Global Information Assurance Certification Paper

Securing Routing Protocols and Access to Nortel Routers
GSEC 1.4B Option 1
Michael Bishop

Abstract

The need for running a routing protocol between a trusted router and an untrusted router on an untrusted network is becoming more common, so the need to secure the trusted router from inadvertently or maliciously receiving routes is required. This paper will describe how to securely receive routes via RIP, OSPF and BGP on a Nortel BayRS router from another device on a network that is not trusted. Nortel Routers have had a heavy configuration reliance on SNMP and access reliance on telnet. The importance of SNMP with BayRS and remote login reliance on telnet will be explained.

History of Nortel Networks Router Configuration

Nortel Networks routers, specifically the BayRS line of routers has historically had a heavy reliance on SNMP. The BayRS line of routers includes BLN, BCN, ASN, Passport, and AN routers. Site Manager is a Graphic User Interface that was designed to make configuring of these routers easier. Their biggest competitor, Cisco has a command line user interface for Cisco IOS. The idea was that the GUI would make configuring a router simple. A Site Manager user connects to the router using SNMP and configures the router by clicking on interfaces and protocols within the GUI to apply to the router. Site Manager sends SNMP MIB updates to the router to correspond to the information entered in the GUI.

The recommended configuration steps were to boot the router with a factory default config that has no interfaces or protocols configured. At the console prompt, run the provided batch script file (usually called INSTALL.BAT). This script runs through several questions in order to configure IP and then SNMP connectivity to the workstation that is running Site Manager. Once that connectivity is established, then the rest of the router is configured through Site Manager

Site Manager vs. BCC

Site Manager was developed to make router configuration and management easier by using a GUI. BCC (Bay Command Console) was developed by Nortel (at the time the company name was Bay Networks) to provide their customer base with command line configuration tool. Because Cisco IOS dominates the router market, many customers demanded a similar configuration interface to

Nortel Routers. Both Site Manager and BCC will lock the router while actively configuring the router, so both cannot be used at the same time. For ease of description, this document will show router configurations using BCC only.

BCC at BayRS version 13.01 became a standard feature of the router code. There are still several configuration options that aren't available in BCC and you must use Site Manager to configure. Some of the lower end routers will have trouble running bcc because it requires 16meg total memory and 2meg free. An important feature of BCC is that the 'show config' command doesn't display default configuration options. BCC will only display settings that are not the default value for an object.

Site Manager has extensive help for each configuration option. Almost every window has a 'help' button to describe the configuration options and the affects of those options. BCC has a BCC help file, but it has little information compared to Site Manager. Several items can be configured in BCC, but are less cryptic to configure using Site Manager.

Below is an example of the SNMP section of the batch file run to configure the router. Notice at the question "Do you want to configure SNMP?"

```
                SNMP Community Management Menu
                ------------------------------

Setting up SNMP community management is optional.

It allows you to limit control of this router to a single
Site Manager workstation at a given IP address.  The default
is to allow any Site Manager from any workstation to manage
and to configure the router.

Note: You can later configure this using Site Manager.

Do you wish to set SNMP community management? (y/n)[n]:
------------------------------------------------------------------------
```

The default answer is no, but notice that this does not mean that SNMP configuration is being skipped. SNMP is configured as the default community Public with a community manager IP address of 0.0.0.0 (which implies any IP address can manager the router through SNMP). Below is the SNMP configured from the above Install.bat script.

```
snmp
  community label public
     access read-write
    manager address 0.0.0.0
    back
  back
back
```

At this point, if you start Site Manager from the PC you would connect using the default read-write community "public" and be able to start using Configuration Manager to configure the router. This can be done to verify connectivity, but the SNMP default community of public should be removed and replaced with a unique community name for read-write access and, if needed, a second community added for read-only access for traps.

In the example below read-write community **sEcr!tRW** has one manager (192.168.169.1). This would be a Site Manager workstation and is the only address that can change a router setting via an SNMP set command. This manager will not receive any SNMP traps from the router. The read-only community **sEcr!tRO** has two managers. Manager 192.168.169.2 is configured to receive generic traps. Generic traps are defined as warm-start, cold-start, and authentication traps that are specifically configured.[1] Manager 192.168.169.3 is configured to receive specific traps. Those are the traps configured as SNMP trap entities and trap events. This example is configured to send traps on entities ip, ospf, and bgp when a fault or warning occurs for the protocol. If an ip interface goes down, a bounce in an OSPF neighbor, or a bounce in a BGP peer occurs, then a warning message is created and an SNMP trap is sent to this manager. The trap event configured below is for entity MIB with a code of '5'. A '5' is the code for a MIB change. So any time any MIB has been changed, either by Site Manager, BCC or CLI, a trap will be sent to the community manager

```
snmp
  community label sEcr!tRW
     access read-write
    manager address 192.168.169.1
       traps none
    back
  back
  community label sEcr!tRO
    manager address 192.168.169.2
    back
       traps generic
    manager address 192.168.169.3
       traps specific
    back
  back
  trap-entity entity ospf slot 1
     fault-log on
     warning-log on
  back
  trap-entity entity bgp4 slot 1
     fault-log on
     warning-log on
  back
  trap-entity entity ip slot 1
     fault-log on
     warning-log on
```

[1] definition of generic comes from Site Manager 'help' button

back
trap-event entity mib event 5
back

SNMP Vulnerability

SNMP has been used to manage network devices since the 1980s without too much concern with the overall vulnerability of the protocol until CERT released a wide-ranging vulnerability advisory for the protocol on February 12, 2002. Titled "Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP). This advisory was initiated by the Oulu University Secure Programming Group (OUSPG) that is based on results from the PROTOS project. PROTOS is the Security Testing of Protocol Implementations. OUSPG states about PROTOS, "The goal is to support proactive elimination of faults with information security implications. Awareness in these issues is promoted. Methods are developed to support customer driven evaluation and acceptance testing of implementations. Improving the security robustness of product is attempted through supporting the development process".[2] What the PROTOS group did was come up with an extensive testing procedure to look for vulnerabilities in multiple vendors' implementation of SNMP. OUSPG picked SNMP because the protocol a mature protocol that is widely used by numerous vendors[3].

In their conclusion for the vulnerability testing of SNMP, the OUSPG states, "The initial results from the c06-snmpv1 tests indicate that implementation errors plague several SNMP products. None from the sample of twelve implementations survived the test-material. This is most alarming since SNMPv1 is widely used in critical parts of network infrastructure.
Since the test-material can discover only a fraction of potential implementation errors, it is likely that we have simply touched the tip of the iceberg. We hope that a wide adoption of this test-suite will raise the overall quality of SNMP products and will help implementers to fix also those vulnerabilities not directly addressed by it."[4] This conclusion is a strong alert to the vulnerabilities found.

Before announcing their report to the public, OUSPG contacted the vendors, to alert them of this vulnerability and allow them time to release a code version that would correct the vulnerabilities their products have with SNMP. OUSPG then worked with CERT to send out a public advisory on the vulnerabilities found (http://www.cert.org/advisories/CA-2002-03.html) and Nortel has it's own response to the CERT advisory as well as a Best Practice Strategy document (http://www.nortelnetworks.com/corporate/technology/snpmv1.html). The best

[2] www.ee.oulu.fi/research/ouspg/protos/ March 19,2003
[3] The Simple Times www.simple-times.org December 2002
[4] www.ee.oulu.fi/research/ouspg/protos/ March 19,2003

practice document is recommending that SNMP enabled devices not be place in parts of the network available to the public or untrusted parties.[5]

A company called SimpleSoft developed an SNMP Vulnerability Probe in response to the CERT advisory called SimpleSlueth. A Demo can be downloaded from their site at www.snmptest.com/SimpleSleuth.html. They'll ask for an e-mail address and other information and send you a key to your e-mail address that is based on the machine id that the demo will be loaded. When running the vulnerability tests against a Nortel BayRS router version 15.3.0.8, it passed every test. The router log was filled with the attempted denial of service attaches. A sample of these logs is listed below.

```
#   60: 04/23/2003 05:51:23.186  TRACE    SLOT  1  SNMP           Code:   8
Agent received unauthorized request from 10.12.132.70 in community public%s%s%s%s%s.

#   61: 04/23/2003 05:51:23.198  TRACE    SLOT  1  SNMP           Code:   8
Agent received unauthorized request from 10.12.132.70 in community public%n%s%x%n%s.

#   62: 04/23/2003 05:51:23.203  TRACE    SLOT  1  SNMP           Code:   8
Agent received unauthorized request from 10.12.132.70 in community %spublic%spublic.

#   63: 04/23/2003 05:51:23.211  TRACE    SLOT  1  SNMP           Code:   8
Agent received unauthorized request from 10.12.132.70 in community .%spublic.%spubl.

#   64: 04/23/2003 05:51:23.221  TRACE    SLOT  1  SNMP           Code:   8
Agent received unauthorized request from 10.12.132.70 in community %n%s%xpublic%n%s.
```

The most common vulnerability with SNMP involves the default configuration. Vendors often use community name of PUBLIC in default configurations. This community name is well known and should be changed using the same naming convention used for user passwords. Keeping these community names would be similar to keeping root or admin enabled with no password. SNMPv1 only checks community name and manager IP to allow read-write access.

SNMPv1, SNMPv2, SNMPv3

SNMPv1 was first standardized in 1988 and has been the network management tool of choice ever since. The problem with SNMPv1 is that is had not security. No authentication of who is requesting the information and no encryption is provided. Functionally, its lacks any mechanism to have one request retrieve multiple sets of data. The only way to retrieve a table is to continually do a 'getnext' until the end of table. Nortel's Site Manager uses SNMPv1 to get and set MIB objects

There is a difference of opinion on how much security SNMPv2 provides. But, SNMPv2 was all about differences of opinions. These differences were the

[5] http://www.nortelnetworks.com/corporate/technology/snpmv1.html February 12, 2002

reason that several subsets evolved (SNMPv2u, SNMPv2* and SNMPv2c). The 'getbulk' command is introduced in SNMPv2. The benefit of getbulk is one request can return a bulk of data. The downside is trying to control receiving too much data from the getbulk command.

SNMPv3 added plenty to the security of the protocol. The protocol adds authentication between the SNMP manager and the SNMP agent to guarantee the integrity of the message. The SNMP messages can be encrypted to add privacy. Agent access control policies can limit a principle to only certain portions of its data. The concept of a principle is defined by William Stallings in The Internet Protocol Journal as "an individual acting in a particular role, a set of individuals, with each acting in a particular role; an application or set of applications; or combinations thereof"[6]

Remote Logins To Nortel Routers

Nortel BayRS routers do not currently have SSH Secure Shell functionality. This functionality has been added to other Nortel product lines like the VPN aggregator Shasta BSN. Because the only remote login option is telnet, a best practice approach should be taken towards telnetting into the router. The path from the source device to the Nortel router should be a trusted network. Source devices on an untrusted network should SSH Secure Shell to a device that does have a path on a trusted network. The telnet from that device to the Nortel router can then be considered using a best practice approach.

Nortel BayRS routers have two logins that are associated with the router. 'Manager' for read/write access and 'User' for read-only access. These logins and their passwords are not part of the router config. The passwords are kept in NVRAM. The login names are part of the system bootstrap so therefore they cannot be removed. Just like root on a Unix box or administrator on an NT machine, it would be beneficial to disable these accounts. Under **access** in BCC there is a parameter **user-manager-lock** that can be enabled to lock these two login names. Certainly, care should be taken to ensure that other login methods exist before disabling these accounts.

A reliable way to configure other login access is through Radius authentication. This would allow the username and password an employee uses on the network to also be used to login to the router. The radius server controls limiting the users access to a router. Below is a sample config to enable radius authentication that is connecting to a radius server 10.12.132.9

```
radius
  radius-client slot 1 address 192.168.100.1
      accounting enabled
      authentication enabled
```

[6] http://www.cisco.com/warp/public/759/ipj_3.pdf December 1998

```
  back
  radius-server address 10.12.32.5
     authentication-server-type primary
     primary-server-secret sEcr!tAuth
  back
back
```

Dynamic Routing Between Companies

Intercompany private VPNs (Virtual Private Networks) are on the rise. Whether it's the financial sector, healthcare, or just independent companies exchanging date, the need to share routes between companies is becoming common. The need for redundancy has increased the need for dynamic routing protocols on untrusted networks. With that need, comes the need to control what dynamic routes enter a network. In a Telecommunication Reports for KMB Video Journal, Paul A. Crotty, group president – New York and Connecticut for Verizon Communications, Inc. states "The events of Sept. 11 will prompt a number of changes in the telecom Industry. You're not going to see the concentration of assets in hubs. There will be more redundancy, more resiliency in the network"[7].

Securing Rip on an Untrusted Network

RIP (Routing Information Protocol) is a metric routing protocol. Routes are sent in IP multicast packet 224.0.0.9 to every device on the network over a fixed interval (default 30 seconds) or when the network topology changes. Even in a switched environment, every device on the network will receive these packets. Nortel Routers configured for RIP will listen for multicast packets sent from other devices and by default, add the route into the routing table.

Referring to Diagram 1, Device A needs to send and receive Rip2 routes. Device A wants to dynamically receive routes 192.168.150.0/24, 192.168.151.64/30 and 192.168.151.128/25 from device B on an untrusted network Z. By default the Nortel Router will accept any route packet that has a source address from network Z and destination 224.0.0.9. The next hop of the route will be the source address of the packet.

[7] www.kmbvideojournal.com/tcreport.htm June 17,2002

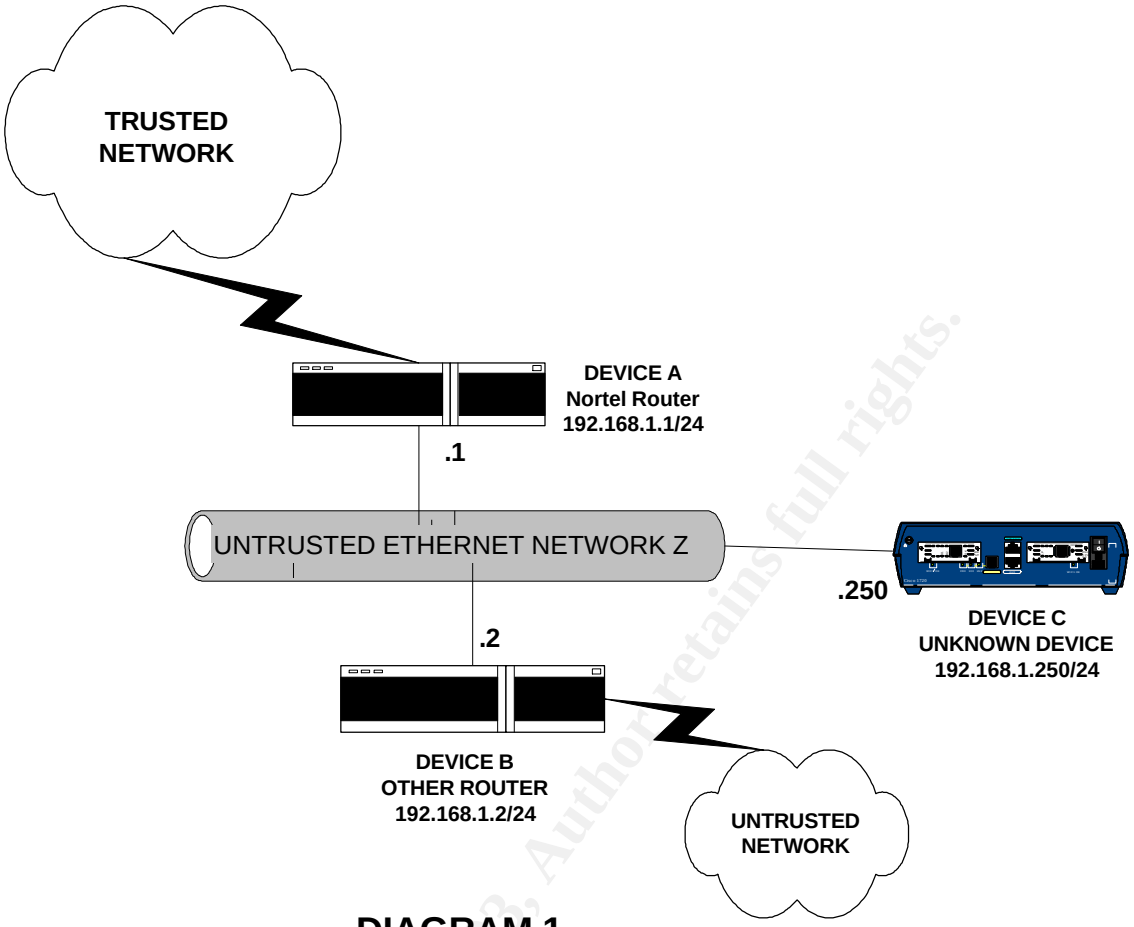

DIAGRAM 1

The following is the default RIP2 configuration on a Nortel Router

```
rip/192.168.1.1# info
  authentication {}
  authentication-type none
  broadcast-timer 30
  def-cost 0
  default-listen disabled
  default-supply disabled
  frsvc disabled
  holddown-timer 90
  listen enabled
  mode poisoned
  rip1-comp disabled
  state enabled
  supply enabled
  timeout-timer 90
  triggered-updates disabled
  ttl 1
  version rip2
```

Unknown device C can easily add routes to Device A's routing table. Below is an example routing table of device A before RIP is enabled on Network Z. All of the RIP routes are coming from trusted network Y.

```
show ip routes                                        Apr 29, 2003
02:57:12 [GMT]

Network/Mask        Proto        Age Slot     Cost  NextHop Address
AS
------------------- ------ --------- ---- --------- --------------- --
---
10.10.10.0/30       RIP            2    1         7 192.168.100.2
10.60.8.248/30      RIP           38    1         2 192.168.1.250
10.100.163.0/30     RIP            2    1         7 192.168.100.2
10.133.11.101/32    RIP            2    1         7 192.168.100.2
10.133.11.103/32    RIP            2    1         7 192.168.100.2
10.133.11.105/32    RIP            2    1         7 192.168.100.2
172.1.1.0/30        RIP            2    1         7 192.168.100.2
192.168.1.0/24      Direct       336    1         0 192.168.1.1
192.168.100.0/24    Direct       336    1         0 192.168.100.1
192.168.166.0/24    RIP            2    1         7 192.168.100.2
192.168.169.0/24    RIP            2    1         7 192.168.100.2

   Total Networks on Slot 1 = 11
```

Below is the routing table with RIP2 enabled with default the parameters. Notice that we do successfully receive the routes expected from device B (in green). Also notice that we are receiving routes from device C and extra routes we didn't want from device B (in red). The route 192.168.166.0/24 received from device C is preferred over the same route received from the trusted network because it has a lower RIP metric.

```
show ip routes                                        Apr 29, 2003
03:12:17 [GMT]

Network/Mask             Proto        Age Slot     Cost  NextHop
Address     AS
------------------- ------ --------- ---- --------- --------------- --
---
10.10.10.0/30       RIP           16    1         7 192.168.100.2
10.12.132.0/24      RIP            1    1         2 192.168.1.2
10.60.8.248/30      RIP           22    1         2 192.168.1.250
10.100.163.0/30     RIP           16    1         7 192.168.100.2
10.133.11.101/32    RIP           16    1         7 192.168.100.2
10.133.11.103/32    RIP           16    1         7 192.168.100.2
10.133.11.105/32    RIP           16    1         7 192.168.100.2
172.1.1.0/30        RIP           16    1         7 192.168.100.2
172.16.0.0/16       RIP            1    1         2 192.168.1.2
192.0.0.0/8         RIP            1    1         2 192.168.1.2
192.168.1.0/24      Direct      1242    1         0 192.168.1.1
192.168.100.0/24    Direct      1242    1         0 192.168.100.1
192.168.100.4/30    RIP            1    1         2 192.168.1.2
192.168.150.0/24    RIP            1    1         2 192.168.1.2
192.168.151.64/30   RIP            1    1         2 192.168.1.2
```

```
192.168.151.128/25  RIP            1    1         2 192.168.1.2
192.168.166.0/24    RIP           23    1         2 192.168.1.250
192.168.169.0/24    RIP           17    1         7 192.168.100.2

   Total Networks on Slot 1 = 18
```

Device C's action may or may not be malicious. Device C may just be misconfigured with RIP. RIP authentication can help prevent an inadvertent RIP announcement affecting your router. By configuring authentication type "simple password", the Nortel router will only accept routes with matching authentication. The following is how to configure simple password authentication.

```
rip/192.168.1.1# info
  authentication sEcr!tAuth
  authentication-type simple-password
  broadcast-timer 30
  def-cost 0
  default-listen disabled
  default-supply disabled
  frsvc disabled
  holddown-timer 90
  listen enabled
  mode poisoned
  rip1-comp disabled
  state enabled
  supply enabled
  timeout-timer 90
  triggered-updates disabled
  ttl 1
  version rip2
```

This prevents the router from accepting routes from a device that doesn't match the authentication password 'sEcr!tAuth' and the Nortel router will log the following entry. The router could also be setup to send an SNMP trap on this event.

```
#    4: 04/28/2003 04:58:07.369  WARNING  SLOT  1  IP            Code:  74
RIP Authentication failed for source 192.168.1.250 on interface 192.168.1.1
Security enabled, received Address Family Identifier 2 Authentication Type 0
```

Rip Authentication would help in identifying misconfigured devices, but isn't much help is someone wants to maliciously send your router RIP updates. The following simple WinDump from a Windows based machine will capture RIP packets sent on a network. WinDump is the tcpdump program for the Windows platform. The authentication password is in clear text and would be simple to duplicate.

```
C:>windump dst 224.0.0.9
22:12:24.373104 IP 192.168.1.1.520 > 224.0.0.9.520:  RIPv2-resp [items 3]: [password
sEcr!tauth] {24.207.233.110/255.255.255.255}(1)[|rip]
22:12:24.786147 IP VENUS.137 > 224.0.0.9.137: udp 50
22:12:26.285805 IP VENUS.137 > 224.0.0.9.137: udp 50
```

```
22:12:27.785745 IP VENUS.137 > 224.0.0.9.137: udp 50
22:12:54.372999 IP 192.168.1.1.520 > 224.0.0.9.520:  RIPv2-resp [items 3]: [password
sEcr!tauth] {24.207.233.110/255.255.255.255}(1)[|rip]
22:13:24.372872 IP 192.168.1.1.520 > 224.0.0.9.520:  RIPv2-resp [items 3]: [password
sEcr!tauth] {24.207.233.110/255.255.255.255}(1)[|rip]
```

Two RIP Route Accept Policies on the Nortel router will both prevent routes from device C and limit the routes from device B. The policy with the higher precedence is applied first. The first policy 'accept networks' accepts network 192.168.150.0/24 exact match and 192.168.151.0/24 range of networks from device 192.168.1.2. The accept policy 'drop-all' has an action of ignore from rip interface 192.168.1.1, so it will ignore all other RIP routes from this interface.

```
rip
  accept polname drop-all
     action ignore
     precedence 5
    match
     rip-interface address 192.168.1.1
     back
    back
    modify
    back
  back
  accept polname accept-networks
     precedence 10
    match
     network address 192.168.150.0 mask 255.255.255.0 match exact
     back
     network address 192.168.151.0 mask 255.255.255.0 match range
     back
     rip-gateway address 192.168.1.2
     back
    back
    modify
    back
  back
back
```

The following routing table shows that we are only receiving the routes expected from the device expected.

```
show ip routes                                        Apr 29, 2003
03:51:56 [GMT]

Network/Mask        Proto        Age Slot     Cost  NextHop Address
AS
------------------- ------ --------- ---- --------- --------------- --
---
10.10.10.0/30       RIP           15    1         7 192.168.100.2
10.100.163.0/30     RIP           15    1         7 192.168.100.2
10.133.11.101/32    RIP           15    1         7 192.168.100.2
10.133.11.103/32    RIP           15    1         7 192.168.100.2
10.133.11.105/32    RIP           15    1         7 192.168.100.2
```

```
172.1.1.0/30         RIP           15    1         7 192.168.100.2
192.168.1.0/24       Direct      3620    1         0 192.168.1.1
192.168.100.0/24     Direct      3620    1         0 192.168.100.1
192.168.150.0/24     RIP           23    1         2 192.168.1.2
192.168.151.64/30    RIP           23    1         2 192.168.1.2
192.168.151.128/25   RIP           23    1         2 192.168.1.2
192.168.166.0/24     RIP           15    1         7 192.168.100.2
192.168.169.0/24     RIP           15    1         7 192.168.100.2

   Total Networks on Slot 1 = 13
```

Securing OSPF on an UnTrusted Network

Unlike RIP, OSPF (Open Shortest Path First) is a link state routing protocol. So, Instead of metric routing updates on regular intervals, LSA (Link State Updates) are sent as changes occur in the network. Because of this structure, networks internal to OSPF cannot be easily filtered from the database. Networks that are imported into OSPF from another routing protocol can be filtered. So, selecting OSPF as the protocol requires a little trust in the neighbor router because the OSPF database information will be shared between routers.

Nortel routers have an OSPF type as broadcast in the default configuration. This is the simplest configuration and allows easy configuration of the router. This will allow any device on the same IP network to become OSPF adjacent as long as it has the same OSPF area, hello interval, dead interval, OSPF type and a unique OSPF router ID. The default configuration is as follows:

```
ospf/192.168.1.1# info
  area 0.0.0.0
  authentication {}
  type broadcast
  priority 1
  transit-delay 1
  retransmission-interval 5
  hello-interval 10
  dead-interval 40
  poll-interval 120
  metric 1
  mtu 1
  mtu-mismatch-detect enabled
  state enabled
```

Using windump, the parameters needed to configure a device can easily be disseminated by capturing OSPF hello packets.

```
C:>windump  -vv dst 224.0.0.5
17:28:19.032561 IP (tos 0xc0, ttl 1, id 215, len 64) 192.168.1.1 > OSPF-ALL.MCAST.NET:
OSPFv2-hello 44: backbone E mask 255.255.255.0 int 10 pri 1 dead 40 dr 192.168.1.1
```

```
17:28:29.032503 IP (tos 0xc0, ttl 1, id 216, len 64) 192.168.1.1 > OSPF-ALL.MCAST.NET:
OSPFv2-hello 44: backbone E mask 255.255.255.0 int 10 pri 1 dead 40 dr 192.168.1.1
17:28:39.032478 IP (tos 0xc0, ttl 1, id 217, len 64) 192.168.1.1 > OSPF-ALL.MCAST.NET:
OSPFv2-hello 44: backbone E mask 255.255.255.0 int 10 pri 1 dead 40 dr 192.168.1.1
17:28:49.032438 IP (tos 0xc0, ttl 1, id 218, len 64) 192.168.1.1 > OSPF-ALL.MCAST.NET:
OSPFv2-hello 44: backbone E mask 255.255.255.0 int 10 pri 1 dead 40 dr 192.168.1.1
```

Using Diagram 1 as a reference, and having Nortel router A wanting to run OSPF with router B, we can see that device C can affect the routing table just as when RIP2 was run with no route policies. Below is the OSPF neighbor and IP routing table. In green are the routes we expect from neighbor 192.168.1.2 and in red are unwanted routes from neighbor 192.168.1.2 and 192.168.1.250.

```
OSPF Dynamic Neighbors
----------------------

                                Neighbor
IP Interface    Router ID       IP Address      State       Type
--------------- --------------- --------------- ----------- ----------
192.168.1.1     192.168.1.2     192.168.1.2     full        Dynamic
192.168.1.1     192.168.1.250   192.168.1.250   full        Dynamic

show ip routes                                        Apr 28, 2003
04:52:46 [GMT]

Network/Mask        Proto        Age Slot     Cost  NextHop Address
AS
------------------- ------ --------- ---- --------- ---------------
0.0.0.0/0           OSPF           2    1     10002 192.168.1.250
10.10.10.0/30       RIP            7    1         7 192.168.100.2
10.12.132.0/24      OSPF          47    1         1 192.168.1.2
10.60.8.248/30      OSPF          52    1     10001 192.168.1.250
10.100.163.0/30     RIP            7    1         7 192.168.100.2
10.133.11.101/32    RIP            7    1         7 192.168.100.2
10.133.11.103/32    RIP            7    1         7 192.168.100.2
10.133.11.105/32    RIP            7    1         7 192.168.100.2
172.1.1.0/30        RIP            7    1         7 192.168.100.2
172.16.0.0/16       OSPF          47    1         2 192.168.1.2
192.0.0.0/8         OSPF          47    1         2 192.168.1.2
192.168.1.0/24      Direct    250663    1         0 192.168.1.1
192.168.100.0/24    Direct      5229    1         0 192.168.100.1
192.168.100.4/30    OSPF          47    1         1 192.168.1.2
192.168.150.0/24    OSPF          47    1         2 192.168.1.2
192.168.151.64/30   OSPF          47    1         2 192.168.1.2
192.168.151.128/25  OSPF          48    1         2 192.168.1.2
192.168.166.0/24    OSPF          48    1         2 192.168.1.2
192.168.169.0/24    RIP            8    1         7 192.168.100.2

   Total Networks on Slot 1 = 19
```

To only receive routes from device B, the Nortel router will need traffic filters. The traffic filters will accept protocol 89 packets (OSPF is IP protocol 89) from device 192.168.1.2 and then drop all other IP protocol 89 packets. The below filter templates and traffic filters will accomplish this.

```
filter-template template-name ospf-neighbor
    match
       protocol 89
      source-network range 192.168.1.2
      back
    back
    actions
    back
  back
  filter-template template-name no-ospf-all
    match
       protocol 89
    back
    actions
       action drop
    back
  back

 traffic-filter filter-name one-neighbor
       precedence 1
       template-name ospf-neighbor
    back
    traffic-filter filter-name no-other-neighbor
       precedence 2
       template-name no-ospf-all
    back
```

To prevent device B's OSPF external routes from getting into device A's OSPF database, an OSPF accept policy to only accept 192.168.150.0/24 exact network and 192.168.151.0/24 range of networks is needed.

```
  accept polname acceptexternal
       precedence 10
     match
       network address 192.168.150.0 mask 255.255.255.0 match exact
       back
       network address 192.168.151.0 mask 255.255.255.0 match range
       back
     back
     modify
     back
   back
   accept polname dontaccept
      action ignore
      precedence 5
     match
       network address 0.0.0.0 mask 0.0.0.0 match range
       back
     back
     modify
     back
```

The combination of traffic filters and OSPF route policy will produce the following routing table. Notice that an extra network 192.168.100.4/30 was not filtered from the routing table event though the route policy doesn't list this network. Device B is running OSPF on this network, so the network becomes an OSPF internal route and can't be filtered by an OSPF accept policy.

```
show ip routes                                        Apr 29, 2003
09:11:32 [GMT]

Network/Mask        Proto        Age Slot     Cost  NextHop Address
AS
------------------- ------ --------- ---- --------- --------------- --
---
10.10.10.0/30       RIP           10    1         7 192.168.100.2
10.100.163.0/30     RIP           10    1         7 192.168.100.2
10.133.11.101/32    RIP           10    1         7 192.168.100.2
10.133.11.103/32    RIP           10    1         7 192.168.100.2
10.133.11.105/32    RIP           10    1         7 192.168.100.2
172.1.1.0/30        RIP           10    1         7 192.168.100.2
192.168.1.0/24      Direct      1822    1         0 192.168.1.1
192.168.100.0/30    Direct     13390    1         0 192.168.100.1
192.168.100.4/30    OSPF         789    1         2 192.168.1.2
192.168.150.0/24    OSPF         789    1         3 192.168.1.2
192.168.151.64/30   OSPF         789    1         3 192.168.1.2
192.168.151.128/25  OSPF         789    1         3 192.168.1.2
192.168.166.0/24    RIP           10    1         7 192.168.100.2
192.168.169.0/24    RIP           10    1         7 192.168.100.2

   Total Networks on Slot 1 = 14
```

Securing BGP on an Untrusted Network

In a Nortel Router, the limitation of routes sent and received is inherent in the configuration. The configuration must explicitly state which routes will be accepted from a BGP peer and there are no known vulnerabilities to this design. All attempts to circumvent with device C were not successful. Referring to diagram 1, the Nortel Router (A), would be configured to accept the routes 192.168.150/24, 192.168.151.64/30 and 192.168.151.128/25 with the following BGP configuration and BGP accept policy.

```
bgp router-id 192.168.1.1
      igp-interaction {ospf rip}
      local-as 64621
     peer local 192.168.1.1 remote 192.168.1.2 as 64600
     back
     accept polname accept-networks
        action accept
        precedence 5
        preference 5
       match
        as asnumber 64600
        back
        network address 192.168.150.0 mask 255.255.255.0 match exact
```

```
  back
  network address 192.168.151.0 mask 255.255.255.0 match range
  back
back
modify
back
```

This would produce the following routing table.

```
show ip routes                                        May 01, 2003
18:52:38 [GMT]

Network/Mask        Proto        Age Slot     Cost  NextHop Address
AS
------------------- ------ --------- ---- --------- ---------------
10.10.10.0/30       RIP            5    1         7 192.168.100.2
192.168.1.0/24      Direct        92    1         0 192.168.1.1
10.100.163.0/30     RIP            5    1         7 192.168.100.2
10.133.11.101/32    RIP            5    1         7 192.168.100.2
10.133.11.103/32    RIP            5    1         7 192.168.100.2
10.133.11.105/32    RIP            5    1         7 192.168.100.2
172.1.1.0/30        RIP            5    1         7 192.168.100.2
192.168.100.0/30    Direct        71    1         0 192.168.100.1
192.168.150.0/24    BGP-4         20    1    122888 192.168.1.2
64600
192.168.151.64/30   BGP-4         20    1    122888 192.168.1.2
64600
192.168.151.128/25  BGP-4         20    1    122888 192.168.1.2
64600
192.168.166.0/24    RIP            5    1         7 192.168.100.2
192.168.169.0/24    RIP            5    1         7 192.168.100.2

   Total Networks on Slot 1 = 14
```

SUMMARY

Configuring a Nortel BayRS router to allow a Site Manager workstation to send SNMP set commands opens up the router to SNMP vulnerabilities. Nortel BayRS routers currently only have telnet (not ssh) capabilities for remote login. Using a Best Practice strategy, the path used for telnet should be a trusted path and BCC should be preferred for all dynamic configurations.

When receiving routes from an untrusted source, RIP2 or BGP give more ability to limit the vulnerability to your network, so therefore limit your risk. Because OSPF forms a link state adjacency to the other router, the database must be shared. Since RIP2 and BGP are distance vector protocols, the routes received are easier to filter. This document explained how to filter incoming routes on these three protocols.

BIBLIOGRAPHY

"PROTOS Test-Suite:c06-snmpv1" 12 February, 2002. URL: http://www.ee.oulu.fi/research/ouspg/protos/testing/c06/snmpv1/index.html (28 April, 2003)

"The Simple Times" December, 2002 URL: http://www.simple-times.org/pub/simple-times/pdf/vol10-num1.pdf (27 April, 2003)

"Surviving the SNMP Vulnerability Scare" 26 February, 2002 UR: http://itmanagement.earthweb.com/columns/article.php/981231 (28 April, 2003)

"Nortel Networks Portfolio Summary in response to CERT SNMP Advisory 12 July, 2002. URL: http://www.nortelnetworks.com/corporate/technology/snpmv1.html (25 April, 2003)

"SNMP Best Practice Strategy" 26 February, 2002 URL: http://www.nortelnetworks.com/corporate/technology/snpmv1.html (25 April, 2003)

CERT Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP) 12 February, 2002 URL: http://www.cert.org/advisories/CA-2002-03.html (25 April, 2003)

"SimpleSoft SNMP Vulnerability Probes" URL: http://www.snmptest.com/SNMPProbe.html (23 April, 2003)

"PROTOS – Security Testing of Protocol Implementations" 19 March, 2003 URL: http://www.ee.oulu.fi/research/ouspg/protos/ (28 April, 2003)

"Readiness, Cooperation Key in Network Rebuild; Future to Bring Redundancy, Less Concentration" 17 June, 2002 URL http://www.kmbvideojournal.com/tcreport.htm (27 April, 2003)

"The Internet Protocol Journal" December, 1998 http://www.cisco.com/warp/public/759/ipj_3.pdf (24 April, 2003)

"WinDump:tcpdump for Windows" 8 August, 2002 URL: http://windump.polito.it/default.htm (24 April, 2003)

Bay Networks. Advanced IP Routing. Billerica: Bay Networks, Inc, 1997

Last Updated: May 25th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event