**Connecting Via Console Cable**

Connect the serial console port on the device to the Male DB-9 Serial Port of a PC using a straight through cable. The serial communications is 9600 Baud, 8 bits, parity none, 1 stop bit, and no flow control.

**Using the Command Line Interface**

There are three modes: non-privileged, privileged, and configuration. In order to execute commands to configure, reload, upgrade, etc, you must be in privilege mode. For help at any time, press <tab> or <?>. Commands may be abbreviated to the extent that no other command is recognized by the abbreviated command. To remove a configuration statement, use “no” in front of it. There is a start-up configuration and a running configuration. To commit changes so they are not lost during power failure or a reload, issue “write memory”. To view the start-up configuration, type “show configuration”. To view the running configuration, type “show run”.

**CLI Navigation Example:**

```
FCX> enable
Password: *********
FCX# configure terminal
FCX(config)# hostname MySwitch
FCX(config)# exit
FCX#wr m
```

**Setting IP Address & default gateway on a switch**

**Notes:** This is for a device running switch code. For devices in Layer-3 mode, refer to “Configuring Router Interfaces” or “Configuring Virtual Router Interfaces” to assign an IP. To assign a default-gateway on a router, use “ip route 0.0.0.0/0 <IP address of Default Gateway>”

**Troubleshooting:** show ip

**Configuration Example:**

```
ip address 192.168.10.2/24
ip default-gateway 192.168.10.1
```

**Setting Passwords**

**Notes:** By default, a device has no passwords assigned and will allow access.

**Configuration Example:**

```
enable
enable telnet password <password>
enable super-user <password>
```

**Password Recovery**

**Prerequisites:** Must have physical access to the switch and console port

**Notes:** Press `b` within 3-seCONDS of power cycling the switch to enter the boot prompt. This removes passwords in the running configuration, so be sure to set passwords. Alternatively, you can reset the configuration to factory defaults by replacing the command “no password” with “use default”. This only effects the running configuration, so be sure to “write mem” or “erase start” once you’re into the CLI. On dual management module chassis, you must pull out the second management module.

**Example:**

```
! Upgrade the boot and monitor images on the management
! and line cards (Only do this if the release specifies an upgraded version)
copy tftp flash 192.168.1.1 xppm03500.bin boot
! Upgrade FPGA’s on line processors (1G & 10G)
copy tftp flash 192.168.1.1 xppm03500.bin boot all
! Upgrade the boot and monitor images on the management
! and line processors (must be release 3.5 or greater)
copy tftp flash 192.168.1.1 xm03600d.bin
! Upgrade mbridge on management modules:
copy tftp mbridge 192.168.1.1 mbridge_03600d.vxs
! Upgrade FPGA’s on line processors (1G & 10G)
copy tftp flash 192.168.1.1 xppm03500.bin boot-pbl all
! If on release 4.0 or greater, you can upgrade all FPGA’s
! on the line processors at once with this command
copy tftp flash 192.168.1.1 lpfpga04000.bin fpga-all all
```

**Upgrading Software**

**Prerequisites:** Refer to the release notes for specific upgrade procedures and requirements

**Notes:** For most devices, there is boot code, monitor code, and a running image. You can store two versions on the device at a time unless both images are 7.2.02 router code or greater on devices with only 8MB flashs.

**Troubleshooting:** show flash

**Typical File names:**

<table>
<thead>
<tr>
<th>Letter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FEB</td>
<td>Boot</td>
</tr>
<tr>
<td>FEM</td>
<td>Monitor</td>
</tr>
<tr>
<td>FES</td>
<td>Switch</td>
</tr>
<tr>
<td>FEL</td>
<td>Base Layer-3</td>
</tr>
<tr>
<td>FER</td>
<td>Full Layer-3</td>
</tr>
<tr>
<td>FES</td>
<td>Switch</td>
</tr>
<tr>
<td>FEM</td>
<td>Monitor</td>
</tr>
<tr>
<td>FEB</td>
<td>Boot</td>
</tr>
</tbody>
</table>

**Example:**

```
copy tftp flash 192.168.10.2 fes04000.bin pri | sec | boot | monitor
```

**Backing up the Configuration**

**Prerequisites:** A TFTP server or Secure Copy program and SSH enabled on the the device
Securing Remote Access with ACL’s

Notes: Creating a standard ACL for use in restricting access. Standard access list are numbered from 1 to 99. Items are grouped by number and executed in order. At the end of each access-list is an explicit “deny ip any”. These ACL numbers are used for restricting access to SSH, Telnet, Web, SNMP, etc.

Troubleshooting: show access-list

Configuration Example:

```
access-list 10 remark MGMT ACCESS
access-list 10 permit host 192.168.10.24
access-list 10 deny host 192.168.20.5
access-list 10 permit 192.168.20.0/24
```

Enabling Secure Shell Access (SSH)

Prerequisites: Standard ACL created (optional)

Notes: Requires username/passwords to be created.

Configuration Example:

```
crypto key generate
user <username> privi 0 password <password>
aaa authentication login default local
ssh access-group 10
ip ssh idle-time 20
ip ssh timeout 60
```

Securing Telnet

Prerequisites: Standard ACL created (optional) and user (if using enable telnet authentication, see example for creating users in Enabling SSH)

Notes: Typically for security, telnet is disabled; however in addition to disabling it (no telnet server), it is advised to secure it as if it was enabled, just in case someone inadvertently turns it on.

Configuration Example:

```
telnet access-group 10
telnet timeout 10
enable telnet authentication
```

Requiring Username and Password to enter Enable Mode

Prerequisites: Local users configured or RADIUS/TACACS+ server for remote authentication

Configuration Example:

```
aaa authentication enable default local
```

Example Commands for TFTP:

```
scp username@192.168.10.1:runConfig myswitch.cfg
scp myswitch.cfg username@192.168.10.1:startConfig
```

Restoring the device:
```
scp username@192.168.10.1:runConfig myswtich.cfg
```

Backing up the device:
```
copy tftp start 192.168.10.2 myswitch.cfg
```

Optional additional configuration: To use the user’s access-level provided in the first initial authentication, instead of requiring users to re-enter their credentials to enter enable (privilege) mode, use the following command:

```
aaa authentication login privilege-mode
```

Securing Web Access

Prerequisites: Standard ACL created (optional) and user (if using aaa authentication, see example for creating users in Enabling SSH)

Notes: By default, the web-server responds and can be authenticated using user “get” and the read-only SNMP community string as the password. Alternatively, if a read-write community string is created, it can be accessed via “set” and the read-write community string. Changing the aaa authentication method will change this behavior. Also, it is advised to change access from http to https or disable it all together with “no web-management http”

Configuration Example:

```
crypto-ssl cert generate
no web-management http
web-management https
web access-group 10
aaa authentication web-server default local
```

Securing Management to Specific Router IPs

Prerequisites: Appropriate telnet/snmp/syslog/ssh/web configurations

Notes: Using a loopback interface is best as it’s not tied to an interface that potential can go down. Some options may not be available on some devices.

Configuration Example:

```
interface loopback 1
ip address 192.168.100.1/32
!
ip telnet source-interface loopback 1
ip ssh source-interface loopback 1
ip web source-interface loopback 1
snmp-server trap source-interface loopback 1
ip syslog source-interface loopback 1
```

Using and Securing SNMPv2

Prerequisites: Standard ACL created for additional security (optional)

Notes: By default, a read-only community string of “public” is defined. It will not appear in the configuration, but is present. You need to change this from the default value. A snmp-server host is the server to which SNMP traps will be sent. IMPORTANT: If you remove all SNMPv2 strings, the system will replace “public” on reload.

Troubleshooting: show smnpr server

Configuration Example:

```
snmp-server host 192.168.10.2
no snmp-server community public ro
snmp-server community <secret> ro 10
snmp-server community <secret> rw 10
```

Using and Securing SNMPv3

Prerequisites: Standard ACL created for additional security (optional)

Notes: SNMPv3 using encryption to send and receive SNMP traffic.

Configuration Example:

```
snmp-server group <group> v3 auth access 10 read all write all notify all
snmp-server user <user> <group> v3 auth md5 <pass> priv aes <pass>
snmp-server host 192.168.10.2 version v3 privacy <user>
```
### Enabling sFlow (RFC 3176)

**Prerequisites:** sFlow collector to receive the sFlow information

**Notes:** sFlow samples packets flowing through the switch and reports them back to a collector for analysis. The devices process the packets in hardware; however, care should be taken in selecting a sample rate as not to overwhelm processing and storage space of the collector. Most devices only sample on the inbound direction, so all ports must be enabled to report all traffic on the device.

**Configuration Example:**

```plaintext
sflow destination 192.168.100.2
sflow sample 512
sflow enable
int e 1 to 24
sflow forwarding
```

### Syslog and NTP Server

**Prerequisites:** A syslog server to receive messages and a NTP time source.

**Notes:** Logging on the devices is limited by space. It’s advised to send a copy to a server for more permanent storage.

**Configuration Example:**

```plaintext
snmp server 192.168.10.3
logging 192.168.10.2
logging buffered 100
```

### Securing the Console Port

**Prerequisites:** aaa authentication methods configured

**Configuration Example:**

```plaintext
enable aaa console
console timeout 10
```

### Creating a IronStack w/ Hitless Failover

**Prerequisites:** FCX Stackable switches

**Notes:** After issuing the command “stack secure-setup” in the privilege level to create the stack, configure two of the stack members with the same priority (this prevents the master from taking back over after a failure). The stack mac can be derived from the mac of one of the devices. It’s used so STP packets, etc are sourced from the same mac before and after failover.

**Troubleshooting:** show stack

**Configuration Example:**

```plaintext
stack unit 1
  priority 250
stack unit 2
  priority 250
stack mac 0024.00e1.1111
hitless-failover enable
```

### Creating a Link Aggregation (Edge Switch)

**Prerequisites:** The ports that are to be aggregated must be the same speed, same VLAN, etc to be combined.

**Notes:** Depending on the device, there may be restrictions on which ports can be combined to create aggregated links. Once created, all configurations for the link aggregation group are done via the primary port.

**Troubleshooting:** show trunk

**Static Configuration Example:**

```plaintext
trunk e 1 to 2
trunk deploy
```

**Dynamic (LACP) Configuration Example:**

```plaintext
int e 1
  link-aggregate configure key 10000
  link-aggregate active
int e 2
  link-aggregate configure key 10000
  link-aggregate active
```

### Creating a Link Aggregation (Core Switch)

**Prerequisites:** v.3.7.00 or greater; otherwise, use configuration for edge switch. The ports that are to be aggregated must be the same speed, same VLAN, etc to be combined.

**Notes:** To enable or disable individual ports within a trunk, you must use the disable/enable command within the lag commands.

**Troubleshooting:** show lag brief

**Static Configuration Example:**

```plaintext
lag blue static id 1
  ports ethernet 3/1 ethernet 7/2
primary port 3/1
deploy
```

**Dynamic (LACP) Configuration Example:**

```plaintext
lag red dynamic id 1
  ports ethernet 3/4 to 3/5
primary port 3/4
deploy
```

### Configuring Multi-Chassis Trunking (MCT)

**Prerequisites:** VLANs created with ports assigned, 802.3ad LAGs setup on non-MCT devices, and ICL port is tagged into vlans that are to use MCT.

**Notes:** Multi-Chassis Trunking is a way to increase redundancy while decreasing complexity in the network. Two NetIron devices may appear logically as one to all downstream devices, allowing for 802.3ad LAG groups to form between the three devices. This allows for one MCT device to fail without a hit to traffic.

**Troubleshooting:** show cluster

**Configuration Example:** Here, a four port LAG will form, 2 from each of A and B

**ROUTER A:**

```plaintext
vlan 4090 name Session-VLAN
  !—Does not have to be 4090
tag e 2/1
  !—Link going between the two routers, called an ICL
router-interface ve 200
int ve 200
  ip addr 10.1.1.1/30
lag blue dynamic
  ports ethernet 3/1 ethernet 4/1
  !—Interfaces that go to non-MCT device
primary port 3/1
deploy
Cluster <name> <ID>  !—ID must match on A and B
  rbridge-id 1
  !—ID must be unique for each device
session-vlan 4090
keep-alive-vlan <#>  !—vlan to use if ICL is lost
  member-vlan 10
  !—vlan(s) that are to traverse the LAG
icl <name> eth 2/1
  !—define ICL to be used for this cluster
peer <ip of B> rbridge-id <ID of B>
icl <name from line above>
deploy
client edge1
rbridge-id 3
  !—This ID must match on both A and B
```
**Creating a management VLAN for switches**

**Prerequisites:** VLAN created with ports assigned.

**Notes:** By default, a switch will respond to requests on all VLAN’s provided the Layer-3 addressing matches. Creating a management VLAN stops that behavior and the switch management will only answer requests the are on the specified VLAN.

**Caveats:** Only one management VLAN can be assigned. If a “ip default-gateway” has already been assigned, it will be moved into the VLAN configuration as “default-gateway”.

**Configuration Example:**

```
vlan 10 name Management
management-vlan
default-gateway 192.168.10.1 1
```

**Dual-Mode Ports**

**Prerequisites:** VLANS created with ports assigned.

**Notes:** In some situations, like connecting to a Cisco ® device or VoIP device, traffic may appear on an interface both tagged and untagged. For example, Cisco native vlan will not have a VLAN tag on a Cisco 802.1Q link. A port that is dual-mode, will send/receive untagged packets and place it into the appropriate VLAN while also accepting normal tagged traffic.

**Configuration Example (Edge Device):**

```
vlan 10 name Voice
tagged e 1
vlan 20 name Data
ntagged e 1
int e 1
dual-mode 20 !— Untagged traffic to VLAN 20
```

**Configuration Example (Core Devices):**

For any given port, only one vlan can be “untagged”.

```
vlan 10 name Voice
tagged e 1/1
vlan 20 name Data
untagged e 1/1
```

By default, ports will remain untagged in the default vlan as you tag them into other vlans unless you remove them. To stop this behavior globally, use the command “no dual-mode-default-vlan”.

```
vlan 1 name DEFAULT-VLAN
no untagged e 1/1
```

**Configuring Power over Ethernet (POE/POE+)**

**Prerequisites:** POE/POE+ Capable switch and ports. POE power supplies installed for the SX chassis.

**Notes:** By default, POE is not enabled on the interfaces. This is because the system will calculate power delivery and if there is not enough power supplies for the configured inline power ports, then starting with the highest interface number (unless power priority is configured), power will be disabled on the excess ports.

**Troubleshooting:** show inline power

**Configuration Example:**

```
int e 1
inline-power
```
Configuring Basic Quality of Service (QoS) for FCX/FWS/FGS

Prerequisites: None.
Notes: QoS prioritizes the use of bandwidth for a link. Tagged traffic will automatically be prioritized based on the 802.1P bit in the 802.1Q tag. Layer-3 prioritization of the DSCP/TOS value requires the trust dscp. Alternatively to trusting dscp, an ACL can be used. The globally defined qos profile specifies how each of the 7 queue will be processed as a percentage of weight (SP means strict priority, the numerical values represent weight)

Configuration Example:
```
qos profile qosp7 sp qosp6 sp qosp5 25 qosp4 25 qosp3 10 qosp2 25 qosp1 10 qosp0 5
int e 1/1
trust dscp
```

Configuring Basic Quality of Service (QoS) for FESX/SX

Prerequisites: None.
Notes: QoS prioritizes the use of bandwidth for a link. Tagged traffic will automatically be prioritized based on the 802.1P bit in the 802.1Q tag. Layer-3 prioritization of the DSCP/TOS value requires the use of an ACL to map the dscp value to the class-of-service(COS) queues. The globally defined qos profile specifies how each of the 7 queues will be processed as a percentage weight.

Configuration Example:
```
qos profile qosp7 sp qosp6 sp qosp5 25 qosp4 25 qosp3 10 qosp2 25 qosp1 10 qosp0 5
ip access-list extended QOS
  permit ip any any dscp-cos-mapping
ipv6 access-list v6qos
  permit ipv6 any any dscp-cos-mapping
int e 1/1
  ip access-group QOS in
  ipv6 traffic-filter v6qos in
```

Configuring Basic Quality of Service (QoS) for MLX/XMR/CES/CER

Prerequisites: None.
Notes: QoS prioritizes the use of bandwidth for a link. Tagged traffic will automatically be prioritized based on the 802.1P bit in the 802.1Q tag. Layer-3 prioritization of the DSCP/TOS value requires the “qos-to-transparent” dscp”. Alternatively to trusting dscp, an ACL can be used. The qos scheduler specifies how much (in percentage) that a specific queue (0-7) has per interface. The values must add up to 100

Configuration Example:
```
qos scheduler profile WRR0 weighted 8 2 25 25 5 25 5 5 ! Defined globally for CES/CER only
int e 1/1
  qos scheduler weighted 10 10 20 10 10 10 20 ! For MLX/XMR
  qos scheduler profile WRR0 ! For CES/CER only
  qos-to-transparent dscp
```

Per VLAN Spanning Tree

Prerequisites: VLAN created with ports assigned
Notes: By default, devices running switch code have Per-VLAN STP running. Devices running router code do not. Default spanning tree priority is 32768.
Troubleshooting: show spanning-tree

Configuration Example:
```
vlan 10
  spanning-tree
  spanning-tree priority 256
```

Per VLAN Rapid Spanning Tree

Prerequisites: VLAN created with ports assigned
Notes: All switches in the VLAN need to be running RSTP. All switch to switch interfaces must be defined as “admin-pt2pt-mac ports”. Priority only needs to be assigned on the primary and backup root switches.
Troubleshooting: show 802-1w

Configuration Example:
```
vlan 10
  spanning-tree 802-1w
  spanning-tree 802-1w priority 256
int e 49
  spanning-tree 802-1w admin-pt2pt-mac
```

MSTP (802.1s) – IEEE based per Vlan Rapid Spanning Tree

Prerequisites: VLAN created with ports assigned
Notes: mstp name and revision number must be same across all switches, in the same region. MSTP operates just like RSTP.
Troubleshooting: show mstp config

Configuration Example:
```
mstp name Campus
mstp revision 1
mstp instance 6 vlan 6
  mstp instance 6 priority 8192
  mstp admin-pt2pt-mac ethe 1/5 to 1/20
mstp start
```

Configuring BPDU Guard

Prerequisites: None.
Notes: Used to prevent rogue switches from connecting to the network. If a STP BPDU is seen on an interface with BPDU guard enabled, the port will be put into an “errdisable” state and must be manually re-enabled by the Administrator. Best used on ports at or near the access layer.
Troubleshooting: show stp-bpdu-guard

Configuration Example:
```
int e 1
  stp-bpdu-guard
```

Configuring Root Guard

Prerequisites: None.
Notes: Used to prevent undesired Spanning Tree topologies. When deployed on a physical port, if the switch receives a BPDU with a lower root priority (i.e. change in root), it ignores the BPDU, and errdisables the ports. The Administrator must then manually disable and re-enable the port, or may set a timeout value.
Troubleshooting: show spanning-tree root-protect

Configuration Example:
```
int e 1
  spanning-tree root-protect
  spanning-tree root-protect timeout 120
```

DHCP Server

Prerequisites: FastIron code 7.1 or greater (7.2 for SX). In an IronStack, “stack-mac” must be configured.
Notes: Up to 1000 DHCP clients. Information will be stored on flash. Multiple pools can be configured.
Troubleshooting: show ip dhcp-server summary and show ip shcp-server bind

Configuration Example:
**SNTP Time Server**

**Prerequisites:** FastIron code 7.3 or greater, NetIron code 5.0 or greater.

**Notes:** MD5 authentication of timeserver packets is optional.

**Troubleshooting:** show sntp server, show sntp association

**Configuration Example:**

```plaintext
! The following gets the time from another server using MD5 (optional) and issues the time to clients sntp server 192.168.100.1 authentication 1 <secret>
sntp poll-interval 1800 !—Adjust polling interval if necessary sntp server-mode authentication <secret> ! The following issues the time to clients using the local time on the device sntp server-mode use-local-clock stratum 3 authentication-key 2 <secret> ! Specify which interface to use as the server ip sntp source-interface loopback 1
```

**Enabling MAC-Based Port Security**

**Notes:** Interface can be set up to accept a certain number of MAC address per port and automatically shutdown/restrict the port if mac changes or more than number of mac addresses are discovered on the port.

**Troubleshooting:** show port security, clear port security

**Configuration Example:**

```plaintext
port-security violation shutdown 10 !—shutdown the port for 10 min autosave 60 !—save learned macs to flash every 60 min int e 1 to 24 port security enable maximum 1 !—Note: 1 is the default, so this command will not show
```

**Enabling 802.1x Port Security**

**Prerequisites:** End devices supporting an 802.1x supplicant and a Radius Server

**Notes:** Various authentication timers and rules for authentication exist. Consult the latest configuration guide for all options.

**Troubleshooting:** show dot1x ...

**Configuration Example:**

```plaintext
aaa authentication dot1x default radius
radius-server host 192.168.1.1 auth-port 1812 acct-port 1813 default key <STRING> dot1x
dot1x-enable enable ethernet 3/1 to 3/24 re-authentication timeout re-authperiod 3600 interface e 3/1 dot1x port-control forced-unauthorized
```

**Overriding 802.1X for specific Macs Example:**

```plaintext
mac filter 1 permit 0050.04ab.9429 ffff.ffff.0000 any int e1/2
```

**Configuring OSPF**

**Prerequisites:** Switch is running Full Layer-3 code and IP address are already assigned to interface or virtual interfaces.

**Notes:** Passive interface do not transmit OSPF hello’s. This is for security on subnets that don’t have neighboring routers. Additionally, consider MD5 authentication of neighbors. Configuring a loopback interface is recommended as the router-id for OSPF.

**Troubleshooting:** show ip ospf

**Configuration Example:**

```plaintext
ip ospf 192.168.10.0/24 192.168.2.1
```

**Enabling Multicast for Layer-2 Switches**

**Notes:** By default, ICMP snooping is disable. This means that any multicast packet will be treated as a broadcast packet. Active should only be used when no routers are configured for IGMP/PIM in the network.

**Configuration Example:**

```plaintext
ip multicast passive
```

**Configuring Router Interfaces**

**Prerequisites:** Switch is in Full Layer-3 code

**Notes:** The route-only statement ensures that no broadcast will leak between the ports that are assigned to the same VLAN. Doing this precludes the need to have every port in its own VLAN.

**Troubleshooting:** show ip int

**Configuration Example:**

```plaintext
int e 1 to 24
ip address 192.168.10.1/24 route-only
```

**Configuring Virtual Router Interfaces**

**Prerequisites:** Switch is in Base Layer-3 or Full Layer-3 code and ports are assigned to a VLAN.

**Notes:** This is to assign a router interface to a group of ports with a VLAN.

**Troubleshooting:** show ip int

**Configuration Example:**

```plaintext
vlan 10 untagged e 1 to 2 router-interface ve 10 interface ve 10 ip address 192.168.10.1/24
```

**Configuring Static Routes**

**Prerequisites:** Switch is running Base Layer-3 or Full Layer-3 code and IP address are already assigned to interface or virtual interfaces.

**Notes:** Although the next hop can be the interface name, Do NOT use this. Always specify the IP address of the next router for which the packets should be sent to.

**Troubleshooting:** show ip route

**Configuration Example:**

```plaintext
ip route 192.168.10.0/24 192.168.2.1
```

**Notes:** In instances where devices that share the port with a PC, but do not support 802.1x authentication, use mac filters to allow specific macs to bypass 802.1.

---

```
ip dhcp-server pool guests
dhcp-default-router 192.168.50.1
dns-server 192.168.10.1
domain-name brocade.com
network 192.168.50.0/24
deploy
!
ip dhcp-server enable
```

---

**Enabling MAC-Based Port Security**

**Notes:** Interface can be set up to accept a certain number of MAC address per port and automatically shutdown/restrict the port if mac changes or more than number of mac addresses are discovered on the port.

**Troubleshooting:** show port security, clear port security

**Configuration Example:**

```plaintext
port-security
violation shutdown 10 !—shutdown the port for 10 min
autosave 60 !—save learned macs to flash every 60 min
int e 1 to 24
port security enable
maximum 1 !—Note: 1 is the default, so this command will not show
```

**Enabling 802.1x Port Security**

**Prerequisites:** End devices supporting an 802.1x supplicant and a Radius Server

**Notes:** Various authentication timers and rules for authentication exist. Consult the latest configuration guide for all options.

**Troubleshooting:** show dot1x ...

**Configuration Example:**

```plaintext
aaa authentication dot1x default radius
radius-server host 192.168.1.1 auth-port 1812 acct-port 1813 default key <STRING> dot1x
dot1x-enable enable ethernet 3/1 to 3/24 re-authentication timeout re-authperiod 3600 interface e 3/1 dot1x port-control forced-unauthorized
```

**Overriding 802.1X for specific Macs Example:**

```plaintext
mac filter 1 permit 0050.04ab.9429 ffff.ffff.0000 any int e1/2
dot1x auth-filter 1
```
interface loopback 1
  ip address 192.168.100.1/32
router ospf
  area 0
  int e 1
    ip ospf area 0
    ip ospf md5-authentication key-id 1 key <shared key>
  int ve 10
    ip ospf area 0
    ip ospf passive

Configuring VRRP

Prerequisites: Switch is running Full Layer-3 code and IP address are already assigned to interface or virtual interfaces.

Notes: VRRP provides redundancy for routers. One router is the owner of the IP and one (or more) routers backup the owner of the IP.

Troubleshooting: show ip vrrp brief

Configuration Example:

ROUTER A:
  router vrrp
  int ve 10
    ip address 192.168.10.1/24
    ip vrrp vrid 10 owner
    ip-address 192.168.10.1
    activate

ROUTER B:
  router vrrp
  int ve 10
    ip address 192.168.10.2/24
    ip vrrp vrid 10
    backup priority 150 track-priority 30
    ip-address 192.168.10.1
    advertise backup
    activate

Configuring VRRP-Extended

Prerequisites: Switch is running Full Layer-3 code and IP address are already assigned to interface or virtual interfaces.

Notes: VRRP Extended is similar to VRRP, except all routers are configured as backups and the backup router with the highest priority is the Master for the IP. In addition, VRRP Extended introduces track-ports. For each track port that is down, the track priority is subtracted from the overall priority. In the example below, if Router A’s track port is down, the overall priority would be 170. Since 170 would be lower than Router B’s priority of 180, Router B will become Master. This is useful to have VRRP-E follow the status of the uplinks from the devices.

Troubleshooting: show ip vrrp-e brief

Configuration Example:

ROUTER A:
  router vrrp-extended
  int ve 10
    ip address 192.168.10.2/24
    ip vrrp-extended vrid 10
    backup priority 200 track-priority 30
    track-port ethernet 1/1
    ip-address 192.168.10.1
    advertise backup
    activate

Enabling Multicast (PIM-DM) for Routers

Prerequisites: A routing protocol and loopback address configured.

Notes: When enabling PIM, the default is Dense Mode. All interfaces that will participate in multicast should have PIM enabled. This includes the router-to-router links and the links to user subnets. Enabling PIM on an interface enables IGMP as well.

Troubleshooting: show ip pim nbr; show ip pim mcache

Configuration Example:

router pim
  int e 1/1
    ip pim

IPv4 GRE Tunnels

Prerequisites: An BigIron or NetIron, or Fastiron with Advanced License.

Notes: On the RX and SX series, a physical loop port is required for hardware based GRE, otherwise, all packets will be processed in software. Also, if able, increase the MTU size to 1500 to prevent software-based fragmentation of packets > 1476. The default MTU size is 1476. Also, the default ospf cost (or auto cost referencing) of a GRE port may cause routes to be not learned across the GRE tunnel via OSPF. Recommend manually setting the ip ospf cost if used.

Troubleshooting:

Configuration Example:

interface tunnel 1	null
  tunnel mode gre ip
  tunnel mtu 1500
  tunnel source 192.168.168.2
  tunnel destination 192.168.168.1
  ip ospf cost 10
  ip ospf area 0
  !
### Configuring VLL with LDP

**Prerequisites:** MPLS capable device with OSPF running and a loopback configured.

**Notes:** Route-only should not be configured on MPLS-Interfaces. FDP and CDP cannot be configured on untagged VLL endpoints (ie. Customer interface). Customer facing interfaces can be tagged or untagged.

**Troubleshooting:** show mpls ldp, show mpls vll

**Configuration Example:**

```
router mpls
mpls-interface e 2/1
ldp-enable
vll Test_VLL 100
vll-peer 192.168.100.100
  !-- Loopback IP of end-point
vlan 100
  untagged e 4/1
  !--Customer Interface
```

### Configuring VPLS with LDP

**Prerequisites:** MPLS capable device with OSPF running and a loopback configured.

**Notes:** Route-only should not be configured on MPLS-Interfaces. Bridge PDU’s (BPDU’s) do not go across VPLS unless you configure “no vpls-bpdu-block” on the physical interface. FDP and CDP cannot be configured on untagged VPLS endpoints (ie. Customer interface). Customer facing Interfaces can be tagged or untagged.

**Troubleshooting:** show mpls ldp, show mpls vlps, show mac vlps

**Configuration Example:**

```
router mpls
  mpls-interface e 2/1
  ldp-enable
  vplsl Test_VPLS 200
  vpls-peer 192.168.100.10 192.168.100.20
    !-- Loopback IP(s) of peer MPLS routers
vlan 100
  untagged e 4/1
  !--Customer Interface
```

### Securing LDP

**Prerequisites:** MPLS Routers using LDP

**Notes:** Requiring authentication of LDP packets provides security.

**Troubleshooting:** show mpls ldp interface; show mpls ldp neighbor;

**Configuration Example:**

```
router mpls
  ldp
    !--Repeat for all other MPLS router loopbacks
session 192.100.255.3 key <secret>
session 192.100.255.1 key <secret>
```

### Configuring VPLS with BGP Autodiscovery

**Prerequisites:** MPLS capable device with OSPF running and a loopback configured.

**Notes:** In Autodiscovery, the vpls-peer does not have to be specified. An extension to BGP is utilized to exchange peer information. This prevents you from having to clear the entire peering session. The endpoints of the VPLS instance are associated via the VCID (200 in this example). The name of the VPLS instance is not exchanged.

**Troubleshooting:** clear ip bgp l2vpn vpls neighbor all; show ip bgp l2vpn vpls sum

**Configuration Example:**

```
int loopback 1
  ip address 10.1.1.1/32
  ip ospf area 0
router bgp
  local-as 10
  !-- Repeat the following for all the iBGP peers in the VPLS network
neighbor 10.1.1.2 remote-as 10
router mpls
  mpls-interface e 2/1
  ldp-enable
  vpls CustomerA 200
  auto-discovery
  vlan 100
  untagged e 4/1
  !--Customer Interface
router bgp
  address-family l2vpn vpls
    !-- Repeat the following for all the iBGP peers in the VPLS network
  neighbor 10.10.1.2 activate
```

### Configuring static LSP (RSVP-TE)

**Prerequisites:** MPLS capable device with OSPF running and a loopback configured.

**Notes:** Specifying a path is optional. If no path is specified, then the standard IP routing or constrained shortest path first (CSPF), if enabled, will be used to build a path.

**Troubleshooting:** show mpls path, show mpls lsp, show mpls route

**Configuration Example:**

```
router mpls
  path R1_to_R3
    !--Path’s are optional
  strict 192.168.100.10
    !- Must go to this device
  loose 192.168.100.50
    !- Take any way to this device
lsp R1_to_R3
to 192.168.100.10
  primary R1_to_R3
    !--Optional
  secondary R1-to_R3_Alt
    !--Alt path
standby
  !- Pre-signal the standby LSP for <50ms failover
```

### Securing RSVP-TE

**Prerequisites:** MPLS Routers using RSVP

**Notes:** Requiring authentication of RSVP packets provides security.

**Troubleshooting:** show mpls rsvp interface; show mpls rsvp session;

**Configuration Example:**

```
router mpls
  mpls-interface e 2/1
  rsvp-authentication key <secret>
```
**Configuring BGP/L3VPN**

**Prerequisites:** MPLS capable device with LDP or RSVP and a loopback configured.

**Notes:** When placing an Interface or VE into a VRF, all previous IP address information will be removed. Route-targets are used to determine which routes shared among customers. In this example, the VRF for Customer A has route distinguisher (rd) of 100:1 and its peer route has an rd of 100:2. Importing and exporting of rd 100:2 allows the router to learn each other’s networks that belong to Customer A.

**Troubleshooting:** show ip bgp <name>; ping vrf <name> <ip address>

**Configuration Example:**

```
!—Create each customer’s VRF Context
vrf CustomerA
    rd 100:1
    route-target both 100:2
    address-family ipv4
interface e 1/1
    vrf forwarding CustomerA
    ip address 172.16.100.1/24
    ip ospf area 1 !—If doing OSPF with customer
    router bgp
        local-as 65001
    !— Repeat the following for all the iBGP peers in the MPLS network
        neighbor 192.168.100.1 remote-as 65001
        neighbor 192.168.100.1 update-source loopback 1
        neighbor 192.168.100.1 password <secret> !—for security
        address-family vpnv4 unicast
    !— Repeat the following for all the iBGP peers in the MPLS network
        neighbor 192.168.100.1 activate
        neighbor 192.168.100.1 send-community extended
    !— Repeat for each customer vrf
        address-family ipv4 unicast vrf CustomerA
        redistribute connected
        redistribute ospf !—If other routers connect via OSPF
        redistribute static !—If static routes exist in VRF
        router ospf vrf customerA !—If using ospf with Customer, configure and
        redistribute into bgp
        area 1
        redistribute bgp

!— Create each customer’s VRF Context
vrf CustomerA
    rd 100:1
    route-target both 100:2
    address-family ipv4
```

**ACL Configuration Example:**

```
ipv6 access-list RemoteAccess
    permit ipv6 host 2100::1 any
    ssh access-group ipv6 RemoteAccess
    telnet access-group ipv6 RemoteAccess
    web access-group ipv6 RemoteAccess
    snmp-server community <secret> ro ipv6 RemoteAccess
```

**Configuring IPv6 Router Interfaces**

**Prerequisites:** IPv6 Router

**Notes:** Enabling IPv6 on the interface will automatically generate a link-local address. Follow the example to add a global address to the interface. Adding route-only ensures that the port will only route and not switch between other ports in the default vlan. For interfaces with computers, the network prefix has to be /64.

**Troubleshooting:** show ip int

**Configuration Example:**

```
interface e 5
    ipv6 enable
    ipv6 address 2001:470:20::1/64
    route-only
```

**Configuring Virtual IPv6 Router Interfaces**

**Prerequisites:** Switch is in Base Layer-3 or Full Layer-3 code and ports are assigned to a VLAN.

**Notes:** This is to assign a router interface to a group of ports with a VLAN. For interfaces with computers, the network prefix has to be /64.

**Troubleshooting:** show ip int

**Configuration Example:**

```
vlan 10
    untagged e 1 to 2
interface ve 10
    ipv6 enable
    ipv6 address 2001:470:10::1/64
```

**Configuring Static Routes**

**Prerequisites:** IPv6 Router and IP address are already assigned to interface or virtual interfaces

**Notes:** Statically assigned IPv6 routes always reference interface and link-local address of the next hop.

**Troubleshooting:** show ipv6 route

**Configuration Example:**

```
ipv6 route 2001:100::1/32 eth 1 fe80::1
```

**Configuring OSPFv3**

**Prerequisites:** IPv6 Router and IP address are already assigned to interface or virtual interfaces

**Notes:** OSPFv3 is exclusively for IPv6. Passive interface do not transmit OSPF hello’s. This is for security on subnets that don’t have neighboring routers. Additionally, consider ipsec authentication of neighbors (example not show). Configuring a loopback interface is recommended as the router-id for OSPFv3.

**Troubleshooting:** show ipv6 ospf

**Configuration Example:**

```
interface loopback 1
    ipv6 enable
    ipv6 address 2001:470:ff::1/128
```

**Securing Access Via IPv6**

**Prerequisites:** None

**Notes:** Since IPv4 and IPv6 are different protocols, access-list created for IPv4 do not apply to IPv6. If you enable IPv6, you must also secure remote access. If you prefer, instead of using access-list to define clients, you can define individual clients (up to 10). For example “web client ipv6 2100:5” or “all-client ipv6 2100:5” to assign web, telnet, snmp, and ssh commands at once. Currently, an IPv6 ACL cannot be applied to SNMPv3 traffic in the command; however, the snmp-client will take care of it.

**Troubleshooting:** show ipv6 access-list all

**Client Configuration Example:**

```
all-client ipv6 2100::1 !—Up to 10 clients can be configured
    telnet client ipv6 2100::1
    snmp-client ipv6 2100::1
    web client ipv6 2100::1
    ip ssh client ipv6 2100::1
```

**ACL Configuration Example:**

```
ipv6 access-list RemoteAccess
    permit ipv6 host 2100::1 any
    ssh access-group ipv6 RemoteAccess
    telnet access-group ipv6 RemoteAccess
    web access-group ipv6 RemoteAccess
    snmp-server community <secret> ro ipv6 RemoteAccess
```
ipv6 router ospf
area 0
interface e 1
ipv6 enable
ipv6 address 2001:470:30::1/126
ipv6 ospf area 0
interface ve 10
ipv6 enable
ipv6 ospf area 0
ipv6 ospf passive

Configuring VRRPv3

Prerequisites: IPv6 Router (NetIron)

Notes: VRRP provides redundancy for routers. Two (or more) routers backup a single IPv6 Address. A common link-local address has to be configured.

Troubleshooting: show ipv6 vrrp brief

Configuration Example:

ROUTER A:
ipv6 router vrrp
int ve 10
ipv6 enable
ipv6 address fe80::1 link-local
ipv6 address 2001:470:10::1/64
ipv6 vrrp vrid 10
  owner
  ipv6-address fe80::1
  ipv6-address 2001:470:10::1
  advertise backup
  activate

ROUTER B:
ipv6 router vrrp
int ve 10
ipv6 enable
ipv6 address fe80::2 link-local
ipv6 address 2001:470:10::2/64
ipv6 vrrp vrid 10
  backup priority 100
  ipv6-address fe80::1
  ipv6-address 2001:470:10::1
  advertise backup
  activate

Configuring an IPv6 over IPv4 Tunnel

Prerequisites: IPv6 Router

Notes: This feature allows two IPv6 networks to be connected via an IPv4 network

Configuration Example:

interface tunnel 1
  tunnel mode ipv6ip
tunnel source 192.168.10.180
tunnel destination 172.32.226.238
ipv6 address 2001:470:a:514::2/64
ipv6 enable

ipv6 route ::/0 tunnel 1