Understand Unified Wireless Network Protocol (CUWN WLC) and Port Matrix

Contents

Introduction

This document describes information about port numbers used by the Unified Wireless solution.

Background Information

The main purpose of this document is to provide a consolidated source of communication protocols that incorporate a CUWN solution. Goals are to implement appropriate firewall and security policies based on this information to properly secure the CUWN infrastructure.

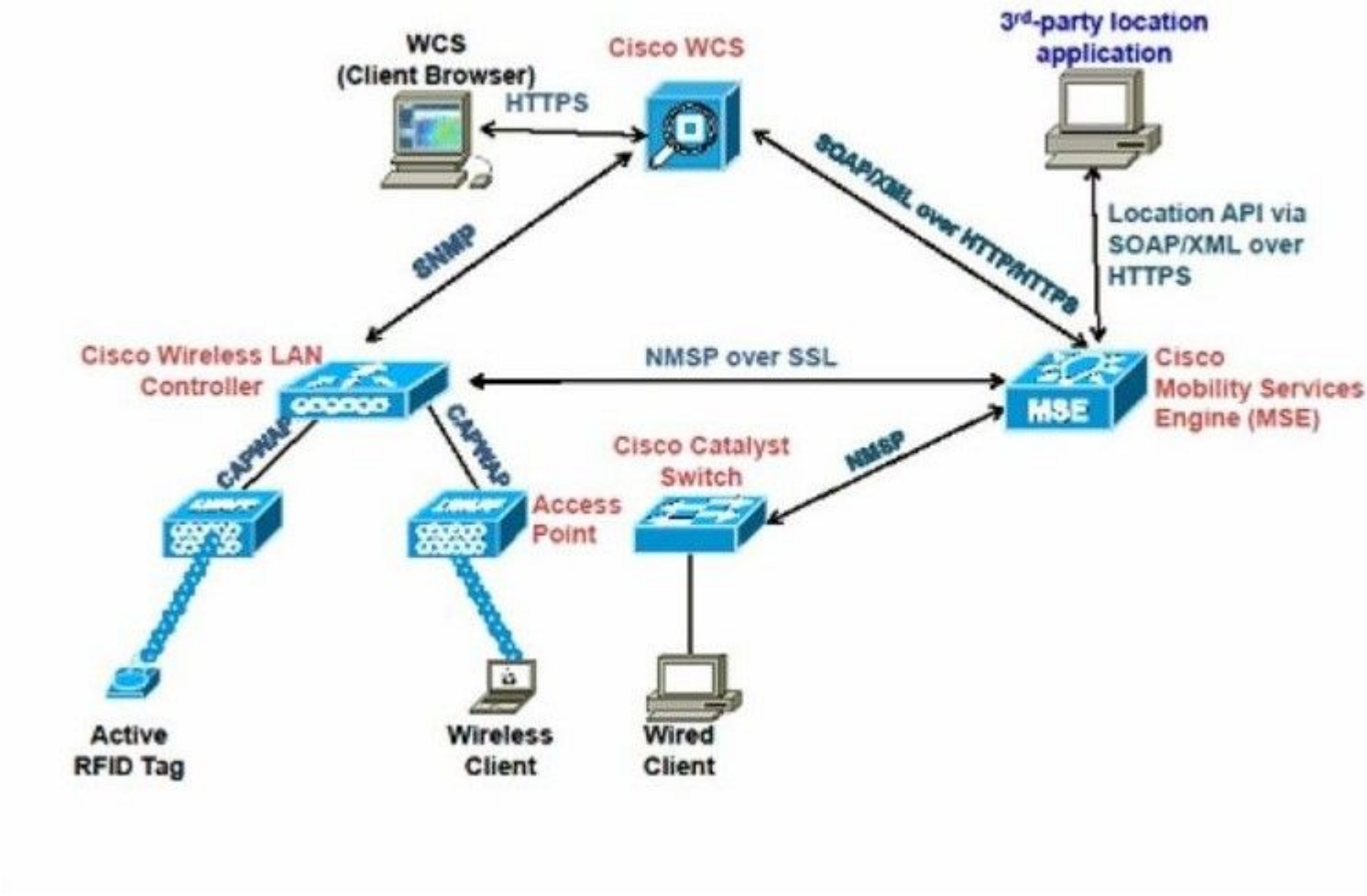
Terms Used

Here is a list of terms used in this document:

- Wireless Control System - WCS
- Network Control System - NCS
- Cisco Prime Infrastructure - PI
- Wireless LAN Controller - WLC
- Mobility Services Engine - MSE
- Operating System - OS
- Access Point - AP
- Secure Shell - SSH
- Simple Mail Transfer Protocol - SMTP
- Authentication, Authorization, and Accounting - AAA
- Domain Name System - DNS
- Identity Services Engine - ISE
- Network Time Protocol - NTP
- Simple Object Access Protocol - SOAP
- High Availability - HA
- Quality of Service - QoS
- Database - DB
- Remote Desktop Protocol - RDP

- Virtual Network Computing - VNC
- Transport Layer Security - TLS
- Cisco Location Control Protocol - LOCP
- Internet Control Message Protocol - ICMP
- Simple Network Management Protocol - SNMP
- Network Mobility Services Protocol - NMSP
- Adaptive Wireless Intrusion Prevention System - AwIPS
- Ethernet over IP - EoIP
- Rogue Location Discovery Protocol - RDLP
- Control and Provisioning of Wireless Access Points - CAPWAP
- Light Weight Access Point Protocol - LWAPP
- Network Spectrum Interface - NSI
- OfficeExtend Access Point - OEAP

Network Overview



Network Diagram

Protocol and Port Number Information

Here is a list of tables in this document:

Table 1. WCS/NCS/PI Protocols and Ports

WCS/NCS/PI Protocols				
Source Device	**Destination Device**	**Protocol**	**Destination Port**	**Description**
WCS/NCS/PI	WLC and MSE	TCP	21	FTP - Used to transfer files

				to/from devices
Various Management Stations	WCS Host Server OS-Linux	TCP	22	SSH - Used for remote Linux Host Access
WCS/NCS/PI	Cisco aIOS® AP	TCP	23	Telnet - Used for Cisco aIOS AP Configuration
WCS/NCS/PI	SMTP mail servers	TCP	25	SMTP - used for fault notifications
AAA Servers/ISE	WCS/NCS/PI	TCP/UDP	49	TACACS+
WCS/NCS/PI	aIOS AP	UDP	53	DNS - used for Cisco aIOS AP Configuration
WLC	WCS/NCS/PI	UDP	69	TFTP - Used to transfer files to/from devices
Various Management Stations	WCS/NCS/PI	TCP	80	HTTP (Configurable at install time)
NTP Server	WLC	UDP	123	NTP
WLC and MSE	WCS/NCS/PI	UDP	161	SNMP discovery, inventory Cisco aIOS AP and others
WLC and MSE	WCS/NCS/PI	UDP	162	SNMP Trap Receiver
Various Management Stations	WCS/NCS/PI	TCP	443	HTTPS (Configurable at install time)
MSE	WCS/NCS/PI	TCP	443	SOAP/XML (SOAP used for MSE Management
WLC	WCS/NCS/PI	UDP	514	Syslog (Optional)
Local only	WCS/NCS/PI	TCP	1299	RMI Registry port (local

				only)
HA Server and Various others	WCS/NCS/PI	TCP	1315	Database Server HA (QoS)
WCS HA Server	WCS/NCS/PI	TCP	1316-1320	HA DB Ports
AAA Servers/ISE	WCS/NCS/PI	UDP	1812/1645	RADIUS
AAA Servers/ISE	WCS/NCS/PI	UDP	1813/1646	RADIUS
Various Management Stations	WCS Host Server OS-Microsoft Windows	TCP/UDP	3389	RDP - Microsoft Windows Remote Desktop (Optional)
Various	WCS/NCS/PI	TCP	5001	Apache Axis SOAP Monitoring: Java Listener
Various Management Stations	WCS Host Server OS-Microsoft Windows	TCP	5500	VNC - (Optional) Used for remote Microsoft Windows Host Access
Various Management Stations	WCS Host Server OS-Microsoft Windows	TCP	5800	VNC - (Optional) Used for remote Microsoft Windows Host Access
Various Management Stations	WCS Host Server OS-Microsoft Windows	TCP/UDP	5900	VNC - (Optional) Used for remote Microsoft Windows Host Access
Local only	WCS/NCS/PI	TCP	6789	RMI Server Port (local only)
MSE - Location Appliance	WCS/NCS/PI	TCP	8001	Location Server Data Sync. Communication Port
Local only	WCS/NCS/PI	TCP	8005	Tomcat Shutdown Port
Local only	WCS/NCS/PI	TCP	8009	Web Server/Java Server Connector (local only)
HA Web Server	WCS/NCS/PI	TCP	8082	HA Web Server Port: Health

				Monitor for WCS HA
Various Management Stations	WCS/NCS/PI	TCP	8456	HTTP Connector
Various Management Stations	WCS/NCS/PI	TCP	8457	HTTP Redirect
Various Management Stations	WCS/NCS/PI	TCP	16113	LOCP TLS Port
WLC	WCS/NCS/PI	UDP	29001-29005	TFTP Child threads
Various	AP	ICMP		ICMP - Optional
WLC	CMX 10.2.X	NMSP, AoA, 80, 443, 161,162	16113, 2003, HTTP, HTTPS, ICMP, SNMP	

Table 2. MSE - AwIPS Protocols

MSE - AwIPS Protocols				
Source Device	**Destination Device**	**Protocol**	**Destination Port**	**Description**
WCS/NCS/PI	MSE	TCP	21	FTP - Used to transfer files to/from devices
Various Management Stations	MSE Host Server OS-Linux	TCP	22	SSH - Used for remote Linux Host Access
WCS/NCS/PI	MSE	TCP	80	HTTP (Configurable at install time)
NTP Server	WLC	UDP	123	NTP

WCS/NCS/PI	MSE	UDP	161	SNMP
MSE	WCS/NCS/PI	UDP	162	SNMP Trap Receiver
WCS/NCS/PI	MSE	TCP	443	HTTPS (Configurable at install time)
WCS/NCS/PI	MSE	TCP	443	SOAP/XML
WCS/NCS/PI	MSE	TCP	8001	HTTPS (Configurable at install time)
WLC	MSE and Spectrum Expert	TCP	16113	NMSP
Various	AP	ICMP		ICMP - Optional

Table 3. MSE - Context Protocols

MSE - Context-Aware and AwIPS Protocols				
Source Device	**Destination Device**	**Protocol**	**Destination Port**	**Description**
WCS/NCS/PI	MSE	TCP	21	FTP - Used to transfer files to/from devices
Various Management Stations	MSE Host Server OS-Linux	TCP	22	SSH - Used for remote Linux Host Access
WCS/NCS/PI	MSE	TCP	80	HTTP (Configurable at install time)
NTP Server	WLC	UDP	123	NTP
WCS/NCS/PI	MSE	UDP	161	SNMP
MSE	WCS/NCS/PI	UDP	162	SNMP Trap Receiver

WCS/NCS/PI	MSE	TCP	443	HTTPS (Configurable at install time)
WCS/NCS/PI	MSE	TCP	443	SOAP/XML
WCS/NCS/PI	MSE	TCP	8001	HTTPS (Configurable at install time)
WLC and Catalyst LAN Switches	MSE and Spectrum Expert	TCP	16113	NMSP
Various	AP	ICMP		ICMP - Optional

Table 4. WLC Protocols

WLC Protocols					
Source Device	**Destination Device**	**Protocol**	**Destination Port**	**Source Port**	**Description**
WCS/NCS/PI	WLC	TCP	21	0:65535	FTP - Used to transfer files to/from devices
WCS and Various Management Stations	WLC	TCP	22	0:65535	SSH - Used for remote Management (Optional)
WCS and Various Management Stations	WLC	TCP	23	0:65535	Telnet - Used for remote Management (Optional)
AAA Servers/ISE	WLC	TCP/UDP	49	0:65535	TACACS+
WCS and Various Management Stations	WLC	UDP	69	0:65535	TFTP - Used to transfer files to/from devices
Various Management Stations	WLC	TCP	80	0:65535	HTTP (Configurable at install time)
WLC	WLC	TCP	91	0:65535	
WLC Mobility Group	WLC	EoIP IP	EoIP IP	0:65535	EoIP Tunnel - Client

members		Protocol 97	Protocol 97		Anchor/Tunneling traffic
NTP Server	WLC	UDP	123	0:65535	NTP
WCS/NCS/PI	WLC	UDP	161	161	SNMP
WCS/NCS/PI	WLC	UDP	162	0:65535	SNMP Trap Receiver
Various Management Stations	WLC	TCP	443	0:65535	HTTPS (Configurable at install time)
WLC and Various Syslog Servers	WLC	UDP	514	0:65535	Syslog (Optional)
AAA Servers/ISE	WLC	UDP	1812/1645	0:65535	RADIUS
AAA Servers/ISE	WLC	UDP	1813/1646	0:65535	RADIUS
AP	WLC	UDP	6352	0:65535	RDLP
Various Management Stations (MSE, Spectrum Expert)	WLC	TCP	16113	0:65535	LOCP TLS Port NMSP
WLC	WLC	UDP	16666	16666	Mobility - non-secured
WLC	WLC	UDP	16667		Mobility - secured ** In release. 5.2+ feature was removed
AP	WLC	UDP	5246-5247	0:65535	CAPWAP Ctl/Data
AP	WLC	UDP	5248	0:65535	CAPWAP Mcast.
Various	AP	ICMP			ICMP - Optional
mDNS	WLC/network	UDP	5353	0:65535	mDNS
RADIUS server	WLC	UDP	1700	0::65535	CoA radius packets

Table 5. AP Protocols

AP CAPWAP-LWAPP Protocols				
Source Device	**Destination Device**	**Protocol**	**Destination Port**	**Description**
Various	AP	UDP	69	TFTP - used for remote code update
Various	AP	TCP	22	SSH - used for optional remote troubleshooting access. Can be administratively disabled.
Various	AP	TCP	23	Telnet - used for optional remote troubleshooting access. Can be administratively disabled.
AP	DNS Server	TCP/UDP	53	DNS
AP	DHCP Server	UDP	68	DHCP
AP	Various	UDP	514	Syslog - Destination configurable. The default is 255.255.255.255.
WLC	AP	UDP	1024 - 65535*	CAPWAP Ctl/Data
WLC	AP	UDP	5248	CAPWAP Mcast.
AP	WLC	UDP	6352	RDLP
AP	Monitor PC	TCP	37540 for 2.4 GHz 37550 for 5GHz	NSI Protocol for SE-Connect
Various	AP	ICMP		ICMP - Optional
AP	AP	UDP	16670	Client policies (AVC)

* - Arbitrary port number is assigned to every AP from the range 1024 - 65535 when the AP joins the WLC. The WLC uses the number as the Destination Port for CAPWAP Ctl/Data as long as the AP is connected.

Table 6. OEAP600 Firewall Protocols

AP CAPWAP-LWAPP Protocols				
Source Device	**Destination Device**	**Protocol**	**Destination Port**	**Description**
WLC	AP	UDP	5246-5247	CAPWAP Ctl/Data