WHITE PAPER

SYSTEMS NETWORK ARCHITECTURE NETWORK MANAGEMENT OPTIONS AND MIGRATION FROM CISCOWORKS BLUE

As the CiscoWorks Blue product family approaches end of life, Cisco Systems® will no longer market Systems Network Architecture (SNA)–specific network management applications. Customers that already license these products may continue to use them and receive support under the terms of the end-of-life announcements. This document addresses the various alternatives available for managing Cisco® routers in an IBM/SNA network, focusing on Data-Link Switching Plus (DLSw+), SNA Switching Services (SNASw), Cisco TN3270 Server, and Channel Interface Processor/Channel Port Adapter (CIP/CPA). These alternatives include using built-in Cisco IOS® Software commands, SNA management applications from IBM, and IP management applications from Cisco and other vendors.

Cisco IOS Software will also continue to include MIB support. The specific protocol MIBs will be discussed later in this document. To find all MIBs supported by Cisco, go to http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

CISCOWORKS BLUE MAPS AND SNA VIEW

These two products are no longer for sale as of December 31, 2003, and will become obsolete December 31, 2006.
See http://www.cisco.com/en/US/partner/products/sw/cscowork/ps2396/prod_eol_notice09186a008032d52a.html for the product end-of-life details.

CiscoWorks Blue Maps was a UNIX-based product that presented a logical view of the Advanced Peer-to-Peer Networking (APPN)/SNASw, Data-Link Switching (DLSw), and remote source-route bridging (RSRB). RSRB is obsolete, so no RSRB management replacement strategy will be discussed. An alternative for APPN is to use the IBM Tivoli NetView SNA Topology Manager feature for APPN networks. Another alternative is to use Cisco IOS Software **`show`** commands such as **`show snasw topology`** and **`show dlsw peers`** or to use the APPN and DLSw MIBs to retrieve this information. See "Cisco IOS Software Management Features," later in this document, for more details.

SNA View correlated SNA resources with the Cisco routers providing DLSw, APPN/SNASw, RSRB, and Cisco TN3270 Server routing for SNA sessions. It had a mainframe component to collect Virtual Telecommunications Access Method (VTAM) SNA information and send it to the UNIX program for correlation with router MIB data and display. In some cases this arrangement will not be difficult to replicate. To find out which SNASw router is providing physical unit (PU) and logical unit (LU) services via dependant LU requestor (DLUR), find the DLUR name on a VTAM PU display. A reasonable naming convention will provide the router name from that SNASw DLUR control point (CP) name.

The case of DLSw correlation is far more complicated. SNA View used a VTAM ISTEXCCS exit to catch Media Access Control (MAC) and Service Access Point (SAP) addresses of PUs connecting into VTAM and correlated them to DLSw circuits on the routers. VTAM has no user interface to display the MAC/SAP addresses, so a naming convention that associates PU names to their branch routers is most helpful. If such a naming convention is not in place, rely on a custom network diagram or table for network operations staff to use, along with a process to isolate the failure, such as checking the following:

- **VTAM PU state**—Reactivate PU or switched major node if needed.
- **DLSw peer state between the host and PU side routers**—If not active, try ping and traceroute between routers or other IP network management tools to help resolve IP network issues.
- **DLSw circuit state and statistics**—See the DLSw troubleshooting guide (referred to in the "DLSw" section) for help with circuit issues.

CISCOWORKS BLUE INTERNETWORK STATUS MONITOR

Internetwork Status Monitor (ISM) is no longer for sale, as of February 18, 2005, and will be obsolete February 18, 2008. See http://www.cisco.com/en/US/prod/collateral/netmgtsw/cscowork/ps5741/ps2393/prod_end-of-life_notice0900aecd8010e87b.html for the complete details.

ISM is basically a router management application, operating on a mainframe under NetView, or until the final version, NetMaster. Many of its features are duplicates of CiscoWorks features on UNIX and Windows systems, so CiscoWorks is a viable replacement for most of ISM's features. See "CiscoWorks Solutions" later in this document for more details.

Customers that prefer to manage Cisco routers from the mainframe can still use the same native RUNCMDs that ISM uses to extract information from Cisco IOS Software. See "NetView" under "Products From IBM and Other Vendors" in this document for more details on configuring a service point on a router. The following is a sample NetView RUNCMD:

`RUNCMD SP=routerpu,APPL=CONSOLE,show interface channel 1/0`

CISCOWORKS SOLUTIONS

The CiscoWorks Routed WAN Management Solution includes access list management; performance measuring (with CiscoWorks Internetwork Performance Monitor); interface status (with CiscoWorks CiscoView); and inventory, configuration, SYSLOG message display, and software update management with Resource Management Essentials (RME). The CiscoWorks LAN Management Solution is another bundle to consider. It includes discovery of the Cisco network, topology views, and VLAN management, along with RME and CiscoWorks CiscoView.

See http://www.cisco.com/en/US/products/sw/netmgtsw/index.html for more details on these and other CiscoWorks bundles, including solutions for voice over IP and network security.

PRODUCTS FROM IBM AND OTHER VENDORS

NetView

IBM Tivoli NetView for Z/OS remains the ultimate network management product for SNA networks, for issuing VTAM commands to display SNA resources and view alerts, and so on. This document does not cover all of the NetView functions. Some components pertinent to this discussion include SNA Topology Manager, Tivoli Monitoring for Network Performance, and OMEGAMON.

Cisco devices can be managed by NetView with a service point configured on the router. It is a good idea to limit service points to core or data center routers because each service point is required to be a VTAM PU.

RUNCMD

To target a router for a NetView RUNCMD, configure a service point on the router. See the Cisco IOS Software IBM Networking Configuration Guide at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fibm_c/bcfpart2/bcfdspu.htm for assistance and examples of how to configure a service point.

The basic format of the command is **`RUNCMD SP=routerpu,APPL=CONSOLE,show interface channel 1/0`**.

Substitute ***`routerpu`*** with the service point PU name known to VTAM and any valid SNASw command at the end. Note that the system services control points (SSCP)–PU session is a single pipe. When enable mode is entered on the router, any operator can use enable mode, not just the operator who entered the enable password.

Use the command lists (CLISTs) shipped with ISM as samples to write your own. http://publib.boulder.ibm.com/tividd/td/TNZOS/SC31-8862-00/en_US/PDF/envl2000.pdf is the NetView documentation on CLISTs.

Alerts

Cisco IOS Software sends SNA alerts to NetView. There are two different mechanisms for getting the alerts to NetView: as Multiple Domain Support-Message Units (MDS-MUs) sent over an LU 6.2 session, or as Network Management Vector Transports (NMVTs) sent over an SSCP-PU session. Inside the MDS-MU or NMVT are the same alert major vector and appropriate alert subvectors.

SNASw uses MDS-MUs for the alerts it generates. NetView must be set up as the focal point (receiver) of alerts. The best and most common way is for NetView to acquire SNASw's network node (NN) server (VTAM) in its "sphere of control." NetView will automatically acquire its local VTAM. To acquire other VTAM NNs, issue the following NetView command:

```
FOCALPT CHANGE,FPCAT=ALERT,TARGET=vtamcpname
```

To verify that this command has been accepted, issue this NetView command:

```
FOCALPT DISPSOC,FPCAT=ALERT
```

When SNASw establishes CP-CP sessions with the VTAM NN server, VTAM will inform SNASw of the NetView alert focal point. SNASw will send its alerts over the CP-CP session, and VTAM will forward them on to NetView. This can be verified with the following Cisco IOS Software command and expected output:

```
#show snasw node | incl Alert
Alert focal point                NETA.VTAM
```

If the output line has no name after **`Alert focal point`**, SNASw will not send its alerts. As an alternative to the above command, name the SNASw CP as the target of the **`FOCALPT CHANGE`** command to set up a direct session to NetView. Because this command creates an additional session, the first method, which names VTAM as the target, is recommended.

SNASw will in turn inform any of its own downstream end nodes (ENs) of the existence of the NetView focal point, so that those ENs may route their alerts through SNASw to be delivered to NetView.

Alerts generated by any other Cisco IOS Software component besides SNASw will send alerts as NMVTs over an SSCP-PU session. A service point must be configured on the router (see the "RUNCMD" section, earlier in this document). No configuration is needed on NetView; the alert will always be delivered on the SSCP-PU session. Verify the router configuration and status with the **`show sna`** command, verifying that the PU_STATUS is active.

SNA Topology Manager

The SNA Topology Manager (SNATAM) displays APPN and subarea networks graphically by retrieving data from VTAM and other supported agents (SNASw is not one) and storing data in its Resource Object Data Model (RODM) database. As a served end node to VTAM, SNASw will appear in SNATAM views, but devices downstream for SNASw will not unless they are directly managed. For more documentation on SNATAM, please see: http://publib.boulder.ibm.com/tividd/td/TNZOS/SC31-8868-00/en_US/PDF/envl5000.pdf

IBM Tivoli Monitoring for Network Performance and OMEGAMON

IBM Tivoli Monitoring for Network Performance (ITMNP) has new features for high performance routing (HPR) and HPR-IP protocol management, primarily by managing VTAM. Use SNASw **`show`** commands to see equivalent information on the router. See http://www-306.ibm.com/software/tivoli/products/monitor-net-performance for more information on ITMNP.

Because of the recent acquisition of the OMEGAMON products, IBM will be putting together a roadmap to position it with ITMNP. Check with IBM for the most current information on this roadmap.

As SNA networks evolve to IP, keep in mind the numerous management tools available to manage IP networks. Although very few of them are aware of SNA resources, many network problems may be viewed as pure IP problems. See “CiscoWorks Solutions,” earlier in this document, for Cisco network management products. Other UNIX-based and Windows-based IP management products include Tivoli NetView and OpenView from Hewlett-Packard.

CISCO IOS SOFTWARE MANAGEMENT FEATURES

Rather than use the CiscoWorks Blue products, some customers use built-in Cisco IOS Software functions to monitor their router-based IBM/SNA networks. Most of these customers probably rely on **`show`** commands, but others use Simple Network Management Protocol (SNMP) MIBs for management. The **`show`** commands can be viewed via a Web interface by configuring **`ip http server`** on Cisco IOS Software to make the router Web accessible. The Cisco IOS Software capabilities will be grouped by protocol.

DLSw

The command **`show dlsw peers`** displays the peer connections to other DLSw routers. An active peer connection has state “CONNECT.”

The command **`show dlsw circuits`** displays the DLSw circuits for this router. Usually there is one circuit per SNA session.

Use the **`detail`** keyword to list details about each peer or circuit, and optionally the output list can be qualified to get details about selected items. A complete list of **`dlsw show`** commands follows:

```
router#show dlsw ?
  capabilities      Display DLSw capabilities information
  circuits          Display DLSw circuit information
  fastcache         Display DLSw fast cache for Fast-Sequenced Transport (FST) and direct
  local-circuit     Display DLSw local circuits
  peers             Display DLSw peer information
  reachability      Display DLSw reachability information
  statistics        Display DLSw statistical information
  transparent       Display MAC address mappings
```

For tips on when to use these and other commands, see the DLSw troubleshooting guide at http://www.cisco.com/warp/customer/697/dlswts1.html and the Cisco IOS Software Command Reference at http://cio.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fibm_r1/br1fprt2/br1fdlsw.htm.

MIBS

Cisco IOS Software supports DLSW-MIB (RFC 2024), which is located at http://www.ietf.org/rfc/rfc2024.txt. Also supported are peer and circuit up/down traps in a Cisco proprietary MIB CISCO-DLSW-EXT-MIB. Use the RFC standard MIB for queries, but listen for the ***cdeTrapTConnUpDown*** and ***cdeTrapCircuitUpDown*** traps from the Cisco extension. Note that Cisco IOS Software does not support any of the traps in the RFC standard. Configure **`snmp-server enable trap dlsw`** on the router to enable traps. It is optional to enable just **circuit** or **tconn** (peer connection) traps. Unless there is a real need to monitor all DLSw circuits, it is probably best to configure **`snmp-server enable trap dlsw tconn`** for peer connection traps only.

To keep track of DLSw peer connections via the MIB, a baseline of configured peers and their current status must be established first. Query ***dlswTConnOperState*** at any router with configured peers. Normally these will be at remote routers; data center (core) routers are often set up

for peers to connect in freely, so any inactive connections will not show up in their ***dlswTConnOperTable***. Listening for ***cdeTrapTConnUpDown*** traps will provide information about any peer state changes. Poll core routers are necessary as a backup in case any traps are lost, because that is not a guaranteed mechanism. Absence of a ***dlswTConnOperTable*** entry indicates that a remote peer connection has gone down. Poll remote routers only as needed to catch newly configured peers or to monitor remote-to-remote peer connections.

While DLSw circuits can also be tracked, it is probably more feasible to use NetView tools to monitor the SNA sessions carried over them.

For statistical and performance measuring, consider monitoring these MIB variables:

dlswTConnStatActiveConnections
dlswTConnStatCloseIdles
dlswTConnStatCloseBusys
dlswTConnOperInDataPkts
dlswTConnOperOutDataPkts
dlswTConnOperInDataOctets
dlswTConnOperOutDataOctets
dlswCircuitStatCreates

SNA Switching Services

SNASw has many **show** commands, with the more commonly helpful ones in *italics*.

```
router#show snasw ?
  class-of-service          Show class of service information
  connection-network        Show connection network information
  directory                 Show directory information
  dlctrace                  Show information from the dlctrace buffer
  dlus                      Show DLUS information
  ipstrace                  Show information from the ipstrace buffer
  link                      Show link information
  lu                        Show DLUR LU information
  mode                      Show mode information
  node                      Show local node information
  pdlog                     Show information from the pdlog buffer
  port                      Show port information
  pu                        Show DLUR PU information
  rtp                       Show HPR RTP connection information
  session                   Show session information
  statistics                Show statistics
  summary-ipstrace          Show information from the summary-ipstrace buffer
  topology                  Show topology database information
```

Use the **detail** keyword with most of these commands to get more information about the resources and use qualifiers to limit the output, if desired. See more details about these commands in the Cisco IOS Software Command Reference at http://cio.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fibm_r2/br2fpt1/br2fsnaw.htm.

Also, visit Cisco.com for an upcoming “SNASw Troubleshooting” guide, which is scheduled for publication by June 2005.

MIBS

SNASw supports the following MIBs:

- APPN-MIB (RFC 2455): http://www.ietf.org/rfc/rfc2455.txt
- APPN-DLUR-MIB (RFC 2232): http://www.ietf.org/rfc/rfc2232.txt
- APPN-TRAP-MIB (RFC 2456): http://www.ietf.org/rfc/rfc2456.txt

Note: The HPR and HPR-IP MIBs are not implemented.

The recommended configuration to enable the most useful APPN traps is **`snmp-server enable trap snasw cp-cp dlus link port`**.

The status of links, ports, connection networks, intermediate sessions, and DLUR-dependant LU server (DLUS) sessions in a SNASw router can be monitored. Pus can also be monitored, but those are more easily monitored from NetView, as are dependent LU sessions.

Begin by querying the APPN and DLUR MIBs for information. The following list is a reasonable start, though all variables may not be necessary, so look through the MIBs for other important variables.

`appnNodeCpName`
`appnNodeEnNnServer`
`appnPortOperState`
`appnPortDlcType`
`appnPortDlcLocalAddr`
`appnLsOperState`
`appnLsPortName`
`appnLsAdjCpName`
`appnLsAdjNodeType`
`appnLsCpCpSessionSupport`
`appnLsRemoteAddr`
`appnVrnPortName`
`appnIsInPriLuName`
`appnIsInSecLuNam`
`appnIsInModeNam`

and from the DLUR MIB:

`dlurDlusSessnStatus`

Note: Identifiers such as link names and port names are retrieved from the index part of the returned MIB value and are not directly accessible objects.

As a branch network node, SNASw does not have a full copy of the APPN network topology database, and thus it does not implement the ***`appnNnTopo`*** tables.

After an initial collection of this MIB data, listen for the following APPN traps to detect resource state changes:

`appnLocalTgCpCpChangeTrap`
`appnPortOperStateChangeTrap`
`appnLsOperStateChangeTrap`

dlurDlusStateChangeTrap

As a backup in case any traps fail to be delivered, query the following MIB variables periodically:

appnNodeEnNnServer
appnPortOperState
appnLsOperState
dlurDlusSessnStatus

For traffic performance and statistical data, consider these variables from the link station table:

appnLsInXidBytes
appnLsInMsgBytes
appnLsInXidFrames
appnLsInMsgFrames
appnLsOutXidBytes
appnLsOutMsgBytes
appnLsOutXidFrames
appnLsOutMsgFrame

Cisco TN3270 Server

The Cisco TN3270 Server **show** commands start with **show extended channel x/y tn3270**, where **x** is the channel interface and **y** is the subinterface. The following table shows useful Cisco TN3270 Server router commands. In these examples, the Cisco TN3270 Server is running on the CIP or CPA card associated with channel interface 1/2.

Table 1. Cisco TN3270 Server Router Commands

Router Configuration Command Line	Description
show extended channel 1/2 tn3270-server	Display the Cisco TN3270 Server configuration parameters for the specified channel and the status of the PUs defined in the server.
show extended channel 1/2 tn3270-server pu PU-NAME	Display the specified channel's Cisco TN3270 Server PU configuration parameters and statistics and all the LUs currently attached to the specified **PU-NAME**.
show extended channel 1/2 tn3270-server nailed-ip IP-ADDRESS	For the specified channel and **IP-ADDRESS**, display mappings between a nailed client IP address and nailed LUs.
show extended channel 1/2 tn3270-server pu PU-NAME lu LU-NUMBER [history]	Display the status of the specified **LU-NUMBER** for the **PU-NAME**. For DLUR, this shows the link and logical form session identifier (LFSID). If the optional **history** command parameter is included, the last few transaction types and sizes are listed.
show extended channel 1/2 tn3270-server client-ip-address CLIENT-IP-ADDRESS	For the specified client IP address, display recent LUs used by that IP address.
show extended channel 1/2 tn3270-	Display information about the DLUR components. List all DLUR links.

Router Configuration Command Line	Description
`server dlur`	

More extensive documentation on these commands is in the Cisco IOS Software command references at http://cio.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fibm_r2/br2fpt1/br2ftnsv.htm.

See the troubleshooting and tracing tips at the bottom of this page http://www.cisco.com/en/US/tech/tk331/tk339/tk658/tech_protocol_home.html.

The Cisco TN3270 Server supports these MIBS:

- **CISCO-TN3270SERVER-MIB**
- **SNA-NAU-MIB**
- **TN3270E-RT-MIB** (for response time reporting)
- **APPN-MIB**
- **DLUR-MIB** (subset)

The following MIB variables and tables give some basic information and statistics:

tn3270sCpuCard
tn3270sLusInUse
tn3270sStatsTable
snaLuSessnStatsTable

To correlate Cisco TN3270 Server client IP addresses to PU and LU names, you must first retrieve the ***tn3270sIpPuIndex*** and ***tn3270sIpLuIndex*** from the **CISCO-TN3270SERVER-MIB** ***tn3270sIpTable*** using the client IP address as an index. (Finding the client IP address is platform specific; on Windows clients, run the command **`winipcfg`** or **`ipconfig`**.) Then go to the **SNA-NAU-MIB** to get the ***snaNodeOperName*** (PU name) using the ***tn3270sIpPuIndex*** as the index to the ***snaNodeOperTable***. Likewise, get the ***snaLuOperName*** from the ***snaLuOperTable*** using ***tn3270sIpLuIndex*** as the index. Now the PU and LU information can be viewed on the NetView.

Although the Cisco TN3270 Server Design Guide refers to some products soon to be unavailable or no longer available, such as ISM and the long-defunct TN3270 Monitor, it still has some excellent troubleshooting concepts in the Network Management chapter at http://www.cisco.com/univercd/cc/td/doc/cisintwk/dsgngde/tn3270/tndg_c4.htm. Substitute MIB queries or show commands to collect some of the information mentioned in that guide.

Channel Interface Processor/Channel Port Adapter

Start at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fibm_r2/br2fpt1/index.htm to see the commands available for configuring and monitoring the CIP/CPA.

The CIP/CPA-specific MIBs are:

- **CISCO-CHANNEL-MIB**
- **CISCO-CIPCMPC-MIB**
- **CISCO-CIPCSNA-MIB**
- **CISCO-CIPLAN-MIB**
- **CISCO-CIPTCPIP-MIB**

- **CISCO-CIPTG-MIB**

The most common command is **`show extended channel`**. It has the following options:

`backup`	`Backup groups`
`cmgr`	`Displays CMPC+ Connection Manager information`
`cmpc`	`CMPC device`
`connection-map`	`Connection map between protocol and CSNA`
`csna`	`CSNA device`
`hsma`	`Displays the HSMA information for the specified interface`
`icmp-stack`	`Internet Control Message Protocol (ICMP) statistics`
`ip-stack`	`IP statistics`
`lan`	`Internal LANs`
`llc2`	`Show channel interface Logical Link Control (LLC) information`
`max-llc2-sessions`	`Maximum Logical Link Control, type 2 (LLC2) session statistics`
`packing`	`Common Link Access for Workstations (CLAW) packing device`
`statistics`	`Channel statistics`
`subchannel`	`Subchannel information`
`tcp-connections`	`TCP connection statistics`
`tcp-stack`	`TCP stack statistics`
`tg`	`CMPC transmission group`
`tn3270-server`	`Cisco TN3270 Server status`
`udp-listeners`	`User Datagram Protocol (UDP) listener statistics`
`udp-stack`	`UDP statistics`

To check CIP CPU, direct memory access (DMA), channel, and memory usage, use the **`show controller cbus`** command. The corresponding command for the extended channel port adapter (XCPA) is **`show controller channel x/0`**. The command also displays hardware and software levels.

This information is also available from the ***cipCardTable*** and ***cipCardDaughterBoardTable*** tables in the **CISCO-CHANNEL-MIB**. ISM specifically queried the following variables:

cipCa**rdEntryName**
cipCardEntryTotalMemory
cipCardEntryFreeMemory
cipCardEntryMajorSwRevisionNr
cipCardEntryMinorSwRevisionNr
cipCardEntryMajorHwRevisionNr
cipCardEntryMinorHwRevisionNr
cipCardEntryCpuLoad1m
cipCardEntryCpuLoad5m
cipCardEntryCpuLoad60m
cipCardEntryDmaLoad1m
cipCardEntryDmaLoad5m
cipCardEntryDmaLoad60m
cipCardDtrBrdType
cipCardDtrBrdChannelLoad1m
cipCardDtrBrdChannelLoad5m
cipCardDtrBrdChannelLoad60m

Other IBM/SNA Protocols

MIBs are available for many of the other protocols, such as Serial Tunneling (STUN), Airline Product Set (ALPS) and source route bridging (SRB). Check http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml for the list of MIBs. Usually the protocol name is part of the MIB—for example, **CISCO-STUN-MIB** for STUN. Likewise, the **show** and **debug** commands are located in the Cisco IOS Software documentation, starting at http://cio.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

204171.u_ETMG_AE_3.05

Printed in the USA