMB: Case insensitive Password length = 1
SMB: Case sensitive Password length = 0
SMB: Reserved(MBZ) = 00000000
SMB: Capabilities (LSW) = 00D4
SMB: ..0. .... ..0. .... = Does not support Large Read&X requests
SMB: ...0 .... ..0. .... = Does not support Server DFS
SMB: .... ..0. .... ..0. .... = Does not support NT Find
SMB: .... ...0 .... ..0. .... = Does not support Lock&Read, Write&Unlock
SMB: .... .... 1... .... = Level II oplocks supported
SMB: .... .... .1. .... = NT 32-bit status codes recognized
SMB: .... .... ..0. .... = Remote APIs via RPC not supported
SMB: .... .... ...1 .... = NT 0.12 SMBs supported
SMB: .... .... .... 0... = Large files not supported
SMB: .... .... .... .1.. = Unicode strings recognized
SMB: .... .... .... ..0. = Read/Write Block Multiplexed not supported
SMB: .... .... .... ...0 = Read/Write Block Raw not supported
SMB: Capabilities (MSW) = 0000

```

```

SMB: 0... .. = Does not support extended security validation
SMB: .0.. .... = Does not support compressed data transfer
SMB: ..0. .... = Does not support Bulk Read and Write
SMB: Byte Count = 71
SMB: Case insensitive password = 00
SMB: Account name =
SMB: Client's Primary Domain =
SMB: Client's native OS = Windows NT 1381
SMB: CIFS 1.1 spec violation = 0
SMB: Client's LANMAN = Windows NT 4.0
SMB:
SMB: ----- Tree Connect AndX Header -----
SMB:
SMB: Word count = 4
SMB: Parameter words = FF00000000000100
SMB: Byte Count = 29
SMB: Byte parameters = 005C005C0052004100470045005C0049005000430024000
00049504300
SMB: AndX command = FF (End of chain)
SMB: AndX reserved(MBZ) = 00
SMB: AndX offset = 0000
SMB: Additional information = 0000
SMB: .... ..0 = Don't disconnect Tid
SMB: Password length = 1
SMB: Byte Count = 29
SMB: Password = 00
SMB: Path = \\RAGE\IPC$
SMB: Service = IPC
SMB:

```

```

----- Frame 15 -----
\"Flags \",\"Frame \",\"Delta Time \",\"Destination \",\"Source
  \",\"Bytes\", \"Protocol \",\"Summary\"
"  ", " 15", "0.000.406 ", "AYPC ", "RAGE ", "
198 ", "CIFS/SMB", " R Tree Connect AndX Service=IPC ,Native File System="

```

```

DLC: ----- DLC Header -----
DLC:
DLC: Frame 15 arrived at 12:59:02.3881; frame size is 198 (00C6 hex) bytes.
DLC: Destination = Station 005054FEEA31
DLC: Source = Station 001083027B34
DLC: Ethertype = 0800 (IP)
DLC:

```

```

IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: .... ...0 = CE bit - no congestion
IP: Total length = 184 bytes
IP: Identification = 51170
IP: Flags = 4X
IP: .1.. .... = don't fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 128 seconds/hops
IP: Protocol = 6 (TCP)
IP: Header checksum = 1B16 (correct)
IP: Source address = [10.48.66.106], RAGE
IP: Destination address = [192.168.10.5], AYPC
IP: No options
IP:
TCP: ----- TCP header -----

```

```

TCP:
TCP: Source port          = 139 (NetBIOS-ssn)
TCP: Destination port    = 1037
TCP: Sequence number     = 590201
TCP: Next expected Seq number= 590345
TCP: Acknowledgment number = 40181
TCP: Data offset         = 20 bytes
TCP: Flags                = 18
TCP:          ..0. .... = (No urgent pointer)
TCP:          ...1 .... = Acknowledgment
TCP:          .... 1... = Push
TCP:          .... .0.. = (No reset)
TCP:          .... ..0. = (No SYN)
TCP:          .... ...0 = (No FIN)
TCP: Window              = 7858
TCP: Checksum            = F7E6 (correct)
TCP: No TCP options
TCP: [144 Bytes of data]
TCP:
NETB: ----- NetBIOS Session protocol -----
NETB:
NETB: Type = 00 (Session data)
NETB: Flags = 00
NETB: Total session packet length = 140
NETB:
SMB: ----- SMB (CIFS) Setup Account AndX Response header -----
SMB:
SMB: Response to frame 14
SMB: SMB Constant
SMB: Command              = 73 (Setup Account AndX)
SMB: Error Class          = 0 (Success)
SMB: Reserved(MBZ)       = 0
SMB: Status               = 0 (OK)
SMB: Flags = 98
SMB: 1... .... = Server Response
SMB: ..0. .... = No Opportunistic file Locking
SMB: ...1 .... = Pathnames are already in canonicalized format
SMB: .... 1... = Pathnames should be treated as caseless
SMB: .... ..0. = Send.No.Ack can not be used as a response
SMB: .... ...0 = Doesn't support Lock&Read, Write&Unlock
SMB: Flags2 = 8003
SMB: 1... .... .... = STRING type is UNICODE
SMB: .0.. .... .... = DOS style Error code
SMB: ..0. .... .... = No Paging IO
SMB: ...0 .... .... = No DFS support
SMB: .... 0... .... = Client not aware of extended security
SMB: .... .... .... .0.. = Don't use message authentication
SMB: .... .... .... ..1. = Client supports extended attributes
SMB: .... .... .... ...1 = Client supports Long file names
SMB: Reserved2(MBZ)      = 0000A9B9522B700714DC0000
SMB: Tree ID             = 0801
SMB: Process ID          = CAFE
SMB: Unauth User ID     = 0801
SMB: Multiplex ID        = 0000
SMB:
SMB: ----- Setup Account AndX Header -----
SMB:
SMB: Word count          = 3
SMB: Parameter words     = 75007C000000
SMB: Byte Count          = 83
SMB: Byte parameters    = 00570069006E0064006F007700730020004E005400200
034002E00300000004E00540020004C0041004E0020004D0061006E0061006700650072002000
34002E003000000005400410043005700450042000000
SMB: AndX command        = 75 (Tree Connect AndX)
SMB: AndX reserved(MBZ) = 00
SMB: AndX offset         = 007C

```

```
SMB: Request Mode = 0000
SMB: .... .... .... ..0 = Not logged in as 'Guest'
SMB: Byte Count          = 83
SMB: Server's Native OS   = Windows NT 4.0
SMB: Server's Native LAN Man = NT LAN Manager 4.0
SMB: Server's Primary Domain = TACWEB
SMB:
SMB: ----- Tree Connect AndX Header -----
SMB:
SMB: Word count          = 3
SMB: Parameter words    = FF008C000100
SMB: Byte Count         = 7
SMB: Byte parameters    = 49504300000000
SMB: AndX command       = FF (End of chain)
SMB: AndX reserved(MBZ) = 00
SMB: AndX offset        = 008C
SMB: Optional support   = 0001
SMB: .... .... .... ..0 = Share not in DFS
SMB: .... .... .... ..1 = Support Search bits
SMB: Byte Count         = 7
SMB: Service            = IPC
SMB: Native File system =
SMB:
```

Related Information

- [Documentation for PIX Firewall](#)
 - [PIX Command Reference](#)
 - [PIX Support Page](#)
 - [Requests for Comments \(RFCs\)](#)
 - [Technical Support – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Sep 26, 2008

Document ID: 18801
