

TechBulletin

29.9.2009

Nordic

Dear reader; we are pleased to bring you another issue of TechBulletin. This issue includes the following:

- [Unified Communications Manager update](#)
 - [VPFM 2.0](#)
 - [IP Flow Manager 1.0.1](#)
 - [Unified Communications Management \(UCM\) within CS1000 rel 6 / CC7 / ICP](#)
- [Unistim 3.3](#)
- [Identity Engine update](#)
- [Miscellaneous](#)
 - [ASCII Configuration Generator](#)
 - [Updated Solution and Configuration Guides](#)

Summer end

With some regret we also have to admit that the summer year 2009 has come to an end; at least at this part of the globe. However, some of you are maybe look forward to some exciting skiing.



TechBulletin

29.9.2009

Nordic

[Unified Communications Manager \(UCM\) update](#)

The new UCM management platform and architecture was presented in the March issue of TechBulletin. UCM offers:

- A common look and feel across applications
- Enables navigation to all management applications with single sign-on and centralized authentication
- Provides integrated workflows for managing unified communications networks
- Decreases the learning curve for IT personnel
- Delivers simplified deployment and system administration configuration
- Offers deployment flexibility (e.g., standalone, integrated, branch resiliency)

Visualization Performance and Fault Manager (VPFM) 2.0

VPFM version 2.0 was released in late June. VPFM can now be installed on the same server as Enterprise Policy Manager and Network Resource Manager. In addition VPFM 2.0 added the following new features:

Security

You can manage users and roles, establish password policies, distribute and maintain Web SSL and SIP TLS security certificates, manage the private certificate authority, and manage sessions of logged on users using Security.

Device and Server credentials editor

You can import a credential set to the UCM and export credential set from the UCM to a local XML file using Device and Server Credentials Editor.

License administration

You can add a license file, export a license file, generate a license report, and refresh the license information using Licensing Administration.

IP Flow Manager (IPFM) 1.0.1

IPFM is another UCM application. Current version is 1.0.1. IPFM supports the UCM architecture and single sign-on. VPMF and IPFM also support exchange of some data. However, IPFM 1.0.1 can not be installed on the same server as VPFM but requires a separate server. Next release of IPFM will allow you to install IPFM on the same server as VPFM.

IP Flow is the collection of IP packet data for the purpose of application performance, trending, accounting, and behavior. Nortel has adopted the standard IPFIX (RFC3917) as the method for collecting IP Flow data. The Nortel IP Flow Manager supports IPFIX, NetFlow v9 and NetFlow v5 as methods for IP Flow data collection.

The key benefit of IPFM is to easily diagnose network application performance issues without adding probes and other hardware at multiple points in the network.

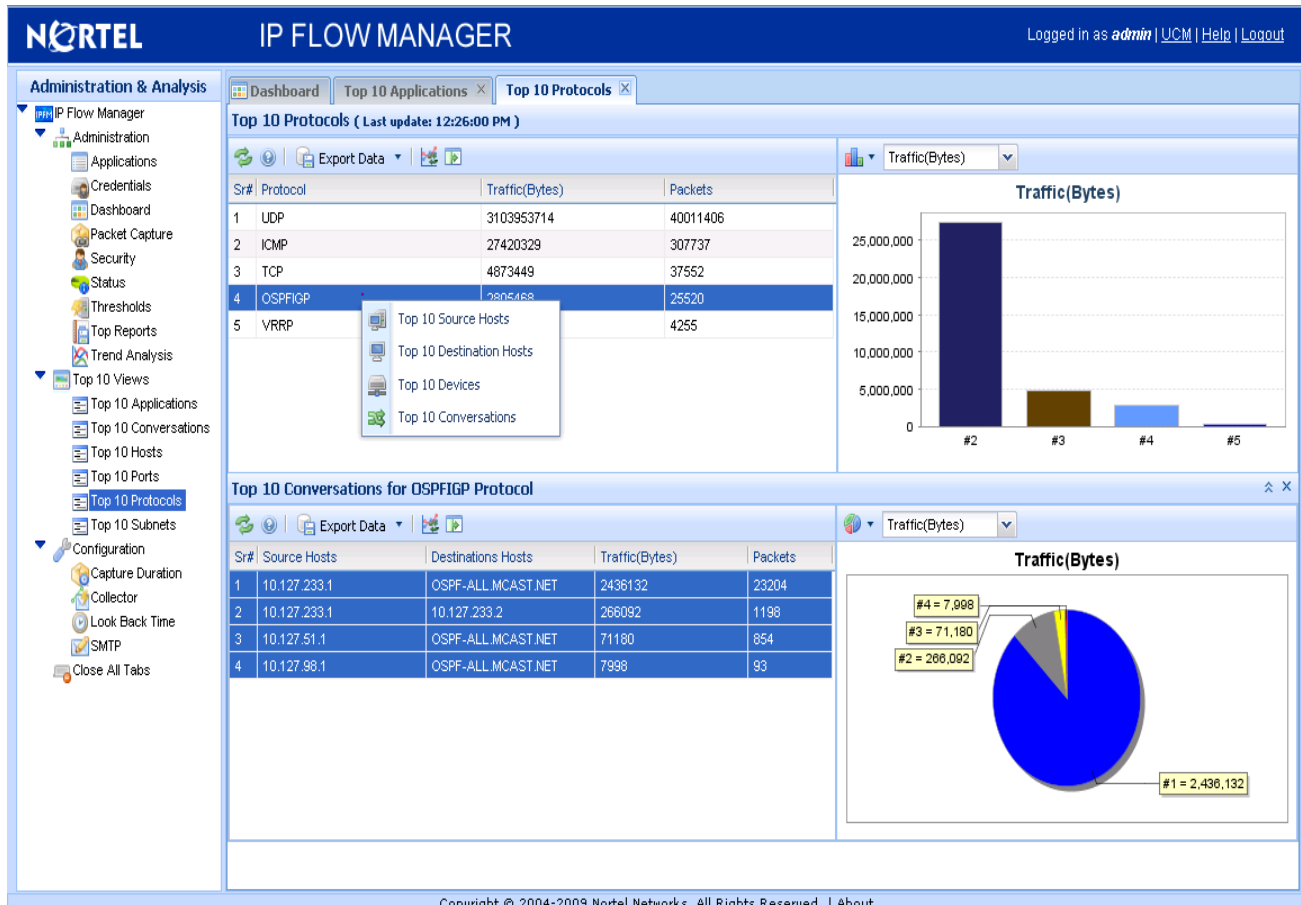
Most Nortel Ethernet Routing Switches (ERS8600, ERS8300, ERS5600, ERS5500 and ERS4500) support IPFIX. IPFIX data can be view from CLI or pointing you web browser on the switch. In fact, using CLI to access IPFIX data on the ERS8600 allows you to view more data than defined in the IPFIX templates. However, the benefit of using IP Flow Manager is that IPFM stores data and allows you to view historic data;

TechBulletin

29.9.2009

Nordic

whereas the CLI or direct web access gives you just a snapshot view. In addition IPFM will process the IPFIX data and present it in a very easy to understand format:



The IPFM gives you better visibility and insight into how applications are used in the network, and by whom. For example, if users start to complain about poor voice quality, the IPFM enables you to look into other application usage that might be contributing to the degradation in voice quality. Through an easy-to-read 'dashboard' and convenient top 10 lists, the IPFM provides details of where excessive bandwidth usage is occurring and who is using it. Pre-defined Top-10 reports include:

- ✓ Applications
- ✓ Conversations
- ✓ Hosts
- ✓ Ports
- ✓ Protocols
- ✓ Subnets

You may also add definitions of your own applications if they are not recognized by IPFM.

TechBulletin

29.9.2009

Nordic

Unified Communications Management (UCM) within CS1000 rel 6 / CC7 / ICP

UCM is introduced as a standard/ mandatory component within the following products:

- CS1000 rel6
- Contact Center 7 (CC7)
- Innovative Communication Portal 1.0 (ICP)

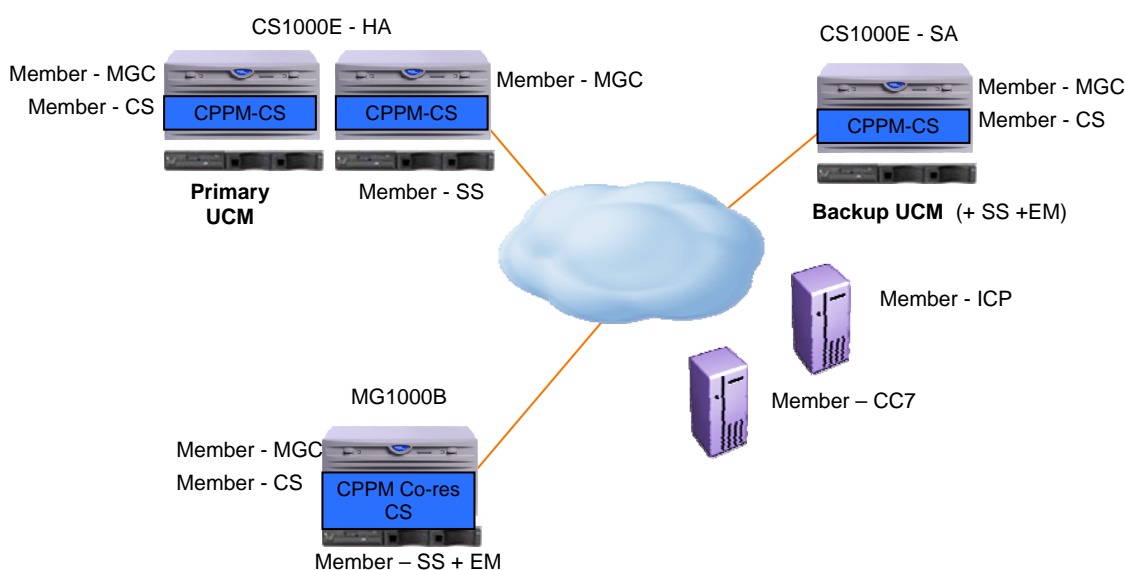
UCM is installed within above products. Only one primary UCM is installed and an optional secondary UCM can be installed per Security Domain. A Security Domain consists of one or many products (from above) and is controlled from the UCM.

UCM has the following features:

1. One central interface with single-sign-on/rolebased authentication + logging to all systems within the network (all CS1000 / CallPilot / CC7 / ICP).
2. Subscriber Manager. Configure Ip-sets
3. Central Patch management. With conflict check of existing patches.
4. Simple Network Management Protocol (SNMP) Profile Manager
5. Software Deployment, deployment & backup of Linux components.
6. IPSec management for Intra System Signalling Security (ISSS).

UCM is the successor of ECM that was introduced with CS1000 rel 5.

Security Domain



TechBulletin

29.9.2009

Nordic

Unistim 3.3 (see Product Bulletin P-2009-0075-Global)

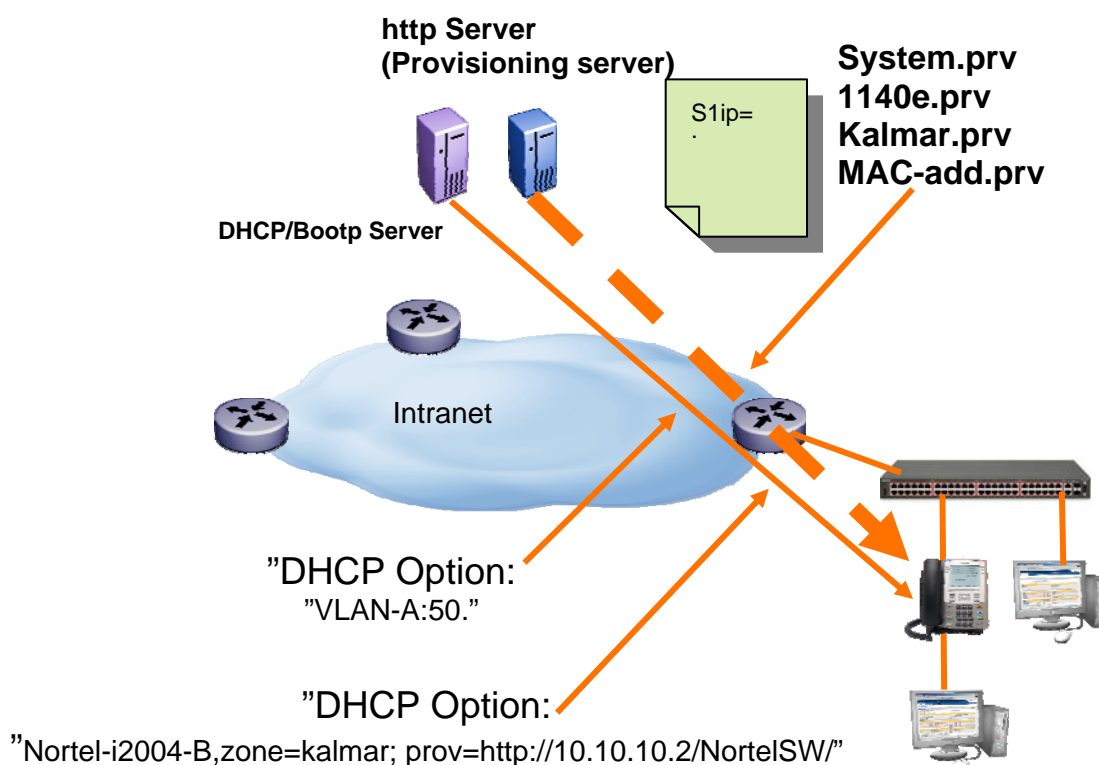
Unistim is the signalling protocol that is used between CS1000 (signalling server) and the the Nortel IP-sets. Unistim 3.3 is the latest firmware for the IP-sets (11xx-serie/12xx-serie and 2007). At the same time Nortel has announced that Unistim 2.2/2.3/3.0/3.1/3.2 is "Manufacture Discontinue" with "End-of-life" (EOL) of those releases to July 2012.

Nortel recommends an upgrade to the latest Unistim (today Unistim 3.3) firmware release at the earliest opportunity.

Unistim 3.3 is supported on CS1000 rel 4.0 / rel 4.5 / rel 5.0 / rel 5.5 /rel 6.0.

What new features will Unistim 3.3 bring to a customer installation?

With Unistim 3.x features of mass deployment of ip-sets, Unistim 3.3 enhances mass deployment and makes it more simple by using an ordinary http-server as an provisioning server (see picture).



Information that can be sent out from the Provisioning Server to the Ip-sets is: LLDP, DSCP-values, Signalling-Server IP-address, CA, 802.1x-settings, SSH-settings, P-bit value, contrast, Node/TN-settings + many more settings.

The new Unistim 4.0 is planned with GA 2009-Q4 with new enhancements.

TechBulletin

29.9.2009

Nordic

Nortel Identity Engines Ignition Portfolio

Network Access Control (NAC) is an appliance or function that ensures that all devices comply with company security policies before they access to the corporate network.

Nortel Identity Engines is considered as a second generation NAC product. It integrates with your current network infrastructure to provide the central policy decision needed to enforce role-based access control. This is done by combining the best elements of the next generation RADIUS /AAA –server, the deep directory integration and the industry’s most advanced standards-based policy engine.

All this is done out of band for maximum scalability and cost effectiveness.

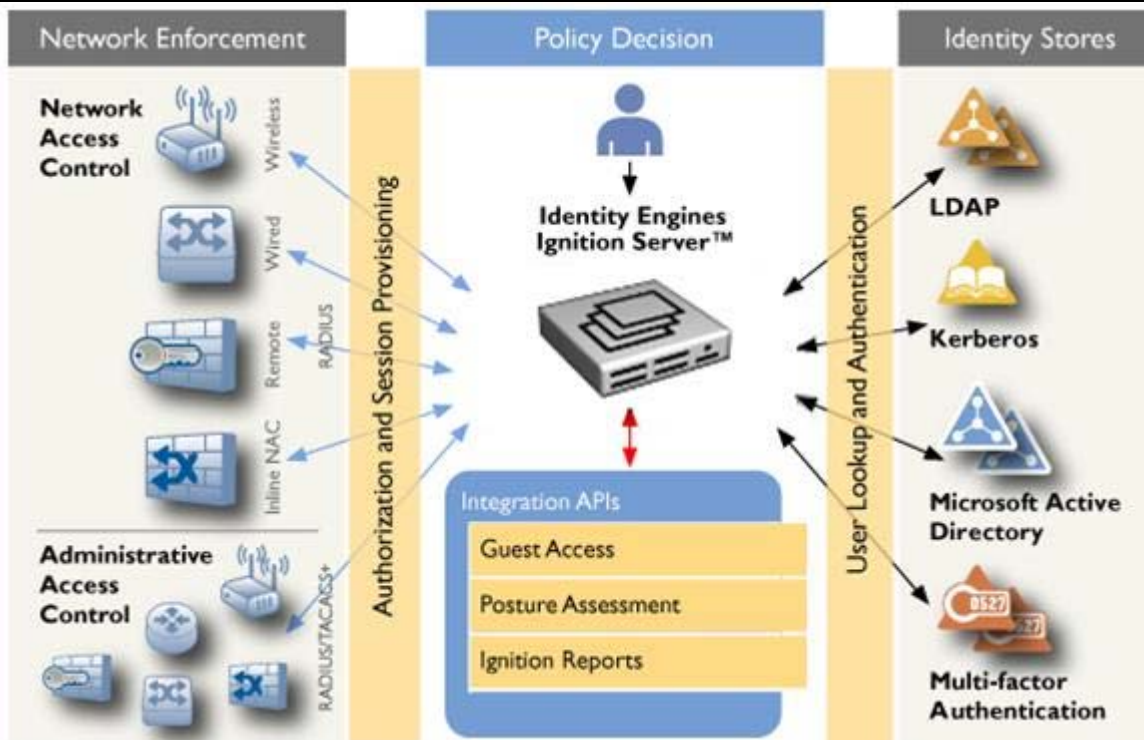
Main components of the solution are:

- **Identity Engines Ignition Server** – centralized policy engine that performs user and context-based authentication and authorization for clients attempting network access
- **Identity Engines Ignition Guest Manager** – allows front desk staff to create temporary guest user accounts
- **Identity Engines Ignition Analytics** – delivers at-a-glance reports highlighting user info, failed authentications, usage summaries, etc.
- **Identity Engines Ignition Posture** – performs device health assessments to ensure that endpoints comply with security policies

This Nortel Network Access Control solution delivers best-in-class policy and role-based access control across wired, wireless and VPN networks. It also supports granular, hierarchical policies based on multiple attributes (e.g., user identity, health of device, day of the week, time of day, access method) with full support for “and” and “or”. Solution also delivers an enterprise-wide guest management solution and reporting capabilities

This kind of solution is needed in network when organizations must control who can access their networks, from where, when, how and with what types of devices or different user types require different levels of access. It also helps when guest users require temporary network access. And last but not least it enforces corporate governance and regulatory compliance requirements.

In following picture you can see Identity Engines main components and how it works.



The Identity Engines Ignition Server sits in the data center, delivering centralized policy decision throughout the network. As such, it communicates with all enforcement points (Ethernet switches, WLAN controllers, VPN Gateways) and all identity stores (e.g., Microsoft Active Directory, Novell eDirectory, Sun Directory, LDAP, RSA SecureID). Users connect to the network through enforcement points and identity information is checked against the identity stores/directories. The Ignition Server compiles all of the information and depending on the chosen corporate security policies, it makes a decision as to the level of access the user will be granted. It then communicates with the enforcement points to enforce that decision. The Ignition Guest Manager, Ignition Posture and Ignition Analytics all work with the Ignition Server in order to provide enhanced functionality (guest management, health checking and reporting).

Key features of the Nortel Identity Engines solution are:

- **Centralized Policy Management** across all network types
- **User Authentication**
- **Directory integration** to support organizations with multiple identity stores
- **Authorization** enforces access control to specific network resource, service or application based on user identity and device context
- **Virtual groups and containers** (e.g., users, authenticators, identity stores) to simplify policy creation
- Comprehensive **reporting** and **analytics**
- **Standards-based** supporting 802.1X, RADIUS, XACML and TNC
- **Device health assessment and compliance** check before network connection is made
- **Ongoing threat analysis** of connected devices for maximum real-time protection



TechBulletin

29.9.2009

Nordic

- **Quarantine and repair** of infected devices
- **Out-of-path deployment** for improved scalability and reduced latency

Customers who will most benefit from this solution are e.g. organizations that have a mobile/telecommuter workforce that occasionally visits the office, or, allow guests to access the LAN/WLAN for Internet access. They might also be organizations who are looking to enforce a centralized enterprise-wide access security policy or are concerned about internal attacks from infected PCs, laptops and other clients.

Users for the product can be any market sectors but especially education, healthcare, medium/large enterprise and government are seen as potential first wave beneficiaries.

Besides existing and potential Nortel LAN customers this solution suits also for non-Nortel data customers who don't have NAC or are looking to improve their NAC solution.

Miscellaneous

Show running config (on ERS stackables) – not quite userfriendly

Most network managers – or anyone that is configuring or managing the Nortel ERS stackable switches dislikes the fact that a 'show running-config' list not only the configuration that has been applied to the switch, but a rather painful long list of default configurations.

The good news is that the next release of ERS4500 (release 5.4) as well the next release of ERS5000 series (release 6.2) will provide an enhanced version of 'show running-config' allowing you to view only the user added configuration and not the defaults.

In the meantime, and for other Nortel stackable switches, we can offer you an ASCII Configuration Generator (ACG) perl script – or a in the form an executable – that will remove all defaults and list only the user added configuration. The perl script has been developed by Nortel Core SE team member Ludovico Stevens and as such is an "unsupported" tool.

ASCII Config Generator (ACG) for Nortel ERS5500, ERS4500, ERS2500, ES470, ES460, BPS2000.

Use the following links to get a copy of the latest version :

- [acg.pl](#) (native perl script, requires perl interpreter)
- [acg.exe](#) (Windows executable, does not require a perl interpreter)

The script connects to the switch via telnet and obtains the output of "show running-config"; if the switch is in RSTP or MSTP modes the script will automatically build the MSTP/RSTP ascii config and include it into the output from "show running-config". The resulting ascii config file is then stripped of default settings (unless a full verbose output is requested via -v flag) and is either displayed to stdout or saved to local file (local to machine executing the script) or saved to file on a remote TFTP server. An additional offline mode is available (via -f flag) to strip default settings from an offline ascii config file.

To run the native perl script **acg.pl** the following Perl CPAN modules are required:



TechBulletin

29.9.2009

Nordic

- Net::Telnet
- Net::TFTP
- Term::ReadKey (this automatically comes bundled with ActiveState Perl)

ActiveState Perl can be freely obtained here: [ActiveState ActivePerl](#)

Alternatively the **acg.exe** version is provided for use with Windows DOS box.

Updated Solution and Configuration Guides

Several new Technical Solution Guides and Technical Configuration Guides have been posted. These documents provide detailed solution overviews with example configurations to make your designs and deployments much easier. Each of these solutions has been thoroughly tested and validated by Nortel and follows all of the recommended Best Practices. Take the guesswork out and simplify your life with these easy to follow blueprints for success.

Key Design Documents and Tools Reference:

http://products.nortel.com/go/product_content.jsp?segId=0&parId=0&prod_id=29580&locale=en-US

Small/Medium/Large/IP Telephony Guides:

<http://support.nortel.com/go/main.jsp?cscat=DOCUMENTATION&poid=22161&viewOptSelect=4|null>

Three Data Center Guides:

<http://support.nortel.com/go/main.jsp?cscat=DOCUMENTATION&poid=21585&viewOptSelect=15|null>

Medical Device Authentication Guide:

<http://support.nortel.com/go/main.jsp?cscat=DOCUMENTATION&poid=22101&viewOptSelect=15|null>

Enterprise Solutions News

The latest edition of Enterprise Solution News can be found at

http://www.nortel.com/multimedia/newsletters/esn/esn_issue23.html

Subscribe to get a copy in your email box.

Also visit <http://blogs.nortel.com/buzzboard/> for news and gossips.

This newsletter is distributed on an “as-is” basis, without warranty of any kind. This newsletter could contain technical inaccuracies or typographical errors. Right to modify or update this information is reserved.