Handling DOCSIS cable modem and MTA configuration files

www.worldwidesupply.net
Goal of the training

• The purpose of this training is to give you a better understanding of CPE config files and how best to use them to your advantage. Regardless of the manufacturer you are currently using be it Cisco, Arris-Motorola or WWS know that the functionality of all CPE’s is the same but each OEM has their particular way of doing things.

• I want to help you create a standard that best fits your needs and customer demands.
Main Topics

1. Service flows and classifiers
2. Global parameters and SNMP configuration objects
3. Managing vendor objects on configuration files
4. Best practices
CM structure and Basic Service flows

Main
{
    NetworkAccess 1;    /* enables packet forwarding */
    GlobalPrivacyEnable 0; /* disables BPI(encryption) */
    MaxCPE 3;           /* allows max 3 user devices */
}

UsServiceFlow         /* creates an upstream service flow */
{
    UsServiceFlowRef 1;    /* SF number */
    QosParamSetType 7;    /* activates SF */
    TrafficPriority 3;    /* sets medium priority */
    MaxRateSustained 128000; /* max upstream transfer rate - 128kb/s */
}

DsServiceFlow         /* creates an downstream service flow */
{
    DsServiceFlowRef 2;    /* SF number */
    QosParamSetType 7;    /* activates SF */
    TrafficPriority 3;    /* sets medium priority */
    MaxRateSustained 1000000; /* max downstream transfer rate - 1Mb/s */
}

NOTE: Ds/UsServiceRef numbers must be unique in cable modem config file
CM Service flows and classifiers

DsServiceFlow
{
   DsServiceFlowRef 1;
   QosParamSetType 7;
   MaxRateSustained 22528000;
   MaxTrafficBurst 10000;
}

DsServiceFlow
{
   DsServiceFlowRef 2;
   QosParamSetType 7;
   TrafficPriority 4;
   MaxRateSustained 10000;
   MinReservedRate 1000; /*min downstream transfer rate - 10 kb/s */
}

UsServiceFlow
{
   UsServiceFlowRef 3;
   QosParamSetType 7;
   MaxRateSustained 4506000;
   MaxTrafficBurst 6000;
   MaxConcatenatedBurst 6000;
   SchedulingType 2;
}

UsPacketClass
{
   ClassifierRef 2;
   ServiceFlowRef 4;
   RulePriority 32;
   LLCPacketClassifier
   {
      EtherType 0x030828;
   }
}

UsPacketClass
{
   ClassifierRef 3;
   ServiceFlowRef 4;
   RulePriority 33;
   IpPacketClassifier
   {
      IpTos 0x6060e0; /*matches ToS 0x06*/
   }
}

DsPacketClass
{
   ClassifierRef 1; /*Classifier number */
   ServiceFlowRef 2;
   RulePriority 32;
   IpPacketClassifier
   {
      IpTos 0x6060e0; /*matches ToS 0x06*/
   }
}

UsServiceFlow
{
   UsServiceFlowRef 4;
   QosParamSetType 7;
   TrafficPriority 4;
   MaxRateSustained 10000;
   MinReservedRate 1000; /*min upstream transfer rate - 10 kb/s */
   SchedulingType 2;
}
CM Global parameters

NetworkAccess 1;
GlobalPrivacyEnable 0;
DownstreamFrequency 410000000; /*optional*/
UpstreamChannelId 3; /*optional*/
MaxCPE 3;
CpeMacAddress 00:00:00:00:00:00; /* device #1 MAC is 00:00... */
CpeMacAddress 11:11:11:11:11:11; /* device #2 MAC is 11:11... */
SwUpgradeFilename "example.bin'';
SwUpgradeServer 10.1.1.1;
MfgCVCDATA 0x3082031c30820204a0030201020107………………..;

Global Parameters explained:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetworkAccess</td>
<td>Controls whether modem forwards data between USB/Ethernet and RF interfaces</td>
<td>0 - forwarding disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - forwarding enabled</td>
</tr>
<tr>
<td>GlobalPrivacyEnable</td>
<td>Enables BPI(encryption on RF interface)</td>
<td>0 - disables BPI</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - enables BPI</td>
</tr>
<tr>
<td>DownstreamFrequency</td>
<td>Specifies downstream channel frequency in Hz</td>
<td>Frequency in HZ</td>
</tr>
<tr>
<td>UpstreamChannelId</td>
<td>Specifies the upstream channel number for that upstream</td>
<td>Desired upstream channel number</td>
</tr>
<tr>
<td>MaxCPE</td>
<td>Number of MAC addresses(computers, network devices), that modem will learn and forward packets from. This includes managed switches, APs etc.</td>
<td>Number of such devices</td>
</tr>
<tr>
<td>CpeMacAddress</td>
<td>Specifies MAC address of a computer/device. Number of CpeMacAddress commands must be less or equal MaxCPE. Usefull when you don't want the modem to learn Access point's IP address</td>
<td>MAC address of one device</td>
</tr>
<tr>
<td>SwUpgradeFilename</td>
<td>Specifies firmware filename on TFTP server.</td>
<td>&quot;filename&quot;</td>
</tr>
<tr>
<td>SwUpgradeServer</td>
<td>Specifies TFTP server IP address</td>
<td>IP address</td>
</tr>
<tr>
<td>MfgCVCDATA</td>
<td>Producers certificate used for firmware upgrade.</td>
<td>Must be used several times to represent whole certificate. Can specify 254 hex chars max at a time.</td>
</tr>
</tbody>
</table>
CM SNMP configuration objects

SNMP access table: (Used to create access SNMP filters from the RF interface to the CM)

```c
SnmpMibObject docsDevNmAccessStatus.1 Integer 4; /* createAndGo */
SnmpMibObject docsDevNmAccessIp.1 IPAddress 192.168.0.1;
SnmpMibObject docsDevNmAccessIpMask.1 IPAddress 255.255.255.0;
SnmpMibObject docsDevNmAccessControl.1 Integer 2; /* read */
SnmpMibObject docsDevNmAccessInterfaces.1 HexString 0x40;
SnmpMibObject docsDevNmAccessCommunity.1 String "some_password";
```

**NOTE:** .1 means that it's first entry - remember to change when adding more.

Nmaccess entries explained:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>docsDevNmAccessStatus</td>
<td>Configures row creation and it's activation</td>
<td>1 - active, 2 - inactive, 4 - create and activate, 5 - create and deactivate, 6 - delete. Stick with 4.</td>
</tr>
<tr>
<td>docsDevNmAccessIp</td>
<td>Specifies source IP of a SNMP query matching this rule.</td>
<td>IP address</td>
</tr>
<tr>
<td>docsDevNmAccessIpMask</td>
<td>Specifies source IP mask of a SNMP query matching this rule.</td>
<td>mask address</td>
</tr>
<tr>
<td>docsDevNmAccessControl</td>
<td>Specifies access privileges</td>
<td>2 - RO, 3 - RW, 4 - RO with traps, 5 - RW with traps, 6 – traps</td>
</tr>
<tr>
<td>docsDevNmAccessInterfaces</td>
<td>Specifies matching interface</td>
<td>0x40 - cable, 0x80 - ethernet, 0xC0,0x00 – both</td>
</tr>
<tr>
<td>docsDevNmAccessCommunity</td>
<td>Specifies the community string</td>
<td>&quot;desired_community_string&quot;</td>
</tr>
</tbody>
</table>
CM SNMP configuration objects

Firewall Rule: (Example to prevent that users send and receive mail traffic trough port 25 (SMTP))

SnmpMibObject docsDevFilterIpControl.7 Integer 1; /* discard */
SnmpMibObject docsDevFilterIpIfIndex.7 Integer 0;
SnmpMibObject docsDevFilterIpDirection.7 Integer 3; /* both */
SnmpMibObject docsDevFilterIpBroadcast.7 Integer 2; /* false */
SnmpMibObject docsDevFilterIpSaddr.7 IPAddress 0.0.0.0;
SnmpMibObject docsDevFilterIpSmask.7 IPAddress 0.0.0.0;
SnmpMibObject docsDevFilterIpDaddr.7 IPAddress 0.0.0.0;
SnmpMibObject docsDevFilterIpDmask.7 IPAddress 0.0.0.0;
SnmpMibObject docsDevFilterIpProtocol.7 Integer 6;
SnmpMibObject docsDevFilterIpSourcePortLow.7 Integer 0;
SnmpMibObject docsDevFilterIpSourcePortHigh.7 Integer 65535;
SnmpMibObject docsDevFilterIpDestPortLow.7 Integer 25;
SnmpMibObject docsDevFilterIpDestPortHigh.7 Integer 25;
SnmpMibObject docsDevFilterIpStatus.7 Integer 4; /* createAndGo */

NOTE: .7 means the index of the entry - remember to change when adding more.

Firewall entries explained:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>docsDevFilterIpControl</td>
<td>Discards or accepts the traffic</td>
<td>1 - discard, 2 – accept</td>
</tr>
<tr>
<td>docsDevFilterIpDirection</td>
<td>Specifies the direction of packet to match.</td>
<td>1 - incoming, 2 - outgoing, 3 - both directions</td>
</tr>
<tr>
<td>docsDevFilterIpBroadcast</td>
<td>Matches ONLY broadcast traffic.</td>
<td>1 - yes, 0 – no</td>
</tr>
<tr>
<td>docsDevFilterIpStatus</td>
<td>Configures row creation and it's activation</td>
<td>1 - active, 2 - inactive, 4 - create and activate, 5 - create and deactivate, 6 - delete. Stick with 4.</td>
</tr>
</tbody>
</table>
Example of a MTA MGCP config file.

```
Main
{
    MtaConfigDelimiter 1;
    SnmpMibObject pktcMtaDevEnabled.0 Integer 1; /* true */
    SnmpMibObject pktcMtaDevRealmOrgName.'BASIC.1' String "CableLabs, Inc.";
    SnmpMibObject pktcMtaDevCmsKerbRealmName.'METASWITCH.EXAMPLE.NET' String "BASIC.1";
    SnmpMibObject pktcNcsEndPntConfigCallAgentId.9 String "WWS.TEST.COM.NET";
    SnmpMibObject pktcNcsEndPntConfigCallAgentUdpPort.9 Integer 2727;
    SnmpMibObject pktcNcsEndPntConfigMWD.9 Integer 10;
    SnmpMibObject pktcNcsEndPntConfigCallAgentId.10 String "WWS.TEST.COM.NET";
    SnmpMibObject pktcNcsEndPntConfigCallAgentUdpPort.10 Integer 2727;
    SnmpMibObject pktcNcsEndPntConfigMWD.10 Integer 10;
    SnmpMibObject pktcMtaDevCmsIpsecCtrl.'WWS.TEST.COM' Integer 2; /* false */
    MtaConfigDelimiter 255;
}
```

NOTE: .9 means the index of the physical telephone port number 1. The ports begin from .9 and can increase depending on the physical ports of the MTA. For example, a MTA with 12 ports can use the .9 as first port and .20 as last port. The configuration of each port can be different.
Example of a MTA SIP config file using Hitron MIBS.

```plaintext
Main
{
    MtaConfigDelimiter 1;
    SnmpMibObject htSipEndPntConfigUserId.9 String "6007" ;
    SnmpMibObject htSipEndPntConfigUserName.9 String "show6007" ;
    SnmpMibObject htSipEndPntConfigUserPassword.9 String "123456" ;
    SnmpMibObject htSipEndPntConfigUserAuthName.9 String "6007" ;
    SnmpMibObject htSipEndPntConfigUserDigitMap.9 String "x[0-9].T" ;
    SnmpMibObject htSipEndPntConfigRegistrarId.9 String "192.168.1.50" ;
    SnmpMibObject htSipEndPntConfigRegistrarSigPort.9 Gauge32 5060 ;
    SnmpMibObject htSipEndPntConfigRegistrarRetryTimeout.9 Gauge32 3601 ;
    SnmpMibObject htSipEndPntConfigProxyId.9 String "192.168.1.50" ;
    SnmpMibObject htSipEndPntConfigProxySigPort.9 Gauge32 5060 ;
    SnmpMibObject htSipEndPntConfigOutboundProxyId.9 String "0.0.0.0" ;
    SnmpMibObject htSipEndPntConfigOutboundProxySigPort.9 Gauge32 0 ;
    SnmpMibObject htSipEndPntConfigUserPacketPeriod.9 Integer 20;
    MtaConfigDelimiter 255;
}
```

NOTE: .9 means the index of the physical telephone port number 1. The ports begin from .9 and can increase depending on the physical ports of the MTA. For example, a MTA with 12 ports can use the .9 as first port and .20 as last port. The configuration of each port can be different.
List of SNMP Objects from some vendors.
This assignment is made by IANA. (http://www.iana.org/assignments/enterprise-numbers/enterprise-numbers)

SnmpMibObject enterprises.8595 /*WWS Technology*/
SnmpMibObject enterprises.1166 /*Motorola (before General instruments)*/
SnmpMibObject enterprises.1429 /*Cisco (before Scientific Atlanta)*/
SnmpMibObject enterprises.4115 /*Arris*/
SnmpMibObject enterprises.2863 /*Technicolor (before Thomson)*/
SnmpMibObject enterprises.4684 /*Ubee (before Ambit)*/
SnmpMibObject enterprises.7432 /*Excentis (this mib objects are commonly used in telephony)*/ ;

SnmpMibObject enterprises.4491 /*CableLabs*/
SnmpMibObject enterprises.4413 /*Broadcom*/
SnmpMibObject enterprises.343 /*Texas Instrument*//(before Intel)
CM and MTA SNMP Vendor objects

Example of useful vendor SNMP objects (WWS).

Wifi

SnmpMibObject enterprises.8595.80211.1.1.0 Integer 2; /*Wifi is enable and the GUI can only be accessed via RF IP*/

SnmpMibObject enterprises.8595.80211.1.4.0 Gauge32 1; /*Controls the wifi channel (1 – 14)*/

SnmpMibObject enterprises.8595.80211.5.1.14.1.3.0 String “El Caribe”; /*Sets the SSID*/ “example branding name (El Caribe) as ssid for all vendors”

SnmpMibObject enterprises.8595.80211.5.1.14.1.5.0 Integer 3; /*Sets the Wifi security to WPA2PSK*/

SnmpMibObject enterprises.8595.80211.5.2.4.1.2.0 String “passw”; /*Sets the WPA password*/ “example MSO national default password (i love el Caribe)

SnmpMibObject enterprises.8595.80211.100.0 Integer 1; /*Apply settings to the hardware*/

Note: any settings made are stored to non-volatile storage ONLY unless this object is set to 1.

Gateway Management

SnmpMibObject enterprises.8595.2.1.2.10.1.2.0 String “pass”; /*Changes the password of the GUI access*/ example (for branding use your MOS name with symbols and numbers since user will change it to its own but if reset to factory it will go back to MSO default configuration easy for support)

SnmpMibObject enterprises.8595.4.1.5.0 IPAddress 192.168.0.10; /*Sets the start IP of the Gateway DHCP*/

SnmpMibObject enterprises.8595.4.1.6.0 Integer 10; /*Sets the number of clients the DHCP server will handle*/
CM and MTA SNMP Vendor objects

Example of useful vendor SNMP objects (WWS).

MTA

SnmpMibObject enterprises.8595.3653.9.5.1 Integer 1; /*Sets the country code to USA for SIP and MGCP*/
SnmpMibObject enterprises.8595.3653.8.2.3.1.14.9 Integer 2; /*Enable SIP 3Way Calling on Port 1*/
SnmpMibObject enterprises.8595.3653.8.2.3.1.14.10 Integer 2; /*Enable SIP 3Way Calling on Port 2*/
SnmpMibObject iso.3.6.1.4.1.8595.3653.8.2.5.1.2.9 Integer 3; /*Enable G.729 on Port 1 (This is for SIP ONLY)*/
SnmpMibObject iso.3.6.1.4.1.8595.3653.8.2.5.1.2.10 Integer 3; /*Enable G.729 on Port 2 (This is for SIP ONLY)*/
SnmpMibObject iso.3.6.1.4.1.8595.3653.8.100.0 Integer 1; /*Apply SIP Changes*/

Note: Any settings made are stored to non-volatile storage ONLY unless this object is set to 1.

Example of handle telephony tones for some vendors that not use country code.

SnmpMibObject enterprises.7432.2.1.1.33.1.2.3.1 Gauge32 425; /*Sets the Dial tone to 425Mhz*/
SnmpMibObject enterprises.7432.2.1.1.33.1.2.6.1 Gauge32 425; /*Sets the Ring Back tone to 425Mhz*/
SnmpMibObject enterprises.7432.2.1.1.33.1.9.6.1 Gauge32 1000; /*Sets the Ring Back tone on to 1000ms*/
SnmpMibObject enterprises.7432.2.1.1.33.1.10.6.1 Gauge32 4500; /*Sets the Ring Back tone off to 4500ms*/

Note: There are many mibs from Excentis, so it's necessary to confirm with the vendor which works for the selected MTA..
Best Practices

1. If there is a doubt of the value of a MIB or how a MIB is used, it’s a good idea to do an SNMPWALK to the CM or MTA.

2. It’s necessary to contact each vendor to obtain the MIBs tree of each one.

3. Most of the parameters of the CM, MTA, Gateway, etc can be managed via config file, and the MIB objects that are used on the config file can be used via SNMPSET.

4. Using the MIB objects of different vendors on a same config file don’t have to be a problem, because the MIBs for each vendor are used only by the CM or MTA of that vendor, the other MIBs are discarded.

5. Minimize risk of FW bugs on the field by testing the feature first, before making it part of the GA (General Available) version.

6. Help your truck roles by predefining configurations.

7. Always attempt to create a national configuration regardless who is your CPE vendors is.

8. Easy management for new hire no need to learn on how to gain access to different vendors CPE.

9. Leverage your device for branding purpose for public hotspot or private hotspot.
Who is Worldwide Supply?

- Worldwide Supply is a OEM CPE vendor specializing in CPE products.
- Networking
- Optics
- Home Plugs
- DOCSIS CPE
Thank you!

Worldwide Supply - Franklin, New Jersey
Corporate Headquarters
One Park Drive
Franklin, NJ 07416
Tel 973-823-6400

Please ask your questions