[COMPANY]
VPN WAN Design and Implementation Guidelines

February, 2002

Prepared By:
Jim Hudson
HTTP://www.hudson-family.com/jim-tech/

Prepared For:
[Company]

Chicago, IL

Table of Contents

1.0 Overview

[Company] engaged to perform an OSPF network design project - requirements discovery and OSPF preliminary architecture design, Proof of Concept testing, and Production design documentation - for the [Company] Wide Area Network (WAN). This document presents the findings, design architecture recommendations, test lab results, production design, and implementation guidelines.

The preliminary design (found in Section 3.0) is based on results using Cisco routers in a lab environment. During the Proof of Concept testing on the [Company]'s Nortel routers, this design was modified to accommodate differences in features between Cisco and Nortel.

The final design resulting from the Proof of Concept lab testing is presented in section 5.0. While the physical implementation of this design was not contracted as part of this project, an implementation guideline is provided in section 6.0. The configuration changes required to implement the production design are presented in section 9.0.

If desired a Statement of Work will be provided to implement this design.

2.0 Network Discovery

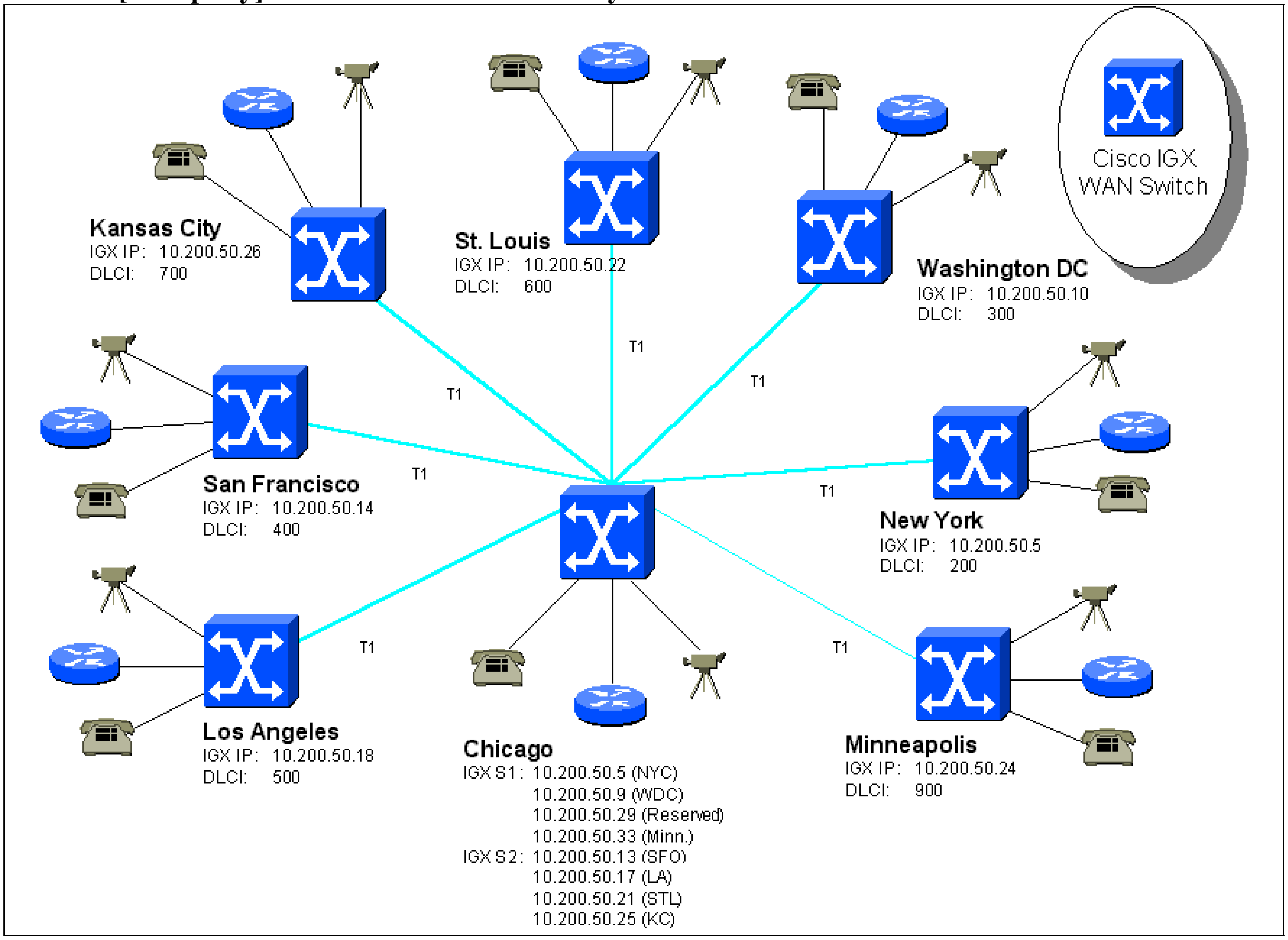
[Company], based in Chicago, IL, currently uses a simple hub and spoke private WAN design from it's headquarters in Chicago, IL, to the following eight remote locations:

- New York, NY
- Washington, DC
- Palm Beach
- Minneapolis
- San Francisco, CA
- Los Angeles, CA
- St Louis, MO
- Kansas City, MO

A Nortel ASN router at each remote site connects back to Chicago via a point-to-point frame relay circuit to a Nortel BLN-2 router. Frame relay services are provided by a Cisco IGX switch located at each location with a T1 circuit back to Chicago. Half of the T1 is used for voice, the other half is configured for the frame relay, data service. RIP-v2 is the IP routing protocol currently in use on the private WAN.

The following diagram (provided by [Company]) depicts this connectivity:

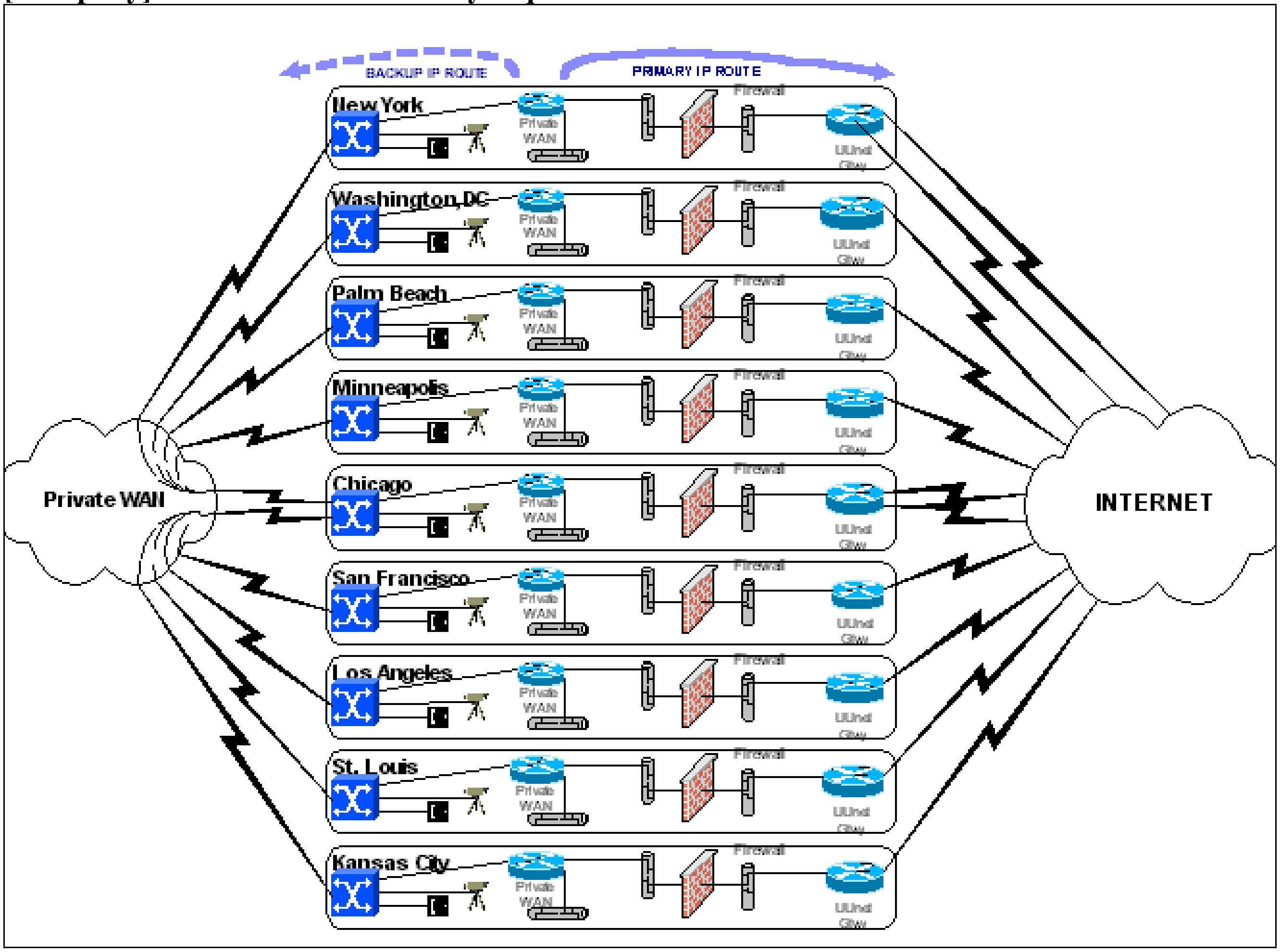
Current [Company] Private WAN Connectivity



[Company] is now in the process of implementing Nokia, Checkpoint FireWall 1 (FW-1) systems at each location with at least one T1 from each site to UUnet for Internet access and VPN service between corporate locations. The primary offices of Chicago and New York will use two T1 circuits each. [Company] plans to migrate their primary data connectivity to the VPN. The private WAN will continue to provide backup site-to-site data communication services. [Company] will reduce the bandwidth allocated for data on the private WAN. The excess private WAN bandwidth will then be reallocated for a videoconference network (yet to be implemented). Voice network traffic will not change.

The following diagram shows the high level conceptual plan for this network:

[Company] NEW WAN connectivity requirement



IP Addressing is the cornerstone of any WAN architecture. Efficient IP Routing is dependant on a logical and efficient address plan. The IP address plan currently in use at [Company] is functional, yet wasteful in its design and may pose long term scalability issues. [Company] indicated that they are unable to change their IP addressing scheme at this time; however, it is important to note the limitations of the current scheme. [Company] uses RFC 1918 10.0.0.0 for their private network address space and use the second octet of the IP address to identify the location and network function. The third octet is used to identify the device type. The fourth octet is used for individual devices. The 10.x private network offers a tremendous amount of address space for growth; however, using the current address plan scheme, [Company] will consume the 10.x network after a total of 20-24 sites.

2.1 VPN WAN Design Requirements

Currently, all inter-site traffic must pass through Chicago. The desire for the VPN is to create a full mesh so that all inter-site traffic can route directly to the destination. In addition to VPN services, the Nokia, Checkpoint systems will also be used for local Internet access. In the case of Chicago, the Nokia systems will also provide access to certain additional corporate resources.

Specific WAN Design Requirements:

- Preference the VPN over the private network for data communications
- Design must be scalable
- Provide dynamic IP reroute in the event of network or network equipment failure
- Simplify IP routing
- Support direct inter-site connectivity
- [Company] prefers an OSPF solution

2.2 Design Recommendation

Many design solutions were tested and reviewed in a lab environment to determine the best solution to meet [Company]'s requirements. Although [Company] preferred an OSPF solution, a BGP (Border Gateway Protocol) network routing architecture running exclusively on the Nortel routers is recommended. The unique features available in BGP provide a more straight-forward and reliable network architecture than is possible with OSPF. A preliminary BGP design is presented in **section 3**. This final design was determined after testing on Nortel equipment in the [Company] Proof of Concept Lab. The high level **final design** description is presented in **section 5.0**.

The high level IP Address plan was also reviewed. It is recommended that [Company] migrate to a more scalable and efficient address plan. This would accommodate more sites in the future and would also accommodate grouping remote sites into regions of contiguous address space. The full mesh design required by [Company] can create significant route convergence overhead as the network grows. I recommend that [Company] monitor route convergence time and establish a full mesh limit not to exceed 12 sites. To grow beyond this point, the WAN design should be organized into logical regions. Each region incorporating a minimum of 3 sites. A central core region of at least two sites would provide route aggregation and provide the transit path for data between regions. One possible regional design concept is briefly described in section 4.0 - Co-Location Disaster Recovery Considerations.

3.0 Preliminary Wide Area Network Plan

The preliminary recommendations presented in this section are based on the initial lab results. Several aspects of this design were modified during the Proof of Concept testing. The final design is presented in section 5.0.

The preliminary design recommendation is for the new WAN is based on the BGP Routing protocol (Border Gateway Protocol) using a single Autonomous System (AS) for each site. [Company]'s desire is to use their VPN as the primary data network path and use the private (IGX) network as the backup path. To support dynamic reroute over the private network in the event of any failure across the VPN, the Nortel routers must be capable of learning and maintaining the link status of the far end router interface through the VPN. BGP is uniquely capable of providing this requirement as it can support end-to-end route availability intelligence over a multi-hop, non-contiguous network (i.e. the Internet). To achieve this in an accurate and efficient manner, [Company] should follow these recommendations:

- The Nortel routers be the only active BGP routers on the WAN.
- Each remote site will be its own Autonomous System (AS).
- All BGP neighbor router interfaces must be explicitly identified.
- Neighbor interfaces must be part of the encryption domain on the firewalls to insure delivery by the VPN to the correct destination.
- The route attributes of the VPN neighbor advertisements must be preferred over other available paths (i.e. the private network).

By defining BGP neighbors and Firewall rules in this manner, the routers will be able to maintain end-to-end route intelligence and provide the desired fail-over routing.

The "Preliminary VPN WAN Design" diagram (in Appendix A) shows a three-site sample of this design which was tested using Cisco routers and Checkpoint firewalls running on Windows 2000.

3.1 BGP Preliminary Design Considerations

The function of the BGP routing protocol is to simplify IP routing information known by router devices on the enterprise. Route decision making efficiency is achieved by minimizing the IP network and routing information required at any one site. The most efficiency is achieved when each site and/or AS can be summarized into a single IP network block. Not only does this provide the most simple design, but also the easiest to manage, troubleshoot, expand and merge.

Significant forethought should be put into the initial design in an effort to keep the IP Address space summarizeable. This forethought will provide a more scaleable, efficient, and reliable enterprise.

The following chart indicates the smallest currently possible IP address summarization available on the [Company] network:

Site	Internal IP Networks currently in use	Summarization Starting Network	Network Mask
Chicago	10.10.0.0 – 10.12.0.0	10.8.0.0	/13
New York	10.20.0.0 – 10.22.0.0	10.16.0.0	/13
Washington DC	10.30.0.0 – 10.32.0.0	10.24.0.0 –10.32.0.0	/13
San Francisco	10.40.0.0 – 10.42.0.0	10.40.0.0	/13
Los Angeles	10.50.0.0 – 10.52.0.0	10.48.0.0	/13
St Louis	10.60.0.0 – 10.62.0.0	10.56.0.0	/13
Kansas City	10.70.0.0 – 10.72.0.0	10.64.0.0 – 10.72.0.0	/13
Palm Beach	10.80.0.0 – 10.82.0.0	10.80.0.0	/13
Minneapolis	10.90.0.0 – 10.92.0.0	10.88.0.0	/13

Based on using the second octet of the IP address to identify the site and network function the existing range of addresses assigned at each site, the smallest summarization possible is “/13”. In the case of Washington and Kansas City, the current addressing does not permit a single summarization. Two “/13” blocks are required.

3.2 BGP neighbors over a VPN

The most straight forward BGP / Firewall combination was desired to minimize firewall rules and overhead. To achieve this, on each local router, BGP neighbors are defined using Nortel’s Circuitless IP address. For all locations, this particular interface should use a 32 bit mask and be in the same “class C” network block. For example, Chicago would use 192.168.1.1 (/32), St. Louis would use 192.168.1.6 (/32). Each router will require a static route for network 192.168.1.0 identifying the firewall (real address) as the next hop. To provide a path from the VPN to the local Circuitless IP interface, the Firewalls require a host address static route (local Circuitless host address) pointing to the local router. VPN encryption domains will be required for the IP Address blocks located at each remote location – including the BGP neighbor host address.

In addition to these BGP neighbors, the private network serial interface of each remote site router will need to be specified as neighbors to Chicago and the Chicago serial interface defined as the BGP neighbor to each remote site. The BGP Peers defined by this neighbor relationship must be specified using the real IP address of the serial interface – not the Circuitless IP address.

This design will result in BGP locating (Circuitless IP) neighbors via the route across the VPN to the remote routers.

3.3 Private Network Routes:

In addition to the Circuitless IP neighbors, BGP neighbors and networks will be learned naturally across the private network. The private frame relay network is hub-and-spoke with no meshing. Since each site is defined as its own Autonomous System (AS), the remote sites will not attempt to use any other site as a transit AS. This is desired in every AS except Chicago. In Chicago, the private network facing interface must advertise all known Intranet networks. This will allow remote sites, in the event of a VPN connectivity failure, to "transit" the Chicago AS to reach other remote site networks. To insure that the VPN is used as the primary route, the route attributes on the outbound BGP advertisements must be given an artificially higher value (less attractive route). This can be accomplished using the Multi-Exit-Discriminator (MED) attribute to advertise a more desirable route through the VPN than over the Private Network.

3.4 IP Address Allocation

IP Address blocks provided by UUNet for each remote site are identified in the following table (data provided by SNR).

#	City	Network	Assigned IP	CIDR #1	CIDR #2
1	Chicago	/24	ISP..148.0	ISP..148.0 - ISP..148.127	ISP..148.128 - ISP..148.255
2	New York	/26	ISP..167.0	ISP..167.0 - ISP..167.31	ISP..167.32 - ISP..167.63
3	Washington DC	/27	ISP..97.160	ISP..97.160 - ISP..97.191	N/A
4	San Francisco	/27	ISP..165.32	ISP..165.32 - ISP..165.63	N/A
5	Los Angeles	/27	ISP..145.192	ISP..145.192 - ISP..145.223	N/A
6	St. Louis	/27	ISP..237.64	ISP..237.64 - ISP..237.95	N/A
7	Kansas City	/27	ISP..129.0	ISP..129.0 - ISP..129.31	N/A
8	West Palm Beach	/27	ISP..127.64	ISP..127.64 - ISP..127.95	N/A
9	Minneapolis	/27	ISP..8.128	ISP..8.128 - ISP..8.159	N/A

Firewall Virtual IP (VIP) and default gateway addresses – assigned by [Company]:

		Private WAN	Private WAN		Firewall	Firewall	
#	City	FR DLCI	FR local IP Gtwy	Internal Gateway	Internal VIP	External VIP	External Gateway
1	Chicago	100	10.200.50.	10.12.50.1	10.12.110.1	ISP..148.6	ISP..148.6
2	New York	200	10.200.50.	10.22.50.1	10.22.120.1	ISP..167.6	ISP..167.1
3	Washington DC	300	10.200.50.	10.32.50.1	10.32.130.1	ISP..97.166	ISP..97.161
4	San Francisco	400	10.200.50.	10.42.50.1	10.42.140.1	ISP..165.38	ISP..165.33
5	Los Angeles	500	10.200.50.	10.52.50.1	10.52.150.1	ISP..149.198	ISP..149.193
6	St. Louis	600	10.200.50.	10.62.50.1	10.62.160.1	ISP..237.70	ISP..237.65
7	Kansas City	700	10.200.50.	10.72.50.1	10.72.170.1	ISP..129.6	ISP..129.1
8	Palm Beach	800	10.200.50.	10.82.50.1	10.82.180.1	ISP..127.71	ISP..127.65
9	Minneapolis	900	10.200.50.	10.92.50.1	10.92.190.1	ISP..8.135	ISP..8.129

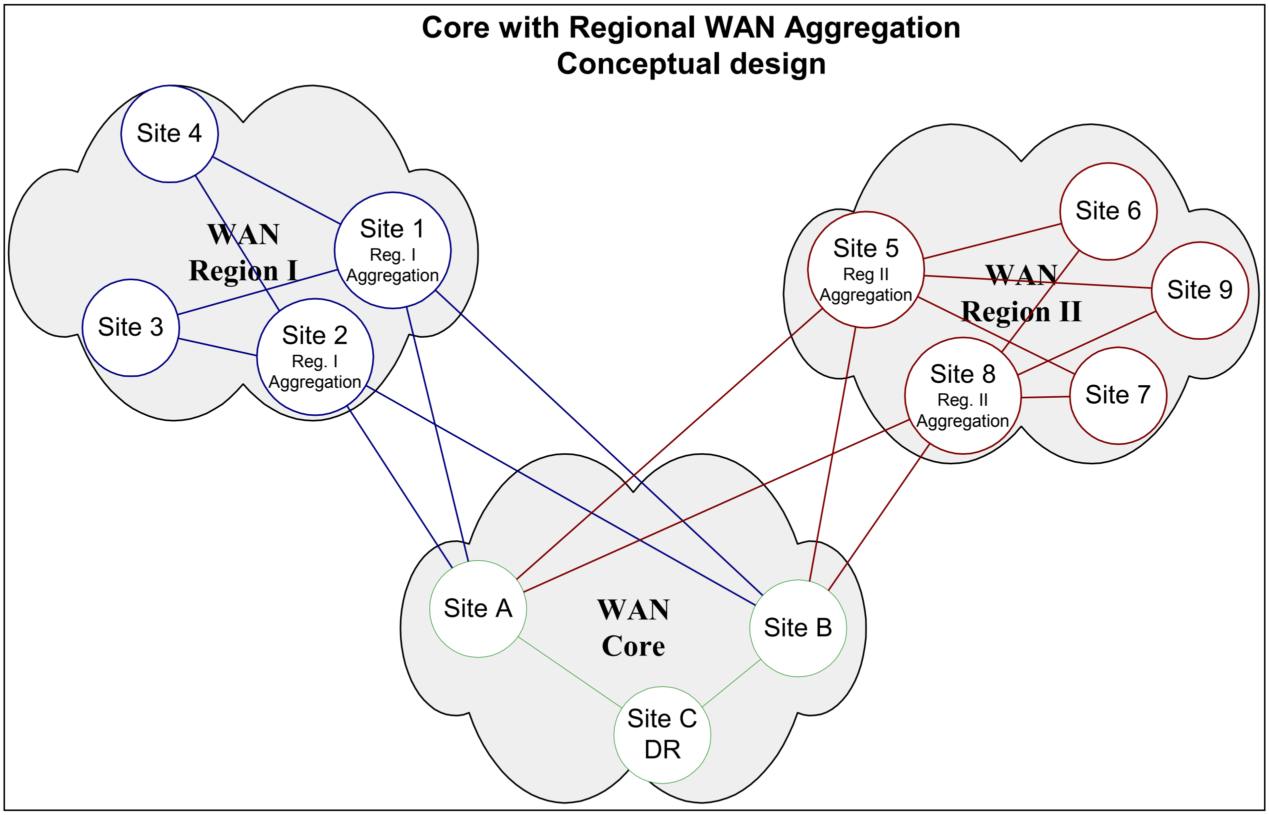
4.0 Co-Location Disaster Recovery Considerations

A co-location (co-lo) disaster recovery site is planned at an IBM facility. To be effective, each remote site should be connected directly through the VPN. Fail-over connectivity to the disaster recovery location is strongly recommended. Extending the private WAN to the disaster recovery location is preferred (in addition to the VPN) as this provides fail-over using different circuits as well as equipment.

Two approaches may be taken when planning for co-lo connectivity – 1) Treat the co-lo as just another VPN remote site; or 2) Logically join it to Chicago extending the private network to create a WAN core. The second approach offers more long-term flexibility in that a redundant core transit AS can be used to reduce routing complexity for the rest of the WAN and provide long term scalability. Combining both approaches offers the most flexibility and reliability.

As the [Company] network grows, creating a core will become more and more important. It is recommended that [Company] consider a regional design with a central core when the network grows to more than 12 sites. In this design, two to three key sites would be defined as core locations (including the Disaster Recovery site). Other remote sites would be grouped by geographical region. The regional boundaries must be well defined and can be somewhat logically based. At least two sites within each region would become aggregation sites for all locations in that region. Aggregation sites would employ redundant connectivity to the Core. The Core must be designed to provide fast and reliable routing to/from aggregate sites, ideally independent of (or in addition to) user service requirements at the core locations. [Company] is now in the progress of implementing VPN service for remote site connectivity. This would not be optimal for Intra-core and Aggregate-to-Core connectivity due to the Firewall and VPN overhead; however, between remote locations within the same region, use of the VPN would be fine.

The following diagram is presented as an example of this design.



The advantage to this type of tiered network connectivity is that the per site connectivity overhead does not need to exceed a finite (known) limit. As the overall network expands, performance on the network can be maintained and grown in a predictable manner.

Assuming that the Disaster Recovery Center is located within the Core, it would remain available via diverse paths from all sites. As the rest of the network grows, connectivity to the core and to the DR site remains simple. One important factor to monitor within the core is bandwidth availability. As more remote regional sites are added, bandwidth requirements to the Core and across the core will also increase. This requires constant performance monitoring and planned growth.

5.0 Final Design - Proof of Concept Lab Results

During the Proof of Concept (POC) testing, it was determined that several changes to the preliminary design would be required. These changes included using BGP ONLY on the Public (VPN) side of the network, and using the real router interface address for BGP peers (not circutless IP addresses). The design changes were due primarily to routing feature differences between Cisco and Nortel; however, due to time constraints, hardware problems, and VPN connectivity issues, extensive configuration options could not be tested.

The final design is presented in this section.

5.1 Design Description

The new VPN WAN will be based on a combination of the existing RIP v2 private network and BGP running on the VPN using a single Autonomous System for each site. [Company]'s desire is to use their VPN as the primary data network path and use the private (IGX) network as the backup path. To support reroute over the private network in the event of any failure across the VPN, the Nortel routers must be capable of maintaining intelligent link status of the far end router interfaces through the VPN as well as over the private network. BGP is uniquely capable of providing this requirement over the VPN as it can support end-to-end route availability intelligence over a multi-hop non-contiguous network (i.e. the Internet). On the private network, RIP v2 will continue to be used as the Interior Gateway Protocol (IGP). The following highlights the design requirements:

- The Nortel routers will be the only active BGP routers on the internal WAN.
- Each remote site will be its own BGP Autonomous System (AS).
- All BGP neighbor router interfaces must be explicitly identified.
- The Private WAN will continue to use RIP v2 as an IGP
- The IP route attributes of RIP and BGP will naturally prefer BGP over RIP thus sending traffic over the VPN as the primary path.

The "Production VPN WAN" diagram (in Appendix A) shows the complete network design.

5.2 BGP Design Considerations

The function of the BGP routing protocol is to simplify IP routing information known by router devices on the enterprise. Route decision making efficiency is achieved by minimizing the IP network and routing information required at any one site. The most efficiency is achieved when each site and/or AS can be summarized into a single IP network block. Not only does this provide the most simple design, but also the easiest to manage, troubleshoot, expand and merge.

Significant forethought should be put into the initial design in an effort to keep the IP Address space summarizeable. This forethought will provide a more scaleable, efficient, and reliable enterprise.

The following chart indicates the currently smallest possible IP address summarization available on the [Company] network:

Site	Internal IP Networks currently in use	Summarization Starting Network	Network Mask
Chicago	10.10.0.0 – 10.12.0.0	10.8.0.0	/13
New York	10.20.0.0 – 10.22.0.0	10.16.0.0	/13
Washington DC	10.30.0.0 – 10.32.0.0	10.24.0.0 –10.32.0.0	/13
San Francisco	10.40.0.0 – 10.42.0.0	10.40.0.0	/13
Los Angeles	10.50.0.0 – 10.52.0.0	10.48.0.0	/13
St Louis	10.60.0.0 – 10.62.0.0	10.56.0.0	/13
Kansas City	10.70.0.0 – 10.72.0.0	10.64.0.0 – 10.72.0.0	/13
Palm Beach	10.80.0.0 – 10.82.0.0	10.80.0.0	/13
Minneapolis	10.90.0.0 – 10.92.0.0	10.88.0.0	/13

Based on using the second octet of the IP address to identify the site and network function the existing range of addresses assigned at each site, the smallest summarization possible is “/13”. In the case of Washington and Kansas City, the current addressing does not permit a single summarization. Two “/13” blocks are required.

5.3 BGP neighbors over a VPN

The most straight forward BGP / Firewall combination was desired to minimize firewall rules and overhead. To achieve this, on each local router, BGP neighbors are defined using the firewall-facing Ethernet interface. To insure that the router uses the VPN to locate its BGP neighbors, a static host route (32 bit mask) is required for each peer pointing to a next hop of the firewall. Based on the encryption domain, the firewalls will then “route” the BGP advertisements through the VPN tunnel to the appropriate destination.

5.4 Private Network Routes:

On the Private Network, RIP v2 will be used as the IGP. This configuration is currently in use on the [Company] WAN, no additional features are required.

5.5 IP Address Allocation

IP Address blocks provided by UUNet for each remote site are identified in the following table (data provided by SNR).

#	City	Network	Assigned IP	CIDR #1	CIDR #2
1	Chicago	/24	ISP..148.0	ISP..148.0 - ISP..148.127	ISP..148.128 - ISP..148.255
2	New York	/26	ISP..167.0	ISP..167.0 - ISP..167.31	ISP..167.32 - ISP..167.63
3	Washington DC	/27	ISP..97.160	ISP..97.160 - ISP..97.191	N/A
4	San Francisco	/27	ISP..165.32	ISP..165.32 - ISP..165.63	N/A
5	Los Angeles	/27	ISP..145.192	ISP..145.192 - ISP..145.223	N/A
6	St. Louis	/27	ISP..237.64	ISP..237.64 - ISP..237.95	N/A
7	Kansas City	/27	ISP..129.0	ISP..129.0 - ISP..129.31	N/A
8	West Palm Beach	/27	ISP..127.64	ISP..127.64 - ISP..127.95	N/A
9	Minneapolis	/27	ISP..8.128	ISP..8.128 - ISP..8.159	N/A

Firewall Virtual IP (VIP) and default gateway addresses – assigned by [Company]:

#	City	Private WAN FR DLCI	Private WAN FR local IP Gtwy	Internal Gateway	Firewall Internal VIP	Firewall External VIP	External Gateway
1	Chicago	100	10.200.50.	10.12.50.1	10.12.110.1	ISP..148.6	ISP..148.6
2	New York	200	10.200.50.	10.22.50.1	10.22.120.1	ISP..167.6	ISP..167.1
3	Washington DC	300	10.200.50.	10.32.50.1	10.32.130.1	ISP..97.166	ISP..97.161
4	San Francisco	400	10.200.50.	10.42.50.1	10.42.140.1	ISP..165.38	ISP..165.33
5	Los Angeles	500	10.200.50.	10.52.50.1	10.52.150.1	ISP..149.198	ISP..149.193
6	St. Louis	600	10.200.50.	10.62.50.1	10.62.160.1	ISP..237.70	ISP..237.65
7	Kansas City	700	10.200.50.	10.72.50.1	10.72.170.1	ISP..129.6	ISP..129.1
8	Palm Beach	800	10.200.50.	10.82.50.1	10.82.180.1	ISP..127.71	ISP..127.65
9	Minneapolis	900	10.200.50.	10.92.50.1	10.92.190.1	ISP..8.135	ISP..8.129

6.0 Network Implementation

The network design described and proposed in this document has been jointly tested in the [Company] proof of concept lab. The completion of this Proof of Concept testing provided input for the Network Implementation.

The network implementation presented in the following sections provides specific configuration details for the [Company] Nortel routers. These configuration details are presented in the overall context of a high level implementation process (order of events). Specific Firewall and VPN capabilities and configurations may be referenced in this document; however, specific Firewall and VPN configurations are not within the scope of this document. [Company] security staff will implement the required VPN changes.

6.1 High-Level Implementation Plan

As with any implementation, continuity of service and service improvement are key factors to keep in mind at every step. Prior to starting any implementation, several factors must be confirmed. They are:

1. Stability of the current environment
2. Well-defined change procedure
3. Implementation steps (implementation script or procedures)
4. Adequate time (change window) to coordinate implementation
5. Verification procedures
6. Back-out plan
7. Completion documentation

The following sections provide the "Implementation steps" to be implemented and the "verification procedures." [Company] will be responsible for the other factors as well as the actual implementation.

6.2 Router Change Implementation Steps

6.2.1 Verify Operational Status

Prior to starting any changes or even scheduling a change, the operational status of the current network environment must be verified. This must include all routers, router interfaces, LAN connectivity, WAN circuits and connectivity, dial backup and Firewall access.

All network connectivity issues must be resolved before proceeding with scheduling or implementing any network changes.

6.2.2 Schedule Network Outage

Once the network is verified to be stable. An outage window may be requested / scheduled to implement network changes. The outage window must provide adequate time to implement the desired changes, back-out the changes if necessary, plus provide additional time to resolve unexpected issues.

6.2.3 Save and Backup Configuration Files

The first step to making a change is to save the current network equipment configurations and back them up. For [Company], this would include the Nortel routers and the Nokia firewalls. The current operational Nortel router configuration files should be saved as the default boot configuration. Configuration files must also be saved in a location locally accessible by technical staff. The local copy of the running production configuration will be used to stage off-line configuration changes.

6.2.4 Make Configuration Changes Off-Line

Given adequate time, the router configuration changes should be made on the local copy of the configuration for each router. When completed, the changes must be saved using a new file name.

All changes should be staged in this manner well before the outage window begins. If possible, these changes should be tested in the lab prior to implementation.

6.2.5 Copy Off-Line Configuration Files to Network Equipment

At the start of the change window, repeat the operational status check.

After verification, copy the new configuration files to its corresponding router. DO NOT overwrite the default running configuration file. Choose a new file name.

6.2.6 Restart Equipment

Sequentially reload the REMOTE routers with the new configuration.
If the new configuration permits intermediate verification prior to implementing the changes on the central site router, verify operational status after each change – prior to reloading the next site.

If any unexpected connectivity issues are discovered during this procedure, the sequential reload methodology will allow for possible detection and correction (or back-out) before all sites are reloaded (committed). This can reduce back-out time, if required.

After all remote router changes are implemented, reload the central site router with the new configuration.

6.2.7 Verify Operational Status

After all devices scheduled to be changed are reloaded, a thorough operational verification of each device should be conducted. This includes checking the status of individual interfaces, protocols, remote accessibility, and routing tables.

6.2.8 Validate Operational Connectivity

In addition to individual device operation, the overall operational status of the new configuration must be conducted to verify that the network is truly operating in the desired configuration. This includes:

1. Proper routing – connectivity between sites over the desired path.
2. Route table verification – insure that the correct networks appear in the routing tables.
3. Verify that removed features are not running.

6.2.9 Save and Backup New Configuration as Default Startup

After complete verification of production operation, copy the OLD default configuration to a new file name and save the new running production configurations as the default boot configuration file. Configuration files must also be saved in a location locally accessible by technical staff. Old configuration files should be maintained for reference and potential future back-out.

In addition to an archive of historical configuration files, it is helpful to document the changes made in new configuration files. This can be as simple as a text file that accompanies the configuration files and helps when reviewing configuration files at a later date.

7.0 Diagrams

Figure 1 Preliminary VPN WAN Lab Design

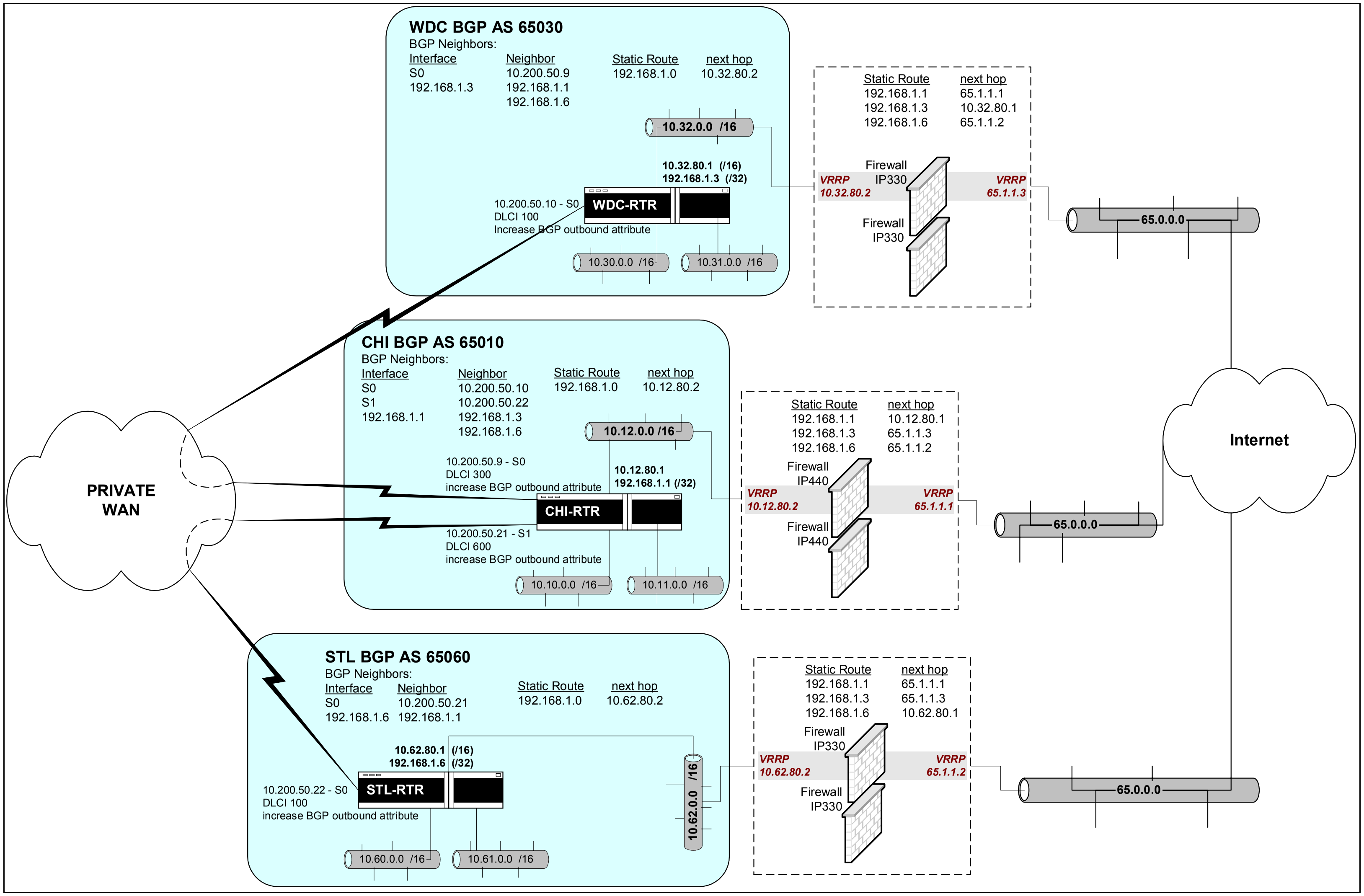
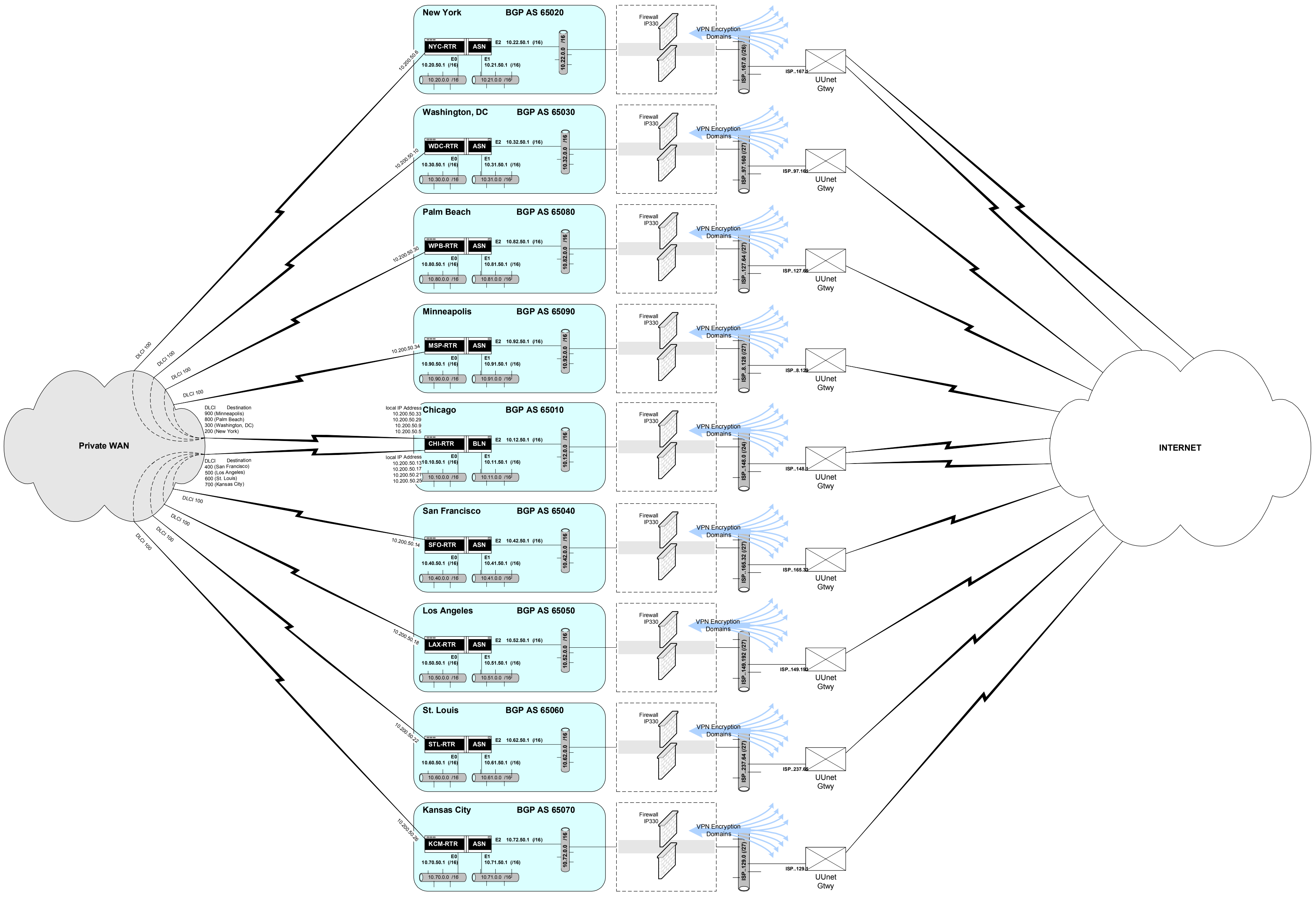


Figure 2 [Company] Production WAN


Private WAN
DLCI 100
DLCI 100
DLCI 100
DLCI 100
DLCI Destination
900 (Minneapolis)
800 (Palm Beach)
300 (Washington, DC)
200 (New York)
DLCI Destination
400 (San Francisco)
500 (Los Angeles)
600 (St. Louis)
700 (Kansas City)
DLCI 100
DLCI 100
DLCI 100
DLCI 100
10.200.50.6
New York
BGP AS 65020
NYC-RTR
ASN
E2 10.22.50.1 (/16)
E0 10.20.50.1 (/16)
E1 10.21.50.1 (/16)
10.20.0.0 /16
10.21.0.0 /16
10.22.0.0 /16
10.200.50.10
Washington, DC
BGP AS 65030
WDC-RTR
ASN
E2 10.32.50.1 (/16)
E0 10.30.50.1 (/16)
E1 10.31.50.1 (/16)
10.30.0.0 /16
10.31.0.0 /16
10.32.0.0 /16
10.200.50.30
Palm Beach
BGP AS 65080
WPB-RTR
ASN
E2 10.82.50.1 (/16)
E0 10.80.50.1 (/16)
E1 10.81.50.1 (/16)
10.80.0.0 /16
10.81.0.0 /16
10.82.0.0 /16
10.200.50.34
Minneapolis
BGP AS 65090
MSP-RTR
ASN
E2 10.92.50.1 (/16)
E0 10.90.50.1 (/16)
E1 10.91.50.1 (/16)
10.90.0.0 /16
10.91.0.0 /16
10.92.0.0 /16
local IP Address
10.200.50.33
10.200.50.29
10.200.50.9
10.200.50.5
Chicago
BGP AS 65010
CHI-RTR
BLN
E2 10.12.50.1 (/16)
E0 10.10.50.1 (/16)
E1 10.11.50.1 (/16)
local IP Address
10.200.50.13
10.200.50.17
10.200.50.21
10.200.50.25
10.10.0.0 /16
10.11.0.0 /16
10.12.0.0 /16
10.200.50.14
San Francisco
BGP AS 65040
SFO-RTR
ASN
E2 10.42.50.1 (/16)
E0 10.40.50.1 (/16)
E1 10.41.50.1 (/16)
10.40.0.0 /16
10.41.0.0 /16
10.42.0.0 /16
10.200.50.18
Los Angeles
BGP AS 65050
LAX-RTR
ASN
E2 10.52.50.1 (/16)
E0 10.50.50.1 (/16)
E1 10.51.50.1 (/16)
10.50.0.0 /16
10.51.0.0 /16
10.52.0.0 /16
10.200.50.22
St. Louis
BGP AS 65060
STL-RTR
ASN
E2 10.62.50.1 (/16)
E0 10.60.50.1 (/16)
E1 10.61.50.1 (/16)
10.60.0.0 /16
10.61.0.0 /16
10.62.0.0 /16
10.200.50.26
Kansas City
BGP AS 65070
KCM-RTR
ASN
E2 10.72.50.1 (/16)
E0 10.70.50.1 (/16)
E1 10.71.50.1 (/16)
10.70.0.0 /16
10.71.0.0 /16
10.72.0.0 /16
Firewall
IP330
VPN Encryption
Domains
ISP..167.0 (/26)
ISP..167.1
ISP..97.160 (/27)
ISP..97.161
ISP..127.64 (/27)
ISP..127.65
ISP..8.128 (/27)
ISP..8.129
ISP..148.0 (/24)
ISP..148.1
ISP..165.32 (/27)
ISP..165.33
ISP..149.192 (/27)
ISP..149.193
ISP..237.64 (/27)
ISP..237.65
ISP..129.0 (/27)
ISP..129.1
UUnet
Gtwy
INTERNET

8.0 BGP Troubleshooting Guide

BGP is a very mature and stable protocol and once the initial hurdles are overcome in establishing connectivity routing works smoothly. During initial setup up of the BGP network or to trouble shoot the production network follow the steps given below to isolate BGP related problems.

8.1 Verify Neighbor Peer Relationship

Before BGP peers can exchange routing information they must first establish a peer relationship. This can be verified in BCC (Bay Console Command) using the command

Bcc> Show bgp peers

In response to the above command, the router will show the status of all BGP peers. A working BGP status between two BGP peers is identified as "**established**". For BGP peer status to be "established" the following must exist:

a. An IGP (interior gateway protocol) route or static route to reach the peer.
b. Both sides of the BGP link should be configured with the correct AS number, peer address, local address, etc.
c. EBGP multihop must be enabled to establish peers across the VPN.

8.2 Verify proper routes are advertised

For BGP to advertise routes -

a. Routes must exist in the routing table of the advertising router
b. Appropriate "announce" policies must exist (be configured) on the advertising router to announce required routes

8.3 Verify BGP routes are accepted

For BGP routes to be placed in the IP routing table (from a remote router) -

a. Appropriate "accept" policies must exist (be configured) on the router accepting the routes
b. Next hop address shown in the "show BGP routes" command must be reachable.

8.4 Additional General Trouble Shooting Logic

The following is a brief overview of the logical flow to isolate network reachability problems. It is not intended to be exhaustive nor command specific, merely the flow of items to check in the network until the problem is identified. The follow-up action based on the results (success or failure) of each step listed will vary from one problem to the next. The answer at each step draws a picture of where the network is working and where a possible problem may be.

Is the device reachable from anywhere?

a. Ping Destination from several workstations
b. Ping destination from the local router
c. Ping destination from the remote router

What routing path is being used to reach the device?

a. Trace route to Destination
b. Trace route from Destination

What other nearby devices are reachable?

a. Ping several devices at same location (different subnet, same subnet)
b. Ping local router interface
c. Ping remote router interface
d. If device is operational – what other devices are reachable FROM that device

Check local and remote switch (or hub) connectivity

a. Check switch connectivity to router
b. Check switch connectivity to device
c. Check ARP cache on router for device
d. Check Address Cache on Switch for device and router

Check for duplicate IP or MAC

a. Check that IP on device is unique
b. Check that correct DHCP address was allocated
c. Check domain (IP and/or Windows) and DNS settings on client

Are the router interfaces operational?

a. Check status of local router interface
b. Check status of VPN interface
c. Check status of Frame Relay (both ends)
d. Check dial-backup status

Check routing protocols

a. Does destination network appear in routing table
b. Check BGP details
c. Check RIP details

Check VPN

a. Check end-to-end connectivity through VPN (several sites)
b. Check VPN encryption domains
c. Check Firewall rules
d. Make sure correct rules are applied
e. Make sure TCP port 179 (BGP) is open through VPN
f. Make sure router has correct Static route pointing to VPN

9.0 Production WAN Nortel Router Configuration Parameters

The following Nortel router configuration changes are provided to assist [Company] with the implementation of the proposed BGP network design. These changes are based on changes that were developed in the Proof of Concept (POC) lab. These changes address only the implementation of BGP on the Public (VPN) network and Private (IGX) network. These changes also assume that [Company] will not require any changes to the existing RIP routing configuration.

It is strongly recommended that [Company] technical staff build new configuration files off-line and implement these changes in a very tightly controlled and monitored manner. Such a process is provided in **Section 6.0**.

9.1 Chicago

Open the local Chicago configuration file in Site Manager. Immediately save the file as a new name (eg. *chi-bgp-new.cfg*). Make the specified changes.

Enable Subnet Zero and Default Routes

From the *Configuration Manger* screen:
>Protocols >IP >Global
    Subnet Zero **Enable**
    Enable Default Route for Subnets **Enable**

Add BGP Protocol

From the *Configuration Manger* screen:
>Circuits >Edit
Select circuit **E32**
Select **Edit**
The Circuit Definition screen for E32 will be displayed.
>Protocols >Add/Delete
    Select **IP**
        RIP
        BGP
        BOOTP (if required)
    Select **OK**

Enter the following on the BGP Configuration screen:
    Identifier **10.12.50.1**
    Local AS **65010**
Select **OK**
On the BGP Peer Screen, enter the following:

Peer Address **10.22.50.1**
Peer AS **65020**
Local Address **10.12.50.1**
Select **OK**

Select **OK** when asked to enable Multi-hop EBGP.

Press **F10** to exit current screen
Select **DONE** to return to Configuration Manager screen.

Add BGP Peers

From the *Configuration Manager* screen:

>Protocols >IP >BGP >Peers
Scroll down the IP interface list and select **10.12.50.1, E32**
Select **BGP Peers**
Select **Add**
Peer Address **10.32.50.1**
Peer AS **65030**
Select **OK**

Select **Add**
Peer Address **10.42.50.1**
Peer AS **65040**
Select **OK**

Select **Add**
Peer Address **10.52.50.1**
Peer AS **65050**
Select **OK**

Select **Add**
Peer Address **10.62.50.1**
Peer AS **65060**
Select **OK**

Select **Add**
Peer Address **10.72.50.1**
Peer AS **65070**
Select **OK**

Select **Add**
Peer Address **10.82.50.1**
Peer AS **65080**
Select **OK**

Select **Add**

Peer Address	**10.92.50.1**
Peer AS	**65090**
Select	**OK**

Select **Done** until returned to the *Configuration Manager* screen.

Specify BGP Accept Policies

>Protocol >IP >Policy Filters >BGP-4 >Accept Policies

Select **ADD**

Name	***Local*-VPN-Accept-List**	(*Local* refers to local site name)
Action	**Accept**	
Networks	Select **List**	

From the Networks Policy Filter List screen, enter each of the 24 remote subnets as follows:

Network Number	Network Mask	Exact / Range
10.20.0.0	**255.255.0.0**	**Exact**
10.21.0.0	**255.255.0.0**	**Exact**
10.22.0.0	**255.255.0.0**	**Exact**
10.30.0.0	**255.255.0.0**	**Exact**
10.31.0.0	**255.255.0.0**	**Exact**
10.32.0.0	**255.255.0.0**	**Exact**
10.40.0.0	**255.255.0.0**	**Exact**
10.41.0.0	**255.255.0.0**	**Exact**
10.42.0.0	**255.255.0.0**	**Exact**
10.50.0.0	**255.255.0.0**	**Exact**
10.51.0.0	**255.255.0.0**	**Exact**
10.52.0.0	**255.255.0.0**	**Exact**
10.60.0.0	**255.255.0.0**	**Exact**
10.61.0.0	**255.255.0.0**	**Exact**
10.62.0.0	**255.255.0.0**	**Exact**
10.70.0.0	**255.255.0.0**	**Exact**
10.71.0.0	**255.255.0.0**	**Exact**
10.72.0.0	**255.255.0.0**	**Exact**
10.80.0.0	**255.255.0.0**	**Exact**
10.81.0.0	**255.255.0.0**	**Exact**
10.82.0.0	**255.255.0.0**	**Exact**
10.90.0.0	**255.255.0.0**	**Exact**
10.91.0.0	**255.255.0.0**	**Exact**
10.92.0.0	**255.255.0.0**	**Exact**

Select **OK**
Select **Done**

Specify BGP Announce Policies

>Protocol >IP >Policy Filters >BGP-4 >Announce Policies
Select **ADD**

Name **CHI-VPN-Announce-List** (*Local* refers to local site name)
Action **Announce**
Route Source Select **Values**
Direct only, deselect all other sources.

Networks Select **List**
From the Networks Policy Filter List screen, enter each of the local (Direct) subnets as follows:

Network Number	Network Mask	Exact / Range
10.10.0.0	**255.255.0.0**	**Exact**
10.11.0.0	**255.255.0.0**	**Exact**
10.12.0.0	**255.255.0.0**	**Exact**

Advertise Select **List**
From the Networks Policy Filter List screen, enter each of the local (Direct) subnets as follows:

Network Number	Network Mask
10.10.0.0	**255.255.0.0**
10.11.0.0	**255.255.0.0**
10.12.0.0	**255.255.0.0**

Add Static routes for BGP Peers

From the *Configuration Manager* screen:
>Protocols >IP >Static Routes
Select **ADD**

Destination IP Address	**10.22.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.12.110.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.32.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.12.110.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.42.50.1**
Address Mask	**255.255.255.255**
Cost	**1**

Next Hop Address	**10.12.110.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.52.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.12.110.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.62.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.12.110.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.72.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.12.110.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.82.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.12.110.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.92.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.12.110.1**
Preference	**16**

Select **OK**
Select **Done**

Save the configuration file. Close the configuration manager session.

9.2 New York

Open the local New York configuration file in Site Manager. Immediately save the file as a new name (eg. nyc-*bgp-new.cfg*). Make the specified changes.

Enable Subnet Zero and Default Routes

From the *Configuration Manger* screen:
>Protocols >IP >Global
Subnet Zero **Enable**
Enable Default Route for Subnets **Enable**

Add BGP Protocol

From the *Configuration Manger* screen:
>Circuits >Edit
Select circuit **E32**
Select **Edit**
The Circuit Definition screen for E32 will be displayed.
>Protocols >Add/Delete
Select **IP**
RIP
BGP
BOOTP (if required)
Select **OK**

Enter the following on the BGP Configuration screen:

Identifier	**10.22.50.1**
Local AS	**65020**

Select **OK**
On the BGP Peer Screen, enter the following:

Peer Address	**10.12.50.1**
Peer AS	**65010**
Local Address	**10.22.50.1**
Select	**OK**

Select **OK** when asked to enable Multi-hop EBGP.

Press **F10** to exit current screen
Select **DONE** to return to Configuration Manager screen.

Add BGP Peers

From the *Configuration Manager* screen:

>Protocols >IP >BGP >Peers
Scroll down the IP interface list and select **10.22.50.1, E32**
Select **BGP Peers**
Select **Add**

Peer Address	**10.32.50.1**
Peer AS	**65030**
Select	**OK**

Select **Add**

Peer Address	**10.42.50.1**
Peer AS	**65040**
Select	**OK**

Select **Add**

Peer Address	**10.52.50.1**
Peer AS	**65050**
Select	**OK**

Select **Add**

Peer Address	**10.62.50.1**
Peer AS	**65060**
Select	**OK**

Select **Add**

Peer Address	**10.72.50.1**
Peer AS	**65070**
Select	**OK**

Select **Add**

Peer Address	**10.82.50.1**
Peer AS	**65080**
Select	**OK**

Select **Add**

Peer Address	**10.92.50.1**
Peer AS	**65090**
Select	**OK**

Select **Done** until returned to the *Configuration Manager* screen.

Specify BGP Accept Policies

>Protocol >IP >Policy Filters >BGP-4 >Accept Policies

Select **ADD**

Name	***Local*-VPN-Accept-List**	(*Local* refers to local site name)
Action	**Accept**	
Networks	Select **List**	

From the Networks Policy Filter List screen, enter each of the 24 remote subnets as follows:

Network Number	Network Mask	Exact / Range
10.10.0.0	**255.255.0.0**	**Exact**
10.11.0.0	**255.255.0.0**	**Exact**
10.12.0.0	**255.255.0.0**	**Exact**
10.30.0.0	**255.255.0.0**	**Exact**
10.31.0.0	**255.255.0.0**	**Exact**
10.32.0.0	**255.255.0.0**	**Exact**
10.40.0.0	**255.255.0.0**	**Exact**
10.41.0.0	**255.255.0.0**	**Exact**
10.42.0.0	**255.255.0.0**	**Exact**
10.50.0.0	**255.255.0.0**	**Exact**
10.51.0.0	**255.255.0.0**	**Exact**
10.52.0.0	**255.255.0.0**	**Exact**
10.60.0.0	**255.255.0.0**	**Exact**
10.61.0.0	**255.255.0.0**	**Exact**
10.62.0.0	**255.255.0.0**	**Exact**
10.70.0.0	**255.255.0.0**	**Exact**
10.71.0.0	**255.255.0.0**	**Exact**
10.72.0.0	**255.255.0.0**	**Exact**
10.80.0.0	**255.255.0.0**	**Exact**
10.81.0.0	**255.255.0.0**	**Exact**
10.82.0.0	**255.255.0.0**	**Exact**
10.90.0.0	**255.255.0.0**	**Exact**
10.91.0.0	**255.255.0.0**	**Exact**
10.92.0.0	**255.255.0.0**	**Exact**

Select **OK**
Select **Done**

Specify BGP Announce Policies

>Protocol >IP >Policy Filters >BGP-4 >Announce Policies

Select **ADD**

Name	***Local*-VPN-Announce-List**	(*Local* refers to local site name)
Action	**Announce**	
Route Source	**Values**	
	Direct only, deselect all other sources.	

Networks **List**

From the Networks Policy Filter List screen, enter each of the local (Direct) subnets as follows:

Network Number	Network Mask	Exact / Range
10.20.0.0	**255.255.0.0**	**Exact**
10.21.0.0	**255.255.0.0**	**Exact**
10.22.0.0	**255.255.0.0**	**Exact**

Advertise Select **List**

From the Networks Policy Filter List screen, enter each of the local (Direct) subnets as follows:

Network Number	Network Mask
10.20.0.0	**255.255.0.0**
10.21.0.0	**255.255.0.0**
10.22.0.0	**255.255.0.0**

Add Static routes for BGP Peers

From the *Configuration Manager* screen:

>Protocols >IP >Static Routes

Select **ADD**

Destination IP Address **10.12.50.1**
Address Mask **255.255.255.255**
Cost **1**
Next Hop Address **10.22.120.1**
Preference **16**
Select **OK**

Select **ADD**

Destination IP Address **10.32.50.1**
Address Mask **255.255.255.255**
Cost **1**
Next Hop Address **10.22.120.1**
Preference **16**
Select **OK**

Select **ADD**

Destination IP Address **10.42.50.1**
Address Mask **255.255.255.255**
Cost **1**
Next Hop Address **10.22.120.1**
Preference **16**
Select **OK**

Select **ADD**

Destination IP Address **10.52.50.1**
Address Mask **255.255.255.255**
Cost **1**

Next Hop Address	**10.22.120.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.62.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.22.120.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.72.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.22.120.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.82.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.22.120.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.92.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.22.120.1**
Preference	**16**

Select **OK**

Select **Done**

Save the configuration file. Close the configuration manager session.

9.3 Washington, DC

Open the local Washington, DC configuration file in Site Manager. Immediately save the file as a new name (eg. wdc-*bgp-new.cfg*). Make the specified changes.

Enable Subnet Zero and Default Routes

From the *Configuration Manger* screen:
>Protocols >IP >Global
Subnet Zero **Enable**
Enable Default Route for Subnets **Enable**

Add BGP Protocol

From the *Configuration Manger* screen:
>Circuits >Edit
Select circuit **E32**
Select **Edit**
The Circuit Definition screen for E32 will be displayed.
>Protocols >Add/Delete
Select **IP**
RIP
BGP
BOOTP (if required)
Select **OK**

Enter the following on the BGP Configuration screen:

Identifier	**10.32.50.1**
Local AS	**65030**

Select **OK**
On the BGP Peer Screen, enter the following:

Peer Address	**10.12.50.1**
Peer AS	**65010**
Local Address	**10.32.50.1**
Select	**OK**

Select **OK** when asked to enable Multi-hop EBGP.

Press **F10** to exit current screen
Select **DONE** to return to Configuration Manager screen.

Add BGP Peers

From the *Configuration Manager* screen:

>Protocols >IP >BGP >Peers
Scroll down the IP interface list and select **10.32.50.1, E32**
Select **BGP Peers**
Select **Add**

Peer Address	**10.22.50.1**
Peer AS	**65020**
Select	**OK**

Select **Add**

Peer Address	**10.42.50.1**
Peer AS	**65040**
Select	**OK**

Select **Add**

Peer Address	**10.52.50.1**
Peer AS	**65050**
Select	**OK**

Select **Add**

Peer Address	**10.62.50.1**
Peer AS	**65060**
Select	**OK**

Select **Add**

Peer Address	**10.72.50.1**
Peer AS	**65070**
Select	**OK**

Select **Add**

Peer Address	**10.82.50.1**
Peer AS	**65080**
Select	**OK**

Select **Add**

Peer Address	**10.92.50.1**
Peer AS	**65090**
Select	**OK**

Select **Done** until returned to the *Configuration Manager* screen.

Specify BGP Accept Policies

>Protocol >IP >Policy Filters >BGP-4 >Accept Policies
Select **ADD**

Name ***Local*-VPN-Accept-List** (*Local* refers to local site name)

Action	**Accept**
Networks	Select **List**

From the Networks Policy Filter List screen, enter each of the 24 remote subnets as follows:

Network Number	Network Mask	Exact / Range
10.10.0.0	**255.255.0.0**	**Exact**
10.11.0.0	**255.255.0.0**	**Exact**
10.12.0.0	**255.255.0.0**	**Exact**
10.20.0.0	**255.255.0.0**	**Exact**
10.21.0.0	**255.255.0.0**	**Exact**
10.22.0.0	**255.255.0.0**	**Exact**
10.40.0.0	**255.255.0.0**	**Exact**
10.41.0.0	**255.255.0.0**	**Exact**
10.42.0.0	**255.255.0.0**	**Exact**
10.50.0.0	**255.255.0.0**	**Exact**
10.51.0.0	**255.255.0.0**	**Exact**
10.52.0.0	**255.255.0.0**	**Exact**
10.60.0.0	**255.255.0.0**	**Exact**
10.61.0.0	**255.255.0.0**	**Exact**
10.62.0.0	**255.255.0.0**	**Exact**
10.70.0.0	**255.255.0.0**	**Exact**
10.71.0.0	**255.255.0.0**	**Exact**
10.72.0.0	**255.255.0.0**	**Exact**
10.80.0.0	**255.255.0.0**	**Exact**
10.81.0.0	**255.255.0.0**	**Exact**
10.82.0.0	**255.255.0.0**	**Exact**
10.90.0.0	**255.255.0.0**	**Exact**
10.91.0.0	**255.255.0.0**	**Exact**
10.92.0.0	**255.255.0.0**	**Exact**

Select **OK**
Select **Done**

Specify BGP Announce Policies

>Protocol >IP >Policy Filters >BGP-4 >Announce Policies

Select **ADD**

Name **_Local_-VPN-Announce-List** (*Local* refers to local site name)
Action **Announce**
Route Source Select **Values**
Direct only, deselect all other sources.

Networks Select **List**

From the Networks Policy Filter List screen, enter each of the local (Direct) subnets as follows:

Network Number	Network Mask	Exact / Range
10.30.0.0	**255.255.0.0**	**Exact**
10.31.0.0	**255.255.0.0**	**Exact**

10.32.0.0	**255.255.0.0**	**Exact**

Advertise Select **List**

From the Networks Policy Filter List screen, enter each of the local (Direct) subnets as follows:

Network Number	Network Mask
10.30.0.0	**255.255.0.0**
10.31.0.0	**255.255.0.0**
10.32.0.0	**255.255.0.0**

Add Static routes for BGP Peers

From the *Configuration Manager* screen:

>Protocols >IP >Static Routes

Select **ADD**

Destination IP Address	**10.12.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.32.130.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.22.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.32.130.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.42.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.32.130.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.52.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.32.130.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.62.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.32.130.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.72.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.32.130.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.82.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.32.130.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.92.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.32.130.1**
Preference	**16**

Select **OK**

Select **Done**

Save the configuration file. Close the configuration manager session.

9.4 San Francisco

Open the local San Francisco configuration file in Site Manager. Immediately save the file as a new name (eg. *sfo-bgp-new.cfg*). Make the specified changes.

Enable Subnet Zero and Default Routes

From the *Configuration Manger* screen:
>Protocols >IP >Global
Subnet Zero **Enable**
Enable Default Route for Subnets **Enable**

Add BGP Protocol

From the *Configuration Manger* screen:
>Circuits >Edit
Select circuit **E32**
Select **Edit**
The Circuit Definition screen for E32 will be displayed.
>Protocols >Add/Delete
Select **IP**
RIP
BGP
BOOTP (if required)
Select **OK**

Enter the following on the BGP Configuration screen:

Identifier	**10.42.50.1**
Local AS	**65040**

Select **OK**
On the BGP Peer Screen, enter the following:

Peer Address	**10.12.50.1**
Peer AS	**65010**
Local Address	**10.42.50.1**
Select	**OK**

Select **OK** when asked to enable Multi-hop EBGP.

Press **F10** to exit current screen
Select **DONE** to return to Configuration Manager screen.

Add BGP Peers

From the *Configuration Manager* screen:

>Protocols >IP >BGP >Peers
Scroll down the IP interface list and select **10.42.50.1, E32**
Select **BGP Peers**
Select **Add**

Peer Address	**10.22.50.1**
Peer AS	**65020**
Select	**OK**

Select **Add**

Peer Address	**10.32.50.1**
Peer AS	**65030**
Select	**OK**

Select **Add**

Peer Address	**10.52.50.1**
Peer AS	**65050**
Select	**OK**

Select **Add**

Peer Address	**10.62.50.1**
Peer AS	**65060**
Select	**OK**

Select **Add**

Peer Address	**10.72.50.1**
Peer AS	**65070**
Select	**OK**

Select **Add**

Peer Address	**10.82.50.1**
Peer AS	**65080**
Select	**OK**

Select **Add**

Peer Address	**10.92.50.1**
Peer AS	**65090**
Select	**OK**

Select **Done** until returned to the *Configuration Manager* screen.

Specify BGP Accept Policies

>Protocol >IP >Policy Filters >BGP-4 >Accept Policies
Select **ADD**

Name	***Local*-VPN-Accept-List**	(*Local* refers to local site name)

Action	**Accept**
Networks	Select **List**

From the Networks Policy Filter List screen, enter each of the 24 remote subnets as follows:

Network Number	Network Mask	Exact / Range
10.10.0.0	**255.255.0.0**	**Exact**
10.11.0.0	**255.255.0.0**	**Exact**
10.12.0.0	**255.255.0.0**	**Exact**
10.20.0.0	**255.255.0.0**	**Exact**
10.21.0.0	**255.255.0.0**	**Exact**
10.22.0.0	**255.255.0.0**	**Exact**
10.30.0.0	**255.255.0.0**	**Exact**
10.31.0.0	**255.255.0.0**	**Exact**
10.32.0.0	**255.255.0.0**	**Exact**
10.50.0.0	**255.255.0.0**	**Exact**
10.51.0.0	**255.255.0.0**	**Exact**
10.52.0.0	**255.255.0.0**	**Exact**
10.60.0.0	**255.255.0.0**	**Exact**
10.61.0.0	**255.255.0.0**	**Exact**
10.62.0.0	**255.255.0.0**	**Exact**
10.70.0.0	**255.255.0.0**	**Exact**
10.71.0.0	**255.255.0.0**	**Exact**
10.72.0.0	**255.255.0.0**	**Exact**
10.80.0.0	**255.255.0.0**	**Exact**
10.81.0.0	**255.255.0.0**	**Exact**
10.82.0.0	**255.255.0.0**	**Exact**
10.90.0.0	**255.255.0.0**	**Exact**
10.91.0.0	**255.255.0.0**	**Exact**
10.92.0.0	**255.255.0.0**	**Exact**

Select **OK**
Select **Done**

Specify BGP Announce Policies

>Protocol >IP >Policy Filters >BGP-4 >Announce Policies
Select **ADD**

Name	***Local*-VPN-Announce-List** (*Local* refers to local site name)	
Action	**Announce**	
Route Source		Select **Values** **Direct** only, deselect all other sources.

Networks	Select **List**

From the Networks Policy Filter List screen, enter each of the local (Direct) subnets as follows:

Network Number	Network Mask	Exact / Range
10.40.0.0	**255.255.0.0**	**Exact**
10.41.0.0	**255.255.0.0**	**Exact**

10.42.0.0	**255.255.0.0**	**Exact**

Advertise Select **List**
From the Networks Policy Filter List screen, enter each of the local (Direct) subnets as follows:

Network Number	Network Mask
10.40.0.0	**255.255.0.0**
10.41.0.0	**255.255.0.0**
10.42.0.0	**255.255.0.0**

Add Static routes for BGP Peers

From the *Configuration Manager* screen:
>Protocols >IP >Static Routes
Select **ADD**

Destination IP Address	**10.12.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.42.140.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.22.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.42.140.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.32.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.42.140.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.52.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.42.140.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.62.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.42.140.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.72.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.42.140.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.82.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.42.140.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.92.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.42.140.1**
Preference	**16**

Select **OK**

Select **Done**

Save the configuration file. Close the configuration manager session.

9.5 Los Angeles

Open the local Los Angeles configuration file in Site Manager. Immediately save the file as a new name (eg. *lax-bgp-new.cfg*). Make the specified changes.

Enable Subnet Zero and Default Routes

From the *Configuration Manger* screen:
>Protocols >IP >Global
Subnet Zero **Enable**
Enable Default Route for Subnets **Enable**

Add BGP Protocol

From the *Configuration Manger* screen:
>Circuits >Edit
Select circuit **E32**
Select **Edit**
The Circuit Definition screen for E32 will be displayed.
>Protocols >Add/Delete
Select **IP**
RIP
BGP
BOOTP (if required)
Select **OK**

Enter the following on the BGP Configuration screen:

Identifier	**10.52.50.1**
Local AS	**65050**

Select **OK**
On the BGP Peer Screen, enter the following:

Peer Address	**10.12.50.1**
Peer AS	**65010**
Local Address	**10.52.50.1**
Select	**OK**

Select **OK** when asked to enable Multi-hop EBGP.

Press **F10** to exit current screen
Select **DONE** to return to Configuration Manager screen.

Add BGP Peers

From the *Configuration Manager* screen:

>Protocols >IP >BGP >Peers
Scroll down the IP interface list and select **10.52.50.1, E32**
Select **BGP Peers**
Select **Add**

Peer Address **10.22.50.1**
Peer AS **65020**
Select **OK**

Select **Add**

Peer Address **10.32.50.1**
Peer AS **65030**
Select **OK**

Select **Add**

Peer Address **10.42.50.1**
Peer AS **65040**
Select **OK**

Select **Add**

Peer Address **10.62.50.1**
Peer AS **65060**
Select **OK**

Select **Add**

Peer Address **10.72.50.1**
Peer AS **65070**
Select **OK**

Select **Add**

Peer Address **10.82.50.1**
Peer AS **65080**
Select **OK**

Select **Add**

Peer Address **10.92.50.1**
Peer AS **65090**
Select **OK**

Select **Done** until returned to the *Configuration Manager* screen.

Specify BGP Accept Policies

>Protocol >IP >Policy Filters >BGP-4 >Accept Policies
Select **ADD**

Name ***Local*-VPN-Accept-List** (*Local* refers to local site name)

Action	**Accept**
Networks	Select **List**

From the Networks Policy Filter List screen, enter each of the 24 remote subnets as follows:

Network Number	Network Mask	Exact / Range
10.10.0.0	**255.255.0.0**	**Exact**
10.11.0.0	**255.255.0.0**	**Exact**
10.12.0.0	**255.255.0.0**	**Exact**
10.20.0.0	**255.255.0.0**	**Exact**
10.21.0.0	**255.255.0.0**	**Exact**
10.22.0.0	**255.255.0.0**	**Exact**
10.30.0.0	**255.255.0.0**	**Exact**
10.31.0.0	**255.255.0.0**	**Exact**
10.32.0.0	**255.255.0.0**	**Exact**
10.40.0.0	**255.255.0.0**	**Exact**
10.41.0.0	**255.255.0.0**	**Exact**
10.42.0.0	**255.255.0.0**	**Exact**
10.60.0.0	**255.255.0.0**	**Exact**
10.61.0.0	**255.255.0.0**	**Exact**
10.62.0.0	**255.255.0.0**	**Exact**
10.70.0.0	**255.255.0.0**	**Exact**
10.71.0.0	**255.255.0.0**	**Exact**
10.72.0.0	**255.255.0.0**	**Exact**
10.80.0.0	**255.255.0.0**	**Exact**
10.81.0.0	**255.255.0.0**	**Exact**
10.82.0.0	**255.255.0.0**	**Exact**
10.90.0.0	**255.255.0.0**	**Exact**
10.91.0.0	**255.255.0.0**	**Exact**
10.92.0.0	**255.255.0.0**	**Exact**

Select **OK**
Select **Done**

Specify BGP Announce Policies

>Protocol >IP >Policy Filters >BGP-4 >Announce Policies

Select **ADD**

Name	***Local*-VPN-Announce-List** (*Local* refers to local site name)	
Action	**Announce**	
Route Source		Select **Values** **Direct** only, deselect all other sources.

Networks	Select **List**

From the Networks Policy Filter List screen, enter each of the local (Direct) subnets as follows:

Network Number	Network Mask	Exact / Range
10.50.0.0	**255.255.0.0**	**Exact**
10.51.0.0	**255.255.0.0**	**Exact**

10.52.0.0	**255.255.0.0**	**Exact**

Advertise Select **List**

From the Networks Policy Filter List screen, enter each of the local (Direct) subnets as follows:

Network Number	Network Mask
10.50.0.0	**255.255.0.0**
10.51.0.0	**255.255.0.0**
10.52.0.0	**255.255.0.0**

Add Static routes for BGP Peers

From the *Configuration Manager* screen:

>Protocols >IP >Static Routes

Select **ADD**

Destination IP Address	**10.12.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.52.150.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.22.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.52.150.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.32.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.52.150.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.42.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.52.150.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.62.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.52.150.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.72.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.52.150.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.82.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.52.150.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.92.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.52.150.1**
Preference	**16**

Select **OK**

Select **Done**

Save the configuration file. Close the configuration manager session.

9.6 St. Louis

Open the local St. Louis configuration file in Site Manager. Immediately save the file as a new name (eg. *stl-bgp-new.cfg*). Make the specified changes.

Enable Subnet Zero and Default Routes

From the *Configuration Manger* screen:
>Protocols >IP >Global
Subnet Zero **Enable**
Enable Default Route for Subnets **Enable**

Add BGP Protocol

From the *Configuration Manger* screen:
>Circuits >Edit
Select circuit **E32**
Select **Edit**
The Circuit Definition screen for E32 will be displayed.
>Protocols >Add/Delete
Select **IP**
RIP
BGP
BOOTP (if required)
Select **OK**

Enter the following on the BGP Configuration screen:

Identifier	**10.62.50.1**
Local AS	**65060**

Select **OK**
On the BGP Peer Screen, enter the following:

Peer Address	**10.12.50.1**
Peer AS	**65010**
Local Address	**10.62.50.1**
Select	**OK**

Select **OK** when asked to enable Multi-hop EBGP.

Press **F10** to exit current screen
Select **DONE** to return to Configuration Manager screen.

Add BGP Peers

From the *Configuration Manager* screen:

>Protocols >IP >BGP >Peers

Scroll down the IP interface list and select **10.62.50.1, E32**

Select **BGP Peers**

Select **Add**

Peer Address **10.22.50.1**
Peer AS **65020**
Select **OK**

Select **Add**

Peer Address **10.32.50.1**
Peer AS **65030**
Select **OK**

Select **Add**

Peer Address **10.42.50.1**
Peer AS **65040**
Select **OK**

Select **Add**

Peer Address **10.52.50.1**
Peer AS **65050**
Select **OK**

Select **Add**

Peer Address **10.72.50.1**
Peer AS **65070**
Select **OK**

Select **Add**

Peer Address **10.82.50.1**
Peer AS **65080**
Select **OK**

Select **Add**

Peer Address **10.92.50.1**
Peer AS **65090**
Select **OK**

Select **Done** until returned to the *Configuration Manager* screen.

Specify BGP Accept Policies

>Protocol >IP >Policy Filters >BGP-4 >Accept Policies

Select **ADD**

Name ***Local*-VPN-Accept-List** (*Local* refers to local site name)

Action	**Accept**
Networks	Select **List**

From the Networks Policy Filter List screen, enter each of the 24 remote subnets as follows:

Network Number	Network Mask	Exact / Range
10.10.0.0	**255.255.0.0**	**Exact**
10.11.0.0	**255.255.0.0**	**Exact**
10.12.0.0	**255.255.0.0**	**Exact**
10.20.0.0	**255.255.0.0**	**Exact**
10.21.0.0	**255.255.0.0**	**Exact**
10.22.0.0	**255.255.0.0**	**Exact**
10.30.0.0	**255.255.0.0**	**Exact**
10.31.0.0	**255.255.0.0**	**Exact**
10.32.0.0	**255.255.0.0**	**Exact**
10.40.0.0	**255.255.0.0**	**Exact**
10.41.0.0	**255.255.0.0**	**Exact**
10.42.0.0	**255.255.0.0**	**Exact**
10.50.0.0	**255.255.0.0**	**Exact**
10.51.0.0	**255.255.0.0**	**Exact**
10.52.0.0	**255.255.0.0**	**Exact**
10.70.0.0	**255.255.0.0**	**Exact**
10.71.0.0	**255.255.0.0**	**Exact**
10.72.0.0	**255.255.0.0**	**Exact**
10.80.0.0	**255.255.0.0**	**Exact**
10.81.0.0	**255.255.0.0**	**Exact**
10.82.0.0	**255.255.0.0**	**Exact**
10.90.0.0	**255.255.0.0**	**Exact**
10.91.0.0	**255.255.0.0**	**Exact**
10.92.0.0	**255.255.0.0**	**Exact**

Select **OK**
Select **Done**

Specify BGP Announce Policies

>Protocol >IP >Policy Filters >BGP-4 >Announce Policies
Select **ADD**

Name	***Local*-VPN-Announce-List** (*Local* refers to local site name)	
Action	**Announce**	
Route Source		Select **Values** **Direct** only, deselect all other sources.

Networks	Select **List**

From the Networks Policy Filter List screen, enter each of the local (Direct) subnets as follows:

Network Number	Network Mask	Exact / Range
10.60.0.0	**255.255.0.0**	**Exact**
10.61.0.0	**255.255.0.0**	**Exact**

10.62.0.0	**255.255.0.0**	**Exact**

Advertise Select **List**

From the Networks Policy Filter List screen, enter each of the local (Direct) subnets as follows:

Network Number	Network Mask
10.60.0.0	**255.255.0.0**
10.61.0.0	**255.255.0.0**
10.62.0.0	**255.255.0.0**

Add Static routes for BGP Peers

From the *Configuration Manager* screen:

>Protocols >IP >Static Routes

Select **ADD**

Destination IP Address	**10.12.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.62.160.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.22.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.62.160.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.32.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.62.160.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.42.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.62.160.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.52.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.62.160.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.72.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.62.160.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.82.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.62.160.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.92.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.62.160.1**
Preference	**16**

Select **OK**

Select **Done**

Save the configuration file. Close the configuration manager session.

9.7 Kansas City

Open the local Kansas City configuration file in Site Manager. Immediately save the file as a new name (eg. *kcm-bgp-new.cfg*). Make the specified changes.

Enable Subnet Zero and Default Routes

From the *Configuration Manger* screen:
>Protocols >IP >Global
Subnet Zero **Enable**
Enable Default Route for Subnets **Enable**

Add BGP Protocol

From the *Configuration Manger* screen:
>Circuits >Edit
Select circuit **E32**
Select **Edit**
The Circuit Definition screen for E32 will be displayed.
>Protocols >Add/Delete
Select **IP**
RIP
BGP
BOOTP (if required)
Select **OK**

Enter the following on the BGP Configuration screen:

Identifier	**10.72.50.1**
Local AS	**65070**

Select **OK**
On the BGP Peer Screen, enter the following:

Peer Address	**10.12.50.1**
Peer AS	**65010**
Local Address	**10.72.50.1**
Select	**OK**

Select **OK** when asked to enable Multi-hop EBGP.

Press **F10** to exit current screen
Select **DONE** to return to Configuration Manager screen.

Add BGP Peers

From the *Configuration Manager* screen:

>Protocols >IP >BGP >Peers
Scroll down the IP interface list and select **10.72.50.1, E32**
Select **BGP Peers**
Select **Add**
    Peer Address **10.22.50.1**
    Peer AS **65020**
    Select **OK**

Select **Add**
    Peer Address **10.32.50.1**
    Peer AS **65030**
    Select **OK**

Select **Add**
    Peer Address **10.42.50.1**
    Peer AS **65040**
    Select **OK**

Select **Add**
    Peer Address **10.52.50.1**
    Peer AS **65050**
    Select **OK**

Select **Add**
    Peer Address **10.62.50.1**
    Peer AS **65060**
    Select **OK**

Select **Add**
    Peer Address **10.82.50.1**
    Peer AS **65080**
    Select **OK**

Select **Add**
    Peer Address **10.92.50.1**
    Peer AS **65090**
    Select **OK**

Select **Done** until returned to the *Configuration Manager* screen.

Specify BGP Accept Policies

>Protocol >IP >Policy Filters >BGP-4 >Accept Policies
Select **ADD**
    Name **_Local_-VPN-Accept-List** (*Local* refers to local site name)

Action	**Accept**
Networks	Select **List**

From the Networks Policy Filter List screen, enter each of the 24 remote subnets as follows:

Network Number	Network Mask	Exact / Range
10.10.0.0	**255.255.0.0**	**Exact**
10.11.0.0	**255.255.0.0**	**Exact**
10.12.0.0	**255.255.0.0**	**Exact**
10.20.0.0	**255.255.0.0**	**Exact**
10.21.0.0	**255.255.0.0**	**Exact**
10.22.0.0	**255.255.0.0**	**Exact**
10.30.0.0	**255.255.0.0**	**Exact**
10.31.0.0	**255.255.0.0**	**Exact**
10.32.0.0	**255.255.0.0**	**Exact**
10.40.0.0	**255.255.0.0**	**Exact**
10.41.0.0	**255.255.0.0**	**Exact**
10.42.0.0	**255.255.0.0**	**Exact**
10.50.0.0	**255.255.0.0**	**Exact**
10.51.0.0	**255.255.0.0**	**Exact**
10.52.0.0	**255.255.0.0**	**Exact**
10.60.0.0	**255.255.0.0**	**Exact**
10.61.0.0	**255.255.0.0**	**Exact**
10.62.0.0	**255.255.0.0**	**Exact**
10.80.0.0	**255.255.0.0**	**Exact**
10.81.0.0	**255.255.0.0**	**Exact**
10.82.0.0	**255.255.0.0**	**Exact**
10.90.0.0	**255.255.0.0**	**Exact**
10.91.0.0	**255.255.0.0**	**Exact**
10.92.0.0	**255.255.0.0**	**Exact**

Select **OK**
Select **Done**

Specify BGP Announce Policies

>Protocol >IP >Policy Filters >BGP-4 >Announce Policies
Select **ADD**

Name	***Local*-VPN-Announce-List** (*Local* refers to local site name)
Action	**Announce**
Route Source	Select **Values** **Direct** only, deselect all other sources.
Networks	Select **List**

From the Networks Policy Filter List screen, enter each of the local (Direct) subnets as follows:

Network Number	Network Mask	Exact / Range
10.70.0.0	**255.255.0.0**	**Exact**
10.71.0.0	**255.255.0.0**	**Exact**

10.72.0.0	**255.255.0.0**	**Exact**

Advertise Select **List**

From the Networks Policy Filter List screen, enter each of the local (Direct) subnets as follows:

Network Number	Network Mask
10.70.0.0	**255.255.0.0**
10.71.0.0	**255.255.0.0**
10.72.0.0	**255.255.0.0**

Add Static routes for BGP Peers

From the *Configuration Manager* screen:

>Protocols >IP >Static Routes

Select **ADD**

Destination IP Address	**10.12.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.72.170.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.22.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.72.170.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.32.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.72.170.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.42.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.72.170.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.52.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.72.170.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.62.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.72.170.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.82.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.72.170.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.92.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.72.170.1**
Preference	**16**

Select **OK**

Select **Done**

Save the configuration file. Close the configuration manager session.

9.8 Palm Beach

Open the local Palm Beach configuration file in Site Manager. Immediately save the file as a new name (eg. *wpb-bgp-new.cfg*). Make the specified changes.

Enable Subnet Zero and Default Routes

From the *Configuration Manger* screen:
>Protocols >IP >Global
Subnet Zero **Enable**
Enable Default Route for Subnets **Enable**

Add BGP Protocol

From the *Configuration Manger* screen:
>Circuits >Edit
Select circuit **E32**
Select **Edit**
The Circuit Definition screen for E32 will be displayed.
>Protocols >Add/Delete
Select **IP**
RIP
BGP
BOOTP (if required)
Select **OK**

Enter the following on the BGP Configuration screen:

Identifier	**10.82.50.1**
Local AS	**65080**

Select **OK**
On the BGP Peer Screen, enter the following:

Peer Address	**10.12.50.1**
Peer AS	**65010**
Local Address	**10.82.50.1**
Select	**OK**

Select **OK** when asked to enable Multi-hop EBGP.

Press **F10** to exit current screen
Select **DONE** to return to Configuration Manager screen.

Add BGP Peers

From the *Configuration Manager* screen:

>Protocols >IP >BGP >Peers
Scroll down the IP interface list and select **10.82.50.1, E32**
Select **BGP Peers**
Select **Add**

Peer Address **10.22.50.1**
Peer AS **65020**
Select **OK**

Select **Add**

Peer Address **10.32.50.1**
Peer AS **65030**
Select **OK**

Select **Add**

Peer Address **10.42.50.1**
Peer AS **65040**
Select **OK**

Select **Add**

Peer Address **10.52.50.1**
Peer AS **65050**
Select **OK**

Select **Add**

Peer Address **10.62.50.1**
Peer AS **65060**
Select **OK**

Select **Add**

Peer Address **10.72.50.1**
Peer AS **65070**
Select **OK**

Select **Add**

Peer Address **10.92.50.1**
Peer AS **65090**
Select **OK**

Select **Done** until returned to the *Configuration Manager* screen.

Specify BGP Accept Policies

>Protocol >IP >Policy Filters >BGP-4 >Accept Policies
Select **ADD**

Name ***Local*-VPN-Accept-List** (*Local* refers to local site name)

Action	**Accept**
Networks	Select **List**

From the Networks Policy Filter List screen, enter each of the 24 remote subnets as follows:

Network Number	Network Mask	Exact / Range
10.10.0.0	**255.255.0.0**	**Exact**
10.11.0.0	**255.255.0.0**	**Exact**
10.12.0.0	**255.255.0.0**	**Exact**
10.20.0.0	**255.255.0.0**	**Exact**
10.21.0.0	**255.255.0.0**	**Exact**
10.22.0.0	**255.255.0.0**	**Exact**
10.30.0.0	**255.255.0.0**	**Exact**
10.31.0.0	**255.255.0.0**	**Exact**
10.32.0.0	**255.255.0.0**	**Exact**
10.40.0.0	**255.255.0.0**	**Exact**
10.41.0.0	**255.255.0.0**	**Exact**
10.42.0.0	**255.255.0.0**	**Exact**
10.50.0.0	**255.255.0.0**	**Exact**
10.51.0.0	**255.255.0.0**	**Exact**
10.52.0.0	**255.255.0.0**	**Exact**
10.60.0.0	**255.255.0.0**	**Exact**
10.61.0.0	**255.255.0.0**	**Exact**
10.62.0.0	**255.255.0.0**	**Exact**
10.70.0.0	**255.255.0.0**	**Exact**
10.71.0.0	**255.255.0.0**	**Exact**
10.72.0.0	**255.255.0.0**	**Exact**
10.90.0.0	**255.255.0.0**	**Exact**
10.91.0.0	**255.255.0.0**	**Exact**
10.92.0.0	**255.255.0.0**	**Exact**

Select **OK**
Select **Done**

Specify BGP Announce Policies

>Protocol >IP >Policy Filters >BGP-4 >Announce Policies
Select **ADD**

Name	***Local*-VPN-Announce-List**	(*Local* refers to local site name)
Action	**Announce**	
Route Source		Select **Values** **Direct** only, deselect all other sources.

Networks	Select **List**

From the Networks Policy Filter List screen, enter each of the local (Direct) subnets as follows:

Network Number	Network Mask	Exact / Range
10.80.0.0	**255.255.0.0**	**Exact**
10.81.0.0	**255.255.0.0**	**Exact**

10.82.0.0	**255.255.0.0**	**Exact**

Advertise Select **List**

From the Networks Policy Filter List screen, enter each of the local (Direct) subnets as follows:

Network Number	Network Mask
10.80.0.0	**255.255.0.0**
10.81.0.0	**255.255.0.0**
10.82.0.0	**255.255.0.0**

Add Static routes for BGP Peers

From the *Configuration Manager* screen:

>Protocols >IP >Static Routes

Select **ADD**

Destination IP Address	**10.12.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.82.180.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.22.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.82.180.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.32.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.82.180.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.42.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.82.180.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.52.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.82.180.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.62.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.82.180.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.72.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.82.180.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.92.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.82.180.1**
Preference	**16**

Select **OK**

Select **Done**

Save the configuration file. Close the configuration manager session.

9.9 Minneapolis

Open the local Minneapolis configuration file in Site Manager. Immediately save the file as a new name (eg. *msp-bgp-new.cfg*). Make the specified changes.

Enable Subnet Zero and Default Routes

From the *Configuration Manger* screen:

>Protocols >IP >Global

Subnet Zero **Enable**

Enable Default Route for Subnets **Enable**

Add BGP Protocol

From the *Configuration Manger* screen:

>Circuits >Edit

Select circuit **E32**

Select **Edit**

The Circuit Definition screen for E32 will be displayed.

>Protocols >Add/Delete

Select **IP**

RIP

BGP

BOOTP (if required)

Select **OK**

Enter the following on the BGP Configuration screen:

Identifier	**10.92.50.1**
Local AS	**65090**

Select **OK**

On the BGP Peer Screen, enter the following:

Peer Address	**10.12.50.1**
Peer AS	**65010**
Local Address	**10.92.50.1**
Select	**OK**

Select **OK** when asked to enable Multi-hop EBGP.

Press **F10** to exit current screen

Select **DONE** to return to Configuration Manager screen.

Add BGP Peers

From the *Configuration Manager* screen:

>Protocols >IP >BGP >Peers
Scroll down the IP interface list and select **10.92.50.1, E32**
Select **BGP Peers**
Select **Add**
Peer Address **10.22.50.1**
Peer AS **65020**
Select **OK**

Select **Add**
Peer Address **10.32.50.1**
Peer AS **65030**
Select **OK**

Select **Add**
Peer Address **10.42.50.1**
Peer AS **65040**
Select **OK**

Select **Add**
Peer Address **10.52.50.1**
Peer AS **65050**
Select **OK**

Select **Add**
Peer Address **10.62.50.1**
Peer AS **65060**
Select **OK**

Select **Add**
Peer Address **10.72.50.1**
Peer AS **65070**
Select **OK**

Select **Add**
Peer Address **10.82.50.1**
Peer AS **65080**
Select **OK**

Select **Done** until returned to the *Configuration Manager* screen.

Specify BGP Accept Policies

>Protocol >IP >Policy Filters >BGP-4 >Accept Policies
Select **ADD**
Name ***Local*-VPN-Accept-List** (*Local* refers to local site name)

Action	**Accept**
Networks	Select **List**

From the Networks Policy Filter List screen, enter each of the 24 remote subnets as follows:

Network Number	Network Mask	Exact / Range
10.10.0.0	**255.255.0.0**	**Exact**
10.11.0.0	**255.255.0.0**	**Exact**
10.12.0.0	**255.255.0.0**	**Exact**
10.20.0.0	**255.255.0.0**	**Exact**
10.21.0.0	**255.255.0.0**	**Exact**
10.22.0.0	**255.255.0.0**	**Exact**
10.30.0.0	**255.255.0.0**	**Exact**
10.31.0.0	**255.255.0.0**	**Exact**
10.32.0.0	**255.255.0.0**	**Exact**
10.40.0.0	**255.255.0.0**	**Exact**
10.41.0.0	**255.255.0.0**	**Exact**
10.42.0.0	**255.255.0.0**	**Exact**
10.50.0.0	**255.255.0.0**	**Exact**
10.51.0.0	**255.255.0.0**	**Exact**
10.52.0.0	**255.255.0.0**	**Exact**
10.60.0.0	**255.255.0.0**	**Exact**
10.61.0.0	**255.255.0.0**	**Exact**
10.62.0.0	**255.255.0.0**	**Exact**
10.70.0.0	**255.255.0.0**	**Exact**
10.71.0.0	**255.255.0.0**	**Exact**
10.72.0.0	**255.255.0.0**	**Exact**
10.80.0.0	**255.255.0.0**	**Exact**
10.81.0.0	**255.255.0.0**	**Exact**
10.82.0.0	**255.255.0.0**	**Exact**

Select **OK**
Select **Done**

Specify BGP Announce Policies

>Protocol >IP >Policy Filters >BGP-4 >Announce Policies
Select **ADD**

Name	***Local*-VPN-Announce-List**	(*Local* refers to local site name)
Action	**Announce**	
Route Source	Select **Values** **Direct** only, deselect all other sources.	

Networks Select **List**

From the Networks Policy Filter List screen, enter each of the local (Direct) subnets as follows:

Network Number	Network Mask	Exact / Range
10.90.0.0	**255.255.0.0**	**Exact**
10.91.0.0	**255.255.0.0**	**Exact**

10.92.0.0	**255.255.0.0**	**Exact**

Advertise Select **List**
From the Networks Policy Filter List screen, enter each of the local (Direct) subnets as follows:

Network Number	Network Mask
10.90.0.0	**255.255.0.0**
10.91.0.0	**255.255.0.0**
10.92.0.0	**255.255.0.0**

Add Static routes for BGP Peers

From the *Configuration Manager* screen:
>Protocols >IP >Static Routes
Select **ADD**

Destination IP Address	**10.12.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.92.190.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.22.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.92.190.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.32.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.92.190.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.42.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.92.190.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.52.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.92.190.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.62.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.92.190.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.72.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.92.190.1**
Preference	**16**

Select **OK**

Select **ADD**

Destination IP Address	**10.82.50.1**
Address Mask	**255.255.255.255**
Cost	**1**
Next Hop Address	**10.92.190.1**
Preference	**16**

Select **OK**

Select **Done**

Save the configuration file. Close the configuration manager session.