



Configuring WAN Links

This chapter covers these topics:

- [Introduction to WAN links](#)
- [Configuring PPP connections](#)
- [Configuring single-channel PPP connections](#)
- [Configuring MP and BACP connections](#)
- [Configuring a nailed MP+ connection](#)
- [Configuring a MAX stack](#)
- [Configuring a Combinet connection](#)
- [Configuring EU connections](#)
- [Configuring an ARA connection](#)
- [Configuring dial-in PPP for AppleTalk](#)
- [Configuring terminal server connections](#)
- [Configuring terminal mode](#)
- [Configuring immediate mode](#)
- [Configuring menu mode](#)
- [Configuring PPP mode](#)
- [Configuring SLIP mode](#)
- [Configuring dialout options](#)

Introduction to WAN links

This chapter describes how to configure various types of links across the WAN. It focuses on the encapsulation issues for these types of connections:

- PPP (Point-to-Point Protocol)

PPP and its multilink variants (MP and MP+) enable dial-in connections from modems or ISDN devices, using one or more channels. The remote devices must have PPP software.

- Combinet

Combinet bridges two network segments at the link level using one or two channels. The remote device is another Combinet bridge.

- EU-UI and EU-RAW

Two types of EU encapsulation: the MAX uses EU-UI when the equipment on the other side of the connection requires the DCE and DTE address fields in the EU header, and when these address fields are absent, the MAX uses EU-RAW. EU connections can be dial-in or dial-out.

EU encapsulation does not support an authentication protocol. CLID authentication is used to match incoming calls to the proper Connection profile when, for example, special filters are applied to certain callers, or some callers route IP and others bridge.

- ARA (AppleTalk Remote Access)

ARA enables a Macintosh user to access AppleTalk devices or IP hosts via modem. The remote Mac must have ARA client software and (if applicable) TCP/IP software.

- Terminal server connections

The MAX terminal server processes asynchronous calls from modems, ISDN modems (V.120 terminal adapters), or raw TCP. Those calls may be logged into the terminal server interface or, if they contain PPP, passed to the router.

Note: Frame Relay, X.25, IP or IPX routing, and bridging all require both connection-specific and more general system configuration. Those topics appear in their own chapters later in this guide.

This chapter does not describe RADIUS user profiles, which serve the same function as resident Connection profiles. If you are using a RADIUS authentication server, see the *MAX RADIUS Configuration Guide*. For details about WAN connection security, see the *MAX Security Supplement*.

The Answer profile

The Answer profile determines whether an incoming call is answered or dropped. If the call does not comply with the Answer profile, the MAX drops the call before answering it.

Most administrators set up the Answer profile to reject calls for which no configured profile is found. When a call has a configured profile, the related encapsulation and session options in the Answer profile are not used-the MAX relies on the connection-specific settings instead. However, if the configured profile is a Name-password profile, the MAX may use the settings in the Answer profile to build the session. The Answer profile contains these parameters:

```
Ethernet
  Answer
    Use Answer as Default=No
    Force 56=No
    Profile Req'd=Yes
    Id Auth=None
    Assign Adrs=No

  Encaps...
    MPP=Yes
    MP=Yes
    PPP=Yes
    COMB=Yes
    FR=Yes
    X25/PAD=Yes
```

```
EU-RAW=Yes
EU-UI=Yes
V.120=Yes
X.75=Yes
TCP-CLEAR=Yes
ARA=Yes
```

```
IP options...
Metric=7
```

```
PPP options...
Route IP=Yes
Route IPX=Yes
Bridge=Yes
Route AppleTalk=Yes
AppleTalk options...
Recv Auth=Either
MRU=1524
LQM=No
LQM Min=600
LQM Max=600
Link Comp=Stac
VJ Comp=Yes
CBCP Enable=No
BACP=No
Dyn Alg=Quadratic
Sec History=15
Add Pers=5
Sub Pers=10
Min Ch Count=1
Max Ch Count=1
Target Util=70
Idle Pct=0
Disc on Auth Timeout=Yes
```

```
COMB options...
Password Reqd=Yes
Interval=10
Compression=Yes
```

```
V.120 options...
Frame Length=260
```

```
X.75 options...
K Window Size=7
N2 Retran Count=10
T1 Retran Timer=1000
Frame Length=2048
```

```
Session options...
RIP=Off
Data Filter=5
Call Filter=3
Filter Persistence=No
Idle=120
TS Idle Mode=N/A
TS Idle=N/A
IPX SAP Filter=1
Max Call Duration=0
Preempt=N/A
Framed Only
```

```
DHCP options...
  Reply Enabled=No
  Pool Number=N/A
  Max Leases=N/A
```

Understanding the Answer profile parameters

This section provides some background information on the Answer profile. For more information about each parameter, see the *MAX Reference Guide*.

Use Answer profile settings as the defaults for externally authenticated calls

Use Answer as Default indicates whether the Answer Profile should override the factory defaults when the MAX validates an incoming call using RADIUS or TACACS.

Forcing 56k data service

Force 56 tells the MAX to use only the 56-kbps portion of a channel, even when all 64 kbps appear to be available. It is useful for answering calls from European or Pacific Rim countries from within North America, when the complete path cannot distinguish between the Switched-56 and Switched-64 data services. It is not needed for calls within North America.

Note: Since the default bandwidth for data calls across R2 lines is 64 kbps, set Force 56 to Yes in any Connection profile which should use 56 kbps over R2 lines.

Requiring a configured profile to answer a call

If you do not require a configured profile for all callers, the MAX builds a temporary profile for unknown callers. Many sites consider this a security breach. Note that setting Profile Req'd to Yes disables Guest access for ARA connections.

Called number and caller-ID authentication

The called number (typically the number dialed by the far end) and CLID (the far-end device's number) may be presented by the phone company as part of the call information and used in a first-level authentication process that occurs before a call is answered. See [Understanding Connection profile parameters](#) for details. See the *MAX Security Supplement* for background information about authentication.

Enabling types of encapsulation

The Encaps subprofile contains settings for each type of link encapsulation that may be supported. If you set an encapsulation type to No in this menu, the MAX does not accept calls of that type.

IP options

In the Answer Profile, the Metric parameter determines the virtual hop count of the IP link when the MAX validates an incoming call using RADIUS or TACACS and Use Answer as Default is enabled.

Setting encapsulation-specific options

See the sections on configuring connections later in this chapter for details on the PPP, Cominet,

and other encapsulation options. The Answer Profile uses these options only when you have not set corresponding options in the caller's configured profile.

X.75 options

The X.75 options enable dial-in access to the terminal server using the X.75 protocol. Full technical specifications for X.75 can be found in the CCITT Blue Book Recommendation X series 1988.

Session options

In the Answer profile, session options set default filters and timers to build connections that use RADIUS (if Use Answer as Defaults is enabled) or Names/Passwords profiles. The Framed Only option can limit terminal server access per user.

DHCP options

In the Answer profile, DHCP options enable the MAX to act as a DHCP server for a local Pipeline unit for connections that use RADIUS (if Use Answer as Defaults is enabled) or Names/Passwords profiles.

Example Answer profile configuration

To set up a basic Answer profile:

1. Open the Answer profile and set Profile Reqd to Yes.
2. Set up CLID (Calling Line ID) or Called Number authentication, if required.
3. Enable dynamic assignment of IP addresses to callers, if appropriate.

```
Ethernet
  Answer
    Profile Reqd=Yes
    Id Auth=None
    Assign Adrs=No
```

4. Make sure you enable the encapsulation types you intend to support. For example:

```
Encaps...
  MPP=Yes
  MP=Yes
  PPP=Yes
  COMB=Yes
  FR=Yes
  X25/PAD=Yes
  EU-RAW=Yes
  EU-UI=Yes
  V.120=Yes
  X.75=Yes
  TCP-CLEAR=Yes
  ARA=Yes
```

5. Enable routing and bridging and specify authentication requirements, as appropriate. For example:

```
PPP options...
```

```

Route IP=Yes
Route IPX=Yes
Route AppleTalk=Yes
Bridge=Yes
Recv Auth=Either

```

6. Set AppleTalk PPP dial-in options in the AppleTalk options menu, if required.
7. COMB options...
Password Reqd=Yes
8. Close the Answer profile.

Connection profiles

Connection profiles define individual connections. For a given encapsulation type, the Connection profile contains many of the same options as the Answer profile.

Note: Settings in a Connection profile always override similar settings in the Answer profile.

Connection profiles contain these parameters:

```

Ethernet
  Connections
    Station=device-name
    Active=Yes
    PRI # Type=National
    Dial #=555-1212
    Calling #=555-2323
    Called #=555-1212
    Route IP=Yes
    Route IPX=No
    Route AppleTalk=Yes
    Bridge=No
    Dial brdcast=N/A

    Encaps=encapsulation-protocol
    Encaps options...
      depends on selected encapsulation-protocol

    IP options...
      LAN Adrs=0.0.0.0/0
      WAN Alias=0.0.0.0/0
      IF Adrs=0.0.0.0/0
      Metric=7
      Preference=100
      Private=No
      RIP=Off
      Pool=0
      Multicast Client=No
      Multicast Rate Limit=5
      Client Pri DNS=0.0.0.0
      Client Sec DNS=0.0.0.0
      Client Assign DNS=Yes
      Client Gateway=0.0.0.0

    IPX options...
      Peer=Router

```

```
IPX RIP=None
IPX SAP=Send
Dial Query=No
IPX Net#=cfff0003
IPX Alias#=00000000
Handle IPX=None
Netware t/o=30
```

AppleTalk options...

```
Peer=Dialin
Zone Name=ENGINEERING
Net Start=2001
Net End=2010
Default Zone=
Zone Name #1=
Zone Name #2=
Zone Name #3=
Zone Name #4=
```

Session options...

```
Data Filter=5
Call Filter=3
Filter Persistence=No
Idle=120
TS Idle Mode=N/A
TS Idle=N/A
Max Call Duration=0
Preempt=N/A
IPX SAP Filter=0
BackUp=
IP Direct=0.0.0.0
FR Direct=No
FR Prof=N/A
FR DLCI=N/A
Framed Only
```

OSPF options

```
RunOSPF=Yes
Area=0.0.0.0
AreaType=Normal
StubAreaDefaultCost=N/A
HelloInterval=40
DeadInterval=120
Priority=5
AuthType=Simple
AuthKey=ascend0
Cost=10
ASE-type=N/A
ASE-tag=N/A
TransitDelay=5
RetransmitInterval=20
```

Telco options...

```
AnsOrig=Both
Callback=Yes
Exp Callback=No
Call Type=Switched
Group=N/A
FT1 Caller=N/A
Data Svc=56KR
Force 56=N/A
Bill #=555-1212
Call-by-Call=N/A
```

```
Transit #=222
Dialout OK=No
```

```
Accounting...
Acct Type=None
Acct Host=N/A
Acct Port=N/A
Acct Timeout=N/A
Acct Key=N/A
Acct-ID Base=N/A
```

```
DHCP options...
Reply Enabled=No
Pool Number=N/A
Max Leases=N/A
```

Note: After you select an encapsulation method in the Encaps option, the Encaps Options subprofile contains settings related to the selected type.

For information on IP, IPX, bridging, OSPF, and AppleTalk configuration, see the appropriate chapter in this guide. For more information about each parameter, see the *MAX Reference Guide*.

Understanding Connection profile parameters

This section provides some background information on Connection profile parameters.

The remote device's station name

The station name is the name of the remote device. Make sure the name matches the remote device name exactly, including case changes.

ISDN call information

PRI # Type enables an AT&T switch to use your dial number when you make a call using T1 channels and ISDN signaling. You can specify National (inside the U.S.), Intl (outside the U.S.) or Local (within your Centrex group).

The dial number

Dial # is the phone number you use to dial out this connection. It can contain up to 24 characters, which may include a dialing prefix that directs the connection to use a trunk group or dial plan; for example: 6-1-212-555-1212. For more details, see [Chapter 2, Configuring the MAX for WAN Access](#).

The called number

Called # (typically the number dialed by the far end) appears in an ISDN message as part of the call when DNIS (Dial Number Information Service) is in use. In some cases, the phone company may present a modified called number for DNIS. Authentication uses this number to direct inbound calls to a particular device from a central rotary switch or PBX. See the *MAX Security Supplement* for details.

The calling number

Many carriers include the calling number (the far-end device's number) in each call. Calling # is the caller ID number that appears on some phones. The MAX also uses Calling # for CLID (Calling Line ID) authentication.

CLID authentication prevents the MAX from answering a connection unless it originates at the specified phone number. The number you specify may also be used for callback security if you configure callback in the per-connection telco options.

Encaps and encaps options

An encapsulation protocol must be specified for each connection, and its accompanying options configured in the Encaps Options subprofile. These are described in separate sections in this chapter.

Routing configurations

Each connection may be configured for IP routing, IPX routing, OSPF routing (which requires IP routing), or AppleTalk routing. Each of these routing setups has a separate subprofile within a Connection profile. See the appropriate chapters later in this guide.

Bridging

Link-level bridging forwards packets to and from remote networks based on the hardware-level address, not a logical network address. Bridge and Dial Brdcast are related parameters. See the chapter on packet bridging later in this guide.

Connection profile Session options

These are the Session Options parameters in a Connection profile:

```

Ethernet
  Connections
    Session options...
      Data Filter=5
      Call Filter=3
      Filter Persistence=No
      Idle=120
      TS Idle Mode=N/A
      TS Idle=N/A
      Max Call Duration=0
      Preempt=N/A
      IPX SAP Filter=0
      BackUp=
      IP Direct=0.0.0.0
      FR Direct=No
      FR Prof=N/A
      FR DLCI=N/A
      Block calls after=0
      Blocked duration
      Framed Only

```

This section provides a brief overview. For details, see the later chapters in this guide and the *MAX Reference Guide*.

Applying data or call filters to a session

Ascend filters define packet conditions. Data filters drop specific packets, and are often used for security purposes. Call filters monitor inactive sessions and bring them down to avoid unnecessary

connection costs. When a filter is in use, the MAX examines every packet in the packet stream and takes action if the defined filter conditions are present. The action the MAX takes depends both on the conditions specified within the filter and how the filter is applied. See [Chapter 7, Defining Static Filters](#).

Timing inactive sessions

The Idle timer specifies how long the connection may remain idle before the MAX drops it. TS Idle Mode parameter specifies whether the MAX uses the terminal server idle timer and, if so, whether it monitors traffic in one or both directions to determine when the session is idle. TS Idle specifies how long the terminal server session can remain idle before the MAX logs out the user and terminates the connection.

Setting a maximum call duration

This parameter sets the maximum duration of an incoming call (1-1440 minutes). The default zero turns off this function. The MAX checks the connection once a minute, so the actual time of the call may be slightly longer than the number of minutes you set.

Allowing bandwidth to be preempted

Preempt specifies the number of idle seconds the MAX waits before it can use one of the channels of an idle link for a new call.

Specifying a backup connection when a nailed connection fails

Backup specifies the name of a Connection profile to use when a nailed connection goes down. For example, if a nailed connection to corporate net #1 is out of service, a backup switched connection to corporate net #2 may be used. You cannot use this parameter to provide alternative lines to a single destination.

IP direct connections

An IP direct connection channels all inbound packets to a specified local host. See [Chapter 10, Configuring IP Routing](#).

Frame Relay redirect connections

A Frame Relay redirect connection channels all inbound packets out to a Frame Relay switch. See [Chapter 4, Configuring Frame Relay](#).

Call blocking

You can specify the number of unsuccessful attempts to place a call that an Ascend unit can make before blocking further attempts to make that connection. After the specified number of attempts have been made and failed, the blocking timer starts. See the *MAX Reference Guide* for more information.

Connection profile telco options

These are the Telco Options parameters in a Connection profile:

```
Ethernet
Connections
```

```
Telco options...
AnsOrig=Both
Callback=Yes
Exp Callback=No
Call Type=Switched
Group=N/A
FT1 Caller=N/A
Data Svc=56KR
Force 56=N/A
Bill #=555-1212
Call-by-Call=N/A
Transit #=222
Dialout OK=No
```

For more complete information on each parameter, see the *MAX Reference Guide*. This section provides a brief overview.

Enabling both dial-in and dial-out on this connection

The AnsOrig parameter specifies whether the MAX can answer incoming calls, dial out, or both. The FT1 Caller parameter specifies whether this MAX can initiate calls on fractional T1 to add switched channels to a nailed MPP connection (only one side of the connection should have this parameter set to Yes).

Setting callback security

When you set Callback to Yes, the MAX hangs up on the caller and dials back immediately using the dial number in this profile. When you set Expect Callback to Yes, the MAX expects the far end to hang up and dial back (recommended when CLID is required on the far end unit and PING or TELNET are in use).

Nailed, switched, and other call types

The Call Type=switched is the default. The other options are nailed, nailed-MPP, and permanent switched connections.

A nailed connection is a permanent link that is always up as long as the physical connection persists. For a nailed connection, you must specify the group number of the nailed channels. You can even combine groups of nailed channels to create a single high-speed nailed connection. For example:

```
Call Type=Nailed
Group=3, 4
```

A nailed/MPP connection combines nailed and switched channels. When you choose this Call Type, you need to specify which side of the link can add switched channels by using the FT1 Caller parameter. See [Example MP connection without BACP](#) for details about the Nailed/Mpp call type.

A permanent switched connection is an outbound switched call that attempts to remain up at all times. If the unit or central switch resets or if the link terminates, the permanent switched connection attempts to restore the link at 10-second intervals, which is similar to the way a nailed connection is maintained. A permanent switch connection conserves connection attempts but causes a long connection time, which may be cost effective for some customers. See the *MAX Reference Guide* for details.

Data service

Data Svc specifies the type of data service the link uses, such as 56K or modem.

Billing numbers

Bill # can specify a billing number for charges incurred on the line. If appropriate, your carrier can provide a billing number that you can use to sort your bill. For example, each department may require its own billing number. The billing number can contain up to 24 characters.

Dialout OK

This specifies whether the Connection profile may be used for dialing out on one of the MAX unit's digital modems. Only if you set Dialout OK to Yes will the local user be allowed access to the immediate modem feature.

Connection profile accounting options

These are the accounting parameters in a Connection profile:

```
Ethernet
  Connections
    Accounting...
      Acct Type=None
      Acct Host=N/A
      Acct Port=N/A
      Acct Timeout=N/A
      Acct Key=N/A
      Acct-ID Base=N/A
```

For more information about each parameter, see the *MAX Reference Guide*. This section provides a brief overview.

Accounting type

You can specify whether this connection uses the default accounting setup (specified in the Ethernet profile), no accounting at all, or the user-specific setup specified here. The MAX supports both RADIUS and TACACS+ accounting.

Accounting host and port

These specify the IP address of a connection-specific accounting server to use for information related to this link, and the UDP port number to use in accounting requests.

Accounting timeout and key

The accounting key is a shared secret (a password shared with the accounting server). The Acct Timeout parameter specifies how long to wait for a response to a RADIUS accounting request. TACACS+ has its own timeout method.

Accounting ID base

This specifies the numeric base (base 10 or base 16) for the session ID.

Connection profile DHCP options

The DHCP parameters in a Connection profile are:

```
Ethernet
  Connections
    DHCP options...
      Reply Enabled=No
      Pool Number=N/A
      Max Leases=N/A
```

For more information about each parameter, see the *MAX Reference Guide*. This section provides a brief overview.

Reply Enabled

This specifies whether the MAX processes DHCP packets and acts as a DHCP server on this connection. If you set this parameter to Yes and the connection is bridged, the MAX responds to all DHCP requests. If you set Reply Enabled to Yes and the connection uses routing, it responds only to Network Address Translation (NAT) DHCP packets from a Pipeline unit. If you set Reply Enabled to No, the MAX does not respond to DHCP requests.

Pool Number

This specifies the IP address pool to use to assign addresses to NAT clients. It is not applicable if you set Reply Enabled to No.

Max Leases

This parameter restricts the number of dynamic IP addresses to be given out through this connection, thus limiting the number of clients on the remote LAN who can access the Internet. It is not applicable if you set Reply Enabled to No.

Name-Password profiles

Name-password profiles provide simple name/password authentication for incoming calls. They are used only if authentication is required in the Answer profile (Recv Auth). The MAX prompts dial-in users for a name and password, matches the input to a Name-password profile, accepts the call, and uses the settings in the Answer profile or a specified Connection profile to build the connection.

Note: If Recv Auth is set to None in the Answer profile, Name-password profiles are not used.

Name-password profiles contain these parameters:

```
Ethernet
  Names / Passwords
    Name=Brian
    Active=Yes
    Recv PW=brianpw
    Template Connection #=0
```

Understanding the Name-password profile parameters

This section provides some background information on Name-password profiles.

Name

The name must exactly match the name specified by a dial-in user, including case changes. We recommend that you do not specify a name that is already in use in a Connection profile. The name can be up to 31 characters.

Active

To enable a Name-password profile for use, set Active to Yes. If you are using a *template* Connection profile to build the session, that profile must also be active.

Password

The password must exactly match the password specified by a dial-in user, including case changes. The password can be up to 20 characters.

Template connection

To use a *template* Connection profile rather than the Answer profile settings to build the session for this Name-password profile, specify the unique portion of the profile's number here. The default zero instructs the MAX to use the Answer profile settings. Any other number denotes a Connection profile. The specified Connection profile must be active.

Template connections may be used to enable or disable group logins. For example, you can specify a Connection profile for the Sales group to use when dialing in, then configure a Name-password profile for each individual salesperson. You can prevent a single salesperson from dialing in by setting Active to No in the Name-password profile, or you can prevent the entire group from logging in by setting Active to No in the Connection profile.

Example Name-Password profile configuration

To configure a Name-Password profile that uses the Answer profile settings:

1. Open a Name-Password profile.
2. Specify the user's name and password, and then activate the profile.

```
Ethernet
  Names / Passwords
    Name=Brian
    Active=Yes
    Recv PW=brianpw
    Template Connection #=0
```

3. Leave the Template Connection # set to 0 to use Answer profile settings.
4. Close the profile.

Note: To set up a dial-in AppleTalk PPP connection using a Name-Password profile, you will also need to set the AppleTalk options parameter Peer=Dialin. See the AppleTalk routing chapter in this guide for more information.

Configuring PPP connections

This section describes how to configure PPP-encapsulated connections. A PPP connection may be one of the following types:

- PPP-a single-channel connection to any remote device running PPP software.
- MP (Multilink PPP)-a multilink connection to an MP-compliant device from any vendor.
- MP with BACP (MP with Bandwidth Allocation Control Protocol)-an MP call that uses BACP to increase or decrease bandwidth on demand.
- MP+ (Multilink PPP with Ascend extensions)-a multilink connection to another Ascend unit, which uses Ascend dynamic bandwidth allocation to increase or decrease bandwidth on demand.

A multilink connection begins by authenticating a base channel. If the connection allows additional bandwidth, the local or remote unit dials another link. For example, if a dial-in Pipeline unit has a single-channel session at 56 Kbps or 64 Kbps and multilink PPP is configured, a second call can combine the first B channel with the second for a transmission rate of 112 Kbps or 128 Kbps.

MAX units can be "stacked" to distribute the bandwidth required for connections across multiple units. See [Spanning multilink or MP+ calls across multiple MAX units](#).

Note: If a connection configured for multilink PPP fails to establish multiple channels, it falls back to a single-channel PPP session. In each case, the PPP parameters are used as part of the connection negotiation. MP, BACP, and MP+ settings are used *in addition to* the single-channel PPP settings.

Configuring single-channel PPP connections

This section describes how to the parameter used for PPP negotiation to establish a single-channel PPP call and to establish the base channel of multilink PPP calls. These are the related parameters:

```

Ethernet
  Answer
    Encaps...
      PPP=Yes

  PPP options...
    Route IP=Yes
    Route IPX=Yes
    Route AppleTalk=Yes
    Bridge=Yes
    Recv Auth=Either
    MRU=1524
    LQM=No
    LQM Min=600
    LQM Max=600
    Link Comp=Stac
    VJ Comp=Yes
    CBCP Enable=No

Ethernet
  Connections

```

```
Encaps=PPP
Encaps options...
  Send Auth=None
  Send PW=N/A
  Recv PW=
  MRU=1524
  LQM=No
  LQM Min=600
  LQM Max=600
  Link Comp=Stac
  VJ Comp=Yes
  CBCP Mode=N/A
  CBCP Trunk Group=N/A
```

For more information about each parameter, see the *MAX Reference Guide*.

Understanding the PPP parameters

This section provides some background information about the PPP parameters.

Enabling routing and bridging in the Answer profile

You must enable routing or bridging in the Answer profile for the MAX to pass the data stream from an answered call to its internal bridge/router software. See the appropriate chapter on routing or bridging later in this guide for more information.

Authentication method used for passwords received from the far end

The Recv Auth parameter specifies which protocol to use for authenticating the password sent by the far end during PPP negotiation. You can specify None, PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), or Either, which includes PAP, CHAP and MS-CHAP (Microsoft Challenge Handshake Authentication Protocol format supported by Windows NT systems). The far end must also support the specified protocol.

Authentication method used for passwords sent to the far end

The Send Auth parameter specifies which protocol to use for the password sent to the far end during PPP negotiation.

Passwords to send to and receive from the far end

The Send PW is the password sent to the remote device. It must match the password expected from the MAX. The Recv PW is the password sent to the MAX from the remote device. It is used to match up the caller to a profile when IP routing is not in use.

Maximum receive units (MRU)

MRU specifies the maximum number of bytes the MAX can receive in a single packet on a PPP link. Usually the default 1524 is the right setting, unless the far end device requires a lower number.

Link quality monitoring (LQM)

The LQM parameters specify whether the MAX monitors the quality of the link. If LQM is set to Yes, you can specify the minimum and maximum duration between reports, measured in tenths of a second.

LQM counts the number of packets sent across the link and periodically asks the remote end how many packets it has received. Discrepancies are evidence of packet loss and indicate link quality problems.

Link and header compression

For data compression to take effect, both sides of a connection must support it. The MAX supports Stac and MS-Stac compression for PPP-encapsulated calls.

Stac compression refers to the Stacker LZS compression algorithm, developed by STAC Electronics, Inc., which modifies the standard LZS compression algorithm to optimize for speed (as opposed to optimizing for compression). Stac compression is one of the parameters negotiated when setting up a PPP connection.

MS-Stac refers to Microsoft LZS Coherency compression for Windows 95. This is a proprietary compression scheme for Windows 95 only (not for Windows NT).

Note: If the caller requests MS-Stac and the matching profile does not specify MS-Stac compression, the connection seems to come up correctly but no data is routed. If the profile is configured with MS-Stac and the caller does not acknowledge that compression scheme, the MAX attempts to use standard Stac compression, and if that does not work, it uses no compression.

VJ Comp applies only to packets in TCP applications, such as Telnet. When you turn it on, the MAX applies TCP/IP header compression for both ends of the link.

CBCP Enable

This parameter in the Answer profile specifies how the MAX responds to caller requests to support CBCP. If CBCP Enable is set to Yes, the MAX positively acknowledges, during LCP negotiations, support for CBCP. If this parameter is set to No, the MAX rejects any request to support CBCP.

CBCP Mode

This parameter specifies what method of callback the MAX offers the incoming caller.

CBCP Trunk Group

This parameter assigns the callback to a MAX trunk group. This parameter is used only when the caller is specifying the phone number the MAX uses for the callback. The value in CBCP Trunk Group is prepended to the caller-supplied number when the MAX calls back.

Note: For more information about CBCP, see the *MAX 6000 Series Reference Guide* and the *MAX 6000 Series Security Supplement*.

Example PPP connection

[Figure 3-1](#) shows the MAX with a PPP connection with a remote user who is running Windows 95 with the TCP/IP stack and PPP dialup software. The dial-in user has a modem, so the call is asynchronous and uses only one channel.

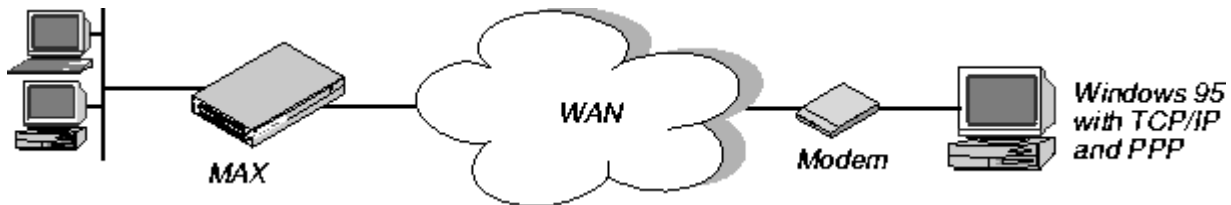


Figure 3-1. A PPP connection

To configure this PPP connection:

1. Make sure the Answer profile enables PPP encapsulation and sets the appropriate routing, bridging, and authentication values. For example:

```

Ethernet
  Answer
    Encaps...
      PPP=Yes

    PPP options...
      Route IP=Yes
      Route IPX=Yes
      Bridge=Yes
      Recv Auth=Either
  
```

2. Close the Answer profile.
3. Open a Connection profile.
4. Specify the name of the remote device and activate the profile. For example:

```

Ethernet
  Connections
    Station=tommy
    Active=Yes
  
```

Note: Make sure that you specify the Station name exactly, including case changes.

5. Select PPP encapsulation and set the appropriate PPP options. For example:

```

Encaps=PPP
Encaps options...
  Send Auth=CHAP
  Send PW=remotepw/A
  Recv PW=localpw
  
```

The Send Auth parameter should be set to CHAP or PAP. Both sides of the connection must support the selected authentication protocol and the selected compression methods.

6. Close the Connection profile.

Enabling PPP outdial for v.110 modems

The MAX can make outgoing calls to a client on the other side of a v.110 terminal adapter using the PPP protocol. This feature also supports the callback feature via v.110 for the MAX Link Client software product.

See [Configuring dialout options](#) for information about enabling dialout using the MAX unit's digital modems.

To enable PPP outdial for v.110 modems:

1. Open a Connection profile configured for async PPP.
2. Open the Telco Options subprofile and specify the following data service:

```
Ethernet
  Connections
    Telco options...
      Data Svc=v110 19.2 56K
```

3. Close the Connection profile.

The Data Svc settings that begin with "v110" enable for V.110 outdial. These settings include the v110 indicator (which tells the MAX to communicate with a V.110 terminal adapter), the bit rate for the connection, and the data service to use. For example:

```
v110 19.2 56k
```

uses a bit rate of 19.2 ("19.2") over a line using the Switched-56 data service. If the MAX cannot sync up with the remote TA using the specified bit rate, it attempts to use one of the other bit rates. See the *MAX Reference Guide* for more details on this Data Svc setting.

Configuring MP and BACP connections

Multilink PPP (MP) uses the encapsulation defined in RFC 1717. MP enables the MAX to interact with MP-compliant equipment from other vendors to use multiple channels for a call. Both sides of the connection must support MP. In addition to the PPP parameters described in [Understanding the PPP parameters](#), these are the parameters related to MP connections without BACP:

```
Ethernet
  Answer
    Encaps...
      MP=Yes
      PPP=Yes

  PPP options...
    Min Ch Count=1
    Max Ch Count=1
```

```
Ethernet
  Connections
    Encaps=MP
    Encaps options...
      Base Ch Count=1
```

If the Bandwidth Allocation Control Protocol (BACP) is enabled, MP connections use that protocol to manage dynamic bandwidth on demand. Both sides of the connection must support BACP. In addition to the PPP parameters, these are the parameters for MP connections with BACP:

```
Ethernet
  Answer
    Encaps...
```

```
MP=Yes
PPP=Yes

PPP options...
  BACP=Yes
  Dyn Alg=Quadratic
  Sec History=15
  Add Pers=5
  Sub Pers=10
  Min Ch Count=1
  Max Ch Count=1
  Target Util=70

Ethernet
  Connections
    Encaps=MP
    Encaps options...
      BACP=Yes
      Base Ch Count=1
      Min Ch Count=1
      Max Ch Count=2
      Inc Ch Count=1
      Dec Ch Count=1
      Dyn Alg=Quadratic
      Sec History=15
      Add Pers=5
      Sub Pers=10
      Target Util=70
```

For more information about each parameter, see the *MAX Reference Guide*.

Understanding the MP and BACP parameters

This section provides some background information on MP and BACP configuration.

MP without BACP

For MP connections without BACP, you can specify the base channel count, which must be greater than or equal to the minimum count and less than or equal to the maximum count specified in the Answer profile. The base channel count specifies the number of channels to use to establish the connection, and this number of channels remains fixed for the whole session.

Enabling BACP for MP connections

You can enable BACP to use that protocol to increase or decrease bandwidth on demand for MP connections. Both sides of the connection must support BACP.

Specifying channel counts

The base channel count specifies the number of channels to use to establish the call. After the base channel or channels have been established, another link must be dialed to add channels. Inc Ch Count and Dec Ch Count specify the number of channels it can add and subtract at one time, respectively. You can also specify a maximum and minimum number of channels that can be allocated to the call. See also Parallel Dial in the System profile.

Dynamic algorithm for calculating bandwidth requirements

Dyn Alg specifies an algorithm for calculating average line utilization (ALU) over a certain number of seconds (Sec History). [Figure 3-2](#) shows how the algorithms weight usage samples.

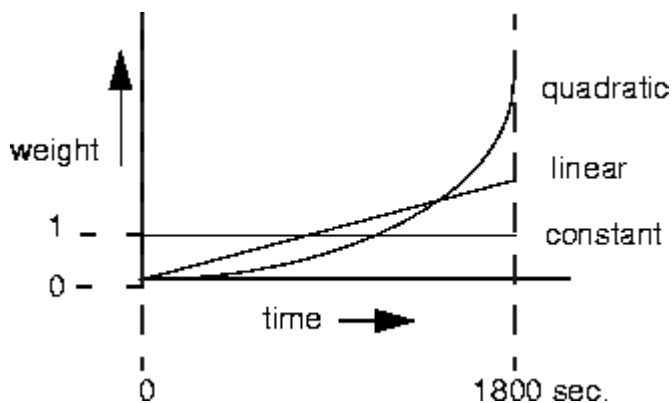


Figure 3-2. Algorithms for weighing bandwidth usage samples

- Quadratic (the default) gives more weight to recent samples of bandwidth usage than to older samples taken over the specified number of seconds. The weighting grows at a quadratic rate.
- Linear gives more weight to recent samples of bandwidth usage than to older samples taken over the specified number of seconds. The weighting grows at a linear rate.
- Constant gives equal weight to all samples taken over the specified number of seconds.

Time period for calculating average line utilization

Sec History specifies a number of seconds to use as the basis for calculating average line utilization (ALU).

Comparing the average utilization to a target utilization

Target Util specifies a percentage of line utilization (default 70%) to use as a threshold when determining when to add or subtract bandwidth.

How long the condition should persist before adding or dropping links

Add Pers specifies a number of seconds for which the ALU must persist beyond the Target Util threshold before the MAX adds bandwidth. Sub Pers specifies a number of seconds for which the ALU must persist below the Target Util threshold before the MAX subtracts bandwidth. When adding bandwidth, the MAX adds the number of channels specified in the Inc Ch Count parameter. When subtracting bandwidth, it subtracts the number of channels specified in the Dec Ch Count parameter, dropping the newest channels first.

Guidelines for configuring bandwidth criteria

When configuring dynamic bandwidth allocation, keep these guidelines in mind:

- The values for the Sec History, Add Pers, and Sub Pers parameters should smooth out spikes in bandwidth utilization that last for a shorter time than it takes to add capacity. Over T1 lines, the MAX can add bandwidth in less than ten seconds; over ISDN lines, the MAX can add bandwidth in less than five seconds.

- Once the MAX adds bandwidth, there is typically a minimum usage charge; thereafter, billing is time sensitive. The Sub Pers value should be at least equal to the minimum duration charge plus one or two billing time increments. Typically, billing is done to the next multiple of six seconds, with a minimum charge for the first thirty seconds. Your carrier representative can help you understand the billing structure of their switched tariffs.
- You can add channels one at a time or in multiples (see the Parallel Dial parameter).
- Avoid adding or subtracting channels too quickly (less than 10-20 seconds apart).

Adding or subtracting channels very quickly leads to many short duration calls, each of which incur the carrier's minimum charge. In addition, adding or subtracting channels too quickly can affect link efficiency, since the devices on either end have to retransmit data when the link speed changes.

Example MP connection without BACP

To configure an MP connection without BACP:

1. Open the Answer profile.
2. Enable PPP and MP encapsulation and specify the appropriate routing, bridging, and authentication values. For example:

```
Ethernet
  Answer
    Encaps...
      PPP=Yes
      MP=Yes

    PPP options...
      Route IP=Yes
      Route IPX=Yes
      Bridge=Yes
      Recv Auth=Either
```

3. Close the Answer profile.
4. Open a Connection profile, specify the name of the remote device, and activate the profile. For example:

```
Ethernet
  Connections
    Station=tcd
    Active=Yes
```

5. Select MP encapsulation and open the Encaps Options subprofile.
6. Configure PPP authentication.

```
Encaps=MP
Encaps options...
  Send Auth=PAP
  Send PW=remotepw
  Aux Send PW=N/A
  Recv PW=localpw
```

7. Set the base channel count. For example, to use two channels for this call:

```
Base Ch Count=2
```

Note: Both sides of the connection should specify the same number of channels.

8. Close the Connection profile.

Example MP connection with BACP

To configure an MP connection using BACP:

1. Open the Answer profile.
2. Enable PPP and MP encapsulation and specify the appropriate routing, bridging, and authentication values. For example:

```
Ethernet
  Answer
    Encaps...
      MP=Yes
      PPP=Yes

    PPP options...
      Route IP=Yes
      Route IPX=Yes
      Bridge=Yes
      Recv Auth=Either
```

3. Enable BACP to monitor bandwidth requirements based on received packets.

```
BACP=Yes
```

4. Close the Answer profile.
5. Open a Connection profile, specify the name of the remote device, and activate the profile. For example:

```
Ethernet
  Connections
    Station=clara
    Active=Yes
```

6. Select MP encapsulation and set the MP authentication options. For example:

```
Encaps=MP
Encaps options...
  Send Auth=PAP
  Send PW=remotepw
  Aux Send PW=N/A
  Recv PW=localpw
```

7. Enable BACP to monitor bandwidth requirements on packets transmitted on this connection, and configure the Ascend criteria for bandwidth management.

```
BACP=Yes
Base Ch Count=1
```

```

Min Ch Count=1
Max Ch Count=2
Inc Ch Count=1
Dec Ch Count=1
Dyn Alg=Quadratic
Sec History=15
Add Pers=5
Sub Pers=10
Target Util=70

```

Note: For optimum performance, both sides of a connection must set the channel count parameters to the same values.

8. Close the Connection profile.

Configuring Ascend MP+ connections

MP+ (Multilink PPP Plus) uses PPP encapsulation with Ascend extensions. MP+ enables the MAX to connect to another Ascend unit using multiple channels. BACP is not required, because the Ascend criteria for adding or dropping a link are part of the MP+ extensions. In addition to the PPP and MP parameters described earlier, these are the parameters for MP+ connections:

```

Ethernet
  Answer
    Encaps...
      PPP=Yes
      MP=Yes
      MPP=Yes

    PPP options...
      Dyn Alg=Quadratic
      Sec History=15
      Add Pers=5
      Sub Pers=10
      Min Ch Count=1
      Max Ch Count=1
      Target Util=70
      Idle Pct=0

Ethernet
  Connections
    Encaps=MPP
    Encaps options...
      Aux Send PW=aux-passwd
      DBA Monitor=Transmit
      Base Ch Count=1
      Min Ch Count=1
      Max Ch Count=2
      Inc Ch Count=1
      Dec Ch Count=1
      Dyn Alg=Quadratic
      Sec History=15
      Add Pers=5
      Sub Pers=10
      Target Util=70
      Idle Pct=0

```

For more information about each parameter, see the *MAX Reference Guide*.

Understanding the MP+ parameters

This section provides some background information on MP+ connections.

Channel counts and bandwidth allocation parameters

BACP and MP+ use the same criteria for increasing or decreasing bandwidth for a connection. For details on the bandwidth allocation parameters, see [Understanding the MP and BACP parameters](#) and [Guidelines for configuring bandwidth criteria](#).

Sending an auxiliary password for added channels

The Aux Send PW parameter can specify another password for authenticating subsequent links as they are dialed. See the *MAX Security Supplement* for details.

Monitoring traffic in one or both directions

DBA Monitor specifies whether bandwidth criteria for adding or dropping links are applied to traffic received across the link, transmitted across the link, or both. If you set DBA Monitor to None on both sides of the link, you disable bandwidth on demand.

Idle percent

Idle Pct specifies a percentage of utilization below which the MAX drops all channels including the base channel. Bandwidth utilization must fall below this percentage on *both sides* of the connection before the MAX drops the link. If the device at the remote end of the link enters an Idle Pct setting lower than the value you specify, the MAX does not clear the call until bandwidth utilization falls below the lower percentage. The default value for Idle Pct is 0, which causes the MAX to ignore bandwidth utilization when determining whether to clear a call and use the Idle timer instead.

Example MP+ configuration

[Figure 3-3](#) shows the MAX connected to a remote Pipeline unit with an MP+ connection.



Figure 3-3. An MP+ connection

To configure an MP+ connection with a remote Ascend unit:

1. Open the Answer profile.
2. Set PPP and MP+ encapsulation to Yes and specify the appropriate routing, bridging, and authentication values. For example:

```
Ethernet
  Answer
    Encaps...
      MPP=Yes
      PPP=Yes
```

```

PPP options...
Route IP=Yes
Route IPX=Yes
Bridge=Yes
Recv Auth=Either

```

3. Close the Answer profile.
4. Open a Connection profile, specify the name of the remote device, and activate the profile. For example:

```

Ethernet
Connections
Station=richard
Active=Yes

```

5. Select MPP encapsulation and set the MP+ authentication options. For example:

```

Encaps=MPP
Encaps options...
Send Auth=PAP
Send PW=remotepw
Aux Send PW=secondpw
Recv PW=localpw

```

6. Configure the DBA Monitor and the Ascend criteria for bandwidth management. For example:

```

Encaps options...
DBA Monitor=Transmit-Recv
Base Ch Count=1
Min Ch Count=1
Max Ch Count=5
Inc Ch Count=1
Dec Ch Count=1
Dyn Alg=Quadratic
Sec History=15
Add Pers=5
Sub Pers=10
Target Util=70
Idle Pct=0

```

Note: For optimum performance, both sides of a connection must set the Base Ch Count, Min Ch Count, and Max Ch Count parameters to the same values.

7. Close the Connection profile.

Configuring a nailed MP+ connection

A Nailed/MPP connection is a nailed connection that can add switched channels for increased bandwidth. When you connect nailed or switched channels end-to-end, you establish a nailed/MPP connection. The MAX dials switched channels when the MAX receives an outbound packet for the far end and cannot forward it across the nailed connection, either because those channels are down or because they are being fully utilized.

If both the nailed and switched channels in a Nailed/MPP connection are down, the connection does not reestablish itself until the nailed channels are brought back up or you dial the switched channels.

The maximum number of channels for the Nailed/MPP connection is either the Max Ch Count or the number of nailed channels in the specified group, whichever is greater. If a nailed channel fails, MAX replaces that channel with a switched channel, even if the call is online with more than the minimum number of channels.

Note: If you modify a Nailed/MPP Connection profile, most changes become active only after the call is brought down and then back up. However, if you add a group number (for example, changing Group=1,2 to Group=1,2,5) and save the modified profile, the MAX adds the additional channels to the connection without having to bring it down and back up.

To configure a Nailed/MPP connection:

1. Configure an MP+ connection, as described in the preceding section.
2. Open the Telco Options subprofile of the Connection profile.
3. Specify that the MAX is the designated caller for the switched part of the connection.

```

Ethernet
  Connections
    Telco options...
      AnsOrig=Call Only
      FT1 Caller=Yes
  
```

Note: On the far end of the connection, set the AnsOrig and FT1 Caller parameters for answering only. Note that the DO HANGUP command only works from the caller end of the connection.

4. Specify the Nailed/Mpp call type, and the group number(s) of its nailed channels. For example:

```

Call Type=Nailed/MPP
Group=1,2
  
```

5. Close the Connection profile.

Spanning multilink or MP+ calls across multiple MAX units

You can configure multiple MAX units to form a stack, or group of MAX units, that allows a Multilink PPP (MP) or MP+ call to span the MAX units in the stack.

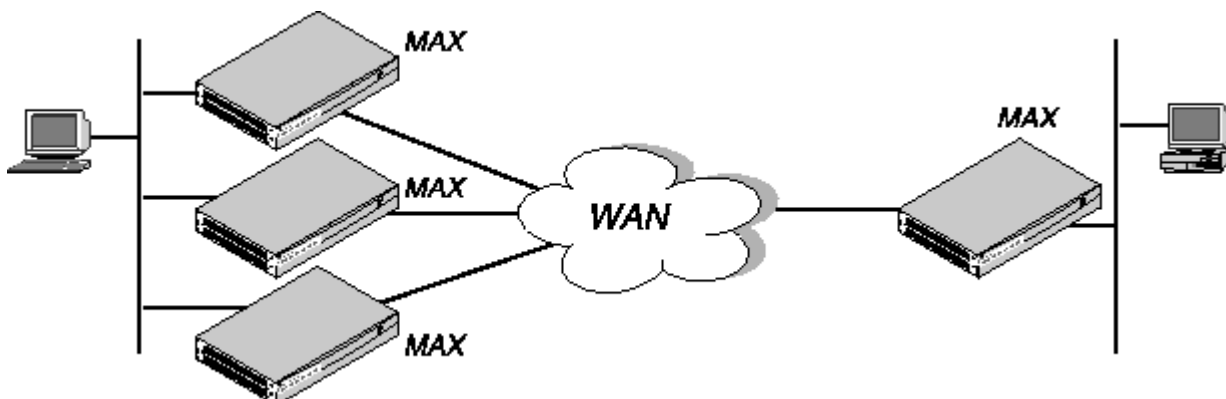


Figure 3-4. A MAX stack for spanning multilink PPP calls (MP) or MP+

Call spanning using a stack configuration can be effective when:

- A MAX running MP+ asks for another phone number, and has no available lines
- A rotary hunt group uses the same phone number to access multiple MAX units, making it impossible to assume that the same MAX that answered the original call will answer a subsequent call.

MP/MP+ call spanning is protocol independent, and works with all protocols supported by the MAX.

Note: Stacking requires any MP caller to use the MP endpoint discriminator. The same is true of MP+. All Ascend products and most other products that support MP or MP+ use an endpoint discriminator, but the specification for MP does not require it.

How MP/MP+ call spanning works

A stack is a group of MAX units that have the same stack information, and are on the same physical LAN. There is no *master* MAX; the MAX units in the stack use an Ethernet multicast packet to locate each other.

Multicast packets usually cannot cross a router, so the MAX units in a single stack must be on the same physical LAN. MAX units running in a stack can generate fairly high levels of network traffic, which is another reason to keep them on the same physical LAN.

Bundle ownership

Although MAX stacks do not have a master MAX, each MP/MP+ bundle has a bundle owner. The MAX that answers the first call in the MP/MP+ bundle is the *bundle owner*. If a bundle spans more than one MAX in a stack, an exchange of information flows between the MAX units in the bundle.

Stacking requires an endpoint discriminator. Every MP/MP+ call that comes to any member of the stack is compared to all existing MP/MP+ calls in the MAX stack to determine whether it is a member of an existing bundle. If the call belongs to an existing bundle, the MAX that answered and the bundle owner exchange information about the bundle. Furthermore, the MAX that answered the call forwards all incoming data packets over the Ethernet to the bundle owner.

Outgoing data

To balance the load among all available WAN channels, outgoing data packets for the WAN are assigned to available channels in a bundle on a rotating basis. If the MAX assigns an outgoing packet to a channel that is not local to the bundle owner, the bundle owner forwards the packet over the Ethernet to the MAX that owns the non-local channel.

Real and stacked channels

For the purpose of this description, *real* channels are those channels that connect directly to the MAX that owns the bundle. *Stacked* channels connect to a MAX that transfers the data to or from the MAX that owns the bundle.

When a MAX has to add a channel for a MP+ or MP-with-BACP call, it provides a local phone number for the new channel. However, sometimes the MAX that answers the call cannot provide a local phone number for the additional channel because all the channels that connect directly to it are busy. In that case, the MAX requests other members of the stack to supply a phone number for the additional channel.

An MP call does not pass phone numbers when it adds a channel. The originator of the call must know all of the possible phone numbers to begin with.

If each MAX in the stack is accessed through a different phone number, the originator of the call must know all of the possible phone numbers. An alternative in this instance is to use BACP or MP+ to obtain the phone number of a MAX with a free channel.

Performance considerations for MAX stacking

There is no limit to the number of *stacked* channels in single call or in a stack of MAX units, other than the limit for each individual MAX. The MAX 6000, MAX 4000, MAX 2000, and MAX 1800 each support up to 40 stacked channels. The MAX 200 Plus supports up to three stacked channels. A MAX can handle n real channels and $n/3$ *stacked* channels.

There is no theoretical limit to the number of MAX units in a stack, other than performance considerations. Since all data from stacked channels crosses the LAN, performance could suffer with a large number of MAX units in the stack and many stacked channels in use.

Performance overhead increases when stacked bundles span multiple boxes. In a bundle of 6 channels, 4 of which are real and 2 are stacked, the overhead is the actual bandwidth of the two stacked channels ($2 \times 64 = 128K$). The actual payload data of the 6 channels with a 2:1 data compression is $6 \times 2 \times 64 = 768K$. The overhead is 128 over 768, or 16%. In a two-channel bundle with one real and one stacked channel, with the same compression, the overhead is 25%.

Take into account that you do not know ahead of time how many bundles will span the stack, or how many multi- or single-channel calls you are going to get. You can base an estimate on your traffic expectations. But in most situations, the majority of bundles will be on a single MAX, for which there is no overhead.

Suggested LAN configurations

Total Ethernet usage is approximately 5116Kbps for a MAX stack handling 82 single-channel calls, 41 two-channel stacked calls, and 41 two-channel nonstacked calls. Since Ethernet capacity generally does not achieve more than 50% utilization, this configuration uses up the available Ethernet bandwidth.

The total number of channels in this configuration is 246. Therefore, a stack of three MAX units, each having three T1 lines with this usage profile, utilizes all of the Ethernet bandwidth.

The basic limitation from the above examples is the speed of the LAN. One way to increase the speed of your LAN is to attach each MAX to a separate port of a 10/100 Ethernet switch, then use a 100Mbps connection to the backbone LAN. This allows each MAX to utilize up to a full 10Mb Ethernet and the entire stack combined can generate up to full 100Mb of Ethernet data. Once again assuming that the 100Mbps is saturated at 50% usage, we can now use up to 51200Kbps of bandwidth, or 10 times more than in the example above. Note that the success of this strategy depends on limiting stacked channels per MAX to the $n/3$ limit mentioned above.

Suggested hunt group configurations

Whenever you have MAX units in a stack, it is important to limit the number of multichannel calls that are split between the MAX units. The following suggested configurations reduce the overhead for a multichannel call by keeping as many channels as possible on the same MAX.

MP+ and MP-with-BACP calls

[Figure 3-7](#) shows the suggested hunt group setup for a typical MAX stack that receives only PPP, MP+, or MP-with-BACP calls. Each MAX has three T1 lines. All the T1 lines in a MAX share a common phone number and they are in a hunt group that does not span MAX units. The illustration shows these three local hunt groups with phone numbers 555-1212, 555-1213, 555-1214. In addition, a global hunt group, 555-1215 spans all the T1s of all the MAX units in the stack.

Users that access the MAX, dial 555-1215, the global hunt group number. The telephone company sets up the global hunt group to distribute incoming calls equally among the MAX units. Namely, the first call dialing 555-1215 goes to MAX#1, the second call to MAX #2, and so on. If you use this configuration, you must configure each of the MAX unit's Line profiles with the local hunt group numbers. For example, for MAX #1 in [Figure 3-7](#), you would set the Ch n # parameters to 12 (the last two digits of the 555-1212 hunt group number).

You can achieve the same distribution without a global hunt group by having one third of the users dial 555-1212, one third dial 555-1213, and one third dial 555-1214. You can leave the Ch n # parameters at their default setting (null) if you do not have a global hunt group.

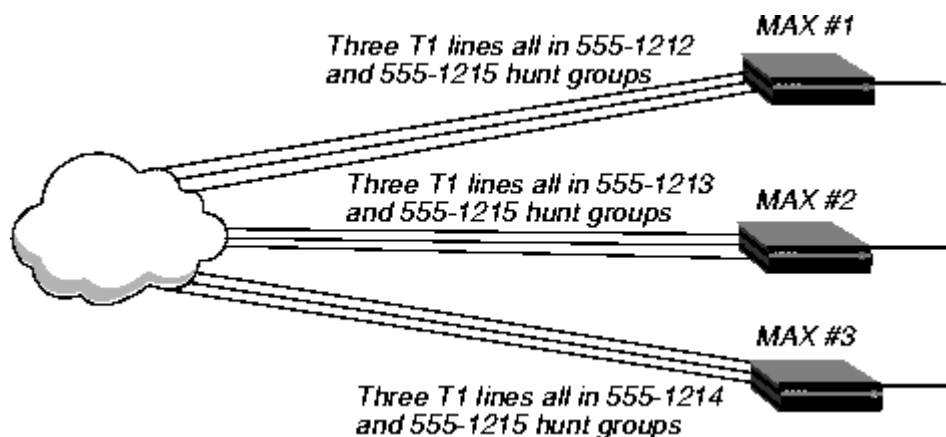


Figure 3-7. Hunt groups for a MAX stack handling both MP and MP+ calls

Viewing [Figure 3-7](#), suppose an MP+ call is connected to MAX #1. When that call needs to add a channel, it requests an add-on number from the MAX, and the MAX returns 12 (for 555-1212) as long as a channel in the local T1 lines is available. This means the bundle does not span multiple MAX units as long as a channel is available in the local hunt group.

The [Figure 3-7](#) configuration tends to break down if MAX units receive MP-without-BACP calls. Spreading the calls across the MAX stack (by dialing the global hunt group) results in the worst possible performance because MP-without-BACP must know all of the phone numbers before the caller places the first call.

MP-without-BACP calls

[Figure 3-8](#) shows a site that supports only MP-without-BACP calls. For this site, the telephone company has set up a global hunt group that first completely fills MAX #1, then continues to MAX #2, and so on. This arrangement tends to keep the channels of a call from being split across multiple MAX units, keeping overhead low.

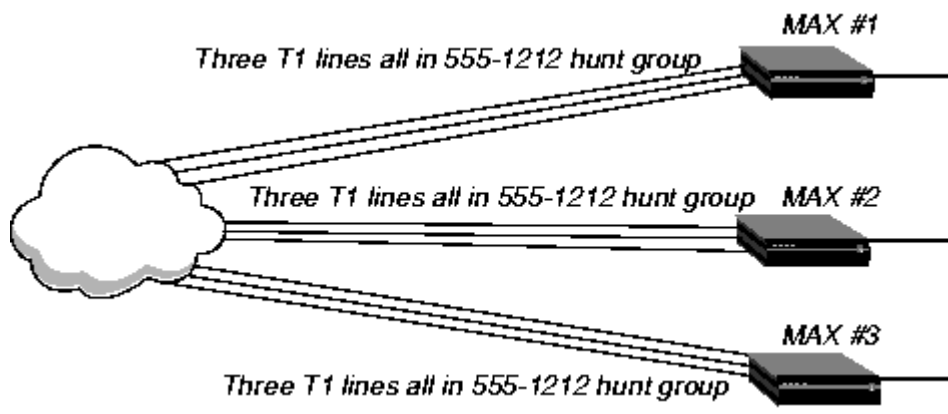


Figure 3-8. Hunt groups for a MAX stack handling only MP-without-BACP calls

MP+ calls and MP calls with or without BACP

For a MAX that receives MP+ calls and MP calls with or without BACP, you can use a configuration similar to the one shown in [Figure 3-7](#). In this case, however, you set up the global hunt group differently than explained in ["MP+ and MP-with-BACP calls."](#) You set up the global hunt group to help prevent MP-without-BACP calls from being split across multiple MAX units in the stack. As in ["MP-without-BACP calls,"](#) calls dialing 555-1215 first completely fill the channels of MAX #1, then continues to MAX #2, and so on.

Both MP+ and MP callers dial the global hunt group number to connect to the stack. The sections ["MP-without-BACP calls,"](#) and [MP+ calls and MP calls with or without BACP](#) explain how the MAX adds channels to MP+ and MP bundles. Be sure to set the Ch n # parameters as explained in ["MP+ calls and MP calls with or without BACP."](#)

MP+ and MP-with-BACP callers do not have to dial the global hunt group numbers to connect. Only the MP-without-BACP callers need to dial the global hunt group. You can achieve an even distribution of MP+ and MP-with-BACP calls by having one third dial 555-1212, one third dial 555-1213, and one third dial 555-1214. You can leave the Ch n # parameters at their default setting (null) in this situation.

Understanding the stack parameters

This section provides some background information about the stack parameters.

Stacking Enabled

This parameter enables the MAX to communicate with other members of the same stack. A MAX can belong to only one stack. All members of the stack use the same stack name and UDP port.

Stack Name

This parameter specifies a stack name. Add a MAX to an existing stack by specifying that name. Create a new stack by specifying a new stack name.

UDP Port

Stacked MAX units communicate with other members of the stack by using an Ethernet multicast packet on the specified UDP port. Since these multicast packets are unlikely to cross a router, and because of the high traffic demands created by a multilink call that spans MAX units, all members of

a stack must reside on the same physical LAN.

For more information about each parameter, see the *MAX Reference Guide*.

Configuring a MAX stack

This section shows how to configure a stack of two MAX units. It does not show the details of configuring hunt groups, which is an important factor for stacked MP connections. For details on hunt groups, see [Chapter 2, Configuring the MAX for WAN Access](#).

To configure a MAX stack, proceed as follows for each MAX in the stack:

1. Open the Ethernet > Mod Config menu, and select Stack Options, as shown in the following sample menu:

```
90-A** Mod Config
  RADIUS Server
  Log
  ATMP
  Modem Ringback=Yes
  AppleTalk
  SNTP Server
  >Stack Options...
  UDP Checksum=No
```

When you press Enter, the Ethernet \> Mod Config \> Stack Options menu appears. For example:

```
90-A** Mod Config
>Stack Options...
Stacking Enabled=Yes
Stack Name=maxstack-1
UDP Port=6000
```

1. Set Stacking Enabled to Yes (Stacking Enabled=Yes).
2. Set the Stack Name parameter to a unique name for the stack.

A stack name is 16 characters or less. This is the name members of a stack use to identify other members of the same stack. The stack name must be unique among all MAX units that communicate with each other, even if they are not on the same LAN.

If a MAX receives calls from two MAX units on different LANs, and the two units are members of different stacks with the same stack name, the MAX receiving the calls assumes the two MAX units with the same stack name are in the same bundle.

Note: Multiple stacks can exist on the same physical Ethernet LAN if the stacks have different names.

3. Specify the UDP port.

This is a reserved UDP port for intrastack communications. The UDP port must be identical for all members of a stack, but is not required to be unique among all stacks.

Disabling a MAX stack

To disable a stack, specify Stacking Enabled=No for each of the MAX units in the stack.

Adding and removing a MAX

You can add a MAX to an existing stack at any time without rebooting the MAX or affecting stack operation. Since a stack is a collection of peers, none keeps a list of the stack membership. The MAX units in a stack communicate when they need a service from the stack.

Removing a MAX from a stack requires care, because any calls using a channel between the MAX to be removed and another MAX in the stack could be dropped. There is no need to reboot a MAX removed from a stack.

Configuring a Combinet connection

The MAX supports Combinet bridging to link two LANs as if they were one segment. For a Combinet connection to work, bridging must be enabled at the system level. See [Chapter 8, Configuring Packet Bridging](#). [Figure 3-9](#) shows a Combinet connection.

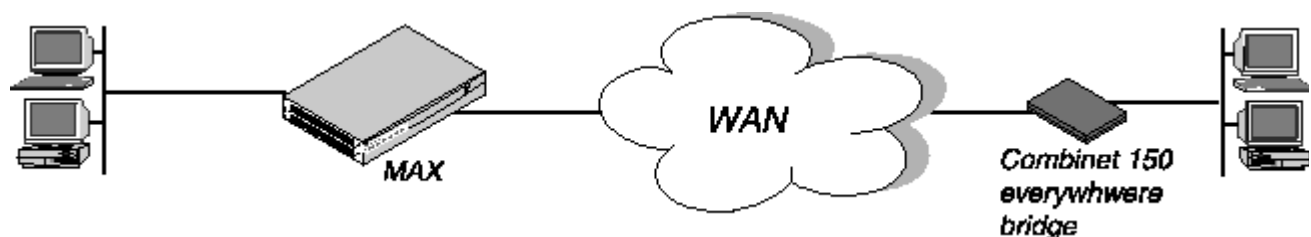


Figure 3-9. A Combinet connection

These are the parameters related to Combinet configuration:

```

Ethernet
  Mod Config
    Bridging=Yes

Ethernet
  Answer
    Encaps...
      COMB=Yes

    COMB options...
      Password Reqd=Yes
      Interval=10
      Compression=Yes

Ethernet
  Connections
    Station=000145CFCF01
    Encaps=COMB
    Bridge=Yes
    Encaps options...
      Password Reqd=Yes
      Send PW=remotepw
      Recv PW=localpw
      Interval=10
      Base Ch Count=2
  
```

Compression=Yes

For more information about each parameter, see the *MAX Reference Guide*.

Understanding Combinet bridging parameters

This section provides some background information on a Combinet configuration.

Specifying the hardware address of the remote Combinet bridge

The Station parameter must specify the MAC (Media Access Control) address of the remote Combinet bridging device.

Enabling bridging

A Combinet connection is always a bridging connection, so the Bridge parameter in the Connection profile must be set to Yes. If the Bridge parameter is N/A, bridging has not been enabled in the Ethernet profile. See [Chapter 8, Configuring Packet Bridging](#).

Requiring a password from the remote bridge

You can specify that an individual Combinet connection does not require a password exchange, even if the Answer profile specifies that Combinet passwords are required.

Specifying passwords to exchange with the remote bridge

The Send PW is the password sent to the remote device. It must match the password expected from the MAX. The Recv PW is the password sent to the MAX from the remote device.

Configuring line-integrity monitoring

Interval specifies the number of seconds between transmissions of Combinet line-integrity packets. You can specify a number between 5 and 50. If the MAX does not receive a Combinet line-integrity packet within the specified interval, it disconnects the call.

Base channel count

The Base Ch Count parameter specifies the base number of channels to use when setting up the call. It can be set to 1 (64 kbps) or 2 (128 kbps).

Compression

This parameter enables or disables STACKER LZS compression/decompression. Both sides of the link must enable compression or it is not used.

Example Combinet configuration

To configure a Combinet connection:

1. Open a Connection profile.
2. Specify the MAC address of the remote device and activate the profile.

```

Ethernet
  Connections
    Station=000145CF01
    Active=Yes

```

3. Configuring bridging options.

```

Bridge=Yes
Dial Brdcast=Yes

```

4. Select Combnet encapsulation and then configure COMB options for this connection. (Leave the default values for Compression and Interval.)

```

Encaps=COMB
  Encaps options...
    Password Reqd=Yes
    Send PW=*SECURE*
    Recv PW=*SECURE*
    Interval=10
    Base Ch Count=2
    Compression=Yes

```

5. Close the Connection profile.

Configuring EU connections

EU encapsulation is a type of X.75 HDLC encapsulation commonly used in European countries. Like PPP, EU runs over synchronous lines. It has no asynchronous mode for connecting to modems. EU encapsulation differs from a PPP or MP+ connection in that it does not support password authentication, IP/IPX address pools, or dynamic bandwidth allocation (DBA). It does support routing and bridging connections.

EU-RAW and EU-UI do not provide password-authentication of incoming calls, so another mode of authentication is typically used to verify the caller when the call is end-to-end ISDN. For details, see the *MAX Security Supplement*.

These are the parameters related to EU configuration:

```

Ethernet
  Answer
    Id Auth=Called Reqd
    Encaps...
      EU-UI=Yes
      EU-RAW=Yes

```

```

Ethernet
  Connections
    Calling #=555-7878
    Called #=555-1212
    Encaps=EU-RAW
    Encaps options...
      MRU=1524

```

```

Ethernet
  Connections
    Calling #=555-7878
    Called #=555-1212
    Encaps=EU-UI

```

```
Encaps options...  
MRU=1524  
DCE Addr=1  
DTE Addr=3
```

For more information about each parameter, see the *MAX Reference Guide*.

Understanding the EU parameters

This section provides some background information on EU parameters.

EU-RAW and EU-UI

EU-RAW is a type of X.75 encapsulation, in which IP packets are HDLC encapsulated together with a CRC field. EU-UI uses the same encapsulation, but contains a smaller header that can contain one value for packets from the caller and another value for packets from the called unit. Most EU connections use EU-RAW.

MRU (Maximum Receive Units)

The MRU parameter specifies the maximum number of bytes the MAX can receive in a single packet on an EU link. Usually the default 1524 is the right setting, unless the far end device requires a lower number. If the administrator of the remote network specifies that you must change this value, enter a number lower than 1524.

DCE (data communications equipment) address

The DCE Addr parameter specifies a value for the calling unit in the EU-UI header. The caller needs to obtain the number you specify and configure their unit accordingly.

DTE (data terminal equipment) address

The DTE Addr parameter specifies a value for the called unit in the EU-UI header. The caller must use the same value for the called unit.

Example EU configurations

[Figure 3-10](#) shows three Connection profiles using EU encapsulation with ID authentication.

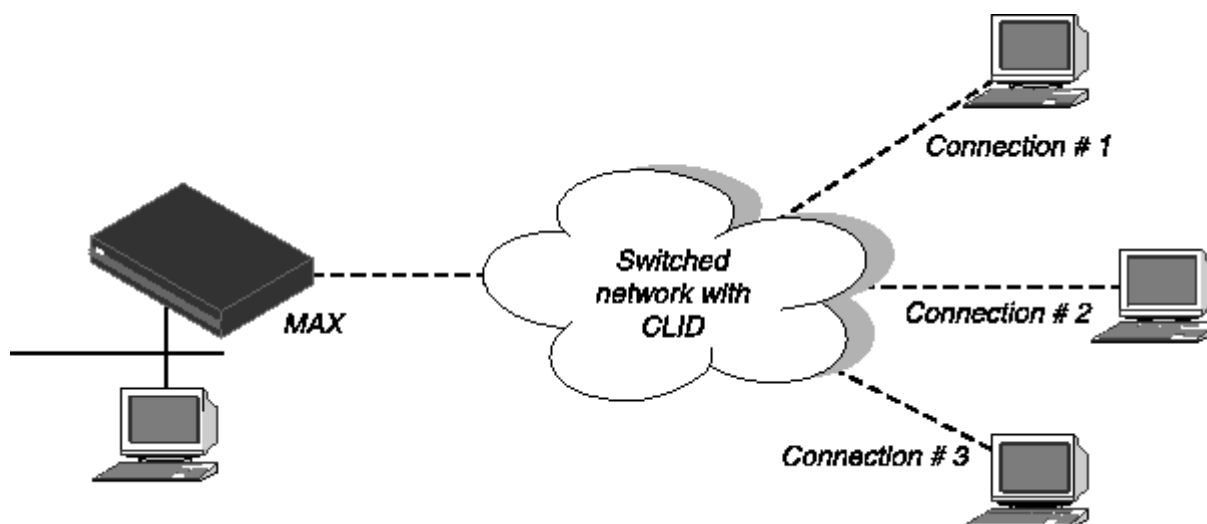


Figure 3-10. EU connection

To configure a connection that uses EU-RAW framing:

1. Open the Answer profile and make sure that EU-RAW encapsulation is enabled.
2. Set Id Auth to Calling Reqd (CLID authentication).

```
Ethernet
  Answer
    Id Auth=Calling Reqd
    Encaps...
      EU-RAW=Yes
```

3. Close the Answer profile.
4. Open a Connection profile and specify the name of the remote device.
5. Activate the profile.

```
Ethernet
  Connections
    Station=remote-device
    Active=Yes
```

6. Specify the calling line number.

```
Calling #=555-1212
```

7. Select the EU-RAW encapsulation type and, if necessary, configure the MRU in the Encaps Options subprofile.

```
Encaps=EU-RAW
Encaps options...
  MRU=1524
```

8. Close the Connection profile.

Example EU-UI connection

To configure a connection using EU-UI framing:

1. Open the Answer profile and make sure that EU-UI encapsulation is enabled.
2. Set Id Auth to Calling Reqd (CLID authentication).

```
Ethernet
  Answer
    Id Auth=Calling Reqd
    Encaps...
      EU-UI=Yes
```

3. Close the Answer profile.
4. Open a Connection profile, specify the name of the remote device, and activate the profile.

```

Ethernet
  Connections
    Station=remote-device
    Active=Yes

```

- Specify the calling line number.

```
Calling #=555-1212
```

- Select the EU-UI encapsulation type.

```
Encaps=EU-UI
```

- In the Encaps Options subprofile, set the DCE and DTE addresses.

```

Encaps options...
  MRU=1524
  DCE Addr=1
  DTE Addr=3

```

- Close the Connection profile.

Configuring an ARA connection

ARA (AppleTalk Remote Access) uses V42 Alternate Procedure as its data link, so it can be used only over asynchronous modem connections.

The parameters related to ARA connections are:

```

Ethernet
  Mod Config
    Appletalk=Yes
    AppleTalk...
      Zone Name=*

```

```

Ethernet
  Answer
    Profile Reqd=Yes
    Encaps...
      ARA=Yes

```

```

Ethernet
  Connections
    Encaps=ARA
    Encaps options...
      Password=*SECURE*
      Max. Time (min)=0

  AppleTalk Options
    Peer=Dialin
    Zone Name=
    AppleTalk Router=Seed
    Net Start=300
    Net End=309
    Default Zone=
    Zone Name #1=
    Zone Name #2=
    Zone Name #3=
    Zone Name #4=

```

For more information about each parameter, see the *MAX Reference Guide*.

Understanding the ARA parameters

This section provides some background information on ARA parameters.

AppleTalk and zone name

The AppleTalk parameter in the Ethernet profile enables the AppleTalk stack in the MAX. If the local Ethernet supports an AppleTalk router with configured zones, the Zone Name parameter should specify the zone in which the MAX unit resides.

Turning off ARA Guest access

When Profile Reqd=Yes in the Answer profile, ARA Guest access is disabled.

A password required from ARA clients

The Password parameter specifies the password sent to the MAX from the ARA client.

Setting the maximum number of minutes for an ARA session

Max Time specifies the maximum number of minutes an ARA session can remain connected. If it is set to zero (the default), the timer is disabled. The maximum connect time for an ARA connection has nothing to do with the MAX Idle Timer. If a connection is configured with maximum connect time, the MAX initiates an ARA disconnect when that time is up. The ARA link goes down cleanly, but remote users are not notified. Users find out the ARA link is gone only when they try to access a device.

Example ARA configuration that allows IP access

This section shows an example ARA configuration that enables a Macintosh with an internal modem dialing into the MAX using the ARA Client software to communicate with an IP host on the Ethernet. A connection that does not require IP access would be a subset of this example. The sample network looks like this:



Figure 3-11. An ARA connection enabling IP access

Note: If IP access is not required, the Connection profile does not need IP routing and the Macintosh client does not need a TCP/IP configuration. For ARA connections that support IP access, the MAX receives IP packets encapsulated in AppleTalk's DDP protocol. It removes the DDP headers and routes the IP packets normally.

The Macintosh ARA Client software must be configured as follows:

- Set the appropriate modem parameters in the ARA Client software to enable the user's async modem to establish a connection with the MAX.
- Specify the right dial-in number in the ARA Client software.

The Macintosh TCP/IP software must be configured as follows:

- Open Transport

The TCP/IP Control Panel has an option to connect by using MacIP. DDP-IP encapsulation requires MacIP. This Control Panel also has an option to configure its IP address manually, via BOOTP, via DHCP, or via RARP. If you assign the Macintosh a permanent IP address, choose Manually. If you assign the MAX an address to the Macintosh from a pool of allocated addresses, choose BOOTP.

- MacTCP

The MacTCP Control Panel should have an icon for ARA. That icon must be selected for DDP-IP encapsulation. This Control Panel also has an option to configure its IP address Manually or from a Server. If you assign the Macintosh a permanent IP address, choose Manually. If you assign the MAX an address to the Macintosh from a pool of allocated addresses, choose Server. *Do not choose "Dynamically" in the MacTCP Control Panel.* That option is not supported in the MAX.

Note: The MAX must be configured as an IP router. At a minimum, the MAX unit's Ethernet interface should be configured with an IP address and a DNS server address. If the ARA client obtains an IP address from the server, you must also configure the MAX for dynamic IP address assignment. See [Chapter 10, Configuring IP Routing](#).

If you configure the MAX for IP routing (Ethernet profile), you can configure an ARA connection that enables IP access as follows:

1. Open the Ethernet profile and set AppleTalk to Yes.
2. If applicable, specify the AppleTalk zone in which the MAX resides.

```

Ethernet
  Mod Config
    Appletalk=Yes
    AppleTalk...
      Zone Name=Engineering
  
```

3. Close the Ethernet profile.
4. Open a Connection profile, specify the dial-in user's name, and activate the profile.

```

Ethernet
  Connections
    Station=mac
    Active=Yes
  
```

5. Select ARA encapsulation and configure the ARA options.

```

Encaps=ARA
Encaps options...
    Password=localpw
    Max. Time (min)=0

```

6. Configure the connection for IP routing.

For example, if the Macintosh software has a hard-coded IP address (Manual):

```

Route IP=Yes
IP options...
    LAN Adrs=10.2.3.4/24

```

Or, if the Macintosh software expects a dynamic IP address assignment:

```

Route IP=Yes
IP options...
    LAN Adrs=0.0.0.0/0
    Pool=1

```

7. Close the Connection profile.

Dial-in PPP support for AppleTalk

You can configure an Ascend unit so that individual users can dial into an AppleTalk network using a PPP dialer, such as AppleTalk Remote Access 3.0 and Pacer PPP. The MAX does not need to be set up as an AppleTalk router to support dial-in PPP to AppleTalk.

Configuring dial-in PPP for AppleTalk

You can set up a MAX to allow an AppleTalk client to dial in using PPP in two ways:

- using a Connection profile
- using a Name/Password profile

Configuring an AppleTalk PPP connection using a Connection profile

1. Open the Ethernet > Mod Config menu.
2. Set Appletalk=Yes.
3. Open the appropriate Connection profile.
4. Set Route Appletalk=Yes.
5. Open the AppleTalk options menu.

```

90-103 apple
AppleTalk options...
    Peer=Dialin
    Zone Name=N/A
    Net Start=N/A
    Net End=N/A

```

6. Set the Peer parameter to indicate whether the connection for this profile is a single user PPP connection or a router

Peer=Dialin indicates that the profile is for a single user PPP connection. All other fields in the AppleTalk options menu are N/A. If you select Peer=Dialin, you have completed the configuration; close the AppleTalk Options menu and save your changes.

Peer=Router indicates that the profile is for a connection with a router (such as an Ascend Pipeline unit). If you select Peer=Router, you will need to configure the other fields in the AppleTalk options menu by continuing with through [step 11](#)

Note: Peer=Router works the same way that AppleTalk routing worked before this feature. The following steps are given here for convenience, and duplicate the existing documentation for AppleTalk routing.

7. Configure the AppleTalk zone name for the Ascend unit in the AppleTalk options submenu of the Ethernet Configuration Profile.

If there are other AppleTalk routers on the network, you must configure the zone names and network ranges to coincide with the other routers on the LAN.

The default for the Zone Name field is blank. Enter up to 33 alphanumeric characters to identify the zone name for the unit you are configuring.

Note: These fields display N/A if you have not enabled AppleTalk in the Ethernet Mod Config menu.

8. Specify whether the Ascend unit is a seed or non-seed router. The default value for AppleTalk Router is Off.
 - o You assign the network range and zone name configuration for a seed router. There must be at least one seed router on a routed AppleTalk network. Select AppleTalk Router=Seed for this option.
 - o A non-seed router learns network number and zone information from other routers. Select AppleTalk Router=Non-Seed for this option.

If you choose Non Seed or Off, then Net Start, Net End, Default Zone, and Zone Name #x are N/A.

If you are configuring a non-seed router and are using Names/Passwords, go to [Configuring an AppleTalk PPP connection using a Name/Password profile](#).

9. If you are configuring the Ascend unit as a seed router, specify the network range for the network to which the Ascend unit is attached.

Net Start and Net End define the network range for nodes attached to this network. Valid entries for these fields are in the range from 1 to 65199. If there are other AppleTalk routers on the network, you must configure the network ranges to coincide with the other routers.

10. Specify the default zone name for nodes on the Ascend unit's internet.

Enter up to 33 alphanumeric characters for the default zone name. The default for this field is blank.

The default zone is the one used by a node in the network for which you are configuring the Connection Profile until another zone name is explicitly selected by the node.

11. Specify the zone names that the platform can seed.

The Pipeline can seed up to 5 zones, and the MAX can seed up to 32. Enter up to 33 alphanumeric characters in zone name fields.

Configuring an AppleTalk PPP connection using a Name/Password profile

1. Open the Ethernet > Mod Config menu.
2. Set Appletalk=Yes.
3. Open the PPP Options menu of the Answer profile.
4. Set Route Appletalk=Yes.
5. Open the Appletalk options submenu of the PPP options menu.

```
90-103 apple
    AppleTalk options...
        Peer=Dialin
```

6. Set the Peer parameter to indicate whether the connection for this profile is a single user PPP connection or a router

Peer=Dialin indicates that the profile is for a single user PPP connection. All other fields in the AppleTalk options menu are N/A. If you select Peer=Dialin, you have completed the configuration; close the AppleTalk Options menu and save your changes.

Peer=Router indicates that the profile is for a connection with a router (such as an Ascend Pipeline unit). If you select Peer=Router, you will need to configure the other fields in the AppleTalk options menu by continuing with Step 7 through Step 11 in [Configuring an AppleTalk PPP connection using a Name/Password profile](#).

Note: Step 7 through Step 11 are given here for convenience, and duplicate the steps for setting up AppleTalk routing in the AppleTalk chapter of this guide.

Configuring AppleTalk connections from RADIUS

You can set up an AppleTalk connection in a RADIUS user profile and configure static AppleTalk routes in a RADIUS pseudo-user file. For more information, see the *MAX RADIUS Configuration Guide*.

Configuring terminal server connections

Terminal server connections are host-to-host connections that use an analog modem, ISDN modem (such as a V.120 terminal adapter), or raw TCP. If you use one of these methods to initiate a call but the call contains PPP encapsulation, the terminal server forwards the call to the MAX router. These are asynchronous PPP calls, and aside from the initial processing, they are handled like regular PPP sessions. (See [Configuring PPP connections](#).)

[Figure 3-12](#) shows a user dialing in via analog modem using dial-up software that does not include PPP. This type of call must be routed first to a digital modem, after which it is forwarded automatically to the terminal server.



Figure 3-12. Terminal server connection to a local Telnet host

Terminal server connections can be authenticated via Connection or Name-password profiles, or through a third-party authentication server such as RADIUS.

Note: Like PPP connections, terminal server connections rely on the Answer profile for default settings and enabling of the encapsulation type. See [Introduction to WAN links](#) for information about the telco options in a Connection profile, which apply equally to PPP or terminal server calls.

Connection authentication issues

When the terminal server receives a forwarded call, the terminal server waits briefly to receive a PPP packet. If it times out waiting for PPP, it sends its Login prompt. When it receives a name and password, it authenticates them against the Connection profile.

If the terminal server receives a PPP packet, instead of sending a Login prompt it responds with a PPP packet and LCP negotiation begins, including PAP or CHAP authentication. The connection is then established as a regular PPP session.

Note: If you do not want your users to share profiles, set the Shared Prof parameter to No. This parameter can be set in Ethernet > Mod Config for all users or in Ethernet > Connections > any profile for a single user. For more details on the Shared Prof parameter, see the *MAX Reference Guide*. To specify shared profiles per user in RADIUS, see the Ascend-Shared-Profile-Enable attribute in the *RADIUS Reference Guide*.

These are some recommended settings for callers with modems and terminal adapters:

- Analog modems and async PPP connections

If the Connection profile specifies PAP or CHAP authentication, the caller's PPP software should not be configured with any expect-send scripts, because the software must start negotiating PPP when the modems connect.

If the Connection profile does not specify PAP or CHAP authentication, configure the caller's PPP software with an expect-send script (expect > *Login:* send <\$username> expect *Password:* send <\$password:>). When the MAX authenticates the connection, the software starts sending PPP packets.

- V.120 terminal adapters and PPP connections

If you configure the V.120 terminal adapter to run the PPP protocol, it handles PAP or CHAP authentication and whatever other PPP or MP features the terminal adapter supports. Typically, the Connection profile requires PAP or CHAP.

- V.120 terminal adapters with PPP turned off

If you configure the V.120 terminal adapter to run without PPP, it does not support PAP or CHAP authentication. If the Connection profile requires PAP or CHAP authentication, the connection fails.

Modem connections

This section shows sample Connection profiles for a terminal server connection established via analog modem. For example, this profile uses only the required parameters for authenticating a terminal server modem connection:

```
Ethernet
  Connections
    Station=uttam
    Active=Yes
    Encaps=PPP
    Encaps options...
      Recv PW=localpw
```

For details on these parameters, see [Understanding the PPP parameters](#).

The next profile shows optional parameters for bringing down the terminal server connection after a specified amount of idle time:

```
Ethernet
  Connections
    Station=uttam
    Active=Yes
    Encaps=PPP
    Encaps options...
      Recv PW=localpw
    Session options...
      TS Idle Mode=Input/Output
      TS Idle=60
```

See [Connection profile Session options](#) and [Configuring single-channel PPP connections](#).

V.120 terminal adapter connections

V.120 terminal adapters (also known as ISDN modems) are asynchronous devices that use CCITT V.120 encapsulation. These are the values that appear to work best for V.120 operation:

- Maximum information field size for send and receive packets = 260 bytes
- Maximum number of retransmissions (N200) = 3
- Logical link ID (LLI) = 256
- Idle timer (T203) = 30 seconds
- Maximum number of outstanding frames = 7

- Modulo = 128
- Retransmission timer (T200) = 1.5 seconds
- Types of frames accepted = UI, I. (I-type frames are recommended.)
- Call placement: The MAX can receive V.120 calls, but cannot place them.

Note: If the connection uses PAP or CHAP authentication, the ISDN terminal adapter should be configured for async-to-sync conversion. In this case, V.120 encapsulation is not required in the Connection profile. See [Connection authentication issues](#).

The V.120 device must be correctly configured to place calls to the MAX. The settings required for compatible operation of a V.120 device and the MAX are listed below. Refer to the V.120 manual for information on entering these settings.

- V.120 maximum transmit frame size = 260 bytes
- V.120 maximum receive frame size = 260 bytes
- Logical link ID = 256
- Modulo = 128
- Line channel speed = Select 56K if the MAX accepts calls from the V.120 device on a T1 line, or if you are not sure that you have 64-kbps channel speed end-to-end.

After checking the configuration of the V.120 device, make sure you enable V.120 calls in the Answer profile:

```

Ethernet
  Answer
    Encaps...
      V.120=Yes

    V.120 options...
      Frame Length=260

```

To configure a connection that uses a V.120 terminal adapter, create a Connection profile such as this:

```

Ethernet
  Connections
    Station=tommy
    Active=Yes
    Encaps=PPP
    Encaps options...
      Recv PW=localpw
    Session options...
      TS Idle Mode=Input
      TS Idle=60

```

See [Connection profile Session options](#) and [Configuring single-channel PPP connections](#).

TCP-clear connections

Username Login

In most cases, use TCP-clear to transport custom-encapsulated data understood by the host and the caller. For example, America Online customers who log in from an ISDN device typically use a TCP-clear connection to *tunnel* their proprietary encapsulation method in raw TCP/IP packets, as shown in [Figure 3-13](#).



Figure 3-13. A TCP-clear connection

Note: A TCP-clear connection is host-to-host: as soon as the MAX authenticates the connection, a TCP connection is established to the host specified in the Connection profile.

First, make sure you enable TCP-clear calls in the Answer profile:

```
Ethernet
  Answer
    Encaps...
      TCP-CLEAR=Yes
```

To configure a TCP-clear connection:

```
Ethernet
  Connections
    Station=richard
    Active=Yes
    Encaps=TCP-CLEAR
    Encaps options...
      Recv PW=localpw
      Login Host=techpubs
      Login Port=23
    Session options...
      TS Idle Mode=Input
      TS Idle=60
```

If you configure DNS, you can enter a hostname for the Login host (such as the *techpubs* example above). Otherwise, specify the host's IP address. The port number is the TCP port on the host to use for the connection. A port number of zero means *any port*.

See also [Connection profile Session options](#) and [TCP Modem connections \(DNIS Login\)](#).

TCP Modem connections (DNIS Login)

This feature allows you to enable or disable TCP modem access to the MAX as well as configure the default port for TCP modem access.

The MAX treats a TCP-encapsulated call between two MAX units over an asynchronous line as if it were a modem. This is referred to as TCP modem. Previously, the MAX would always allow such calls. Now, you can disable TCP modem connections to the MAX. In addition, you can change the TCP port used for these connections. Previously the default port for TCP modem access was 150. It is now 6150.

[Figure 3-14](#) illustrates an example TCP modem setup. A user dialing into an ISP first connects to telephone switch, which then establishes a connection to a MAX. This local MAX has a TCP-Clear connection configured in RADIUS to a MAX at an ISP. Typically, this connection is over Frame Relay. The remote user appears to be directly connected to the ISP MAX; the local MAX merely passes the data through. The ISP MAX typically authenticates remote users.

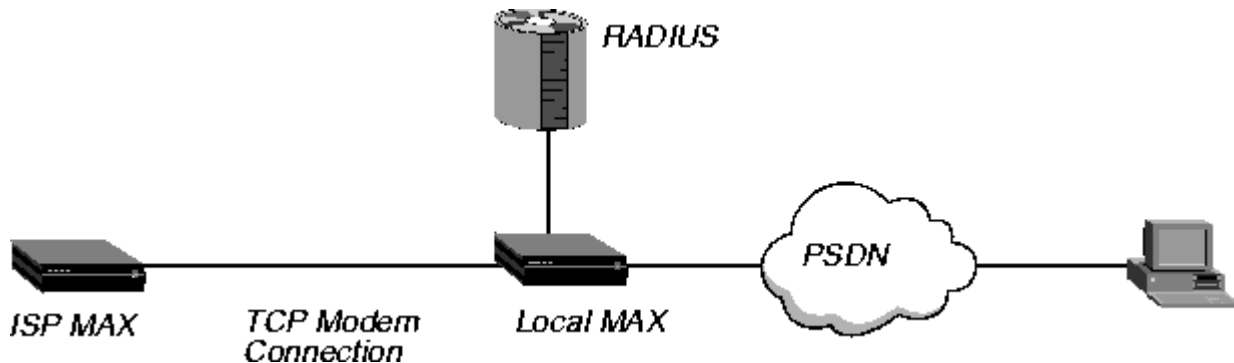


Figure 3-14. Sample TCP modem connection

For more information about TCP modem connections, refer to the *RADIUS Guide*.

Enabling terminal server calls and setting security

The terminal server can provide a command-line interface or a menu of Telnet hosts that dial-in users can log into. Or, you can configure an *immediate mode* to automatically present the user with a login prompt to a host, bypassing the terminal server interface altogether.

- Terminal mode

Users who have access to the command-line can see information about your network by using administrative terminal server commands. You can also allow them to initiate their own Telnet, Rlogin, or TCP connections to hosts.

- Immediate mode

In immediate mode, the terminal server initiates a Telnet, Rlogin, or TCP connection to one specified host without every giving the dial-in user with a choice. The login and password entered by the user will be those required by the host, not by the terminal server.

- Menu mode

The menu interface lists up to four local hosts. Users select a hostname to initiate a Telnet session to that host. The menu interface with four hosts looks like this:

```
Up to 16 lines of up to 80 characters each
will be accepted. Long lines will be truncated.
```

Additional lines will be ignored

1. host1.abc.com
2. host2.abc.com
3. host3.abc.com
4. host4.abc.com

Enter Selection (1-4, q)

To configure the terminal server mode:

1. Open Ethernet > Mod Config > TServ Options.
2. Enable incoming terminal server calls.

```

Ethernet
  Mod Config
    TServ options...
      TS Enabled=Yes

```

3. Password-protect terminal mode.

```

Passwd=tspassword
Security=Partial

```

4. Close the Ethernet profile.

The terminal server security mode can be none, partial, or full. The setting determines whether users are prompted for a login name and password before entering the terminal server. Its meaning is partly dependent on whether users log into menu mode or terminal mode, and whether they are allowed to toggle between these two modes.

- If you set security mode to none, users are not prompted for a login name and password.
- If you set security mode to partial, users are prompted for a name and password only when entering terminal mode, not for menu mode.
- If you set security mode to full, users are prompted for a name and password upon initial login, no matter what interface appears.

Understanding modem parameters

Calls from analog modems are directed first to the MAX digital modems, where the connection must be negotiated before being directed to by the terminal server software.

To affect how the modem negotiation and data packetizing occurs, you can set the following parameters:

```

Ethernet
  Mod Config

```

```
TServ options...
V42/MNP=Will
Max Baud=33600
MDM Trn Level=-13
Cell First=No
Cell Level=-18
7-Even=No
Packet Wait Time=2
Packet characters=0
```

This section provides background information on the modem configuration parameters.

Digital modem error control

The digital modems negotiate LAPM/MNP error control with the analog modem at the other end of the connection according to how this parameter is set. It can request LAPM/MNP and accept the call anyway if it is not provided, request it and drop the call if it is not provided, or not use LAPM/MNP error control at all.

Setting a maximum baud rate

Typically, the digital modems start with the highest possible baud rate (3360) and negotiate down to the rate accepted by the far end modem. You can adjust the maximum rate to bypass some of the negotiation cycles, provided that no inbound calls use a baud rate higher than what you specify here.

Specifying the default modem transmit level

When a modem calls the MAX, the unit attempts to connect at the transmit attenuate level you specify. This is the amount of attenuation in decibels the MAX should apply to the line, causing the line to lose power when the received signal is too strong. Generally, you do not need to change the transmit level. However, when the carrier is aware of line problems or irregularities, you may need to alter the modem's transmit level.

Rockwell modem code has been modified to make the transmit level programmable, so users can change the default setting for their specific connection. Transmitting at higher level helps certain modems with near-end-echo problems.

Attempting cellular connections first

The MAX supports cellular modem calls. The user can also set the gain level of the modem for cellular communication.

Cell First determines whether the MAX first attempts cellular modem or conventional modem negotiation when answering incoming calls. If the first negotiation fails, the MAX attempts the other negotiation.

Cell Level determines the gain level of the cellular modem.

7-bit even parity

The MAX does not use 7-bit even parity on outbound data unless you set this parameter to Yes. Most applications do not use 7-bit even parameter.

Support for specialized applications on modem connections

Packet Wait time specifies the maximum amount of time in milliseconds that any received data can wait before being passed up the protocol stack for encapsulation.

Packet Characters specifies the minimum number of bytes of received data that should accumulate before the data is passed up the protocol stack for encapsulation.

Note: Be sure to take into account modem speeds when calculating these values.

Example

To sets the maximum negotiable baud rate for incoming calls from analog

1. Open Ethernet > Mod C0.0Cg > TServ Options.
2. Set the maximum negotiable baud rate to 26400:

```

Ethernet
  Mod C0.0Cg
    TServ options...
      Max Baud=26400

```

3. Close the Ethernet profile.

C0.0Cguring terminal

When a user communicates with the terminal server itself (rather than a host in immediate the MAX establishes a session between the remote user's PC and the terminal server. To affect how the MAX establishes a session and what commands are available to the user, you can set these parameters:

```

Ethernet
  Mod C0.0Cg
    TServ options...
      Silent=No
      Clr Scrn=Yes
      Passwd=
      Banner=** Ascend Terminal Server **
      Login Prompt=Login:
      Prompt Format=Yes
      Passwd Prompt=Password:
      Prompt = ascend%
      Term Type= vt100
      Login Timeout= 60
      ...
      Telnet=Yes
      Rlogin=No
      Def Telnet=Yes
      Clear Call=No
      Telnet
      Local Echo=No
      Buffer Chars=Yes
      ...
      3rd Prompt=
      3rd Prompt Seq=N/A
      IP Addr Msg=N/A

```

Understanding the terminal mode parameters

This section provides background information on the terminal mode configuration parameters.

Controlling how the screen appears to users while the connection is set up

Silent determines whether status messages appear or not while the connection is being established. Clr Scrn can be set to clear the screen when the MAX establishes a connection.

Setting the terminal mode password

Passwd specifies a password up to 15 characters. This is the password terminal server users will be prompted for when establishing a connection to the terminal server itself.

Setting the login banner and prompts

When the MAX establishes the terminal server session, the system displays the banner "***Ascend Terminal Server ***" or a different banner you have configured.

Login Prompt and Password Prompt specify what the user sees while logging in, by default:

Login:

Password:

The Login prompt can be up to 80 characters and consist of more than one line if Prompt Format is set to Yes. To specify a multi-line prompt, set Prompt Format to Yes and use "\n" to represent a carriage return/line feed and "\t" to represent a tab.

Specifying the command-line prompt

Prompt specifies the command-line prompt, which by default is:

```
ascend%
```

Be sure to include a trailing space if desired.

Another login prompt for RADIUS-authenticated logins

The 3rd Prompt is another login prompt, and 3rd Prompt Seq specifies whether the third prompt appears before or after the regular terminal server login prompts.

For RADIUS-authenticated logins, some servers require the third prompt and that it appears last in the login sequence. This is the default setting.

Some ISPs use a terminal server that follows a login sequence different from that used by Ascend, for example, that includes a menu selection prior to login. Administrators at those sites can configure 3rd prompt to appear first to mimic that terminal server and retain compatibility with client software in use by subscribers. See the *MAX Reference Guide* for more details.

Affecting Telnet and Rlogin session defaults

You can enable or disable the use of the RLOGIN, and TELNET commands at the terminal server

command-line. When they are enabled, you can set parameters to affect session defaults. (Users can modify some of these default values on the command line.)

Term Type specifies a default terminal type, such as the vt100.

Clear Call specifies whether when the user terminates a Telnet or Rlogin session, the connection terminates as well.

Buffer Chars determines whether the terminal server buffers input characters for 100 milliseconds before forwarding them to the host, or sends the characters as received.

Telnet Mode specifies whether binary, ascii, or transparent mode is the default for Telnet sessions. Def Telnet instructs the terminal server to interpret unknown command strings as the name of a host for a Telnet session. Local Echo sets a global default for echoing characters locally, which can be changed for an individual session within Telnet.

Displaying a message when informing users of their address

The terminal server displays "Your IP address is..." (followed by the assigned address). You can change that default message.

Specifying a login timeout

The MAX disconnects users if they have not completed logging in when the number of seconds set in the Login Timeout field has elapsed. A user has the total number of seconds indicated in the Login Timeout field to attempt a successful login. This means that the timer begins when the login prompt appears on the terminal server screen, and continues (is not reset) when the user makes unsuccessful login attempts.

Example terminal mode configuration

This example configures the password and makes the Rlogin option available to dial-in users. Note that you enable the Telnet option by default.

1. Open Ethernet > Mod Config > TServ Options.
2. Specify the terminal server password.
3. Configure a multi-line login prompt.

```
Ethernet
  Mod Config
    TServ options...
      Login Prompt=Welcome to Ascend Remote Server\nEnter y
      Prompt Format=Yes
```

4. Enable the use of the Rlogin command in terminal mode.

```
Passwd=tspasswd
Rlogin=Yes
```

5. Close the Ethernet profile.

Configuring immediate mode

When dial-in calls are directed immediately to a host, the MAX establishes a session between the remote user's PC and that host via Rlogin, Telnet, or TCP. To affect how the MAX establishes a session, you can set these parameters:

```
Mod Config
  TServ options...
    Immed Service=None
    Immed Host=N/A
    Immed Port=N/A
    Telnet Host Auth=No
```

Understanding the immediate mode parameters

This section provides background information on the immediate mode configuration parameters.

Specifying the type of immediate service

Immed Service enables a particular type of service for establishing an immediate host connection for dial-in users. You can specify Telnet, Raw-TCP, Rlogin, or X25-PAD. For details on X.25, see [Chapter 6, Configuring X.25](#).

For Telnet service, you can set the Telnet Host Auth parameter to bypass the terminal server authentication and go right to a Telnet login prompt.

The host and the port on which the connection is made

Specify the hostname or address to which users will be connected in terminal server immediate mode. You can also specify a TCP port number to use for the connections.

Example immediate mode configuration

This example configures immediate Telnet service that relies on the Telnet host for authentication.

1. Open Ethernet > Mod Config > TServ Options.
2. Set the Immed Service parameter to Telnet.
3. Specify the name or IP address of the Telnet host.
4. If appropriate, specify the TCP port to use on the Telnet host.
5. Set the Telnet Host Auth parameter to Yes.

```
Ethernet
  Mod Config
    TServ options...
      Immed Service=Telnet
      Immed Host=host1.abc.com
      Immed Port=23
      Telnet Host Auth=Yes
```

6. Close the Ethernet profile.

Configuring menu mode

You can set up the terminal server to display a menu of up to four Telnet hosts that dial-in users can select for logging in. You can set up menu mode with these parameters:

```
Ethernet
  Mod Config
    TServ options...
      Initial Scrn=Cmd
      Toggle Scrn=No
      Remote Conf=No
      Host #1 Addr=0.0.0.0
      Host #1 Text=
      Host #2 Addr=0.0.0.0
      Host #2 Text=
      Host #3 Addr=0.0.0.0
      Host #3 Text=
      Host #4 Addr=0.0.0.0
      Host #4 Text=
```

Understanding the menu mode parameters

This section provides background information on the menu mode configuration parameters.

Specifying menu mode as the initial interface

Initial Scrn determines whether the terminal server brings up a menu interface first for interactive users initiating connections. Depending on the Toggle Scrn setting, users may be able to switch to the command-line interface from menu mode by pressing the zero key. The Security setting determines whether a login and password will be required when entering the menu interface.

Obtaining the menu from RADIUS

Remote Conf specifies that the terminal server menu and list of hosts will be obtained from a RADIUS server.

Specifying the hostnames and addresses of up to four Telnet hosts

The Host and Text parameters expect an IP address and hostname, respectively, for up to four Telnet hosts.

Example menu mode configuration

This example allows the menu to appear at login and specifies four hosts; this example also cannot enter the command-line.

1. Open Ethernet > Mod Config > TServ Options.
2. Specify that dial-in users are in menu mode initially.

```
Ethernet
  Mod Config
    TServ options...
      Initial Scrn=Menu
```

3. Specify the IP addresses and hostnames of up to four hosts appearing in the menu.

```
Ethernet
```

```
Mod Config
  TServ options...
    Host #1 Addr=10.2.3.4
    Host #1 Text=host1.abc.com
    Host #2 Addr=10.2.3.57
    Host #2 Text=host2.abc.com
    Host #3 Addr=10.2.3.121
    Host #3 Text=host3.abc.com
    Host #4 Addr=10.2.3.224
    Host #4 Text=host4.abc.com
```

See [Enabling terminal server calls and setting security](#) for an example menu. Dial-in users will be able to Telnet to these hosts by selecting the hostname or IP address.

4. Close the Ethernet profile.

Configuring PPP mode

Users who are logged into the terminal server in terminal mode can invoke an async PPP session by using the PPP command, initiating PPP mode. Or, even if users do not have access to the command line, they can begin an async PPP session from an application such as Netscape Navigator or Microsoft Explorer. For example, if a user initiates a session from Windows 95, which has a resident TCP/IP stack, the async PPP session can begin immediately without entering the terminal server interface. These parameters configure PPP mode:

```
Ethernet
  Mod Config
    TServ options...
      PPP=No
      ...
      PPP Delay=5
      PPP Direct=No
      PPP Info=mode
```

Understanding the PPP mode parameters

This section provides some background information on the PPP mode configuration parameters.

Enabling PPP mode

You can prevent users from initiating PPP sessions by setting PPP to No.

PPP delay

PPP Delay specifies the number of seconds the terminal server waits before transitioning to packet-mode processing.

PPP direct

PPP Direct specifies whether to start PPP negotiation immediately after a user enters the PPP command in the terminal server interface, or to wait to receive a PPP packet from an application. (Some applications expect to receive a packet first.)

The message informing users they are in PPP mode

You can specify that no message appear, or choose between *PPP Mode* and *PPP Session*.

Example PPP configuration

This example enables PPP direct mode:

1. Open Ethernet > Mod Config > TServ Options.
2. Enable the use of the PPP command in terminal mode.
3. Enable PPP direct negotiation.

```

Ethernet
  Mod Config
    TServ options...
      PPP=Yes
      PPP Direct=Yes

```

4. Close the Ethernet profile.

Configuring SLIP mode

If you enable SLIP mode in the terminal server, users can initiate a SLIP session and then run an application such as FTP in that session. SLIP mode configuration uses these parameters.

```

Ethernet
  Mod Config
    TServ options...
      SLIP=No
      SLIP BOOTP=N/A
      IP Netmask Msg
      IP Gateway Adrs Msg
      Slip Info

```

Understanding the SLIP mode parameters

This section provides some background information on the SLIP mode configuration parameters.

Enabling SLIP (Serial Line IP) sessions

You can disable or enable SLIP sessions by using the SLIP parameter.

Allowing users to obtain an IP address from a BOOTP server

SLIP BOOTP enables the terminal server to respond to BOOTP within SLIP sessions. If it is enabled, a user who initiates a SLIP session can get an IP address from the designated IP address pool via BOOTP. If it is disabled, the terminal server does not run BOOTP; instead, the user is prompted to accept an IP address at the start of the SLIP session

IP Netmask Msg

This parameter enables you to specify text message. You can enter up to 64 characters. The default is `Netmask:` (IP Netmask Msg does not apply unless you set SLIP Info to Advanced.)

IP Gateway Adrs Msg

This parameter specifies the text the MAX displays before the MAX IP address field in the SLIP session startup message. You can enter up to 64 characters. The default is `Netmask: (IP Netmask Msg does not apply unless you set SLIP Info to Advanced.)`

SLIP Info

- **Basic:** Enables the MAX to report the SLIP user's IP address and the Maximum Transmission Unit (MTU).
- **Advanced:** Enables the MAX to report the SLIP user's IP address, the MTU, the Netmask, and the Gateway to SLIP users. Note that the gateway is the MAX unit's IP address.

Example SLIP configuration

This example enables SLIP sessions and specifies that the terminal server will respond to BOOTP in SLIP sessions:

1. Open `Ethernet > Mod Config > TServ Options`.
2. Enable the use of the SLIP command: `SLIP=Yes`.
3. Enable the use of BOOTP in SLIP sessions: `Slip Bootp=Yes`.

```

Ethernet
  Mod Config
    TServ options...
      SLIP=Yes
      SLIP BOOTP=Yes

```

4. Close the Ethernet profile.

Configuring dialout options

The terminal server has access to the MAX digital modems, and can be used to enable users on the local network to dialout using those modems. You can enable local dialout using these parameters:

```

Ethernet
  Mod Config
    TServ options...
      Modem dialout=No
      Immediate Modem=N/A
      Imm. Modem port=N/A
      Imm. Modem Pwd=N/A

```

Understanding the dialout parameters

This section provides some background information on the dialout configuration parameters.

Enabling dialout

If you enable Modem dialout, local users can connect to the terminal server via Telnet and then issue AT commands to the modem as if connected locally to the modem's asynchronous port.

Enabling direct access dialout

If you enable Immediate Modem service, users telnet to a particular port on the MAX and the MAX provides Immediate Modem dialout service. The port number configured for Immediate Modem dialout tells the MAX that all telnet sessions initiated with that port number want modem access. Immediate Modem service has its own password (up to 64 characters. If the Imm. Modem Pwd is non-null, users will be prompted for a password before being allowed access to a modem.

How the modem dialout works

If you enable dialout (not Immediate Modem), users can access a modem as follows: Telnet to the MAX from a workstation. For example:

```
Telnet max01
```

1. Invoke the terminal server command-line interface (System > Sys Diag > Term Serv).

Users see the terminal server prompt, for example:

```
ascend%
```

2. Enter the terminal server Open command.

```
ascend% open
```

Without an argument, the Open command sets up a virtual connection to the first available digital modem. Alternatively, the user can specify a particular modem by including its slot and item number as an argument to the command; for example:

```
ascend% open 7:1
```

3. Use the standard Rockwell AT commands to dial out on the modem, just as if using a modem connected directly to a workstation. For example:

```
ATDT 1V1 ^M
```

4. To suspend a virtual connection to a digital modem and return to the terminal server prompt, press Ctrl-C three times.

```
^C^C^C
```

5. To resume the suspended virtual connection:

```
ascend% resume
```

6. To terminate a virtual connection:

```
ascend% close
```

How immediate modem works

Immediate Modem enables users to access a modem directly by Telnetting to the specified port. For example, users can access a modem as follows:

1. Telnet to the MAX from a workstation, specifying the immediate modem port number on the command line. For example:

```
Telnet max01 5000
```

Where *max01* is the system name of the MAX and *5000* is the Immediate Modem Port.

2. Use the standard Rockwell AT commands to dial out on the modem, just as if using a modem connected directly to a workstation. For example:

```
ATDT 1V1 ^M
```

3. Press Ctrl-C to terminate the connection.

Example dialout configuration

This example enables direct access on port 5000:

1. Open Ethernet > Mod Config > TServ Options.
2. Enable the use of the modem dialout.
3. Enable the direct access (immediate modem) feature.

```
Ethernet
  Mod Config
    TServ options...
      Modem dialout=Yes
      Immediate Modem=Yes
```

4. Specify on which port the immediate modem feature will function.
5. Specify a password for modem access.

```
Ethernet
  Mod Config
    TServ options...
      Imm. Modem port=5000
      Imm. Modem Pwd=dialoutpwd
```

6. Close the Ethernet profile.

[HOME](#) [CONTENTS](#) [PREVIOUS](#) [NEXT](#) [INDEX](#)

techpubs@eng.ascend.com

Copyright © 1998, Ascend Communications, Inc. All rights reserved.