

# RELEASE NOTE V!CAS

July 15, 1997

---

## New System Software:

### *Release 4.4 Revision 8*

This document describes the new features, enhancements, bug-fixes, and changes to the V!CAS System Software since Release 4.4 Revision 7.

<b>What's New in Revision 8</b>	<a href="#">Upgrading System Software</a> . . . . .	2
	<a href="#">Access List Extensions</a> . . . . .	3
	<a href="#">Dynamic Name Server Address Resolution</a> . . . . .	5
	<a href="#">Special IP Interfaces</a> . . . . .	6
	<a href="#">Van Jacobson Header Compression</a> . . . . .	7
	<a href="#">Wildcards for Calling Party's Address</a> . . . . .	7

Features appearing in previous Software Releases are documented in the *V!CAS User's Guide* (Document #70016) which is available in Adobe's PDF format via BinTec's HTTP server at <http://www.bintec.de>.

## Upgrading System Software

1. Retrieve the current system software image from BinTec's HTTP server at <http://www.bintec.de>.
2. With this image you can upgrade the V!CAS with the **update** command from the SNMP shell via a remote host (i.e. using telnet, minipad, or isdnlogin) or by using the **BOOT-monitor** if you are logged in directly on the console.

Information on using the BOOTmonitor can be found in the *V!CAS User's Guide* under *Firmware Upgrades*.

**Note:** When upgrading system software, it is also recommended that you use the most current versions of *BRICKware for Windows* and *UNIXTools*. Both can be retrieved from BinTec's HTTP server.

# What's New in What's New in Revision 8

4.4 Revision 8:

Released: 15.07.97

## Features:

### Access List Extensions

Access Lists have been extended to include support for:

- [Port Ranges for IP Access Lists](#)
- [Access List Violation Actions](#)
- [Access List Violation Reporting](#)




#### Port Ranges for IP Access Lists

Port Ranges can now be configured for Access Lists (Allow and Deny lists) making it easier to apply an access list to a range of ports.

##### Configuration

In past releases access lists had to be configured for each restricted port. Using the new **PortRange** variables, an access list can be applied to match a complete range of ports. By default these variables are set to "-1"; when set to any other value the respective access list is extended to match all packets within the range of ports. Note that the **PortRange** variables define the last port number in the range (and not the total number of ports).

New Variable	Extends Port Range to:
<i>ipAllowSrcPortRange</i>	$ipAllowSrcPort \leq Range \leq ipAllowSrcPortRange$
<i>ipAllowDstPortRange</i>	$ipAllowDstPort \leq Range \leq ipAllowDstPortRange$
<i>ipDenySrcPortRange</i>	$ipDenySrcPort \leq Range \leq ipDenySrcPortRange$
<i>ipDenyDstPortRange</i>	$ipDenyDstPort \leq Range \leq ipDenyDstPortRange$

Port Ranges can easily be configured via Setup Tool in the    menu, by selecting "specify range" in the **Specify Port** field.

## Access List Violation Actions

Previously the V!CAS always refused IP packets that were restricted by a configured IP access list (*ipDenyTable*) by sending an “ICMP Destination Unreachable” message to the sender. The new *ipExtIfAccessAction* variable (*ipExtIfTable*) defines the default action to take when an Access List is breached.

### Configuration

*ipIfExtAccessAction* may be set to:

- `ignore` The V!CAS simply discards packets (default).
- `refuse` The V!CAS discards the packet and transmits an “ICMP Destination Unreachable” message to the sender.

## Access List Violation Reporting

With Access List reporting you can now gather information about security breaches on the V!CAS. Each time the V!CAS receives a packet the configured access lists are applied. If a packet is restricted by a matching access list a brief report can be generated.

Violation Reports are generated via syslog and are saved in the *biboAdmSyslogTable*. This makes it possible to save Access List reports to remote loghosts. By default, reporting is disabled.

The new *ipExtIfAccessReport* variable (*ipExtIfTable*) defines how the V!CAS reports access list violations and may be:

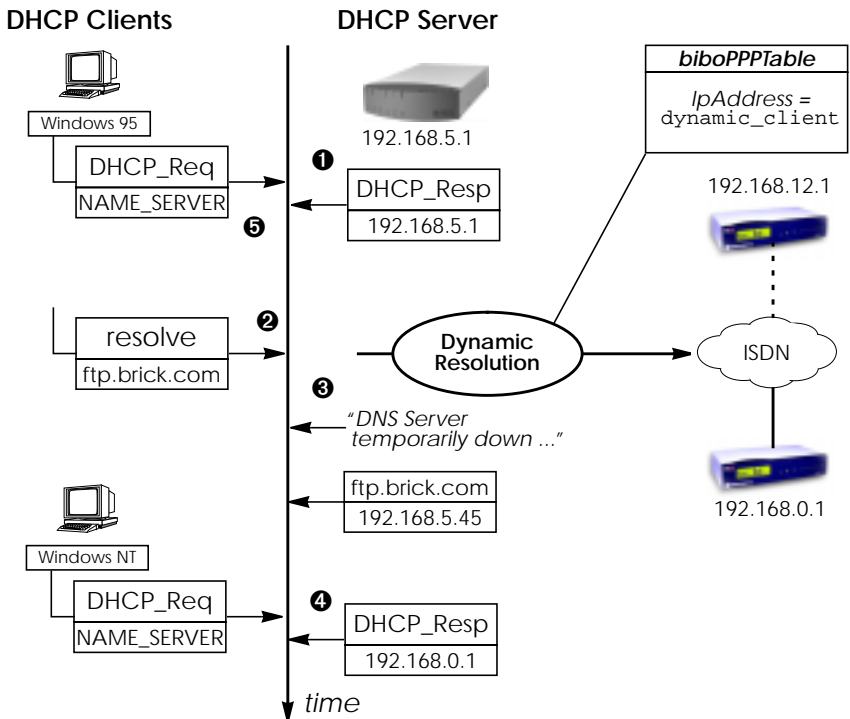
- `info` A syslog message containing the protocol, IP addresses, and port numbers is generated in the syslog table (default value).
- `dump` In addition to the same report generated for `info` the first 64 bytes of the IP packet are dumped (in hex format) to the syslog table.
- `none` No reports are generated.

**NOTE:** **Logging Access List Reports to remote log hosts via syslog.**  
Reports use level = info, facility = error.

## Dynamic Name Server Address Resolution

As documented in the *User's Guide* the V!CAS can operate as a DHCP server. As of Revision 8 the V!CAS attempts to determine the DNS server's address dynamically if one isn't already configured as follows.

DHCP clients that request the DNS server's IP address from the V!CAS are always given the current address set in ***biboAdmNameServer*** if one is configured; otherwise the value of ***biboAdmNameServ2*** is used. If neither variable is set the V!CAS sends it's own IP address and attempts to resolve the name server's address dynamically (see below) using DNS Negotiation over PPP after the first resolution request is received.



- 1 If no DNS server is configured, the V!CAS sends it's own IP address.

- ② Upon receipt of first name resolution request, the V!CAS parses the ***biboPPTable*** for partners that support DNS negotiation; i.e., ***IpAddress*** field is set to ***dynamic\_client***.
- ③ While attempting to configure it's DNS server, DNS requests are answered with "DNS Server temporarily down".
- ④ Once the DNS's address is successfully negotiated, the V!CAS can inform subsequent DHCP requests for a name server with it's newly configured address.
- ⑤ Clients that were given the V!CAS' address as name server can't be informed of the "new" address. For these hosts, the V!CAS simply continues relaying resolution requests to the actual DNS server.

## Special IP Interfaces

In previous releases two special IP interfaces (***ifIndex*** 0 and 1) were available on the V!CAS. Beginning with revision 8, a third interface, the "IGNORE" interface, (***ifIndex*** 2) has been added. These special interfaces are now listed in the V!CAS' ***ifTable***.

<b>ifTable inx</b>	<b>ifTable Index</b>	<b>Meaning</b>
<b>00</b>	<b>0 (REFUSE)</b>	When packets are routed to this interface, the packet is discarded and an "ICMP Destination unreachable" message is sent to the sender.
<b>01</b>	<b>1 (LOCAL)</b>	Packets routed to this interface are given to an appropriate internal process on the V!CAS.
<b>02</b>	<b>2 (IGNORE)</b>	Packets routed to this interface are discarded. No response is sent to the sender.

**TIP:** Special IP interfaces are useful for Extended IP routes. For example an extended IP route could be used to routes all DNS requests received from a specific host to the IGNORE interface.

## Van Jacobson Header Compression

The VICAS now supports Van Jacobson TCP/IP header compression (VJHC) according RFC 1144. TCP/IP header compression is a method used to reduce the size of TCP/IP packets and provides improved performance (line efficiency) for dialup connections.

### Configuration

VJHC can be configured for selected WAN partners via SetupTool or the SNMP shell.

- Setup Tool

In the **WAN PARTNER** → **ADD** → **ADVANCED SETTINGS** menu, select either on or off in the “Van Jacobson Header Compression” field.

- SNMP Shell

In the ***biboPPPTable***, set the new ***VJHeaderComp*** variable to either enabled or disabled.

**TIP:** VJHC is required for accessing Deutsche Telekom’s T-Online via PPP in Germany.

## Wildcards for Calling Party’s Address

Wildcard characters can now be used in the *Number* field of the ***biboDialTable*** to match different Calling Party’s Numbers at connection time. (The same wildcards are already supported in X.25 in the ***x25RouteTable***.) Wildcards may also be used from Setup Tool in the **WAN PARTNERS** → **ISDN NUMBERS** menu.

This means you don’t have to configure separate Dial Table entries for each MSN your partner may be calling from. The table below lists the currently supported wildcards.

### biboDialNumber Wildcard Matching

*	Match zero or more digits. 45* matches any number beginning with 45, i.e., 45, 4512, 4512345, 459, etc.
?	Match any single digit. 5? matches 50 through 59.

[ ]	Brackets denote a set of possible digits to match. A hyphen may be used for inclusive ranges. 21[45] only matches 214 or 215 (4 or 5) 21[6-8] matches 216, 217, 218 (6 through 8, inclusive) 21[^9] matches 210 through 218. (not 9)
{ }	Curly braces denote an optional string to match. {0911}2145 matches 09112145 and 2145 (optional)

If the Calling Party's Number from the incoming call matches a **DialTable** entry with wildcards and an entry without wildcards, the entry without wildcards is always used.

**NOTE:** Configuring wildcards from the SNMP shell. A **DialNumber** containing a **?** must be quoted using double quotes (") to avoid the SNMP shell from interpreting the character as a help command.

```
myVICAS:biboDialTable > biboDialNumber:05="09115678?"
05: biboDialNumber.10001( rw):      "09115678?"
myVICAS:biboDialTable >
```

## Enhancements

### Setup Tool

An internal cache has been implemented within Setup Tool that greatly reduces the time required to load and manipulate large configuration files (configurations with more than 100 dialup partners).

### Bugfixes

#### PPP

- Response packets (access list restrictions) and other packets that can't be routed no longer affect the **ShortHold** timer for PPP connections.



## TCP

- Under certain circumstances an initial connection to a particular TCP service (telnet, capi, rfc1006, http) hindered subsequent connections to the same service. Previously, this problem could only be resolved by rebooting the system. This problem has been corrected in revision 8.
- A protocol problem hindered the V!CAS from accepting TCP connections from some UNIX systems (i.e. SVR4). This has been corrected.

## ISDN

- Previously, ISDN connections with 1TR6 PBXes that weren't operating in conformance to 1TR6 were closed. In particular, when an empty Cause W-Element was sent in the STAT message. Since many devices exhibit this behaviour the 1TR6 protocol on the V!CAS has been adapted to be more tolerant.
- The V!CAS is much more stable when used in connection with ISDN leased line configurations.

