Radvision ViaIP™ Enhanced Communications Server

The ECS (Enhanced Communications Server) is dedicated software that offers a gatekeeper and a number of additional associated services, such as logging and billing.

Figure 2. A gnu-gk status port telnet session
Testing was carried out using ECS version 3.2.2. Check the documentation for the version you are supplied with for system hardware and software requirements.

ECS installation

The software can be downloaded to the Windows® desktop of the host machine – it may also be supplied on a CD. The test PC was a Windows® 2000 Professional system.
The unzipped software contains a number of PDF files including Release Notes and a User Manual. Every configuration page also has a help link which offers thorough contextual help. Installation is described in Chapter 1 of the accompanying User Manual while the necessary pre-requisites are described in its Appendix A. The following list, used during the testing process, shows how pre-requisites should be configured:
1 The SNMP service was set up as described for Windows® 2000.
2 The Internet Information Server was configured in accordance with the instructions.
3 The ftp service (for reading the log files) was not configured, but this did not appear to matter.
4 The machine was brought up to date with operating system updates, patches and so on.
5. Anti-virus software, a personal firewall and VNC remote access software — which were all already installed on the gatekeeper host — were updated. These additional items are not required by the ECS but were deemed appropriate to maintain the system's security in an educational environment.
Once the pre-requisites have been configured, installation is a relatively simple process. The files supplied are extracted to a suitable location and then a setup.exe program handles installation and registration.

ECS configuration

In order to configure the ECS gatekeeper, it is necessary to log in from a web browser. You will need the administrator password for the ECS that you wish to configure (on first use this will be User: Admin, password: null). Enter the numeric IP address of the host that is running ECS as a URL in the browser address bar. This should bring up a log-in page which allows the entry of a user name and password. Enter a user name and password that enables 'administrator' rights. This should lead to a page entitled 'Product Family Entry Point'. On first use it is recommended that the supplied default Admin password be changed to something more secure.
In order to update the password to something more secure, it is necessary to log 'Admin' in as

local administrator, then click the ‘Global’ icon. This offers a list of users and applications. Select the admin account and click the change password button at the bottom left in order to reset the password. Once the change has been uploaded, click the ‘ECS’ icon to access administration of the local gatekeeper. This will lead to the configuration pages for the ECS.

ECS configuration and administration is via a web browser which accesses an interface consisting of tabbed pages, buttons and pop-up windows. These are considered in turn below. Where a setting is not explicitly referred to here, it can be left as it appears by default.

The configuration described below does not include inter-working with a Cisco® H.323 proxy (or MCM), a Cisco® PIX firewall, or any other firewall/security solution. The gatekeeper administrator of course needs to address the network security of the gatekeeper itself and the terminals that are registered with it.

The ECS has a sophisticated list of parameters that can be altered and set. This guide considers only those necessary for compliance and inter-working with the JVCS.

Gatekeeper ID : this can be any unique identifying text string.
Dial Plan: must be version 2.
DHCP environment in the zone: this should be detected and checked/unchecked automatically.
Who can Register: for security it is advised that “Only predefined endpoints” is selected.
Calls
Figure 4. ECS: Settings>Calls

Settings page

Basics
Figure 3. ECS: Settings>Basics
Configuring an H.323 Gatekeeper for use with the JANET Videoconferencing Service
GD/VTAS/016 20
Routing Mode: ‘Direct’
The other options that should be checked on this page are: Accept calls, Immediate call proceeding and Reject the call in case the call cannot be connected.
Capacity
The bandwidth settings will depend on local conditions and your network connection to the Regional Network. Note that the settings are in bits, so a maximum endpoint setting of 1Mbit/s would be entered as: 1000000. It is not necessary to enter any values here if the number of endpoints that can register simultaneously do not merit it.
Dial Plan
Figure 5. ECS: Settings>Dial Plan
Strip zone prefixes should be checked. No other options should be checked here. There is no need to enter a value for Replace stripped prefix with. The default hop count is 9 and this can remain unchanged. This figure represents the number of times the request will be forwarded for address resolution before the location request expires.
Supplementary Services
No configuration necessary. All active options should be unchecked.
Logs
It is at the discretion of the administrator whether they wish to enable logging, and if so, the

level of logging that they wish to enable. Bear in mind that a high level of logging creates a lot of files and is only recommended for testing and debugging.
Billing, LDAP, Authorisation, DNS, Central Database, Security, Alternate Gatekeeper, Firewall, Advanced
There is no need to configure any of these settings for the gatekeeper to inter-work with the JVCS-IP.
The ‘Alternate Gatekeeper’ setting is for a situation where there is a back-up gatekeeper for critical services. It has no relevance to the dialling scheme implementation.
Some ‘Advanced’ settings will be checked by default. It is recommended that these are left as auto-detected.

Registration restrictions

This page is used to control access to the gatekeeper. There are various levels of access, based on Alias Format and/or IP addresses. It is recommended that access to the gatekeeper is restricted to known IP addresses. These can be defined by individual endpoint IP addresses (with the subnet mask 255.255.255.255) or groups of IP addresses, with appropriate subnet masks. Entries are added by using the Add… pop-up window. This also includes an Upload button which should be used each time an entry is made. By highlighting an entry in the table, it is possible to edit or delete that entry.
The simplest configuration is to allow access only to defined IP addresses.

Endpoints

This page shows which endpoints are currently registered.

Services (Gatekeeper zone configuration)

The gatekeeper is ‘told’ about its own zone by selecting the Services tab and then selecting the entry in the services list. For JVCS configuration, select the entry Zone prefix 1 and click ‘Edit’. A pop-up window will allow configuration of the details for this zone. In the Prefix field, enter the zone prefix that has been supplied by the JVCS-MC. This will be in the form: 0044xxxxx . The Zone prefix 2 entry exists for cases where a single gatekeeper is controlling two discrete zones. This will not normally be the case. Global service should be set as ‘no’ (this value is read only), and the Allow access for boxes can be left unchecked.

Call control, forwarding

For use with the JVCS-IP there is no need to configure any settings on these pages.

Hierarchy (remote zones and the GDS)

The Hierarchy page is used to tell the gatekeeper about other gatekeepers and should be used to tell this gatekeeper about the national directory gatekeepers. Because ‘Parent’ and/or ‘Child’ gatekeepers are a concept that is not shared by all manufacturers’ gatekeepers, it is necessary to define remote gatekeepers as ‘Neighbors’. There are three tabs on the left hand side of the Hierarchy Page. Select the Neighbors tab. Select the Add…. Button at the bottom right of the screen. A pop-up will appear:

Figure 6. ECS: Hierarchy>Neighbors>Add
In the prefix field enter 0044 (the zone of the JANET(UK) national gatekeeper), and add an appropriate description. Enter the first IP address that will have been supplied by the JVCS-MC for the national directory gatekeeper. No other fields should be checked or altered. Once the information has been entered, click the Upload button. The JANET(UK) directory gatekeeper should now appear as an entry in the neighbour list. Repeat this process for the second national directory gatekeeper, but this time leave the prefix as null – i.e. do not enter any value. This should cause the second directory to be queried if there is no response from the first.

Topology

There is no need to change any of the pages that configure Call Control, Forwarding, or Topology for basic inter-working with the JVCS-IP.

Saving configuration changes

After making any changes to the ECS configuration, the Upload button at the top left hand side becomes live. It is necessary to Upload any changes in order for them to be remembered in the configuration. Pop-up windows should be uploaded using the buttons that confirm and save any change. There is no need to reboot the server or restart the gatekeeper for these changes to take effect and be written to the gatekeeper configuration.

Radvision® ECS references

Product Documentation - Available on registration

`http://www.radvision.com/NBU/Customer+Support/`

Radvision ViaIP™ Enhanced Communications Server

`http://www.radvision.com/NBU/Products/viaIP+Custom+Solutions/Gatekeeper+%28EC`
