SME Communications

subject: ***COMPAS 136391***
IP Office IP Port Matrix, Release 7.0
Issue: 3.0

date: **10th January 2011**

from: **Tim Riches**
+44 (0)1707 364289
timriches@avaya.com

Abstract

This document covers the IP port usage of the Release 7.0 IP Office solution components.

Avaya - Proprietary
Use pursuant to Company instructions.
Design template 1.0. COMPAS 108698 01/2005

1. Introduction 3
1.1. Roles and Responsibilities 3
1.2. Glossary of Terms 3
2. Avaya Port Matrix – IP Office R7.0 3
Defining TCP/IP Ports 5
What are ports and how are they used? 5
Port Type Ranges 5
Well Known Ports 5
Registered Ports 5
Dynamic Ports 6
Sockets 6
TFTP Port Usage 7
IP Office IP Port Usage 8
1. References 12
1. Change History 12

1. Introduction

This document covers the IP port usage of the IP Office solution components: Each document major issue reflects the status of one release of IP Office. See the change history for a list of IP Office releases and document issues.

Section 2 is the core of any customer facing documentation, none of the other document content should be used.

1.1. Roles and Responsibilities

Details	Role	Initials
Tim Riches +44 (0)1707 364289 timriches@avaya.com	Author	TJR

1.2. Glossary of Terms

2. Avaya Port Matrix – IP Office R7.0

ALL INFORMATION IS BELIEVED TO BE CORRECT AT THE TIME OF PUBLICATION AND IS PROVIDED "AS IS". AVAYA INC. DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND FURTHERMORE, AVAYA INC. MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE INFORMATION PROVIDED HEREIN WILL ELIMINATE SECURITY THREATS TO CUSTOMERS' SYSTEMS. AVAYA INC., ITS RELATED COMPANIES, DIRECTORS, EMPLOYEES, REPRESENTATIVES, SUPPLIERS OR AGENTS MAY NOT, UNDER ANY CIRCUMSTANCES BE HELD LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, EXEMPLARY, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF THE INFORMATION PROVIDED HEREIN. THIS INCLUDES, BUT IS NOT LIMITED TO, THE LOSS OF DATA OR LOSS OF PROFIT, EVEN IF AVAYA WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOUR USE OF THIS INFORMATION CONSTITUTES ACCEPTANCE OF THESE TERMS.

© 2011 Avaya Inc. All Rights Reserved. All trademarks identified by the ® or ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners.

Defining TCP/IP Ports

What are ports and how are they used?

TCP and UDP use ports (defined at http://www.iana.org/assignments/port-numbers) to route traffic arriving at a particular IP device to the correct upper layer application. These ports are logical descriptors (numbers) that help devices multiplex and de-multiplex information streams. Consider your desktop PC. Multiple applications may be simultaneously receiving information. In this example, email may use destination TCP port 25, a browser may use destination TCP port 80 and a telnet session may use destination TCP port 23. These logical ports allow the PC to de-multiplex a single incoming serial data packet stream into three mini-streams inside the PC. Furthermore, each of the mini-streams is directed to the correct high-level application because the port numbers identify which application each data mini-stream belongs. Every IP device has incoming (Ingress) and outgoing (Egress) data streams.

Ports are used in TCP and UDP to name the ends of logical connections which carry data flows. TCP and UDP streams have an IP address and port number for both source and destination IP devices. The pairing of an IP address and a port number is called a socket (discussed later). Therefore, each data stream is uniquely identified with two sockets. Source and destination sockets must be known by the source before a data stream can be sent to the destination. Some destination ports are “open” to receive data streams and are called “listening” ports. Listening ports actively wait for a source (client) to make contact to a destination (server) using a specific port that has a known protocol associate with that port number. HTTPS, as an example, is assigned port number 443. When a destination IP device is contacted by a source device using port 443, the destination uses the HTTPS protocol for that data stream conversation.

Port Type Ranges

Port numbers are divided into three ranges: Well Known Ports, Registered Ports, and Dynamic Ports (sometimes called Private Ports).

Well Known Ports are those numbered from 0 through 1023.

Registered Ports are those numbered from 1024 through 49151

Dynamic Ports are those numbered from 49152 through 65535

The Well Known and Registered ports are assigned by IANA (Internet Assigned Numbers Authority) and are found here: http://www.iana.org/assignments/port-numbers.

Well Known Ports

For the purpose of providing services to unknown clients, a service listen port is defined. This port is used by the server process as its listen port. Common services often use listen ports in the well known port range. A well known port is normally active meaning that it is “listening” for any traffic destined for a specific application. For example, well known port 23 on a server is actively waiting for a data source to contact the server IP address using this port number to establish a Telnet session. Well known port 25 is waiting for an email session, etc. These ports are tied to a well understood application and range from 0 to 1023.

In UNIX and Linux operating systems, only root may open or close a well-known port. Well Known Ports are also commonly referred to as “privileged ports”.

Registered Ports

Unlike well known ports, these ports are not restricted to the root user. Less common services register ports in this range. Avaya uses ports in this range for call control. Some, but not all, ports used by Avaya in this range include: 1719/1720 for H.323, 5060/5061 for SIP, 2944 for H.248 and others. The registered port range is 1024 – 49151. Even though a port is registered with an application name, industry often uses these ports for different applications. Conflicts can occur in an enterprise when a port with one meaning is used by two servers with different meanings.

Dynamic Ports

Dynamic ports, sometimes called “private ports”, are available to use for any general purpose. This means there are no meanings associated with these ports (similar to RFC 1918 IP Address Usage). These are the safest ports to use because no application types are linked to these ports. The dynamic port range is 49152 – 65535.

Sockets

A socket is the pairing of an IP address with a port number. An example would be 192.168.5.17:3009, where 3009 is the socket number associated with the IP address. A data flow, or conversation, requires two sockets – one at the source device and one at the destination device. The data flow then has two sockets with a total of four logical elements. Each data flow must be unique. If one of the four elements is unique, the data flow is unique. The following three data flows are uniquely identified by socket number and/or IP address.

Data Flow 1:	172.16.16.14:1234	-	10.1.2.3:2345
Data Flow 2:	172.16.16.14.123**5**	-	10.1.2.3:2345
Data Flow 3:	172.16.16.14:1234	-	10.1.2.4:2345

Data flow 1 has two different port numbers and two different IP addresses and is a valid and typical socket pair.

Data flow 2 has the same IP addresses and the same port number on the second IP address as data flow 1, but since the port number on the first socket differs, the data flow is unique.

Therefore, if one IP address octet changes, or one port number changes, the data flow is unique.

Figure 1, below is an example showing ingress and egress data flows from a PC to a web server.

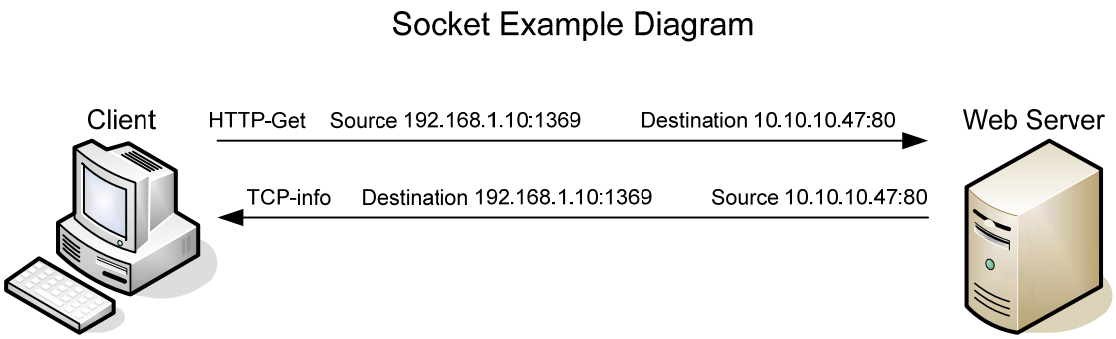

Figure 1. Socket Example

Notice the client egress stream includes the client’s source IP and socket (1369) and the destination IP and socket (80). The ingress stream has the source and destination information reversed because the ingress is coming from the server.

TFTP Port Usage

IP Office, Upgrade wizard and VM Pro all use TFTP for commands and data transfer. IP Office implements a variation of the TFTP Transfer Identifier mechanism (TID) defined by RFC 1350.

The general mechanism is each has a TFTP listener on port 69, any received command (READ request) is responded to with a TFTP response (WRITE request) to port 69. Any subsequent data transfer uses the source ports from both request and response. e.g:

IP Office Manager (Upgrade Wizard)	**IP Office**
TFTP Read, src port 2421, dst port 69 ->	
	<- TFTP Write, src port 4153, dst port 69
	<- TFTP Data packet (1..n), src port 4153, dst port 2421
TFTP Acks (1..n), src port 2421, dst port 4153	

IP Office IP Port Usage

Following table lists the UDP and TCP port usage for the IP Office solution, comprising:

- IP Office
- IP Office on Linux
- IP Office Manager
- Voicemail Pro
- Upgrade Wizard (now part of IP Office Manager)
- Phone Manager
- Soft Console
- one-X Portal for IP Office
- Customer Call Reporter
- System Status Application
- System Monitor
- Applications Appliance

Service	Ports (Protocol)	Applies to	Required for	Enabled by	Authentication of service configuration	Authentication of service use
SSH	22 (TCP)	IP Office on Linux	Remote maintenance connection	None	None	Password + username
SMTP client	25 (TCP)	IP Office, IP Office on Linux	Email transmission from IP Office	Configuration setting	Username + Password	None
TIME	37 (UDP)	IP Office, Manager, Voicemail Pro	TIME (RFC868) Service supported by Manager and VMPro. Requested by IP Office	Configuration setting	None	None
DNS	53 (UDP)	IP Office, Any	DNS Server Name Service	Configuration setting	Username + Password	None
DHCP Server	67 (UDP)	IP Office, Any	IP Office DHCP service to clients, including IP Phones	Configuration setting	Username + Password	None
DHCP Client	68 (UDP)	IP Office, IP Office on Linux	IP Office obtaining DHCP address from a server	Configuration setting	Username + Password	None
BOOTP Server	67 (UDP)	Manager	Offering IP address & firmware to IP Office	Configuration setting	Username + Password	None
BOOTP Client	68 (UDP)	IP Office, IP Office on Linux	Obtaining IP address & firmware for IP Office from Manager	Configuration setting	Username + Password	None
TFTP	69 (UDP) See note 1 below	IP Office, IP Office on Linux, Legacy Manager, Voicemail Pro, Upgrade Wizard, Phone Manager, Soft Console	IP Office status, configuration data, program data, Whois #1	Security Setting	Username + Password	Obfuscated password
HTTP	80 (TCP)	IP Office, IP Office on Linux, Manager, Customer Call Reporter	File transfer Web client Access	Configuration setting	Username + Password	None

Service	Ports (Protocol)	Applies to	Required for	Enabled by	Authentication of service configuration	Authentication of service use
NTP	123 (UDP)	IP Office, IP Office on Linux	NTP (RFC4330) Service	Configuration setting	None	None
SNMP Agent	161 (UDP) configurable 161, 1024-65535	IP Office, IP Office on Linux	Read-only access to MIB entries	Configuration setting	Username + Password	Community String
SNMP Trap	162	IP Office, IP Office on Linux	Trap generation fro IP Office	Configuration setting	Username + Password	Community String
LDAP	389 (TCP + UDP)	IP Office, IP Office on Linux	Import of directory information from LDAP database	Configuration setting	Username + Password	Kerberos 4 or simple password
HTTPS	443 (TCP)	IP Office, IP Office on Linux, Customer Call Reporter, Voicemail Pro	Provisioning Avaya Softphone File transfer Web client access	Configuration setting	Username + Password	Shared secret (Softphone) X.509 certificate (IP Office)
IKE	500 (UDP)	IP Office, IP Office on Linux	Form IPSec associations with remote security devices	Configuration setting, requires licence	Username + Password, licence verification	IPSec (shared secret) MD5 or SHA
Syslog client	514 (UDP)	IP Office, IP Office on Linux	Syslog client	Configuration setting	Username + Password	None
RIP	520 (UDP)	IP Office, IP Office on Linux	Exchange routing information with adjacent IP routers, or receive information only	Configuration settings	Username + Password	None
Network Relay	833 (UDP)	IP Office, IP Office on Linux	Network Relay	None	None	None
L2TP	1701 (UDP)	IP Office	Form layer 2 tunnels to remote network devices	Configuration setting	Username + Password	CHAP
H.323 discovery	1718 (TCP)	IP Office, IP Office on Linux	Offering H.323 service to IP phones	Configuration setting	Username + Password	Shared Secret (Password), HMAC-SHA1-96
H.323 status	1719 (TCP)	IP Office, IP Office on Linux	Offering H.323 service to IP phones	Configuration setting	Username + Password	Shared Secret (Password), HMAC-SHA1-96
H.323 Signalling	1720 (TCP)	IP Office, IP Office on Linux	Offering H.323 service to IP phones	Configuration setting	Username + Password	Shared Secret (Password), HMAC-SHA1-96
Log4j	4560 (TCP)	One-X Portal for IP Office	Log4j socket appender	None	N/A	None
Python2.6	7070 (TCP)	IP Office on Linux, Applications Appliance	Web Control Panel access	None	None	Password + username
HTTP	8000 (TCP)	Voicemail Pro	Web client Access	Installation setting	Install option	Username + password
Tomcat shutdown	8005 (TCP)	One-X Portal for IP Office	Tomcat shutdown listener	None	N/A	None
HTTP	8080 (TCP)	One-X Portal for IP Office	Web client Access	Installation setting	Install option	Username + password
HTTPS	8443 (TCP)	One-X Portal for IP Office	Web client access	Installation setting	Install option	Username + password
JMX	8666 (TCP)	One-X Portal for IP Office	Java Management Extensions	Installation setting	Install option	Username + password
JDBC	9092 (TCP)	One-X Portal for IP Office	Database client listener	None	Install option	Username + password

Service	Ports (Protocol)	Applies to	Required for	Enabled by	Authentication of service configuration	Authentication of service use
SIP	5060 (TCP+UDP)	IP Office, IP Office on Linux	SIP Trunks, SIP Registrar, SIP Proxy	Configuration setting	Username + Password	MD5 CHAP
RTP/RTCP	X to X+1024 (UDP)	IP Office, IP Office on Linux, Voicemail Pro	X configurable by Manager, default range 49152-53246, min start 1024, min end 2048.	Configuration setting	Username + Password	
acmsComms	10334	IP Office on Linux	Media Server usage	None	None	None
aSoftMS	42000+ (UDP)	IP Office on Linux	Allocating connections between Media Server and IP Phones	None	None	None
Voicemail	50791 (UDP)	IP Office, IP Office on Linux	Voicemail licence polling port	Security Setting, Configuration setting	Username + Password	None
Solomail	50793	IP Office, IP Office on Linux	TAPI Wave Driver – audio stream interface for TAPI-based applications	See TAPI	See TAPI	None
Monitor	50794 (UDP+TCP)	IP Office, IP Office on Linux System Monitor (UDP)	Event, trace and diagnostic outputs	Always enabled	None	Password
Voicenet	50795	IP Office	Small Community Networks – peer-to-peer trunk signalling	Configuration setting	Password	None
PC Partner	50796 (TCP)	IP Office, IP Office on Linux, Phone Manager, Soft Console	Control of telephones from Phone Manager, Soft Console	Security Setting	Username + Password	Password
TAPI	50797 (TCP)	IP Office, IP Office on Linux	Control of telephony via TAPI, first or third party	Security Setting, Third party TAPI requires licence	Username + Password, Licence verification	None
Dongle server	50780 (UDP)	IP Office	Dongle proxy	Hidden Configuration setting	Username + Password	None
EConf	50801	IP Office	Voice conferencing application	Security Setting, Requires licence	Username + Password, licence verification	None
Who Is #2	50802 (TCP)	IP Office, IP Office on Linux	TCP discovery	Security setting	None	None
Configuration service - unsecured	50804 (TCP) configurable 49152-65280	IP Office Manager	IP Office Configuration	Security settings	Password + username	HMAC SHA-1 challenge sequence
Configuration service – secured (TLS)	50805 (TCP) configurable 49152-65280	IP Office Manager	IP Office Configuration	Security settings	Password + username	HMAC SHA-1 challenge sequence, X.509 certificate.
SSI service - unsecured	50808 (TCP) configurable 49152-65280	System Status Application	IP Office status information	Security settings	Password + username	HMAC SHA-1 challenge sequence
Security Settings service - unsecured	50812 (TCP) configurable 49152-65280	IP Office Manager	IP Office security configuration	Security settings	Password + username	HMAC SHA-1 challenge sequence
Security	50813	IP Office Manager	IP Office security	Security	Password +	HMAC SHA-1

Service	Ports (Protocol)	Applies to	Required for	Enabled by	Authentication of service configuration	Authentication of service use
settings service – secured (TLS)	(TCP) configurable 49152-65280		configuration	settings	username	challenge sequence
EnhTSPI service - unsecured	50814 (TCP) configurable 49152-65280	one-X Portal for IPO	IP Office CTI control	Security settings	Password + username	HMAC SHA-1 challenge sequence

3. References

No.	Name	Issue	ID	Author
[a]	DEFINITY Single Connect IP Terminal Protocol Specification	2.6	CID 77121	Rob Mitchell
[b]	IP Office Service Access Protocol	1.1	CID 136988	Tim Riches
[c]				
[d]				

4. Change History

Issue	Date		Modified by
1.0	26th Nov 2010	Issue 1.x release for IP Office Release 6.0	TJR
2.0	7th January 2011	Issue 2.x release for IP Office Release 6.1	TJR
3.0	10th January 2011	Issue 3.x release for IP Office Release 7.0	TJR