NORTEL NETWORKS™

Pre-Sales Engineering
Tips & Tricks

Volume 1, July 2003

Editor's Note

Throughout this year, we have listened to your needs through on-going communication surveys and focus groups. As a result we are now publishing "Pre-Sales Engineering: Tip & Tricks". This publication will specifically address tips, tricks and design information on trouble shooting, configuring, and interoperability on a broad range of Enterprise product portfolios and solutions. Its purpose is to provide you with a reference tool that will assist you in your understanding solution requirements in network designs, design validations, customer trials, demos and application testing/staging.

This publication will evolve based on your content and information requirements, therefore please feel free to provide feedback on the design and organization of this publication to: pnf@nortelnetworks.com.

Sincerely,
Nortel Networks Enterprise Communications

IN THIS ISSUE

IN THE SPOTLIGHT

Mobile Enterprise Users: Contivity's Silver Bullet

A large wireless provider recently evaluated the use of Contivity in their GPRS network. Their goal was to determine a solution that they would recommend to their enterprise customers who wanted enterprise remote access over their (the service providers) GPRS network. For the trial, the service provider evaluated common enterprise services such as email, web, and information downloads. While Contivity is a well known Secure Remote Access device for telecommuters and work day extenders, it also has several features that are necessary for the public wireless arena.

First and foremost of these is security. Given Contivity's track record in this arena, this is a really easy sell. Contivity is the market leader for enterprise VPNs. Security comes in the form of Encryption to prevent wireless lurkers from reading your traffic as well as authentication which prevents unauthorized access to the enterprise network. Both features are table stakes in any remote access strategy and Contivity is second to none in this area.

In addition, many other features fit well into the wireless public networks. During this trial, compression, link keepalives, and ease of provisioning proved invaluable and were very well received by the service provider.

One of the byproducts of security is greater bandwidth requirements. In a wireless network, bandwidth is very precious, and at times, costly. By utilizing compression, trial downloads proved to have less time to download than non-compressed traffic. Thus, the enterprise could gain security and have less time to download traffic. This feature was available when using the Contivity Client on a laptop. When using the Movian Client with an hp iPAQ Pocket PC, compression was not available and the expected results were true (longer download times). Security was enabled but at the expense of larger downloads.

The keepalive mechanism available with Contivity also proved very valuable. For this feature, we tuned the Contivity keepalive to the GPRS Watcher application. The Watcher application monitors the physical wireless layer to keep contact with the Wireless end user device. If both keepalives are coordinated, then the condition of a "hung" user can be avoided. A hung user occurs when Contivity believes its client is still available but the Watcher application has lost contact with its Wireless end user device. Thus, by coordinating the keepalives, both applications, Watcher and Contivity, should timeout at the same time.

Finally, the customer was extremely impressed with the intuitive GUI interface and the ease of provisioning users. Once again, this comes from years of experience and refinement. Changes in trial parameters were easily accommodated by making changes at the Group level rather than modifying each user. Since this customer was evaluating our solution against other competitors, this may be a well known feature internally to Nortel, but should be stressed to customers because it is truly a differentiator.

DID YOU KNOW...

..there is a Remote Office Q/A available on-line?

If you have a question and are in need for an answer regarding a Nortel remote office solution, you can email remoteoffice@nortelnetworks.com.

...about Nortel Networks Customer Support Email Notifications?

You can use Nortel Networks Customer Support Email Notifications to alert you automatically when new software, documentation, or training is made available on the Customer Support website? You select the products, set the type of information to receive, and choose how often you'd like to check for new items - and you can turn off this feature at any time.

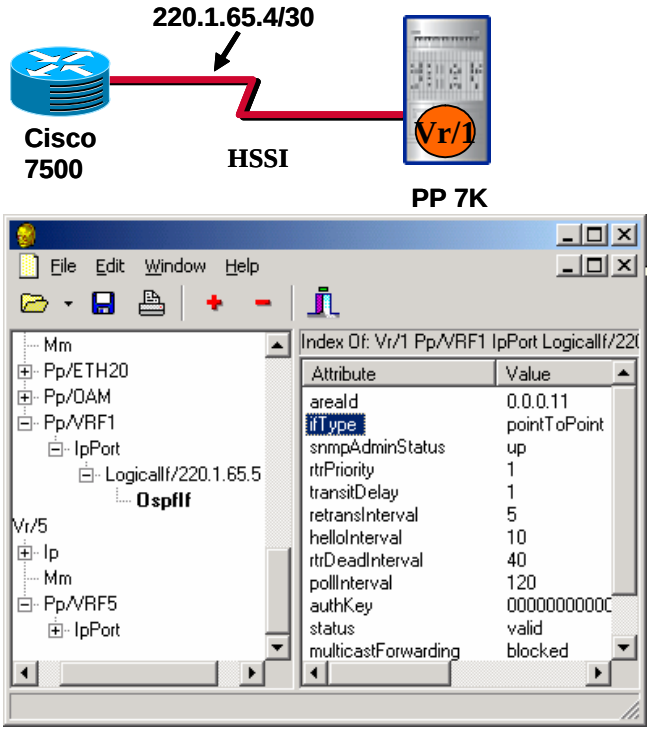
It's easy to do! If you already have a Nortel Networks User ID/Password you can simply Modify Your Profile. (an easy check to see if you are already personally registered is when you can login to the Customer Support website, in the upper left hand corner your name will appear and advise if you are logged in or not).

If your name does not appear, you must Register with Nortel Networks first and then you can Modify Your Profile to receive

TECHNOLOGY

OSPF iftype Parameter Mismatch on WAN Links

While configuring OSPF on a HSSI interface between a PP 7K and a Cisco router, as shown below, it was observed, that the OSPF state machine runs the SPF algorithm and forms the adjacency and reaches the FULL state but the routes do not get populated in the routing database.



Upon debugging it was found that the PP7k set the value of the iftype parameter to broadcast on all the protocol ports. The Cisco router, on the other hand sets it PointToPoint. If the iftype value does not match the routes do not get populated. Once the iftype on the PP7K was changed to pointToPoint the routes were populated in the routing database.

This situation also occurs while connecting Contivity with a router running BayRS.

Multicast IP Television Solutions Reference Design

This Solutions Reference Design is a working document that establishes a known working implementation of IP multicast distribution for the delivery of high quality television services. Such a solutions offering can be used in the service provider space for revenue production purposes as well as in the enterprise arena for corporate television or high quality streaming webcast services. The focus of this SRD will be on multicast technology supported on the Passport 8600 and BayStack product lines.
Solutions Reference Design

Secure Socket Layer Virtual Private Network: SSL VPN-Citrix Technical Configuration Guide

This Technical Configuration Guide describes the use of Citrix with the Alteon SSL VPN product. Examples are provided showing how to securely access applications hosted by Citrix MetaFrame XP using the native Citrix Client as well as the Citrix Java Client.
SSL VPN-Citrix Technical Config Guide

IP-PBX/ PBX/ KEY SYSTEMS

BCM 3.0 Multimedia Call Center

Have you ever had a question regarding the main link for accessing the BCM 3.0 Multimedia Call center home page? The page link below is the starting point for customer demos when you need to show how the application works. Once you login as agent 3 for the MMC on separate PC with i2004 setup as agent phone, you will be able to open the Welcome -Exotic Travel Co. page as a home user on another PC and click on the link of interest. The link on page is set with call back number for BCM to call from the Call Center. The link is Click on this icon to start a web Browser and Phone session, or Click on this icon to start a web Browser only session. The home user will be able to fill in with preference for the African Safari trip and start the connection to the Multimedia Call Center.

The link below is the starting point for Multimedia Call center for Customer Demos.
http://IPADDRESS:6800/ivb-html/demo/Mainpage.html

BCM 3.0 Voice Mail Reset

Have you ever tried to login into CallPilot and were prompted with a dialog box indicating password incorrect and your demo is about to start in 10 minutes? Here is a step by step procedure to reset the Voice Mail.

Login to CallPilot Manager and reset the password on the specific mailbox that you cannot login to (It will then be 0000).

If you cannot find/remember the CallPilot Manager password it can be reset (see steps outlined below from 20 Chapter 2 Using CallPilot Manager from the user docs "CallPilot Manager Set Up and Operation Guide" from early BCM 3.5 documentation - this is valid on BCM 2.5, 3.0 as well.)

To reset the System Administrator password: CallPilot Manager

If you forget the System Administrator password, you must reset the password through a telephone on your system. The password resets to the default password 0000. You must then log on toCallPilot Manager using the default password 0000 and create a new password.

To reset the System Administrator password: Business Communications Manager and CallPilot 100/150

Note: If you reset the System Administrator password, log on to CallPilot Manager and create a new password immediately to prevent unauthorized access to the system. While the default password is used CallPilot Manager or Call Center is open to unauthorized access. For additional security, change the Administration Password regularly.

1) Press ≤·°..

The Voicemail DN appears on your display.

2) Press ·.

3) Enter Resetsmpswd or ‡.‡.°‡.‡‡·. **(73738767793)**

and press OK or ℰ.

4) Press YES.

5) Follow the instructions in "Starting CallPilot Manager" on page 18 to log on to CallPilot Manager.

6) Use the default password 0000 to log on.

Create a new System Administrator password.

Set <xxxx>

OK

Pswd:

RETRY OK

Pswd:

RETRY OK

Reset pswd?

YES NO

Exit

Connecting the i2002/i2004 IP Phone to the BayStack 460-24T-PWR

By default, when you attach an i2004 or i2002 IP Phone to a BayStack 460-24T-PWR that is running software version 2.3.0.9, power will not be supplied to the phone. You must make a change in order for power to be delivered to the phone. Making this change will affect the entire switch unit and it cannot be made on a per port basis. However, this setting can be different between units in a stack. The command below is a valid command in both version 2.3.0.9 of BayStack 460-24T-PWR code (the code the switch currently ships with) as well as BoSS 3.0 code. Please note that this change is not necessary when using BoSS 3.0 code since this setting is a default.

This command cannot be entered from the system console menu; it must be entered from the Command Line Interface. This change can also be made from the Web Interface as well as Java Device Manager.

To display the current Power over Ethernet settings, issue the following command in the CLI:

460-24T-PWR>sho poe-main-status

PoE Main Status - Stand-alone

Available DTE Power:	200 Watts
DTE Power Status:	Normal
DTE Power Consumption:	0 Watts
DTE Power Usage Threshold:	80 %
Power Pairs:	Spare
Traps Control Status:	Enable
PD Detect Type:	802.3af
Power Source Present:	AC Only
DC Source Type:	BayStack 10
DC Source Configuration:	Power Sharing

The "PD Detect Type" is the parameter that must be changed to support the i2002 and i2004 Phone. Enter configuration mode in the Command Line Interface and issue the following command at the CLI prompt:

poe poe-pd-detect-type 802dot3af_and_legacy

Issuing the 460-24T-PWR>sho poe-main-status command again will show the following:

460-24T-PWR(config)#sho poe-main-status
PoE Main Status - Stand-alone

Available DTE Power:	200 Watts
DTE Power Status:	Normal
DTE Power Consumption:	2 Watts
DTE Power Usage Threshold:	80 %
Power Pairs:	Spare
Traps Control Status:	Enable
PD Detect Type:	802.3af and Legacy
Power Source Present:	AC Only
DC Source Type:	BayStack 10
DC Source Configuration:	Power Sharing

Power should now be applied to the phone.

To change the setting for a different unit in a stack, issue the following command:
poe poe-pd-detect-type unit X 802dot3af_and_legacy
where "X" is the unit number.

NETWORK MANAGEMENT

The Misunderstood Windows Client

The OTM Windows client-server architecture is often misunderstood. Many make the assumption that the OTM Windows clients will function as would a traditional dumb client, assuming that there would be no impact on the network. But in reality, there are several databases that reside on the OTM Windows client and network bandwidth provisioning should be considered when deploying an OTM server with Windows clients. The OTM server provides the database for the common data that is shared with the clients, so it's important to ensure adequate bandwidth between the server and clients. However, certain functions that are performed on the OTM Windows client will require a direct connection to the PBX. Because of this, the OTM Windows clients must be running at the time of the scheduled event.

As you can see, it is important that OTM is engineered appropriately prior to deployment.

Some things to remember:

- Station Administration runs primarily on the client and will only communicate with the server to obtain common data. When making a station change on an OTM Windows client, the client must set up a connection with the PBX to implement the change. (In a true client-server architecture, the bulk of the tasks would be executed by the server connecting directly to the PBX with minimal processing being done by the client.)
- Other applications like Maintenance, Inventory, IP Trunk, IP Line, GCAS/CRS Billing, also operate primarily on the OTM Windows client with minimal server involvement, except during the startup of the application.
- The OTM Telecom Billing System operates primarily on the client and obtains OTM Directory information from the server.
- Applications such as Data Buffering and Access (DBA), LDAP Synchronization, and user group set-up and configuration will operate entirely on the server but can also be accessed via a Windows client.
- In most situations we do not recommend deployment of OTM Windows clients in a WAN environment. Specific bandwidth requirements must be met in order for the OTM Windows clients to function appropriately. As an alternative for remote management access, OTM Windows clients can be positioned throughout the LAN and accessed remotely using PC Anywhere.
- The Web applications operate on the server and

use a Web browser client for access.

OTM is a product that has evolved and will continue to evolve into a completely Web based architecture. Since this is an ongoing evolution, not all of the OTM applications have been ported to the Web user interface (thus the current requirement for the Windows clients). As we move forward, our continued management strategy is to Web enable the remaining OTM Windows applications which will resolve many of the client-server bandwidth requirement issues. We are also actively looking at methods of providing improved management integration with other telephony systems such as CallPilot and BCM.

ROUTERS / SWITCHES

Configuring SNMPv3 on the Passport 8600

This document provides an overview of how to configure SNMP Version 3 on the Passport 8600. Step-by-step configuration of SNMPv3 users and views are provided using both the command line interface and Java Device Manager. In addition, the document provides an overview of managing the Passport 8600 with Optivity NMS through SNMPv3.
Configuring SNMPv3

SECURITY / VPN

Contivity 4.7 NAT (Network Address Translation) configuration technical guide

The Contivity Secure 4.7 release offers multiple new secure routing features that allow Contivity to better participate dynamic and complex L3 routed VPN implementations. Increased functionality around Contivity's ability to provide Network Address Translation is one the key routing functional areas that we continue to greatly enhance the product line.

Network Address Translation allows a network to use one set of network addresses internally and a different set when dealing with external networks. When an internal machine sends a packet to the outside, NAT modifies the source address of the packet to make the packet look as if it is coming from a valid address. When an external machine sends a packet to the inside, NAT modifies the destination address to turn the externally visible address into the correct internal address. NAT can also modify the source and destination port numbers.

The Contivity NAT Services Technical Configuration Guide provides general guidelines for various network scenarios that a network engineer might typically run into.
Contivity NAT Services Technical Config Guide

OPTICAL / STORAGE

OM5200 GFSRM Card Supported Protocols:

Protocols: FC-100 MM (850 nm), FICON (850nm) FC-100 SM (1310nm), FICON SM (1310nm)
Native bit rate: 1062.5M (8B10B)
Supporting client interface: GFSRM
Supporting line interface: 2.5G Flex OCLD
Line bit rate: OC-48 on the line side
Performance monitoring: 8B10B on client

Protocols: GbE MM, GbE SM
Native bit rate: 1250M (8B10B) line code
Supporting client interface: GFSRM
Supporting line interface: 2.5G Flex OCLD
Line bit rate: OC-48 on the line side
Performance monitoring: 8B10B on client

For the GFSRM connecting to a 2.5G Flex OCLD on the same shelf, the remote OCLD/OTR connectivity can be a 2.5G Fix OCLD, a 2.5G Flex OCLD or a 2.5G Flex OTR.
If an OCLD is selected, then the client interface card must be a GF SRM, or a SONET OCI or a Fix rate OCI (since the bit rate is OC-48).

Use of Multimode Fiber with the OPTera Metro 3000

Apart from the 100FX-MM and 1000Base-SX OPTera Packet Edge cards, optical interfaces on the OPTera Metro 3000 are intended to be used with single mode fiber cable. Multimode fiber is not supported, nor specified by Nortel for OM3000 applications.

Theoretical studies carried out by the optical development in the past have attempted to quantify the performance of single mode based systems over multimode fiber. These studies focused on the lower bit-rate SONET interfaces; namely the OC-3 and OC-12 IR and LR interfaces. Distance limitations of these

interfaces over multimode fiber would be dispersion limited. OC-3 rate interfaces (either IR or LR) might be expected to reach 3.2 km over multimode fiber, and OC-12 IR interfaces might reach 800 meters. It is important to stress that these are theoretical values. The circumstances under which these distances can be achieved is not specified or controlled by Nortel.

The design of the hardware can impact the applicability of these results and should be considered. OC-12 LR/ER or OC-48 interfaces use single-mode fiber in their pigtails, for example, and so shouldn't be used with multimode fiber.

Customers using multimode fiber typically want to use it to transport a small number of low speed interfaces (e.g. DS-1s). This application would be appropriate for a number of legacy asynchronous transport multiplexers, such as the FMT-6 and FMT-150 products that were previously sold by Nortel (since spun off to CTDI). These products are sold with ultimode interfaces and support transmission over multimode fiber. They can act as tributaries to the OM3000 in a "book ended" fashion if multimode transmission is a small part of a larger transport network.

EIM migration consideration for OM33/3400

This document outlines the considerations and recommendations for customers with previous deployments of the Ethernet Inverse Multiplexer (EIM) on the OPTera 3300/3400 platforms. Information is provided with respect to supported migration paths as well as the supported hardware for the targeted software level. Primarily, it is to make one aware of the change in support status of the EIM circuit card at releases 9.12 and 11.1 and the options available for a transition to the OPTera Packet Edge/Resilient Packet Ring and/or Point To Point circuit cards.
EIM Migration