

Release Note

Software Release 2.3.2

For AR410 Branch Office Routers and AR700 Series Routers

Introduction	2
Hardware Platforms	2
AR410 Hardware Platform	2
Expansion options	4
Software Features - All Models	5
Asynchronous Call Control	5
Compression and Encryption Services	5
Firewall	6
Frame Relay	7
Interfaces	9
IPv6	10
Telnet and Ping to IPv6 Link-local Addresses	12
Operations	13
Public Key Infrastructure (PKI)	14
Trigger Facility	16
Software Features - AR700 Series Routers	16
AR Router GUI	16
Software Features - AR410 Branch Office Routers	17
Chapter 3: Interfaces	17
Chapter 9: Internet Protocol (IP)	19
Chapter 2: Switching	20
Errata	22
IPv6 Filters	22

Introduction

Allied Telesyn International announces the release of Software Release 2.3.2 on the AR410, AR720, and AR740 routers. This release note describes software features that are new since Software Release 2.3.1. It should be read in conjunction with the Quick Install Guide, Quick Start Guide or User Guide, Hardware Reference and Software Reference for your router or switch. These documents can be found on the Documentation and Tools CD-ROM packaged with your router, or on the support site at:
www.alliedtelesyn.co.nz/documentation/documentation.html.

The main new features in Software Release 2.3.2 (document number C875-59027-00 REV A) are:

- Support for the AT-AR410 Router.
- Support for the AT-AR011V2 ECMAC V2, Compression/Encryption MAC card for the AT-AR410 Router.
- The AR Router GUI for the AT-AR700 Series Routers provides enhanced management, troubleshooting, and configuration options.



WARNING: *Information in this document is subject to change without notice and does not represent a commitment on the part of Allied Telesyn International. While every effort has been made to ensure that the information contained within this document and the features and changes described are accurate, Allied Telesyn International can not accept any type of liability for errors in, or omissions arising from the use of this information.*

Hardware Platforms

Software Release 2.3.2 is available for the following hardware platforms:

- AR410 Router (not yet released).
- AR720 Router.
- AR740 Router.

AR410 Hardware Platform

The AT-AR400 series is a new series of routers. This series is currently represented by the AT-AR410 router, with further models under development. AR400 routers are high-performance broadband routers featuring multiple 10BASE-T/100BASE-TX ports and VLAN support.

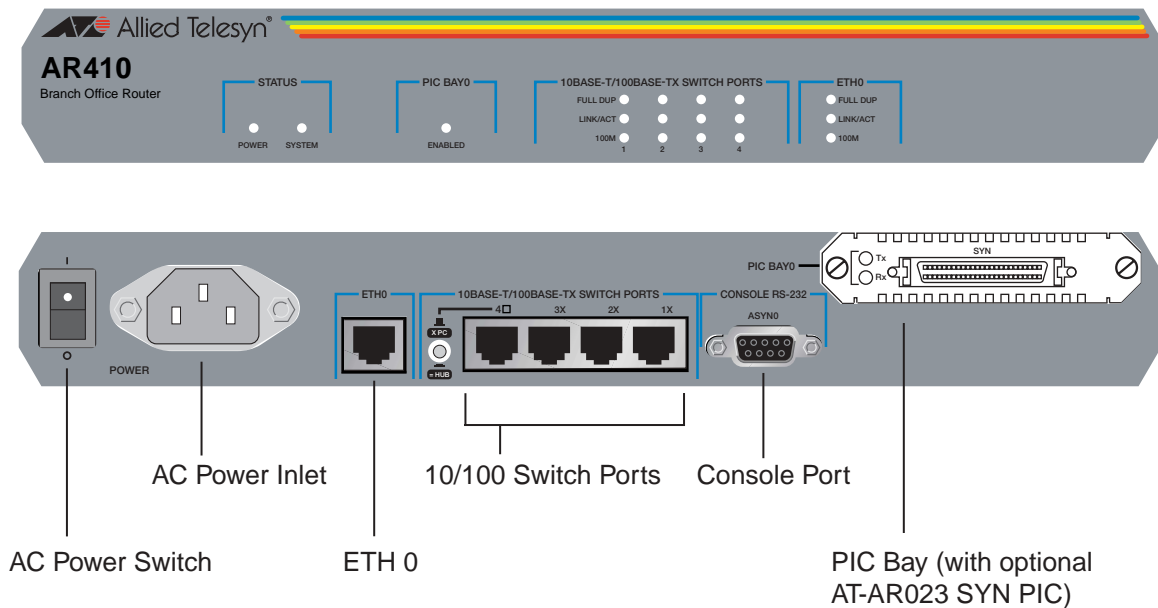
PIC bays add expansion flexibility by allowing the installation of PIC cards, which are available with ISDN (PRI E1/T1, BRI S/T, or BRI U), 10BASE-T, synchronous, or asynchronous ports.

Main features of the AT-AR410 router are:

- 66 MHz RISC processor.
- 16 MBytes of synchronous DRAM.
- 8 MBytes of FLASH memory (1MByte protected boot code area, 7 MByte available for storing files: enough for two full software releases).

- 4 x 10/100 Mbps full duplex Ethernet LAN switch ports.
- 1 x 10/100 Mbps full duplex Ethernet WAN (ETH0) port.
- 1 RS-232 asynchronous (ASYN0) configuration port (maximum speed 115200 bps).
- 1 PIC bay for an optional Port Interface Card.
- 1 MAC slot for an optional MAC compression/encryption card.
- Universal AC power supply (100-240 VAC and 50–60Hz).

Figure 1: Front and rear panels of the AT-AR410 Series router.



There are no user-selectable jumpers or DIP switches on AR400 Series routers.

The RS-232 asynchronous serial port (ASYN 0) can be used as a general purpose port for terminals, printers or modems. The default communications settings are:

- 9600 bps
- 8 data bits
- 1 stop bit
- no parity
- hardware flow control.

Power Supply

The AT-AR410 has a universal AC input connector and a power switch on its rear panel. The router requires a power input of 100-240 VAC and 50–60Hz.



Some interfaces that may be installed in the router are not transformer isolated. This means they will be referenced to the frame ground of the equipment and may be damaged if connected to an interface on another piece of equipment which is at a different ground potential.

LEDs and what they mean

Functions of the AR410's LEDs are shown in Table 1 on page 4. Additional LEDs may be present if a PIC is installed. Functions of PIC LEDs are described in the *Port Interface Card Hardware Reference*.

Table 1: AR410 System LEDs

LED	State	Function
Power	Green	The router is receiving power and the power switch is in the ON position
System	Amber	Lit briefly during power-up. If it stays on appears at other times, there may be a malfunction.
	Off	Normal operation
Enabled (PIC Bay 0)	Green	A PIC card is correctly installed and has been detected by the router
	Off	No card is installed
Full	Green	The corresponding port is operating at full-duplex
	Off	The corresponding port is operating at half-duplex
Link/ACT	Green	A link has been established through the corresponding port
	Flashing	Data is being transmitted through the corresponding port
	Off	No link is present through the corresponding port
100M	Green	The corresponding port is operating at 100Mbps
	Off	The corresponding port is operating at 10Mbps

Expansion options

The PIC bay can accommodate any of the following PICs:

- AT-AR020 PRI E1/T1 PIC, one Primary Rate E1/T1 port.
- AT-AR021(S) BRI-S/T PIC, one Basic Rate ISDN S/T port.
- AT-AR021(U) BRI-U PIC, one Basic Rate ISDN U port.
- AT-AR022 ETH PIC (legacy), one Ethernet LAN AUI/10BASE-T port. (Availability may depend on region.)
- AT-AR023 SYN PIC, one Synchronous port with universal 50-way AMPLIMITE connector.
- AT-AR024 ASYN4 PIC, four Asynchronous ports with RJ-45 connectors.

The MAC slot can accommodate any one of the following MAC cards:

- AT-AR010 EMAC, Encryption MAC card.
- AT-AR011 ECMAC, Compression/Encryption MAC card.(Availability may depend on region.)
- AT-AR011V2 ECMAC V2, Compression/Encryption MAC card.(Availability may depend on region.)
- AT-AR012 CMAC, Compression MAC card.



MACs should only be installed by authorised service personnel. Unauthorised opening of the router lid may cause danger of injury from electric shock, damage to the router, and invalidation of the product warranty.

Software Features - All Models

The following features are available on all routers supported by this release, unless otherwise stated:

Asynchronous Call Control

Call definitions provide the basic mechanism for controlling access to asynchronous services provided by or through the router. Each port used for an asynchronous service must be associated with at least one call definition. With Software Release 2.3.2, a port may be associated with multiple call definitions.

Compression and Encryption Services

SHOW ENCO command

The SHOW ENCO command has been enhanced to display output from a router with a MAC card installed. There is new example output and an additional parameter has been added to the command (see Figure 2 on page 6 and Table 2 on page 6).

Figure 2: Example output from the SHOW ENCO command for a router with a MAC card installed.

```

ENCO Module Configuration

Hardware ..... MAC
Lowest valid channel ..... 1
Highest valid channel ..... 511
Compression Statistics Enabled ..... FALSE
Diffie Hellman Priority ..... HIGH

SW Processes available
  RSA - RSA Encryption
  DH  - Diffie Hellman

MAC Processes available
  DES - DES Encryption
  3DES - Triple DES Encryption
  STAC - Stac Compression
  HMAC - Message Digest
  
```

Table 2: New parameter displayed in the output of the SHOW ENCO command.

Parameter	Meaning
MAC Processes available	A list of the MAC-based processes available to the ENCO module for processing user data packets; one or more of "NONE", "DES", "3DES", "STAC", or "HMAC".

Firewall

HTTP Proxy

The performance of the HTTP proxy has been enhanced.

HTTP Proxy Logging

URL requests and cookies that are denied are logged by the firewall and for each denial an entry appears in the list of recent firewall “deny events”. To display this list, use the command:

```
SHOW FIREWALL EVENT=DENY
```

If the event is for a denied URL request then up to 29 characters of the requested URL are displayed. If the event is for a blocked cookie then up to 18 characters of the name of the domain trying to set the cookie are displayed.

An entry similar to that for the SHOW FIREWALL EVENT command is also placed in the router log. To view this entry use the command:

```
SHOW LOG
```

The firewall can be configured to send notification of “deny events”.

ADD FIREWALL POLICY HTTPFILTER command

In the command description of the ADD FIREWALL POLICY HTTPFILTER command the http filter file is specified as a .txt but the example uses a .htp, which the router/switch will not let you create. The correct example is below:

To add the contents of the file banned.txt to the HTTP filter of firewall policy zone1 for filtering outbound HTTP sessions, use the command:

```
ADD FIREWALL POLICY=zone1 HTTPFILTER=banned.txt
```

Frame Relay

SHOW FRAMERELAY command

The COUNTER parameter of the SHOW FRAMERELAY command has been modified. There is new example output and ten new parameters have been added to display general configuration counters and counters from the interface MIB and the Frame Relay MIB for the Frame Relay interface and each DLC (see Figure 3 on page 8 and Table 3 on page 9).

Figure 3: .Example output from the SHOW FRAMERELAY COUNTER command.

```

Interface Counter:

fr0          401 seconds      Last change at:      10 seconds
Interface Counter
  ifInOctets          935      ifOutOctets          550
  ifInUcastPkts       0        ifOutUcastPkts       41
  ifInNUcastPkts      0        ifOutNUcastPkts      0
  ifInDiscards        0        ifOutDiscards        0
  ifInErrors          0        ifOutErrors          0
  ifInUnknownProtos  0        ifOutQLen            0

  ifInNullCircuits    0        ifOutNullCircuits    0
  ifNoHLReceiveFunction 0        ifBadPackets         0
  ifGoodConfiguration 2        cllmMessagesReceived 19
  shortFrames         0        lostTxReadyInds      0
  inLMIStatus         33       outLMIStatusEng       33
  inLMIFullStatus     7        outLMIFullStatusEng  7

DLCI: 0
  State              Active
  Created            6        Last Changed         6
  statusActive       0        statusInactive       0
  inOctets           555       outOctets            520
  inFrames           40        outFrames            40
  BECNs Received    0        FECNs Received       0
  notEnabled         0        ECPNotOpen           0
  congestionDiscards 0
  cllmCongestionMild 0        cllmCongestionSevere 0
  cllmDiscarding    0        cllmNetworkTrouble  0

DLCI: 21
  State              Inactive
  Created            1000      Last Changed         37000
  statusActive       6        statusInactive       1
  inOctets           0        outOctets            30
  inFrames           0        outFrames            1
  BECNs Received    0        FECNs Received       0
  notEnabled         0        ECPNotOpen           0
  congestionDiscards 0
  cllmCongestionMild 4        cllmCongestionSevere 4
  cllmDiscarding    11       cllmNetworkTrouble  0

TOTAL
  inOctets           555       outOctets            550
  inFrames           40        outFrames            41
  BECNs Received    0        FECNs Received       0

General Counter:
  configBadInstance  0        configBadProtocol    0
  configUnusedInstance 0        dataReqNullFrame     0
  dataReqBadInstance 0        compEventBadUserId   0
  encryptEventBadUserId 0        encrStarEventBadUserId 0
  idleBadInstance    0        idleUnusedInterface  0
  interRxCompBadInst 0

```

Table 3: New parameters displayed in the output of the SHOW FRAMERELAY COUNTER command .

Parameter	Meaning
inLMISatus	The number of LMI keep alive status messages received by a Frame Relay interface.
outLMISatusEnq	The number of LMI keep alive status enquiries sent by a Frame Relay interface.
TinLMIFullStatus	The number of LMI full status messages received by a Frame Relay interface.
outLMIFullStatusEnq	The number of LMI full status enquiries sent by a Frame Relay interface.
statusActive	The number of messages received indicating that a circuit is currently active.
statusInactive	The number of messages received indicating that a circuit is currently inactive.
clmCongestionMild	The number of CLLMs received by a circuit indicating mild congestion.
clmCongestionSevere	The number of CLLMs received by a circuit indicating severe congestion.
clmDiscarding	The number of CLLMs received by a circuit indicating discarding.
clmNetworkTrouble	The number of CLLMs received by a circuit indicating network trouble.

Interfaces

SET ASYN command

The LOGIN parameter has been added to the SET ASYN command. The command syntax for the LOGIN parameter is:

```
SET ASYN[=asyn-number] [LOGIN={ON|OFF|YES|NO|TRUE|FALSE}]
```

The LOGIN parameter specifies whether a user is able to log in to the ASYN port and issue commands on the router. If ON is specified users will be able to login to the router. If OFF is specified users will not be able to log in to the router. No command prompt is displayed, no characters will be echoed by the port and any input received by the port will be ignored. The default is ON.

The ATTENTION parameter of the SET ASYN command has been enhanced to include the value *alphabetical control char*. The command syntax for the ATTENTION parameter is:

```
SET ASYN[=asyn-number] [ATTENTION={BREAK|alphabetical control char | ^[ | NONE}]
```

The value *alphabetical control char* is the '^' character followed by any alphabetical character in upper or lower case, e.g. ^A, ^b, ^z.

The ATTENTION parameter specifies the character used to return from an active session (e.g. a Telnet connection) to the router prompt. If '^' with an alphabetical character is specified then the attention character is the [Ctrl] key and the specified alphabetical character key held down simultaneously. Similarly, '^[' means the attention character will be set to the [Ctrl] key with the '[' key. The default is BREAK (the [Break] key) for asynchronous ports, and ^P (the [Ctrl/P] key) for Telnet connections to the router.

IPv6

Static Tunnels

IPv6 subnets can be linked over an IPv4 tunnel by configuring static tunnels. When a tunnel is created, a virtual interface to that tunnel is also created, with an interface name of *virt*. Software Release 2.3.2 expands the functionality of these virtual interfaces, so that they behave in the same way as other physical interfaces.

To link two IPv6 networks through an IPv4 tunnel, first create the tunnel on each router, using the command:

```
ADD IPV6 TUNNEL LOCAL=ipv4add TARGET=ipv4add
```

This command creates a virtual tunnel interface, with an interface name of *virt*, and assigns it a link-local IPv6 address. The first tunnel created is numbered *virt0*, and each succeeding tunnel is given the next available instance number. Each virtual interface behaves as a normal IPv6 interface. The LOCAL parameter is the IPv4 address of the Ethernet, VLAN or PPP interface through which packets will be sent and received on the local router. The TARGET parameter is the IPv4 address of the remote router's Ethernet, VLAN or PPP interface.

The link-local address assigned to the tunnel interface will be of the form:

```
fe80::<local-ipv4-address>:<target-ipv4-address>
```

where *local-ipv4-address* and *target-ipv4-address* are in hexadecimal. For example, if one end of a tunnel is created using the command:

```
ADD IPV6 TUNNEL LOCAL=192.168.1.2 TARGET=192.168.1.1
```

the interface's link-local address will be fe80::c0a8:0102:c0a8:0101.

Once the tunnel has been created, add a route on each interface to direct traffic to the other IPv6 network through the tunnel, using the command:

```
ADD IPV6 ROUTE=ipv6add INT=tunnel-interface
```

where *ipv6add* is the address of the IPv6 network on the other router (not the IPv6 address of the tunnel), and *tunnel-interface* is the interface that the router created when the tunnel was created (e.g. *virt0*).

Tunnel interface names, instances and IPv6 address, and other information can be displayed for all tunnels that are configured on the router, using the command:

```
SHOW IPV6 TUNNEL
```

To display information about a specific tunnel, use the command:

```
SHOW IPV6 INTERFACE=tunnel-interface
```

To delete a tunnel from an interface, use the command:

```
DELETE IPV6 TUNNEL=ipv6add
```

The IPv6 address in the TUNNEL parameter of the DELETE command is the first link-local address of the tunnel (the address that the router assigned to the tunnel when it was created). This address will have the format:

```
fe80::<local-ipv4-address>:<target-ipv4-address>
```

Configuration Example: Tunnelling over an IPv4 network

A tunnel allows IPv6 packets to be routed between IPv6-aware nodes that are only connected by an IPv4 network. The addresses used in this example are shown in Table 4 on page 11, and the configuration is shown in Figure 4 on page 11.

Figure 4: Example of a static tunnel.

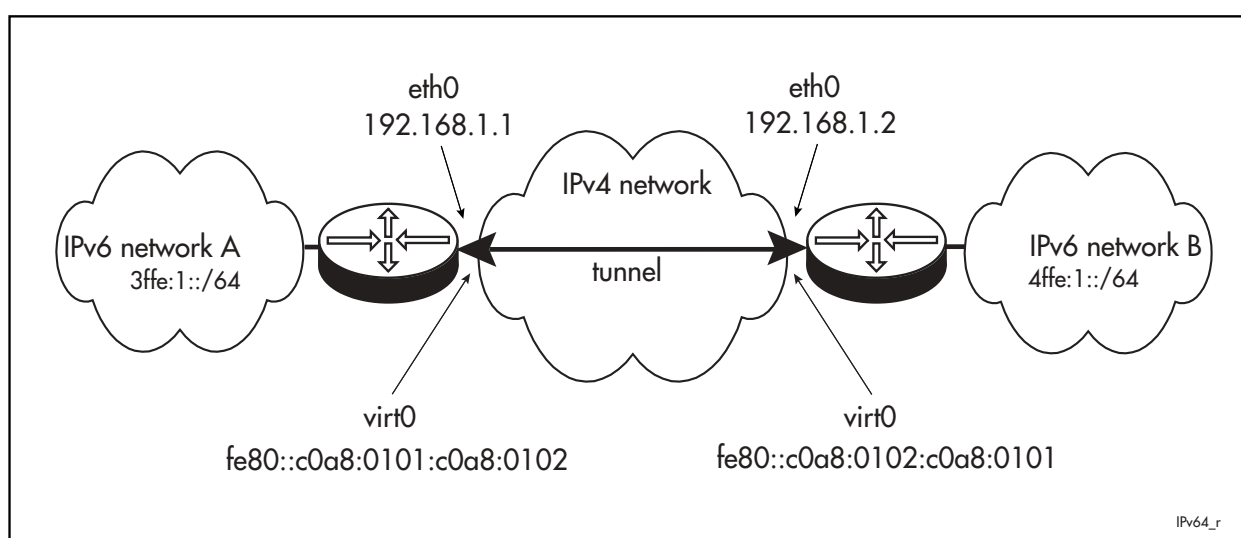
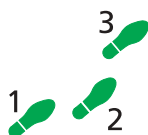


Table 4: IPv4 and IPv6 interfaces and addresses used in this example.

Router	IPv4 address	IPv6 prefix of IPv6 network
A	192.168.1.1	3ffe:1::/64
B	192.168.1.2	4ffe:1::/64



To configure a tunnel:

1. Enable IP and add an interface to each router.

Details on configuring basic IPv4 routing can be found in “A Basic TCP/IP Setup” on page 10-48 of *Chapter 10, Internet Protocol (IP)*.

On router A, use the commands:

```
ENABLE IP
ADD IP INTERFACE=eth0 IPADDRESS=192.168.1.1
```

On router B, use the commands:

```
ENABLE IP
ADD IP INTERFACE=eth0 IPADDRESS=192.168.1.2
```

2. Enable IPv6 on both routers.

Once the IPv4 connection is working correctly, enable IPv6 on each router, using the command:

```
ENABLE IPV6
```

3. Create a tunnel between the two routers.

On router A, use the command:

```
ADD IPV6 TUNNEL LOCAL=192.168.1.1 TARGET=192.168.1.2
```

This command creates an IPv6 interface (virt0 if this is the first tunnel created), with link-local address fe80::c0a8:0101:c0a8:0102.

On router B, use the command:

```
ADD IPV6 TUNNEL LOCAL=192.168.1.2 TARGET=192.168.1.1
```

This command creates an IPv6 interface (virt0 if this is the first tunnel created), with link-local address fe80::c0a8:0102:c0a8:0101.

The LOCAL parameter is the IPv4 address of the router at the local end of the tunnel, so for router A the LOCAL parameter is A's IPv4 address and the TARGET parameter is B's IPv4 address. For router B the LOCAL parameter is B's IPv4 address and the TARGET parameter is A's IPv4 address.

4. Create a route for the tunnel

Add a route on each router, pointing to the IPv6 network on the other router.

On router A, use the command:

```
ADD IPV6 ROUTE=4ffe:1::/64 INT=virt0
```

On router B, use the command:

```
ADD IPV6 ROUTE=3ffe:1::/64 INT=virt0
```

Note that the NEXTHOP parameter is not necessary for a tunnel.

5. Test the routes.

On router A, use the command:

```
PING fe80::c0a8:0101:c0a8:0102%virt0
```

On router B, use the command:

```
PING fe80::c0a8:0102:c0a8:0101%virt0
```

Adding IPv6 Routes

For VIRT interfaces, created when a static tunnel is added, and PPP interfaces, it is not necessary to specify a NEXTHOP parameter in the command:

```
ADD IPV6 ROUTE
```

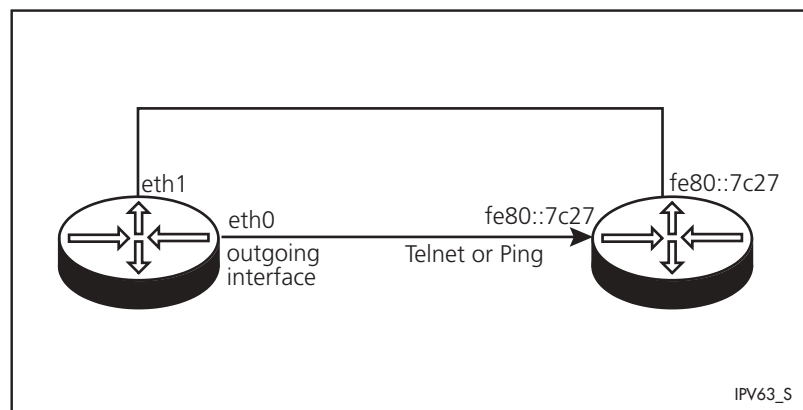
Telnet and Ping to IPv6 Link-local Addresses

When an interface is created, the router will perform stateless address autoconfiguration to assign an IPv6 address to the interface, by adding the interface's MAC address to the reserved IPv6 prefix fe80::. These addresses are only link-local addresses, which are sufficient for communication among

devices on the same link. With Software Release 2.3.2, several interfaces can be given the same link-local address, as specified in RFC 2373 "IP Version 6 Addressing Architecture".

Pinging or Telnetting to an IPv6 link-local address therefore requires interface information as well as the address, because a single link-local address can belong to several interfaces. To Ping or Telnet to a link-local address, specify the interface out which the Ping or Telnet request is sent, as well as the address. This interface is the interface, on the router from which the Telnet request originates, that is connected to the required destination interface (Figure 5 on page 13).

Figure 5: The outgoing interface to specify when Pinging or Telnetting to an IPv6 link-local address.



The Telnet syntax is:

```
TELNET ipv6-address%interface
```

For example:

```
TELNET fe80::7c27%eth0
```

The Ping syntax is:

```
PING ipv6-address%interface
```

For example:

```
PING fe80::7c27%eth0
```

The interface can also be specified when setting Ping defaults with the SET PING command. If a source IPv6 address is also specified with the SIPADDRESS parameter in the PING or SET PING commands, the source address must be on the outgoing interface. The SIPADDRESS cannot be a link-local address.

Operations

SHOW FLASH command

The "Required free block" parameter has been added to the output of the SHOW FLASH command to enhance the display of general status information about the FLASH File System (FFS). There is new example output and an additional parameter (see Figure 6 on page 14 and Table 5 on page 14).

Figure 6: Example output from the SHOW FLASH command.

```

FFS info:
global operation ..... none
compaction count ..... 256
est compaction time ... 88 seconds
files .....          1420044 bytes   (4 files)
garbage .....          19652 bytes
free .....             526384 bytes
required free block ... 131072 bytes
total .....            2097152 bytes

diagnostic counters:
event      successes      failures
-----
get        0                0
open       0                1
read       0                0
close      0                0
complete   0                0
write      0                0
create     0                0
put        0                0
delete     0                0
check      0                0
erase      0                0
compact    0                0
verify     0                0
-----

```

Table 5: New parameter displayed in the output of the SHOW FLASH command.

Parameter	Meaning
Required free block	The minimum contiguous working space. This amount of FLASH memory must remain available. Therefore, it is not included in the "free" entry.

Public Key Infrastructure (PKI)

SET PKI command

For the SUBJECTALTNAME parameter of the SET PKI command the maximum length of the value *name* is 64 characters.

The command syntax for the SET PKI SUBJECTALTNAME command is:

```
SET PKI [SUBJECTALTNAME={ipadd|name}]
```

where *name* is a character string, 1 to 64 characters in length. Valid characters are any printable characters. If the name contains spaces, it must be enclosed in double quotes. Wildcards are not allowed.

ADD PKI CERTIFICATE command

An error message is displayed if the user attempts to set a proxy address when the LOCATION parameter is set to anything other than HTTP for the ADD PKI CERTIFICATE command. In previous software releases the user could specify either LDAP or HTTP for the LOCATION parameter and set the PROXYADDRESS parameter of the optional HTTP to use.

SHOW PKI CERTIFICATE command

Four additional parameters have been added to the output of the SHOW PKI CERTIFICATE=*name* command and there is new example output (see Table 7 on page 15 and Table 6 on page 15).

Figure 7: Example output from the SHOW PKI CERTIFICATE=*name* command.

```

Certificate:
  name ..... router1
  state ..... TRUSTED
  manually trusted .... FALSE
  type ..... EE
  source ..... COMMAND

  version ..... V3
  serial number ..... 3bf1 c141 [1005699393]
  signature alg ..... SHA1 with RSA
  public key alg ..... RSA
  not valid before .... 03:55:03 - 14-Nov-2001 (GMT)
  not valid after .... 04:25:03 - 14-Nov-2002 (GMT)
  subject ..... cn=router1, dc=foo, dc=bar, dc=com
  issuer ..... dc=foo, dc=bar, dc=com

  MD5 fingerprint ..... e81e bb17 deb3 664d 91e3 5c58 c890 aae1
  SHA1 fingerprint .... d662 ba63 ecb9 be83 0962 9ca1 5888 1bee d96b 67d6
  key fingerprint ..... 49d4 4919 106f ea71 21c7 7bef ab69 48c1 0ca8 99d2

  key usage ..... Digital Signature
  subject key ID ..... e70d3c808b6d747f2a415ccf7efc8e16a94c9f8d
  authority key ID .... dcc16049a4e158dcda046cecb90b91c9a94c6800

  validation path ..... <- foobar[ manually trusted, self-signed ]

Source Location:
  type ..... LDAP
  IP address ..... 192.168.100.200
  distinguished name  cn=router1, dc=foo, dc=bar, dc=com

```

Table 6: New parameters displayed in the output of the SHOW PKI CERTIFICATE=*name* command.

Parameter	Meaning
MD5 fingerprint	The MD5 fingerprint of the certificate.
SHA1 fingerprint	The SHA1 fingerprint of the certificate.
subject key ID	ID used to distinguish this key from other keys owned by the same user.
authority key ID	ID is used to determine which of the CAs keys was used to sign this certificate.

Trigger Facility

SET TRIGGER command

For the SET TRIGGER=*trigger-id* INTERFACE command, the EVENT parameter has been made optional.

```
SET TRIGGER=trigger-id [ INTERFACE[=interface] ] [ EVENT={UP |
DOWN | FAIL | ANY} ] [ CIRCUIT=miox-circuit ] [ CP={APPLE | ATPC |
BCP | CCP | DCP | DNCP | IPCP | IPXCP | LCP} ] [ DLCI=dlci ]
[ AFTER=hh:mm ] [ BEFORE=hh:mm ] [ {DATE=date | DAYS=day-list} ]
[ NAME=name ] [ REPEAT={YES | NO | ONCE | FOREVER | count} ]
[ TEST={YES | NO | ON | OFF | TRUE | FALSE} ]
```

The INTERFACE parameter defines an interface (link) trigger and specifies the interface to monitor. The EVENT parameter specifies a link (interface) status change event. The CIRCUIT parameter may be used if INTERFACE specifies an X.25 T interface. The CP parameter may be used if INTERFACE specifies a PPP interface. The DLCI parameter may be used if INTERFACE specifies a Frame Relay interface. The general trigger parameters may also be specified. The type of trigger cannot be changed.

Software Features - AR700 Series Routers

AR Router GUI

The AR Router GUI enables the user to perform limited monitoring, configuration, and troubleshooting of router operations. The router supports Microsoft® Internet Explorer 5.x. Javascript must be enabled.

To access the GUI:

- Enable IP
- Give eth0 an IP address using the command:

```
ADD IP INTERFACE=eth0 IPADDRESS=ipadd MASK=mask
```

Also, to access the GUI from a PC on a different subnet:

- create a route to the subnet of the PC using the command:

```
ADD IP ROUTE=ipadd INTERFACE=interface NEXTHOP=ipadd
```

Then:

- If you access the Internet through a proxy server, set your browser to bypass the proxy for the interface's IP address.
- Point your web browser at the interface's IP address.
- At the login prompt, enter the user name and password.

```
User Name: manager
```

```
Password: friend
```

The home page is displayed. Select options to configure and manage the router.

Software Features - AR410 Branch Office Routers

Chapter 3: Interfaces

SET ETH MAXBANDWIDTH command

The SET ETH MAXBANDWIDTH command is new. The command syntax is:

```
SET ETH=n MAXBANDWIDTH=0..100000
```

where:

- *n* is the number of the Ethernet interface.

This command imposes a maximum bandwidth limit on an Ethernet interface. This command is only valid for some interfaces. If it is not valid for a particular interface an appropriate error message will be displayed.

The MAXBANDWIDTH parameter is measured in 1000s of bits/s. If the bandwidth specified is 0 this feature is turned off, i.e., there is no limiting imposed. If $0 < \text{MAXBANDWIDTH} = 128$ is specified a bandwidth limit of 128000bits/s is used.

For example, to set a maximum bandwidth limit of 10Mbit/s on the ETH0 interface, use the command:

```
SET ETH=0 MAXBANDWIDTH=10000
```

SHOW ETH COUNTER command

The COLLISION parameter of the SHOW ETH COUNTER command has been modified. If the Ethernet interface hardware does not report collision statistics the collision frequency values are all displayed as zero.

The DIAGNOSTIC parameter of the SHOW ETH COUNTER command has been modified. If this parameter is specified, diagnostic counters specific to the router's Ethernet hardware are displayed. The output is divided into two parts, *device independent* counters which are the same for all router models, and *device dependent* counters which differ depending the type of hardware the interface uses (Table 8 on page 18).

Two new parameters have been added to the output of the SHOW ETH COUNTER command and two existing parameters have been modified (see Table 7 on page 18 and Table 8 on page 18). There is new example output (see Figure 8 on page 18).

Figure 8: Example output from the SHOW ETH COUNTERS=DIAGNOSTIC command for 91C111-based hardware.

```

ETH instance 0:          14 seconds   Last change at:          1 seconds

Device Independent Diagnostic Counters

EthProtoCacheHit          4      EthProtoCacheMiss        2
DSAPProtoCacheHit        0      DSAPProtoCacheMiss        0
SNAPProtoCacheHit        0      SNAPProtoCacheMiss        0
RxFIFOOverrun            0      TxFIFOUnderrun            0
RxTooFewBuffers          0      TxTooManyFragments        0
BusError                  0      TxDescriptorAreaFull      0
Reset                     0      TxFrameTooLong            0
LoadCAMFailure            0      TxLostInterrupt           0

Device Dependent Diagnostic Counters (91C111 hardware)

LinkChanges                1      FrameTooShorts            0
AutoNegCompletes          1      FrameMuchTooLongs         0

```

Table 7: Modified parameters in the output of the SHOW ETH COUNTER=DIAGNOSTIC command.

Counter	Meaning
LinkChanges	(91C111 hardware) The number of times the Ethernet link status (up, down, or unknown) changed.
AutoNegCompletes	(91C111 hardware) The number of times the Ethernet hardware completed negotiating a set of operating parameters with the link partner (a hub or switch) to which it is connected.

Table 8: Modified parameters in the output of the SHOW ETH COUNTER=DIAGNOSTIC command.

Counter	Meaning
FrameTooShorts	(91C111 hardware) The number of received frames that were shorter than the minimum permitted frame size.
FrameMuchTooLongs	(91C111 hardware) The number of received frames that were longer than the 91C111's internal buffer size.

SHOW ETH STATE command

A new parameter, Max BW limit, has been added to the output of the SHOW ETH STATE command and there is new example output (see Figure 9 on page 19, Figure 10 on page 19, Figure 11 on page 19, and Table 9 on page 19).

Figure 9: Example output from the SHOW ETH STATE command for 68360-based or SONIC-based hardware.

```

State for ETH instance 0:

Link ..... up
Speed ..... 10 Mbps
Max BW limit ..... 10000 Kbps
Duplex mode ..... half

```

Figure 10: Example output from the SHOW ETH STATE command for 100Mbps interfaces in the default configuration (with link speed auto-negotiation enabled).

```

State for ETH instance 0:

Link ..... up
Speed ..... 100 Mbps
Max BW limit ..... 1000 kbps
Duplex mode ..... full
Auto-negotiation ..... complete

Link partner capabilities
  Auto-negotiation ..... yes
  100BASE-TX full duplex ..... yes
  100BASE-TX ..... yes
  10BASE-T full duplex ..... yes
  10BASE-T ..... yes

```

Figure 11: Example output from the SHOW ETH STATE command for 100Mbps interfaces with link speed set manually.

```

State for ETH instance 0:

Link ..... up
Speed ..... 100 Mbps
Max BW limit ..... 1000 kbps
Duplex mode ..... half
Auto-negotiation ..... disabled

```

Table 9: New parameter displayed in the output of the SHOW ETH STATE command.

Parameter	Meaning
Max BW limit	The maximum bandwidth limiting imposed on the link, in a number of "kbps" or "None" (no bandwidth limiting).

Chapter 9: Internet Protocol (IP)

The INTERFACE parameter for the ADD IP DNS and SET IP DNS commands has been amended to include VLAN interfaces.

The INTERFACE parameter specifies a PPP, Ethernet, or VLAN interface over which the router will learn the address of a primary and/or a secondary name server.

Chapter 2: Switching

The Switching chapter is new since Software Release 2.3.1 and is appended to this document. The Switching chapter describes how to configure switchports, VLANs, Quality of Service (QoS) on the router. The following Switch commands in this document have been enhanced since Software Release 2.3.1b.

SHOW SWITCH command

The SHOW SWITCH command has been enhanced to display the ageing timer state as either enabled or disabled. There is a new example output and an additional parameter (see Figure 12 on page 20 and Table 10 on page 20).

Figure 12: Example output from the SHOW SWITCH command.

```

Switch Configuration
-----
Switch Address..... 00-00-cd-00-7a-47
Ageing Timer..... Enabled (300 Seconds (Fixed))
Backoff..... Aggressive
Back Pressure..... On
Broadcast Frame Limit..... 25%
Buffer Pool Settings..... Adaptive
Excessive Collision Drop..... Drop
Flow Control..... On
UpTime..... 00:10:32
Config Time..... 00:01:02
-----

```

Table 10: New parameter in the output of the SHOW SWITCH COUNTER command.

Parameters	Meaning
Ageing Timer	This indicates whether the Aging Timer feature is Enabled or Disabled. The time that a MAC address entry remains in the address lookup table cannot be altered.

SHOW SWITCH COUNTER command

The counters displayed by the SHOW SWITCH COUNTER command have been enhanced to show more information about communication between the switch chip and router CPU. There is new example output and the parameters have changed (see Figure 13 on page 21 and Table 11 on page 21).

Figure 13: Example output from the SHOW SWITCH COUNTER command.

```

Switch Counters
-----
Switch instance:          0

Packet DMA counters:
Receive:
  Octets                  486
  Packets                  6
  Discards                 0
  TooFewBuffers           0
  FIFOOverruns            0
  FrameTooLongs           0
  QueueLength             0
Transmit:
  Octets                  482
  Packets                  6
  Discards                 0
  DescriptorAreaFilled   0
  FIFOUnderruns          0
  Aborts                  0
  QueueLength             0

General counters:
  Resets                  1
-----

```

Table 11: New parameters in the output of the SHOW SWITCH COUNTER command.

Parameters	Meaning
Packet DMA Counters	
Receive	Counters for packets received.
Octets	The number of octets received by the CPU from the switch chip.
FIFOOverruns	The number of times reception of a packet failed because of a FIFO overrun.
FrameTooLongs	The number of received packets that exceeded the maximum permitted frame size.
Transmit	Counters for packets transmitted.
Octets	The number of octets transferred from the CPU to the switch chip, including framing.
FIFOUnderruns	The number of times transmission of a packet failed because of a FIFO underrun.

SHOW SWITCH PORT command

The information displayed by the SHOW SWITCH PORT command has been enhanced to show the link state, the port speed and the duplex mode of the specified switch port. There is new example output and two new parameters (see Table 14 on page 22 and Table 12 on page 22).

Figure 14: Example output from the SHOW SWITCH PORT command.

```

Switch Port Information
-----
Port..... 1
Description..... To upstairs hub port 4
Link State ..... Up
Configured speed/duplex..... Autonegotiate
Actual speed/duplex ..... 10Mbps, half duplex
Port-based VLAN..... Design (2)
Send tagged packets..... Yes
-----

```

Table 12: New parameters in the output of the SHOW SWITCH PORT command.

Parameter	Meaning
Link State	The link state of the port, one of "Up" or "Down".
Actual speed/duplex	The port speed and duplex mode that this port is actually running at, if the port is Up. If the port is Up then one of "Autonegotiate" or a combination of a speed (one of "10Mbps" or "100Mbps") and a duplex mode (one of "half duplex" or "full duplex").

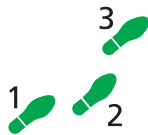
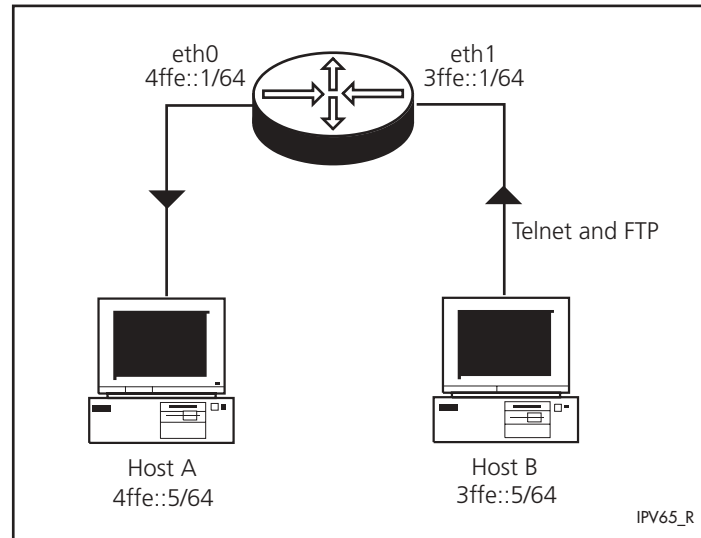
Errata

IPv6 Filters

The configuration example for IPv6 filters in the *Internet Protocol version 6 (IPv6)* chapter should be replaced with the following example.

In this example, there are two hosts, A and B. Host A needs to be accessed by Telnet and FTP from Host B. Other traffic from B to A is blocked by the filter, except neighbour discovery, which is required for basic IPv6 routing. This configuration is shown in Figure 15 on page 23.

Figure 15: Example showing host and router connections.



To configure the required IPv6 filters:

1. Configure IPv6 and add the interfaces

Enable IPv6, using the command:

```
ENABLE IPV6
```

Create the interfaces and assign IPv6 addresses to them, using the commands:

```
CREATE IPV6 INT=eth0
CREATE IPV6 INT=eth1
ADD IPV6 INT=eth0 IP=4ffe::0001/64
ADD IPV6 INT=eth1 IP=3ffe::0001/64
```

2. Assign a filter to the router's interface to Host B

```
SET IP INT=eth1 IP=3ffe::0001/64 FILTER=1
```

3. Add entries to the filter to allow Telnet and FTP traffic

To enable Telnet and FTP access to Host A from Host B, add the following filter entries:

```
ADD IPV6 FILTER=1 ENTRY=1 SOURCE=3ffe::0005
DESTINATION=4ffe::0005 PROTOCOL=TCP SPORT=ANY DPORT=23
LOG=HEADER

ADD IPV6 FILTER=1 ENTRY=2 SOURCE=3FFE::0005
DESTINATION=4FFE::0005 PROTOCOL=TCP SPORT=ANY DPORT=21
LOG=HEADER SESSION=ANY

ADD IPV6 FILTER=1 ENTRY=3 SOURCE=4FFE::0005
DESTINATION=3FFE::0005 SESSION=ANY PROTOCOL=TCP
SPORT=ANY DPORT=FTPDATA LOG=HEADER
```

4. Add entries to the filter to allow Neighbour Discovery traffic

In addition to the Telnet and FTP filter entries, it is necessary to explicitly allow IPv6 Neighbour Discovery (ND) traffic from Host B to Host A, because this traffic is required to enable basic connectivity between devices. The following filter entries allow the types of ICMP traffic that are typically IPv6 ND traffic to pass through the router:

```
ADD IPV6 FILTER=1 ENTRY=4 SOURCE=3FFE::/64 PROTOCOL=ICMP  
ICMPATYPE=135 ICMPCODE=ANY
```

```
ADD IPV6 FILTER=1 ENTRY=5 SOURCE=3FFE::/64 PROTOCOL=ICMP  
ICMPATYPE=136 ICMPCODE=ANY
```