SERVICE PROVIDER INFRASTRUCTURE SECURITY BEST PRACTICES

Yusuf Bhaiji – Cisco Systems

© 2005 Cisco Systems, Inc. All rights reserved.

Agenda

- Infrastructure Security Overview
- Preparing the Network
- Router Security: A Plane Perspective
- Tools and Techniques
- Conclusions

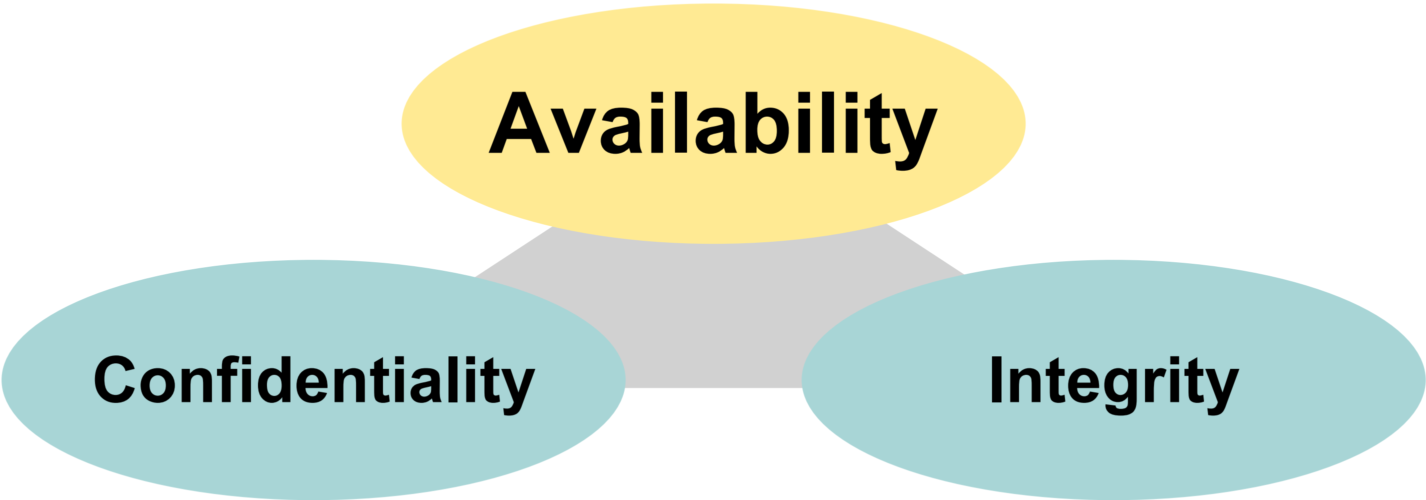
© 2005 Cisco Systems, Inc. All rights reserved.

Agenda

- Infrastructure Security Overview
- Preparing the Network
- Router Security: A Plane Perspective
- Tools and Techniques
- Conclusions

© 2005 Cisco Systems, Inc. All rights reserved.

The Security Trinity



- **Confidentiality**
- **Integrity**
- **Availability**

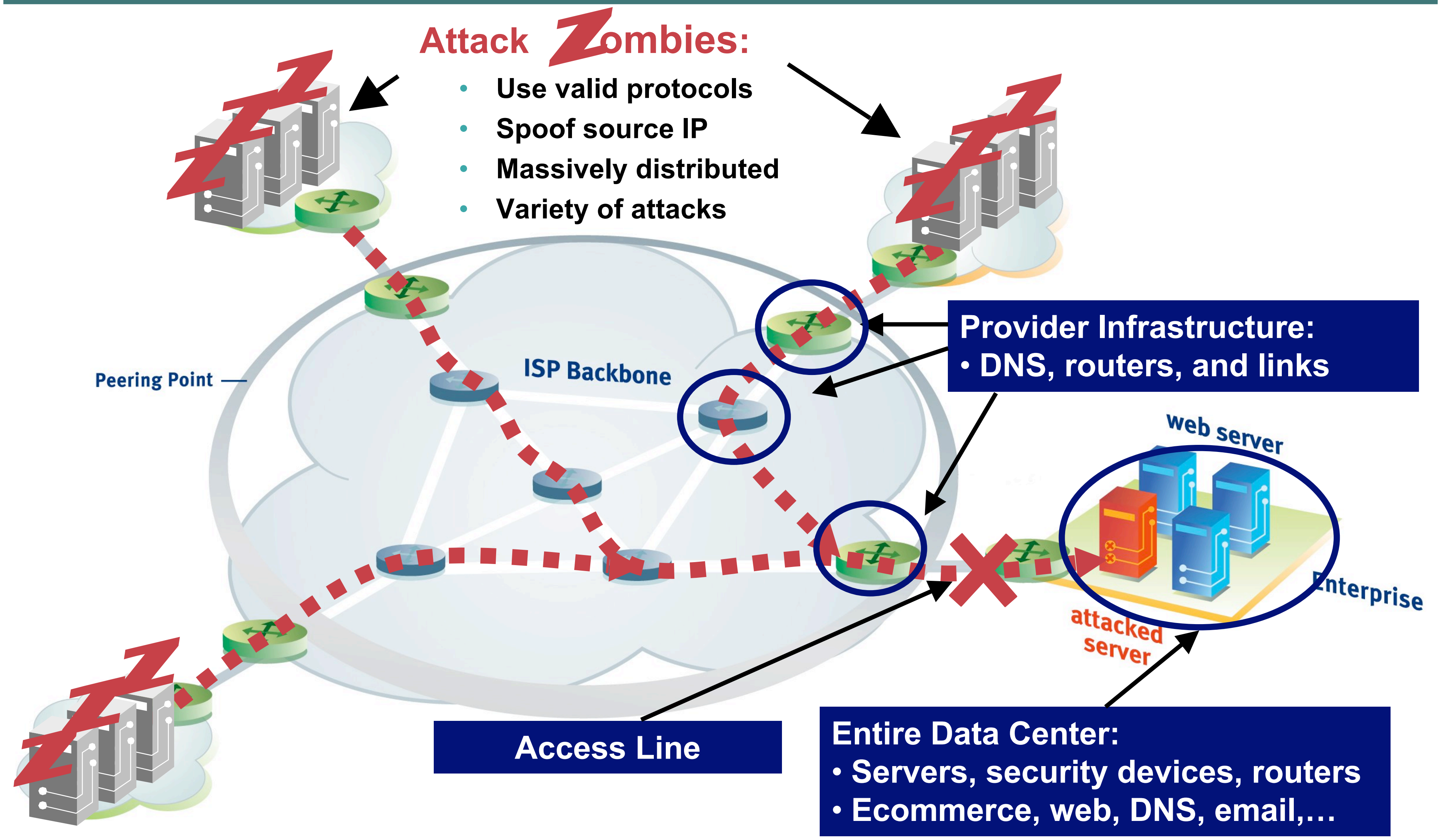
© 2005 Cisco Systems, Inc. All rights reserved.

Network Availability: Protect the Infrastructure

- We have a multitude of end device security products and technologies but the core is critical
- Remember: availability
  - Protecting the infrastructure is the most fundamental security requirement
- Infrastructure protection should be included in all disaster recovery and high availability designs
  - Part of network design
- Without an available core, no services (e.g. voice) can be delivered

© 2005 Cisco Systems, Inc. All rights reserved.

DDoS Vulnerabilities
Multiple Threats and Targets



© 2005 Cisco Systems, Inc. All rights reserved.

Denial of Service Trends

- **Multi-path**
  - Truly distributed
    - Routeservers, large botnets
- **Multi-vector**
  - SYN AND UDP AND…
- **Increased use “state”**
  - Looks like valid traffic (e.g. http get)
  - Can consume resources at various levels of the network
- **Financial incentive**
  - SPAM, DoS-for-hire
  - Large, thriving business
  - Forces us to reassess the risk profile

© 2005 Cisco Systems, Inc. All rights reserved.

Infrastructure Attacks

- The infrastructure is no longer a "black box"
  - Sites with Cisco documents and presentations on routing protocols (and I don't mean Cisco.com)
  - Marked increase in presentations about routers, routing and Cisco IOS® vulnerabilities at conferences like Blackhat, Defcon and Hivercon
  - Router attack tools and training are being published
- Why mount high-traffic DDOS attacks when you can take out your target's gateway routers?
- Hijacked routers are valuable in the spam world, which has a profit driver
- Router compromise (0wn3d) due to weak password

© 2005 Cisco Systems, Inc. All rights reserved.

From Bad to Worms

- Old worms never die!
  - Millions of CodeRed(!) and Slammer packets still captured daily
- Most worms are intended to compromise hosts
- Worm propagation is dependant on network availability
- Worms and DoS can be closely related
  - Secondary worm effects can lead to denial of service
  - Worms enable DoS by compromising hosts → BOTnets
- Perimeters are crumbling under the worm onslaught (VPN/mobile workers, partners, etc.)
- Don’t neglect virii!

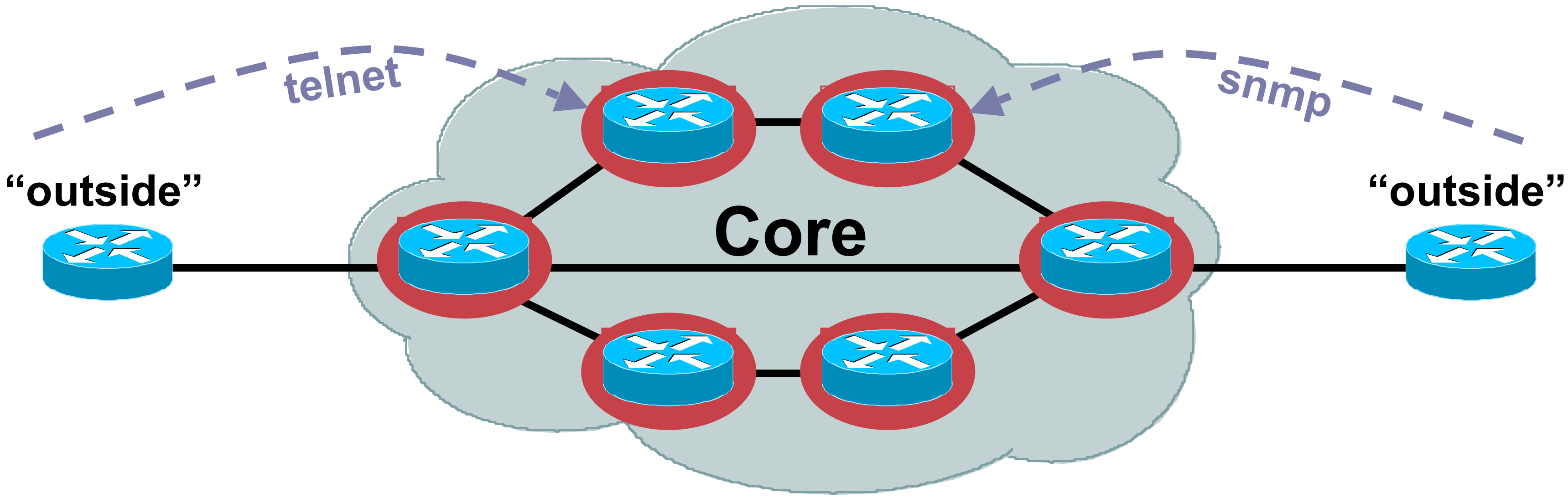
© 2005 Cisco Systems, Inc. All rights reserved.

Worms and the Infrastructure

- **Worms typically infect end-stations**
- **To date, worms have not targeted infrastructure BUT secondary effects have wreaked havoc**
  - **Increased traffic**
  - **Random scanning for destination**
  - **Destination address is multicast**
  - **Header variances**
- **At the core SP level, the aggregate affects of a worm can be substantial**

© 2005 Cisco Systems, Inc. All rights reserved.

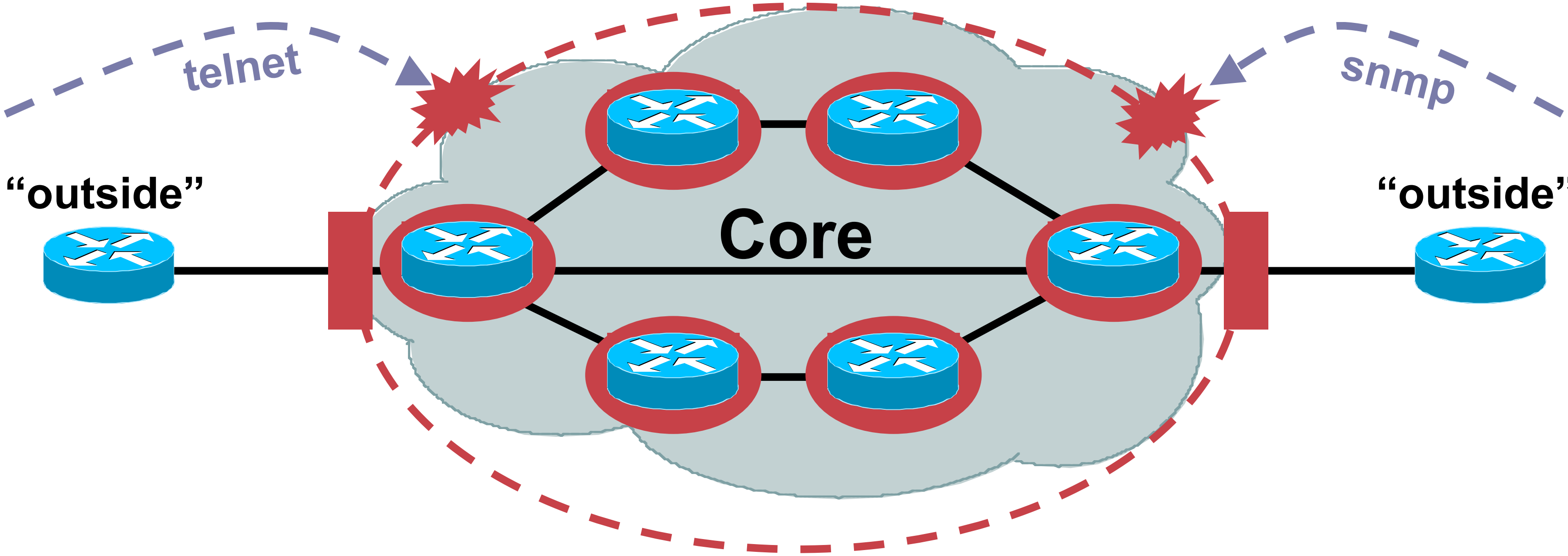
The Old World: Network Edge



- **Core routers individually secured**
- **Every router accessible from outside**

© 2005 Cisco Systems, Inc. All rights reserved.

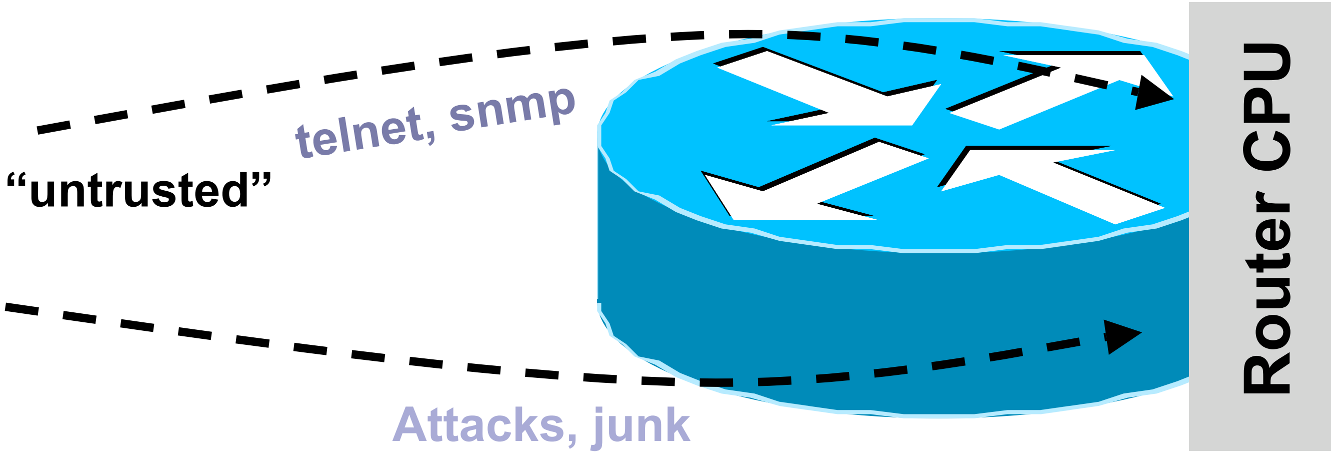
The New World: Network Edge



- Core routers individually secured PLUS
- Infrastructure protection
- Routers generally NOT accessible from outside

© 2005 Cisco Systems, Inc. All rights reserved.

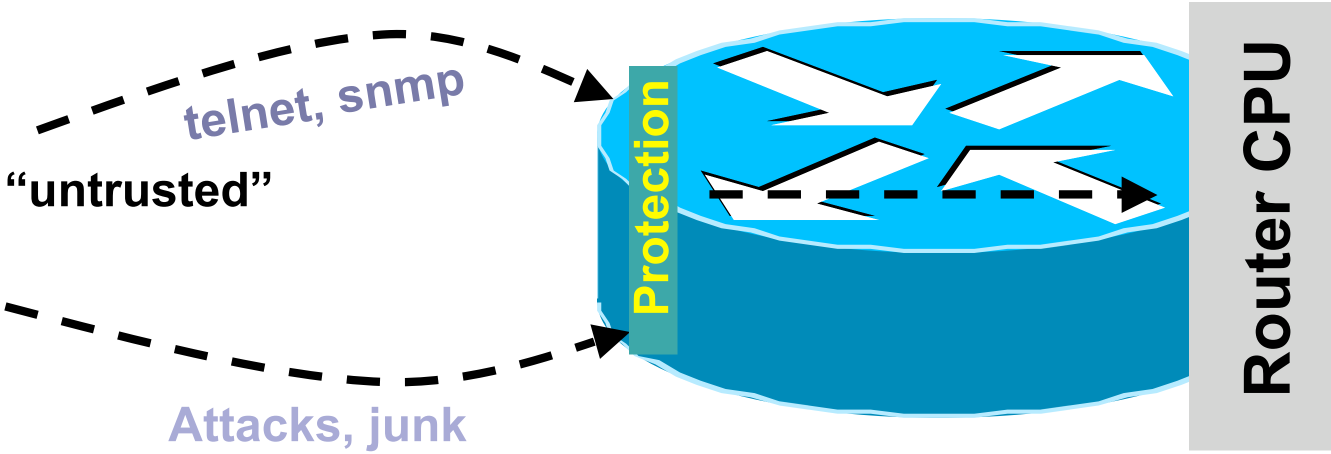
The Old World: Router Perspective



- **Policy enforced at process level (VTY ACL, SNMP ACL, etc.)**
- **Some early features such as ingress ACL used when possible**

© 2005 Cisco Systems, Inc. All rights reserved.

The New World: Router Perspective



- Central policy enforcement, prior to process level
- Granular protection schemes
- On high-end platforms, hardware implementations

© 2005 Cisco Systems, Inc. All rights reserved.

Agenda

- Infrastructure Security Overview
- Preparing the Network
- Router Security: A Plane Perspective
- Tools and Techniques
- Conclusions

© 2005 Cisco Systems, Inc. All rights reserved.

Preparing the Network

- This is a whole topic onto itself
  - Best practices can help prevent infection
  - Attack mitigation is rarely effective without best practice deployment
- "I want to stop the DoS but I haven't implemented XYZ yet" or "I don't know who to contact"
- Best practices can be tough to deploy, but the benefits are immeasurable

© 2005 Cisco Systems, Inc. All rights reserved.

Preparing the Network

- **Limit attack vectors**
  - Traffic filtering both incoming AND outgoing connections
  - Source address validation (ACL and/or uRPF)
  - RFC2827 filtering where applicable
  - BGP policy enforcement
- **Identify/detect attacks**
  - Develop network baseline, including traffic analysis
  - Logging and log analysis
  - IDS at strategic locations

© 2005 Cisco Systems, Inc. All rights reserved.

Preparing the Network

- Periodic security scans of internal network to identify policy violations
- Ongoing security vulnerability awareness
- Routine security auditing
- Event monitoring and correlation for firewalls, IDS, network devices and servers

© 2005 Cisco Systems, Inc. All rights reserved.

Infrastructure Specific Protection Techniques

- **Protect the infrastructure itself from attack**
  - From the inside—users/customers
  - From the outside—peers/upstreams
- **Methodology:**
  - Erect an edge barrier (infrastructure ACLs)
  - Focus on the device specific configuration (receive ACL and control plane policing)
  - Understand the platform architecture and how it impacts security

© 2005 Cisco Systems, Inc. All rights reserved.

Device Hardening

- **Turn off unused services**

```
no service udp-small-servers
no service tcp-small-servers
...
```

- **Use "secret" passwords—"service password encryption" is reversible**

```
enable secret MySecurePassword
```

- **Use secure device access**

```
aaa new-model
aaa authentication login default group tacacs+ local
```

  Don't forget authorization and accounting!

- **Use authenticated routing protocols**
- **NTP: time is critical for security correlation**
- **Use the data!**

  MRTG, perl-foo, etc.

© 2005 Cisco Systems, Inc. All rights reserved.

Infrastructure Best Practices

Harden Routers and Switches

- Develop and deploy standard configs that reflect security policy
  - Leverage configuration tools like RANCID
- Understand the technology (e.g. VLAN security principles)
- Understand the architecture, performance characteristics and features of the devices

© 2005 Cisco Systems, Inc. All rights reserved.

Agenda

- Infrastructure Security Overview
- Preparing the Network
- Router Security: A Plane Perspective
- Tools and Techniques
- Conclusions

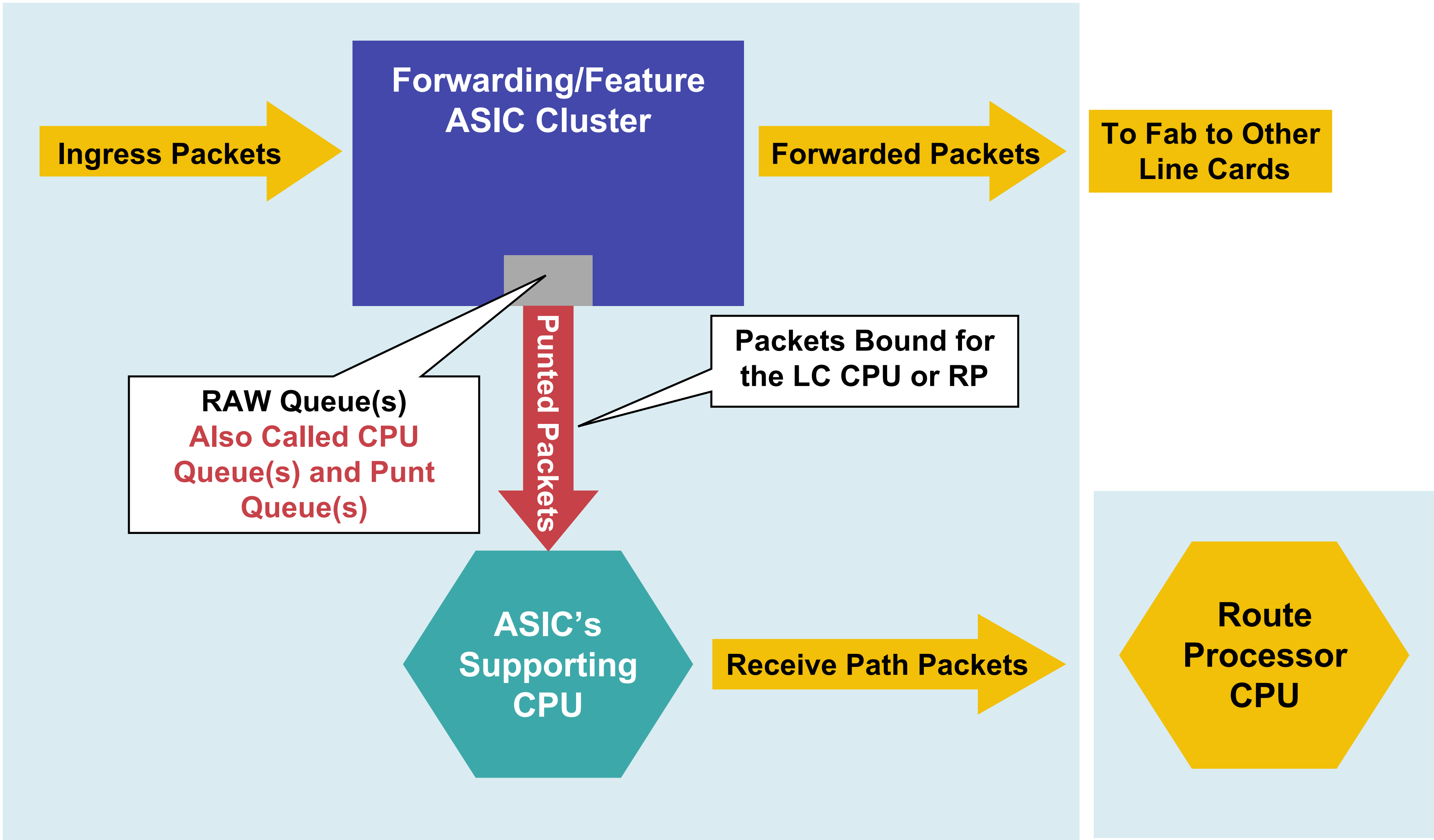
© 2005 Cisco Systems, Inc. All rights reserved.

Routers and Planes

- A network device typically handles traffic in the data/forwarding plane, the control plane, and the management plane
- Traffic in the data/forwarding plane is always destined through the device, and is:
  - Implemented in hardware on high end platforms
  - CEF switched (in the interrupt) in software switched platforms
- Traffic to the control/management plane is always destined to the device and is handled at process level ultimately:
  - In hardware switched platforms, control/management plane traffic is sent to the RP/MFSC and then sent to the process level for processing
  - In software switched platforms, it is sent directly to the process level for processing
- Some data plane traffic also reaches the control plane
  - Packets that are not routable reach to control plane so that ICMP unreachable messages can be generated
  - Packets that have IP options set are also handled by the processor

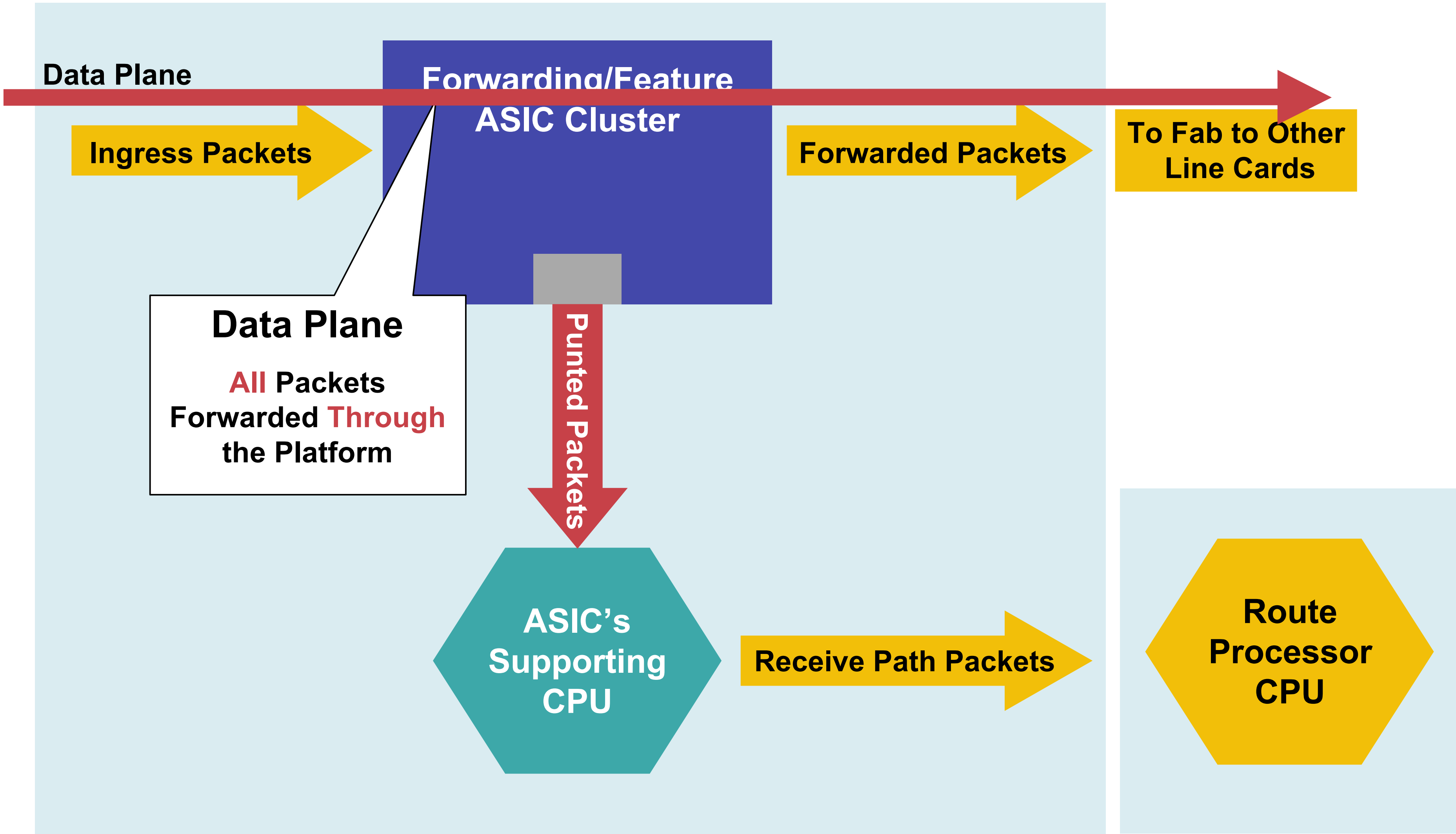
© 2005 Cisco Systems, Inc. All rights reserved.

ASIC-Based Platform: Main Components



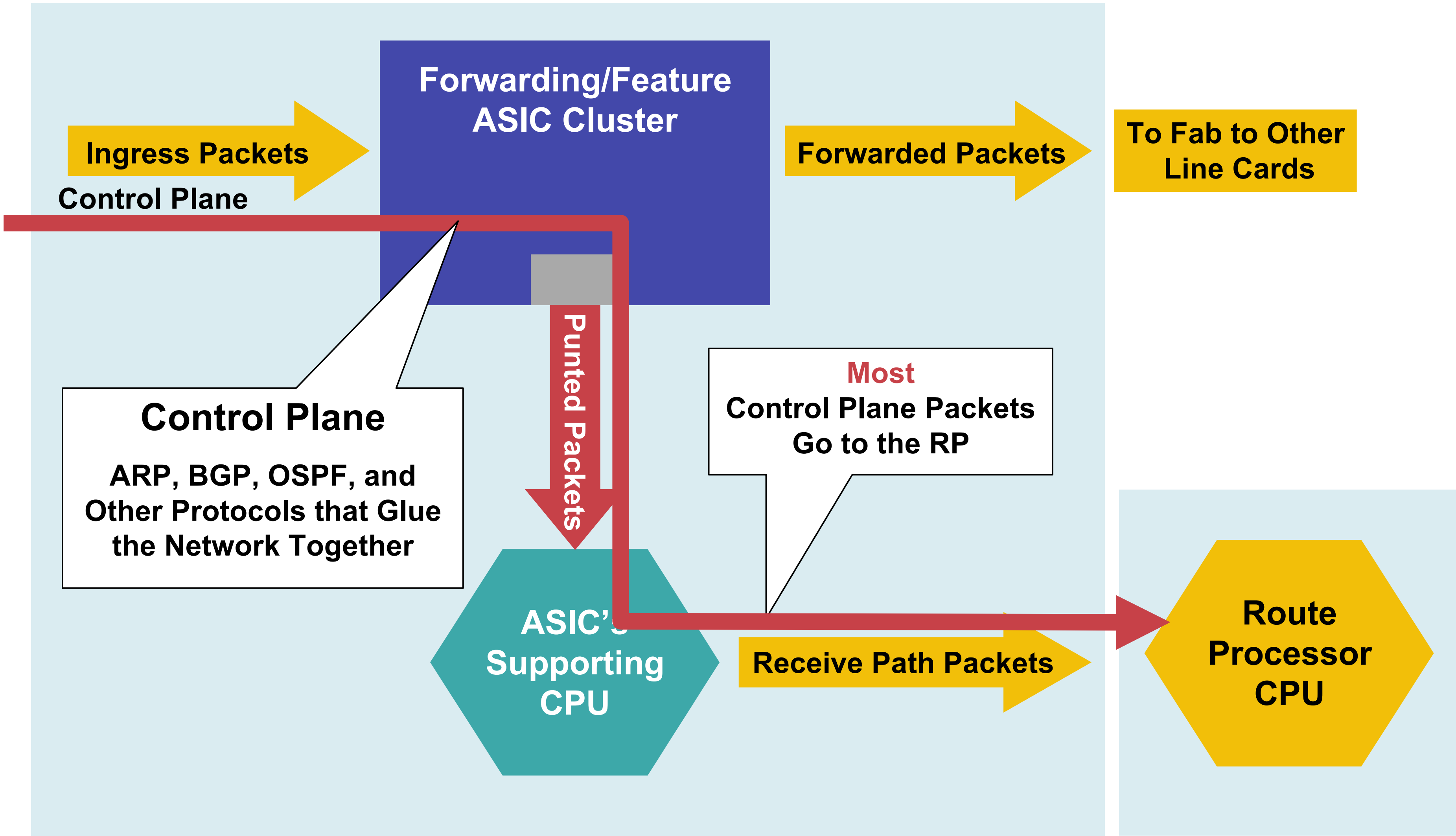
© 2005 Cisco Systems, Inc. All rights reserved.

Data Plane



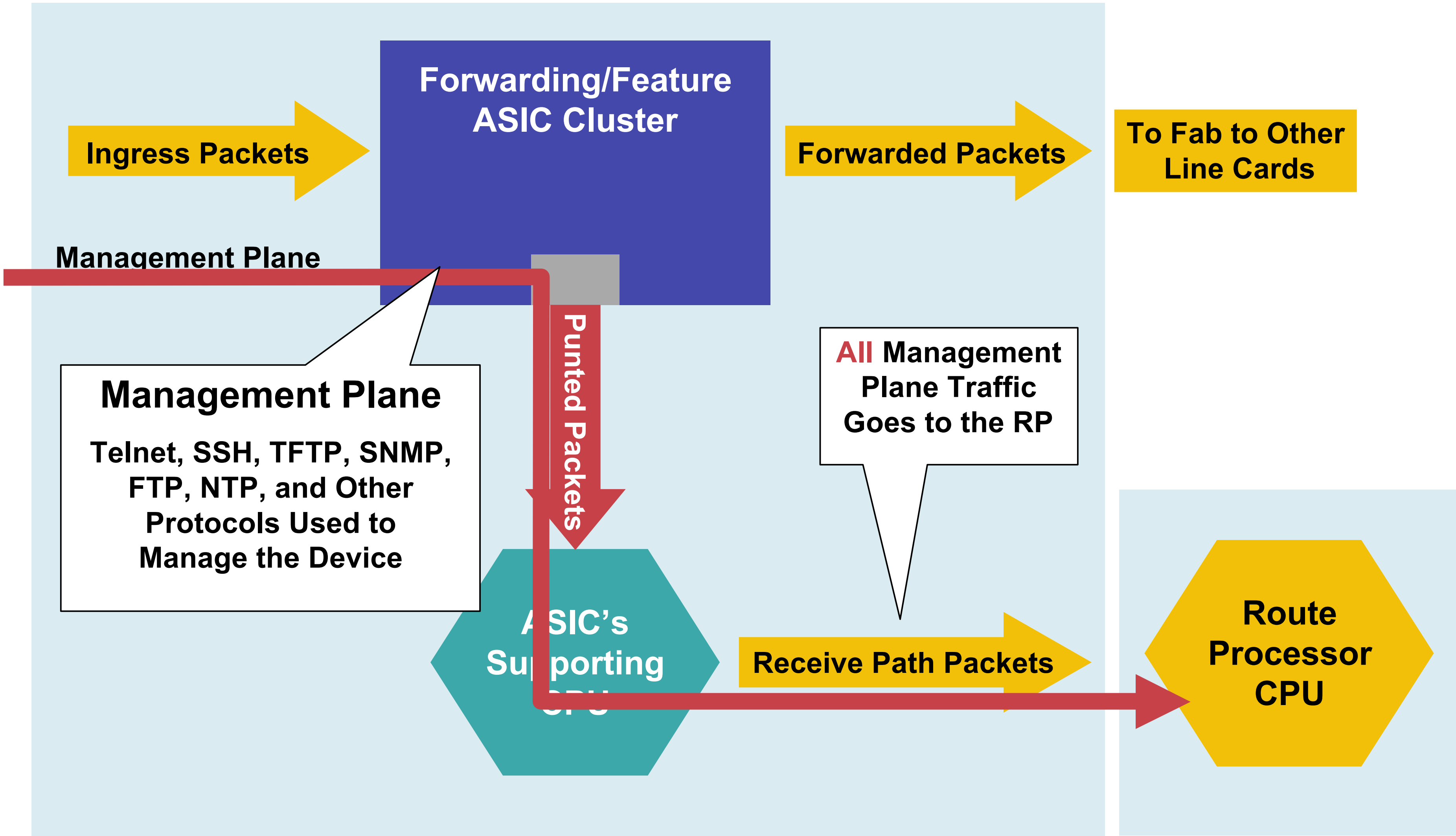
© 2005 Cisco Systems, Inc. All rights reserved.

Control Plane



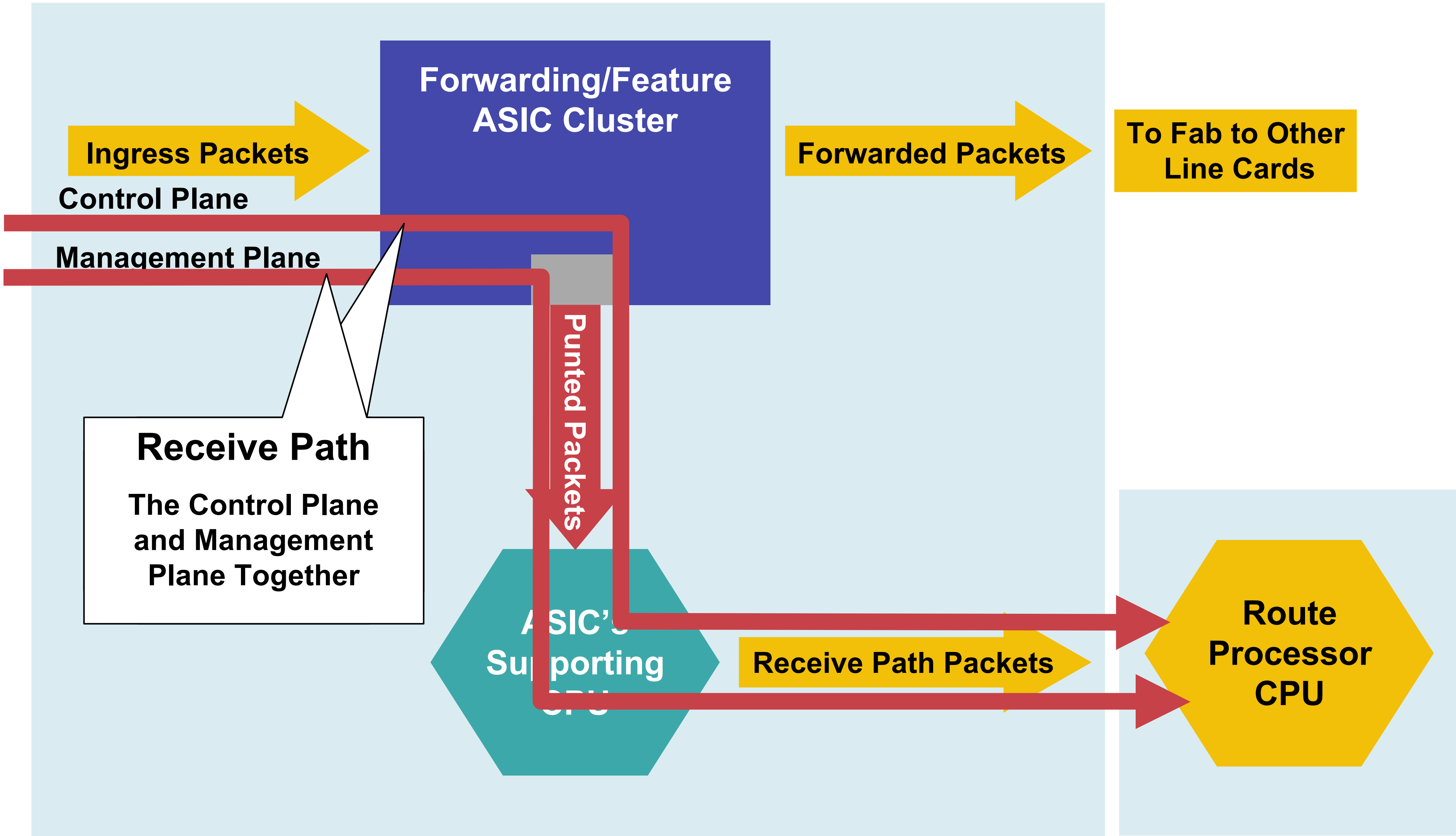
© 2005 Cisco Systems, Inc. All rights reserved.

Management Plane



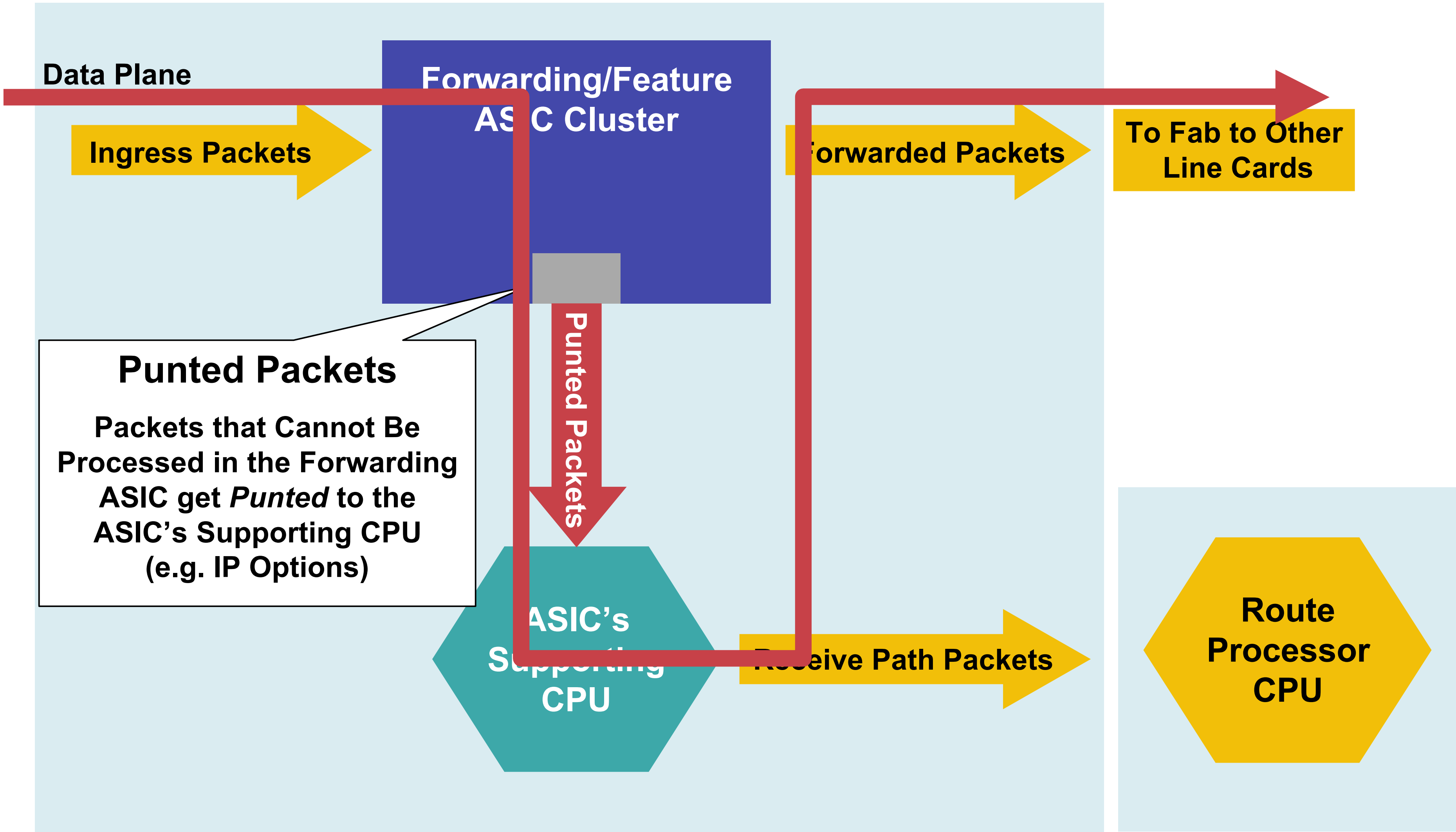
© 2005 Cisco Systems, Inc. All rights reserved.

Receive Path



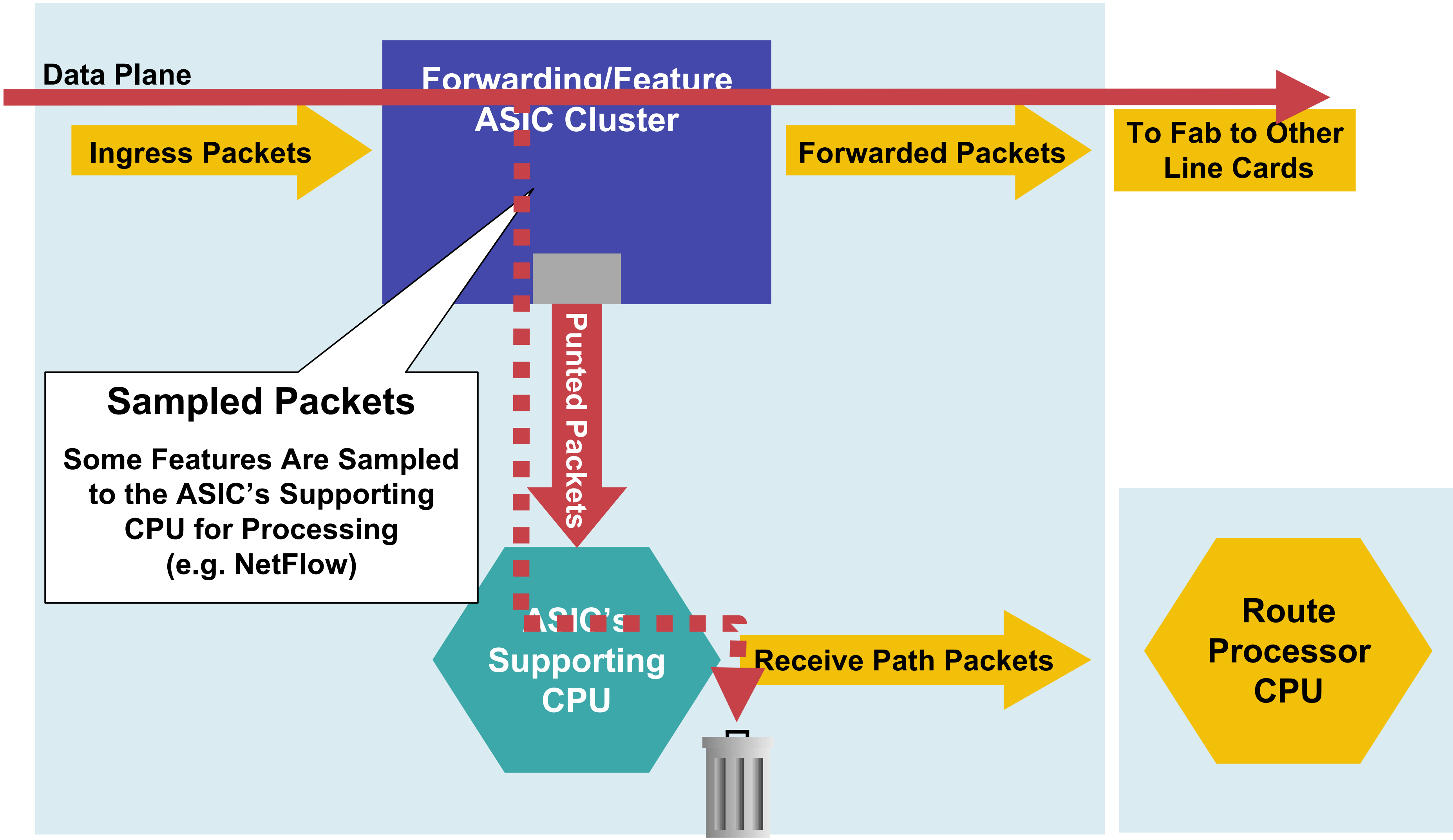
© 2005 Cisco Systems, Inc. All rights reserved.

Feature Punt



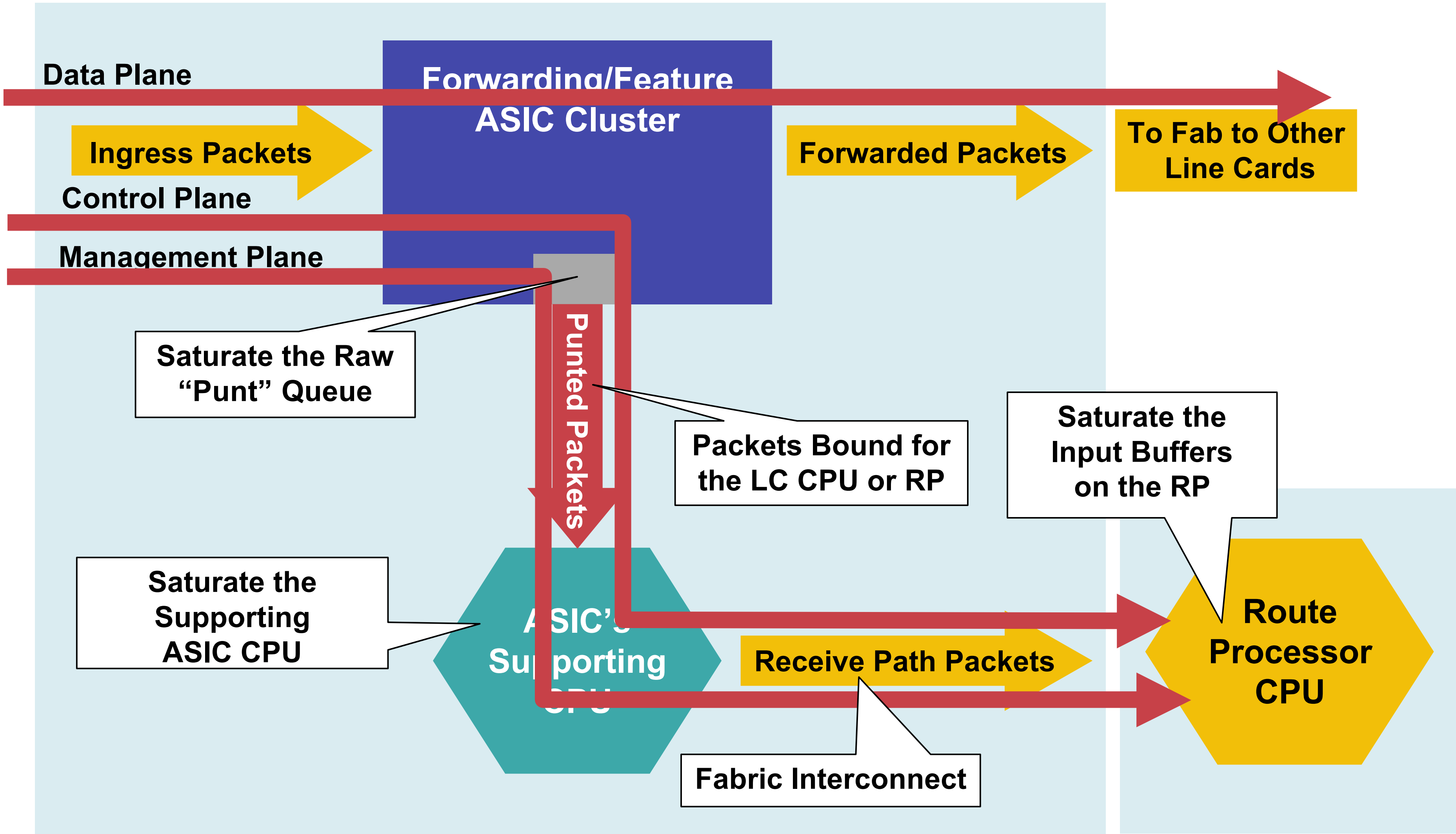
© 2005 Cisco Systems, Inc. All rights reserved.

Sampled Feature



© 2005 Cisco Systems, Inc. All rights reserved.

Receive Path Attack Vectors



© 2005 Cisco Systems, Inc. All rights reserved.

Router Risk Assessment

- **Direct router attacks usually target:**
  - Bandwidth saturation (data plane)
  - Control and/or management plane (receive path traffic on the control and management plane)
  - Saturate the punt path out of the forwarding/feature ASIC by abusing the TCP/IP standards (data plane traffic that is punted from the forwarding/feature ASIC)
- **High level of control plane activity can cause various side effects**
  - High route processor CPU utilization (near 100%)
  - Loss of keep-alives and routing protocol updates
  - Route flaps and major network transitions
  - Indiscriminate packet drops of incoming packets when memory and buffers are unavailable for legitimate IP data packets
  - Slow or unresponsive interactive sessions via Command Line Interface (CLI)
- **Attacks can be intentional or unintentional**

© 2005 Cisco Systems, Inc. All rights reserved.

Agenda

- Infrastructure Security Overview
- Preparing the Network
- Router Security: A Plane Perspective
- Tools and Techniques
- Conclusions

© 2005 Cisco Systems, Inc. All rights reserved.

Taking a Measured Approach

- **The techniques we will be discussing are extremely useful, but they must be applied in an architecturally-sound, situationally-appropriate, and operationally-feasible manner**
- **Don’t try to do all this at once—pick a technique with which you are comfortable and which you think will benefit you the most, and start there**
- **Pilot your chosen technique in a controlled manner, in a designated portion of your network**
- **Take the lessons learned from the pilot and work them into your general deployment plan and operational guidelines**

© 2005 Cisco Systems, Inc. All rights reserved.

Control Plane Protection Evolution

- **Infrastructure ACLs (iACLs)**
  - Create policies (ACLs or MQC) for control plane traffic to block all unwanted IP traffic destined to the core
  - Applied to ALL ingress port—affects ALL traffic (control and data plane)
- **Receive Path ACLs (rACLs)**
  - Create ACLs to block all all unwanted IP traffic destined to the core
  - Global (single) configuration affects all “receive path” packets
  - Only affects control plane traffic
- **Control Plane Policing (CoPP)**
  - Extends rACLs by adding Modular QoS CLI (MQC) policing
  - Widespread platform support

© 2005 Cisco Systems, Inc. All rights reserved.

INFRASTRUCTURE ACLS (iACL)

© 2004 Cisco Systems, Inc. All rights reserved.

Infrastructure ACLs (iACL)

- **Basic premise: filter traffic destined TO your core routers**

  Do your core routers really need to process all kinds of garbage?

- **Develop list of required protocols that are sourced from outside your AS and access core routers**

  Example: eBGP peering, GRE, IPSec, etc.

  Use classification ACL as required

- **Identify core address block(s)**

  This is the protected address space

  Summarization is critical → simpler and shorter ACLs

© 2005 Cisco Systems, Inc. All rights reserved.

Infrastructure ACLs (iACL)

- Infrastructure ACL will permit only required protocols and deny ALL others to infrastructure space
- ACL should also provide anti-spoof filtering
  - Deny your space from external sources
  - Deny RFC1918 space
  - Deny multicast sources addresses (224/4)
  - RFC3330 defines special use IPv4 addressing

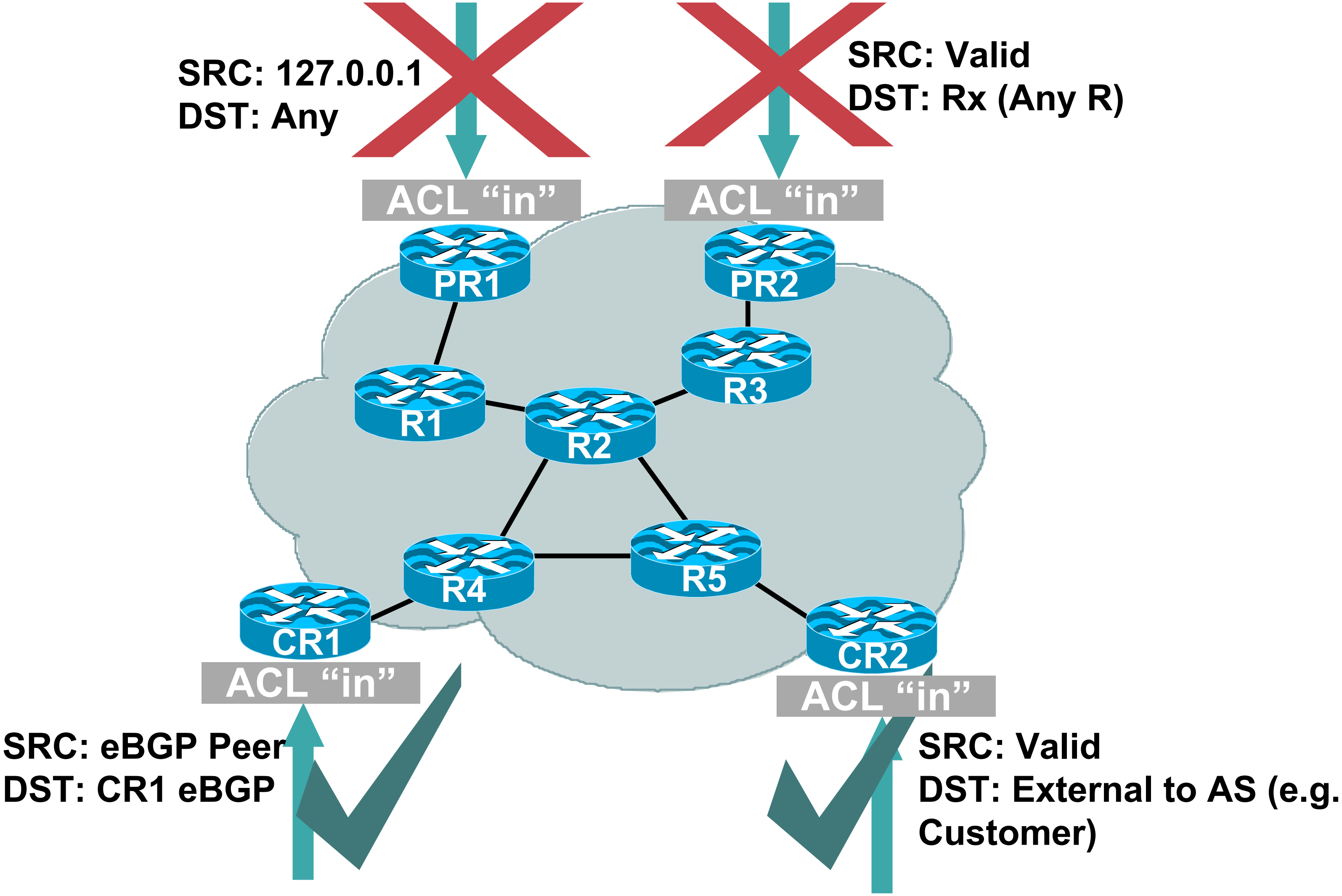
© 2005 Cisco Systems, Inc. All rights reserved.

Infrastructure ACLs (iACL)

- **Infrastructure ACL must permit transit traffic**
  - Traffic passing through routers must be allowed via permit IP any any
- **ACL is applied inbound on ingress interfaces**
- **Fragments destined to the core can be filtered via fragments keyword**

© 2005 Cisco Systems, Inc. All rights reserved.

Infrastructure ACL in Action



© 2005 Cisco Systems, Inc. All rights reserved.

IP Fragments and Security

- **Fragmented Packets can cause problems...**
- **Fragmented packets can be used as an attack vector to bypass ACLs**
- **Fragments can increase the effectiveness of some attacks by making the recipient consume more resources (CPU and memory) due to fragmentation reassembly**

© 2005 Cisco Systems, Inc. All rights reserved.

iACLs and Fragments

- Fragments can be denied via an iACL
- Denies fragments and classifies fragment by protocol:

```
access-list 110 deny tcp any core_CIDR fragments
access-list 110 deny udp any core_CIDR fragments
access-list 110 deny icmp any core_CIDR fragments
```

© 2005 Cisco Systems, Inc. All rights reserved.

IP Options

- Provide control functions that may be required in some situations but unnecessary for most common IP communications
- IP Options not switched in hardware
- Complete list and description of IP Options in RFC 791
- Drop and ignore reduce load on the route processor (RP)
- Caution: some protocols/application require options to function:
  - For example: strict/loose source routing, resource reservation protocols (RSVP) and others
- ip access-list extended drop-ip-option
  - deny   ip any any option any-options
  - permit ip any any
- ip options drop
- ip options ignore—router ignores options
  - Best practice when router doesn't need to process options
  - "ignore" not available on all routing platforms
  - Available in 12.0(22)S, 12.3(4)T and 12.2(25)S http://www.cisco.com/en/US/products/sw/iosswrel/ps1829/products_feature_guide09186a00801d4a94.html

© 2005 Cisco Systems, Inc. All rights reserved.

Using Classification ACL to build iACL

- Iterative Deployment
- Typically a very limited subset of protocols needs access to infrastructure equipment
- Even fewer are sourced from outside your AS
- Identify required protocols via classification ACL
- Deploy and test your ACLs

© 2005 Cisco Systems, Inc. All rights reserved.

Step 1: Classification

- **Traffic destined to the core must be classified**
- **NetFlow can be used to classify traffic**
  - **Need to export and review**
- **Classification ACL can be used to identify required protocols**
  - **Series of permit statements that provide insight into required protocols**
  - **Initially, many protocols can be permitted, only required ones permitted in next step**
  - **Log keyword can be used for additional detail; hits to ACL entry with *log* will increase CPU utilization: impact varies by platform**
- **Regardless of method, unexpected results should be carefully analyzed → do not permit protocols that you can't explain!**

© 2005 Cisco Systems, Inc. All rights reserved.

Step 2: Begin to Filter

- **Permit protocols identified in step 1 to infrastructure only address blocks**
- **Deny all other to addresses blocks**
  - **Watch access control entry (ACE) counters**
  - **Log keyword can help identify protocols that have been denied but are needed**
- **Last line: permit ip any any ← permit transit traffic**
- **The ACL now provides basic protection and can be used to ensure that the correct suite of protocols has been permitted**

© 2005 Cisco Systems, Inc. All rights reserved.

Steps 3 and 4: Restrict Source Addresses

- **Step 3:**

  ACL is providing basic protection

  Required protocols permitted, all other denied

  Identify source addresses and permit only those sources for requires protocols

  e.g., external BGP peers, tunnel end points

- **Step 4:**

  Increase security: deploy destination address filters if possible

- **Example - Protecting Your Core: Infrastructure Protection Access Control Lists:**

  http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

© 2005 Cisco Systems, Inc. All rights reserved.

Example: Infrastructure ACL

! Deny our internal space as a source of external packets

```
access-list 101 deny ip our_CIDR_block any
```

! Deny src addresses of 0.0.0.0 and 127/8

```
access-list 101 deny ip host 0.0.0.0 any
access-list 101 deny ip 127.0.0.0 0.255.255.255 any
```

! Deny RFC1918 space from entering AS

```
access-list 101 deny ip 10.0.0.0 0.255.255.255 any
access-list 101 deny ip 172.16.0.0 0.0.15.255 any
access-list 101 deny ip 192.168.0.0 0.0.255.255 any
```

© 2005 Cisco Systems, Inc. All rights reserved.

Example: Infrastructure ACL

! The only protocol that require infrastructure access is eBGP. WE have defined both src and dst addresses

```
access-list 101 permit tcp host peerA host peerB eq 179
access-list 101 permit tcp host peerA eq 179 host peerB
```

! Deny all other access to infrastructure

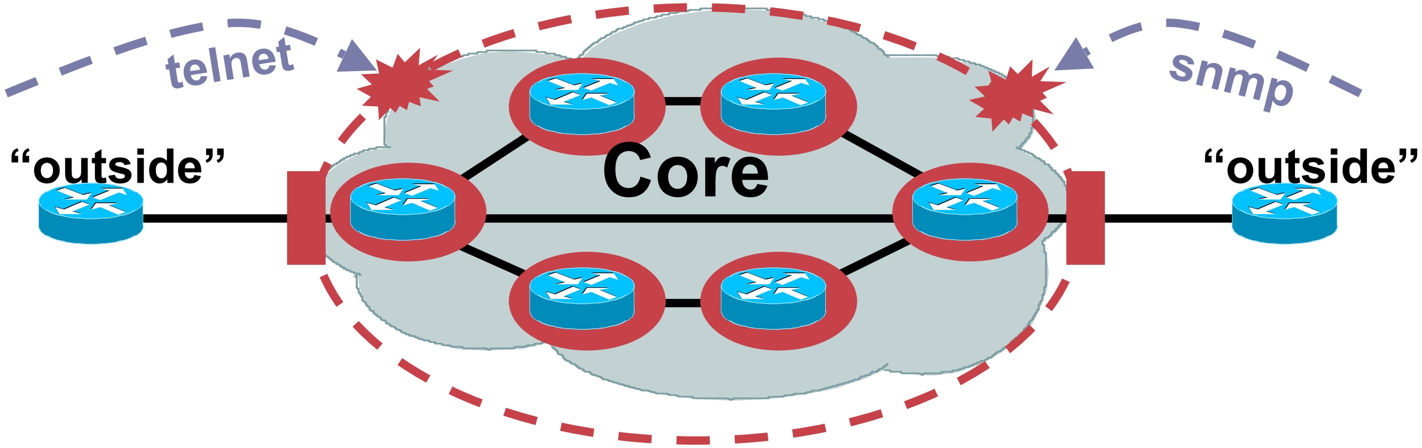
access-list 101 deny ip any core_CIDR_block

! Permit all data plane traffic

```
access-list 101 permit ip any any
```

© 2005 Cisco Systems, Inc. All rights reserved.

Infrastructure ACLs



- Edge "shield" in place
- Not perfect, but a very effective first round of defense
  - Can you apply iACLs everywhere?
  - What about packets that you cannot filter with iACLs?
  - Hardware limitations
- Next step: secure the control/management planes per box

© 2005 Cisco Systems, Inc. All rights reserved.

RECEIVE ACCESS-CONTROL LIST (rACL)

© 2004 Cisco Systems, Inc. All rights reserved.

Receive ACLs (rACLs)

- Receive ACLs filter traffic destined to the RP via receive adjacencies
- rACLs explicitly permit or deny traffic destined to the RP
- rACLs do NOT affect transit traffic
- Traffic is filtering on the ingress line card (LC), prior to route processor (RP) processing
- rACLs enforce security policy by filtering who/what can access the router

© 2005 Cisco Systems, Inc. All rights reserved.

Receive ACL Command

- Introduced in 12.0(21)S2/12.0(22)S

```
ip receive access-list [number]
```

- Standard, extended or compiled ACL
- As with other ACL types, show access-list provide ACE hit counts
- Log keyword can be used for more detail
- Example – IP Receive ACL

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1829/products_feature_guide09186a00805e9255.html

© 2005 Cisco Systems, Inc. All rights reserved.

Receive Adjacencies

- CEF entries for traffic destined to router, not through it
  - Real interface IP addresses
  - Loopback IP addresses

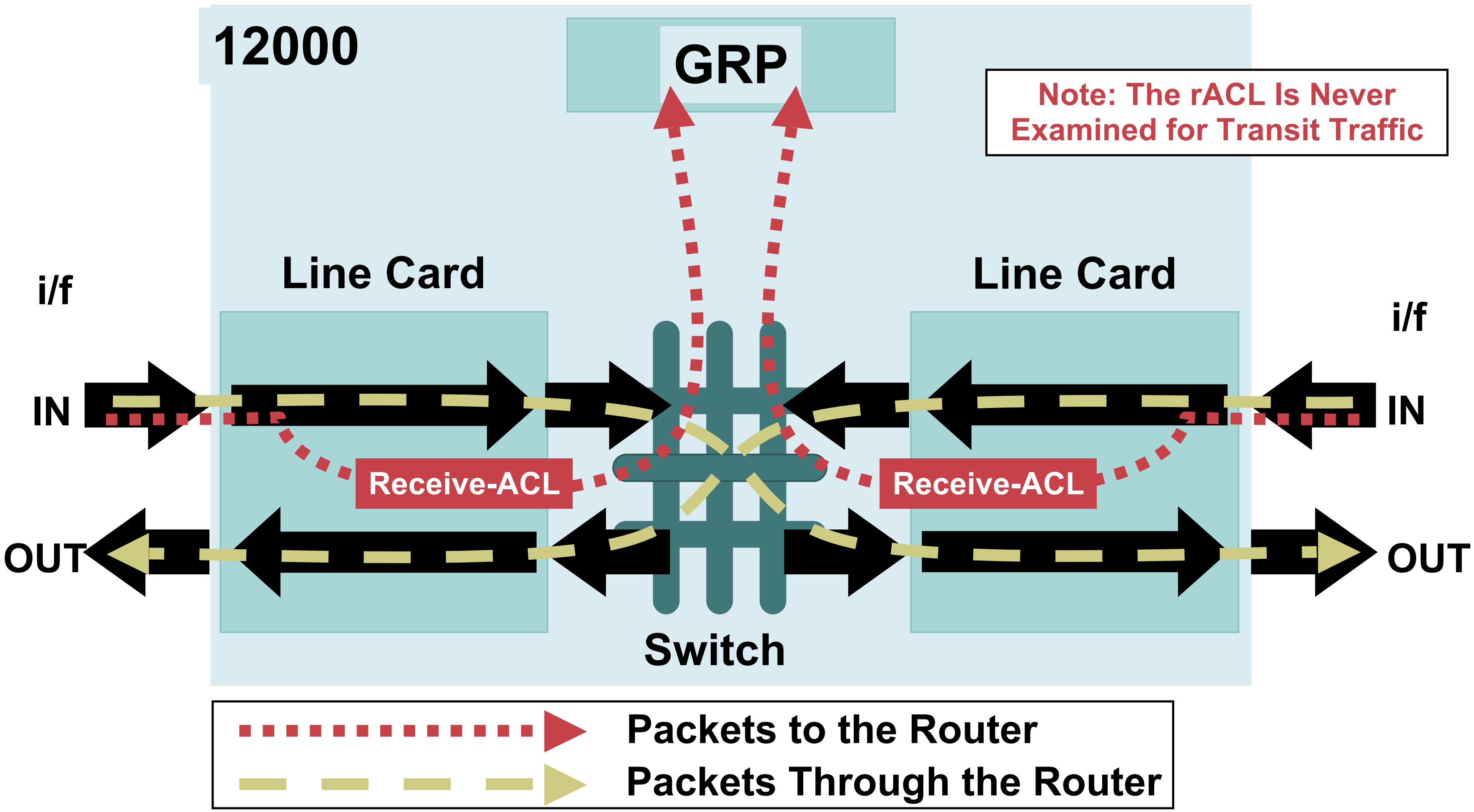
```
12000-1#sh ip cef
Prefix               Next Hop             Interface
10.1.2.0/24          172.16.1.216         GigabitEthernet3/0
10.1.3.0/24          172.16.1.216         GigabitEthernet3/0
172.16.1.196/32       receive
(172.16.1.196 is an interface IP address)
```

- Packets with next hop receive are sent to the router for processing
  - Some are handled directly by the LC
  - Others must be sent to the RP (GRP or PRP)
- Traffic usually routing protocols, management, multicast control traffic

© 2005 Cisco Systems, Inc. All rights reserved.

Receive ACL Traffic Flow

Router(config)# [no] ip receive access-list <num>



© 2005 Cisco Systems, Inc. All rights reserved.

riACLs and Fragments

- Fragments can be denied via an rACL
- Denies fragments and classify fragment by protocol:

```
access-list 110 deny tcp any any fragments
access-list 110 deny udp any any fragments
access-list 110 deny icmp any any fragments
```

© 2005 Cisco Systems, Inc. All rights reserved.

Using Classification ACL to build rACL

- **Iterative Deployment**
- **Develop list of required protocols**
- **Develop address requirements**
- **Determine interface on router**
  - **Does the protocol access 1 interface?**
  - **Many interfaces?**
  - **Loopback or real?**
- **Deployment is an iterative process**
  - **Start with relatively “open” lists → tighten as needed**

© 2005 Cisco Systems, Inc. All rights reserved.

rACL: Iterative Deployment

- **Step 1: Identify required protocols via classification ACL**
  - Permit any any for various protocols
  - Get an understanding of what protocols communicate with the router
  - Logging can be used for more detailed analysis
- **Step 2: Review identified packets, begin to filter access to the GRP**
  - Using list developed in step 1, permit only those protocols
  - Deny any any at the end → basic protection AND identify missed protocols

© 2005 Cisco Systems, Inc. All rights reserved.

rACL: Iterative Deployment

- **Step 3: Limit source address block**

  Only permit your CIDR block in the source field

  eBGP peers are the exception: they will fall outside CIDR block

- **Step 4: Narrow the rACL permit statements: authorized source addresses**

  Increasingly limit the source addresses to known sources: management stations, NTP peers, etc

© 2005 Cisco Systems, Inc. All rights reserved.

rACL: Iterative Deployment

- **Step 5: Limit the destination addresses on the rACL**
  - **Filter what interfaces are accessible to specific protocols**
  - **Does the protocol access loopbacks only? Real interfaces?**

© 2005 Cisco Systems, Inc. All rights reserved.

rACL: Sample Entries

```
ip receive access-list 110
```

- **Fragments**

```
access-list 110 deny any any fragments
```

- **OSPF**

```
access-list 110 permit ospf host ospf_neighbour host 224.0.0.5
! DR multicast address, if needed
access-list 110 permit ospf host ospf_neighbour host 224.0.0.6
access-list 110 permit ospf host ospf_neighbour host local_ip
```

- **BGP**

```
access-list 110 permit tcp host bgp_peer host loopback eq bgp
```

- **EIGRP**

```
access-list 110 permit eigrp host eigrp_neighbour host 224.0.0.10
access-list 110 permit eigrp host eigrp_neighbour host local_ip
```

© 2005 Cisco Systems, Inc. All rights reserved.

rACL: Sample Entries

- **SSH/Telnet**

```
access-list 110 permit tcp management_addresses host loopback eq 22
access-list 110 permit tcp management_addresses host loopback eq telnet
```

- **SNMP**

```
access-list 110 permit udp host NMS_stations host loopback eq snmp
```

- **Traceroute (router originated)**

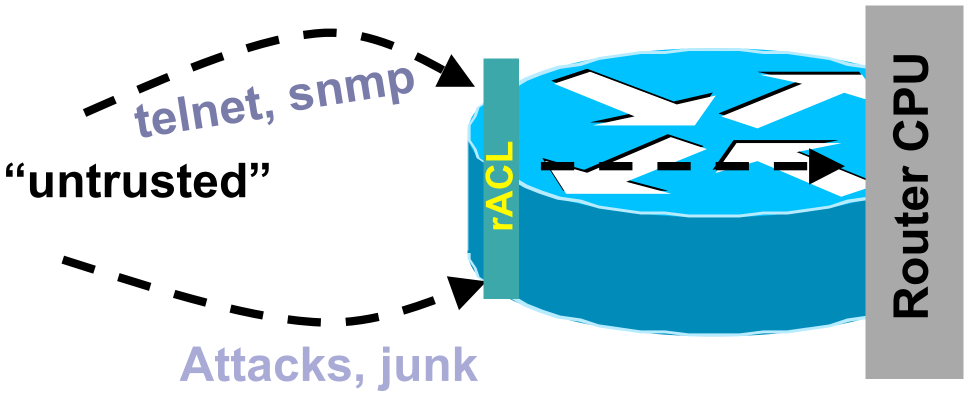
```
!Each hop returns a ttl exceeded (type 11, code 3) message and the final
destination returns an ICMP port unreachable (type 3, code 0)
access-list 110 permit icmp any routers_interfaces ttl-exceeded
access-list 110 permit icmp any routers_interfaces port-unreachable
```

- **Deny Any**

```
access-list 110 deny ip any any
```

© 2005 Cisco Systems, Inc. All rights reserved.

Receive ACLs



- **Contain the attack: compartmentalize**
  - **Protect the RP!**
- **Widely deployed and highly effective**
  - **If you have platforms that support rACLs, start planning a deployment**
  - **rACL deployments can easily be migrated to control plane policing (next topic)**
- **Limited platform support**
- **Lack of granularity**

© 2005 Cisco Systems, Inc. All rights reserved.

CONTROL PLANE POLICING (CoPP)

© 2004 Cisco Systems, Inc. All rights reserved.

Control Plane Policing (CoPP)

- **rACLs are great but**
  - **Limited platform availability**
  - **Limited granularity—permit/deny only**
- **Need to protect all platforms**
  - **To achieve protection today, need to apply ACL to all interfaces**
  - **Some platform implementation specifics**
- **Some packets need to be permitted but at limited rate**
  - **Think ping :-)**

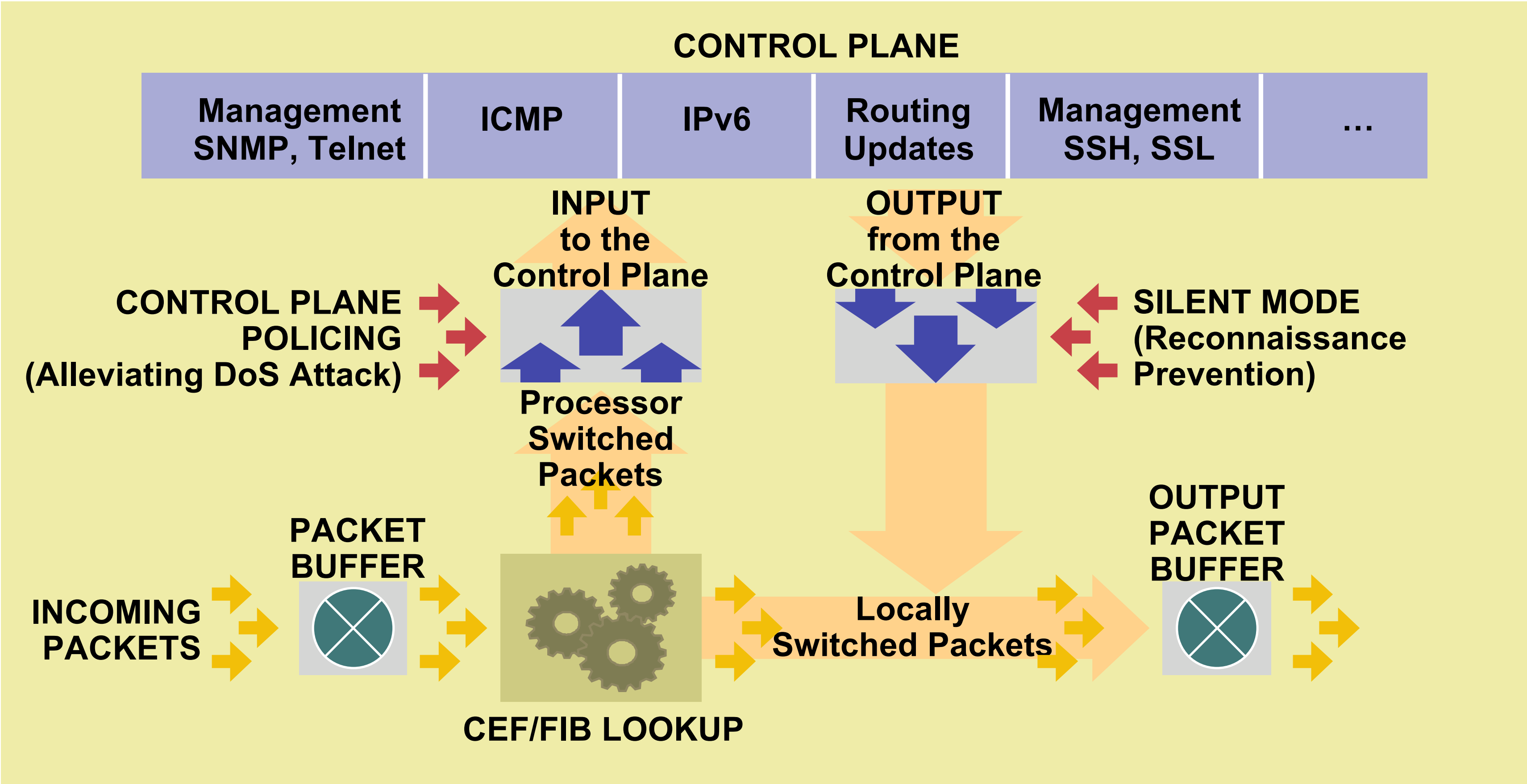
© 2005 Cisco Systems, Inc. All rights reserved.

Control Plane Policing (CoPP)

- CoPP uses the Modular QoS CLI (MQC) for QoS policy definition
- Consistent approach on all boxes
- Dedicated control-plane "interface"
  - Single point of application
- Highly flexible: permit, deny, rate limit
- Extensible protection
  - Changes to MQC (e.g. ACL keywords) are applicable to CoPP

© 2005 Cisco Systems, Inc. All rights reserved.

Control Plane Policing Feature



© 2005 Cisco Systems, Inc. All rights reserved.

Configuring CoPP

- **CoPP policy is applied to the control-plane itself**

```
Router(config)# control-plane
Router(config-cp)# service-policy input  control-
plane-policy
```

- **Three required steps:**
  - **Class-map**
    - **Setup class of traffic**
  - **Policy-map**
    - **Define the actual QoS policy: rate limiting and actions**
  - **Apply CoPP policy to control plane “interface”**

© 2005 Cisco Systems, Inc. All rights reserved.

Deploying CoPP

- Do you know what rate of TCP/179 traffic is normal or acceptable?
- rACL are relatively simple to deploy
    - I know that I need BGP/OSPF/etc., deny all else
- To get the most value from CoPP, detailed planning is required
    - Depends on how you plan to deploy it
    - bps vs. pps
    - in vs. out

© 2005 Cisco Systems, Inc. All rights reserved.

Deploying CoPP

- **One option: mimic rACL behavior**
  - Apply rACL to a single class in CoPP
  - Same limitations as with rACL: permit/deny only
- **Recommendation: develop multiple classes of control plane traffic**
  - Apply appropriate rate to each
  - "Appropriate" will vary based on network, risk tolerance, risk assessment
- **Flexible class definition allows extension of model**
  - Fragments, TOS, ARP

© 2005 Cisco Systems, Inc. All rights reserved.

Step 1: Classification

- **Identity traffic destined to routers**
  - Some is easy (BGP, OSPF, etc.)
  - What else?
- **NetFlow can be used to classify traffic**
  - Need to export and review
- **Classification ACL can be used to identify required protocols**
  - Series of permit statements that provide insight into required protocols
  - Initially, many protocols can be permitted, only required ones permitted in next step
- **Regardless of method, unexpected results should be carefully analyzed → do not permit protocols that you can't explain!**

© 2005 Cisco Systems, Inc. All rights reserved.

Step 2: Policy Creation

- **Define classification policy**
  - Group IP traffic types identified in step 1 into different classes
    - Critical—traffic crucial to the operation of the network
    - Important—traffic necessary for day-to-day operations
    - Normal—traffic expected but not essential for network operations
    - Undesirable—explicitly “bad” or “malicious” traffic to be denied access to the RP
    - Default—all remaining traffic destined to RP that has not been identified
- **Create ACLs to define traffic**
  - Use ACLs with unique numbers to represent each class defined above
- **Create class maps to collect access-lists**
  - Associate the traffic separation ACLs developed above with class-maps with “descriptive” names
    - Use the simple “match access-group <*acl-number*>” format
    - Add the “match protocol” format as necessary (e.g. ARP)
    - Use class-default to identify all unclassified packets

© 2005 Cisco Systems, Inc. All rights reserved.

Step 2: Policy Creation

Packet Classification

The Router IP Address for Control/Management Traffic Is 10.1.1.1

- Critical—ACL 120
- Important—ACL 121
- Normal—ACL 122
- Undesirable—ACL 123
- Default—no ACL required

```
! CRITICAL -- Defined as routing protocols
access-list 120 permit tcp host 10.1.1.2 eq bgp host 10.1.1.1 gt 1024
access-list 120 permit tcp host 10.1.1.2 gt 1024 host 10.1.1.1 eq bgp
access-list 120 permit tcp host 10.1.1.3 eq bgp host 10.1.1.1 gt 1024
access-list 120 permit tcp host 10.1.1.3 gt 1024 host 10.1.1.1 eq bgp
access-list 120 permit ospf any host 224.0.0.5
access-list 120 permit ospf any host 224.0.0.6
access-list 120 permit ospf any any
```

```
! IMPORTANT -- Defined as traffic required to access and manage the router
access-list 121 permit tcp host 10.2.1.1 host 10.1.1.1 established
access-list 121 permit tcp 10.2.1.0 0.0.0.255 host 10.1.1.1 range 22 telnet
access-list 121 permit tcp host 10.2.2.1 host 10.1.1.1 eq 443
access-list 121 permit udp host 10.2.2.2 host 10.1.1.1 eq snmp
access-list 121 permit udp host 10.2.2.3 host 10.1.1.1 eq ntp
```

© 2005 Cisco Systems, Inc. All rights reserved.

Step 2: Policy Creation

Packet Classification (Cont.)

- Critical—ACL 120
- Important—ACL 121
- Normal—ACL 122
- Undesirable—ACL 123
- Default—No ACL required

```
! NORMAL -- Defined as other traffic destined to the router to track and limit
access-list 122 permit icmp any any ttl-exceeded
access-list 122 permit icmp any any port-unreachable
access-list 122 permit icmp any any echo-reply
access-list 122 permit icmp any any echo
access-list 122 permit icmp any any packet-too-big
```

Allows router originated traceroute

```
! UNDESIRABLE -- Defined as traffic explicitly blocked (known malicious)
access-list 123 permit udp any any eq 1434
access-list 123 permit ip any any fragments
```

Use “permit” Here because the police action will be “drop/drop” for conform/exceed-actions

© 2005 Cisco Systems, Inc. All rights reserved.

Step 2: Classification Policy

- **Create class-maps to complete the traffic-classification process**

  Use the access-lists defined on the previous slides to specify which IP packets belong win which classes

- **Class-maps permit multiple match criteria, and nested class-maps**

  match-any requires that packets meet only one "match" criteria to be considered "in the class"

  match-all requires that packets meet all of the "match" criteria to be considered "in the class"

- **A "match-all" classification scheme with a simple, single-match criteria will satisfy initial deployments**

- **Traffic destined to the "undesirable" class should follow a "match-any" classification scheme**

```
! Define a class for each "type" of traffic and associate the appropriate ACL
class-map match-all CoPP-critical
  match access-group 120
class-map match-all CoPP-important
  match access-group 121
class-map match-all CoPP-normal
  match access-group 122
class-map match-any CoPP-undesirable
  match access-group 123
```

© 2005 Cisco Systems, Inc. All rights reserved.

Step 3: Policing Policy

Class-maps Defined in Step 2 Need to Be "Enforced" by Using a Policy-Map to Specify Appropriate Service Policies for Each Traffic Class

- **For example:**
  - For critical traffic, no policy is specified—critical traffic has unrestricted access to the route processor
  - For undesirable traffic types, all actions are unconditionally "drop" regardless of rate
  - For important and normal traffic types, all actions are "transmit" to start out
  - For default traffic, rate-limit the amount of traffic permitted above a certain bps
  - Note: all traffic that fails to meet the matching criteria belongs to the default traffic class, which is user configurable, but cannot be deleted

```
! Example "Baseline" service policy for each traffic classification
policy-map CoPP
  class CoPP-critical
    police 8000 1500 1500 conform-action transmit exceed-action transmit
  class CoPP-undesirable
    police 8000 1500 1500 conform-action drop exceed-action drop
    <or simply>
    drop
  class CoPP-important
    police 125000 1500 1500 conform-action transmit exceed-action transmit
  class CoPP-normal
    police 15000 1500 1500 conform-action transmit exceed-action transmit
  class class-default
    police 8000 1500 1500 conform-action transmit exceed-action drop
```

© 2005 Cisco Systems, Inc. All rights reserved.

Step 4: Apply Policy to “Interface”

Apply the Policy-Map Created in Step 3 to the “Control Plane”

- The new global configuration CLI “control-plane” command is used to enter “control-plane configuration mode”
- Once in control-plane configuration mode, attach the service policy to the control plane in either the “input” or “output” direction
  - Input—applies the specified service policy to packets that are entering the control plane
  - Output—applies the specified service policy to packets that are exiting the control plane
- A service policy may be applied to the control plane in one or both directions (two separate statements)

Centralized CoPP:

```
Router(config)# control-plane
Router(config-cp)# service-policy [input | output] <policy-map-name>
```

Distributed CoPP (DCoPP):

```
Router(config)#control-plane slot <n>
Router(config-cp)#service-policy input control-plane-in <policy-map-
name>
```

```
! Example
! This applies the policy-map to the Control Plane
control-plane
  service-policy input CoPP-In
```

© 2005 Cisco Systems, Inc. All rights reserved.

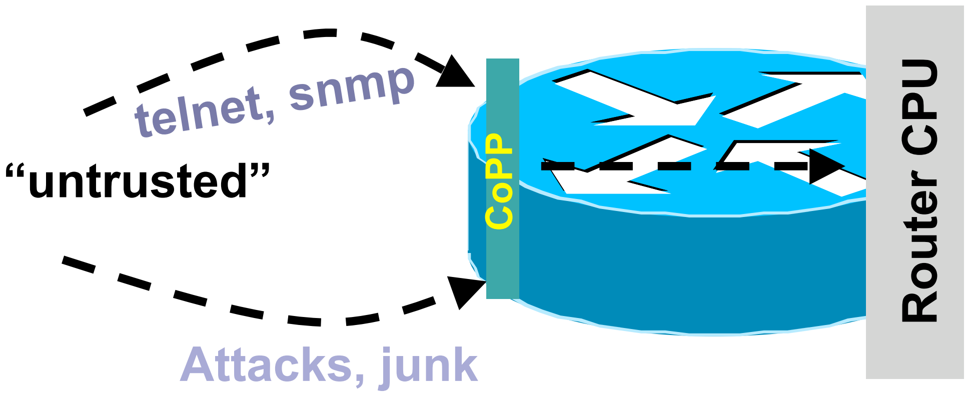
Show Policy-map Command

```
Router#show policy-map control-plane input
 Control Plane

  Service-policy input: CoPP

    Class-map: Classify (match-all)
      16 packets, 2138 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group 120
      police:
          cir 125000 bps, bc 1500 bytes
        conformed 16 packets, 2138 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          transmit
        conformed 0 bps, exceed 0 bps

    Class-map: class-default (match-any)
      250 packets, 84250 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      police:
          cir 8000 bps, bc 1500 bytes
        conformed 41 packets, 5232 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        conformed 0 bps, exceed 0 bps
Router#
```

- Service-policy input: CoPP — Service Policy Map name and “direction”
- Class-map: Classify (match-all) — Class-map name and “criteria”
- 16 packets, 2138 bytes — Number of packets/bytes matched
- Match: access-group 120 — ACL name/number
- police (Classify) — police “action”
- Class-map: class-default (match-any) — Default class
- police (class-default) — police “action”

© 2005 Cisco Systems, Inc. All rights reserved.

Control Plane Policing



- Superset of rACL: start planning your migrations
- Provides a cross-platform methodology for protecting the control plane
    - Consistent "show" command and MIB support
- Granular: permit, deny and rate-limit
- Default-class provides flexibility
- Platform specifics details: centralized vs. distributed vs. hardware

© 2005 Cisco Systems, Inc. All rights reserved.

Agenda

- Infrastructure Security Overview
- Preparing the Network
- Router Security: A Plane Perspective
- Tools and Techniques
- Conclusions

© 2005 Cisco Systems, Inc. All rights reserved.

Summary

- **Understand the risk**
  - **Take infrastructure protection into account in network design**
- **Want to deploy voice? Want to deploy video? Want to deploy xyz?**
  - **All services deployment depend on an available infrastructure**
- **Understand the techniques/features and apply them appropriately**
  - **Edge filters: iACLs**
  - **Control plane traffic filtering: rACL**
  - **Next-phase of control plane filtering (including policing): CoPP**
- **Each feature has pros/cons**
  - **Ultimately, mix and match as needed: remember defense in depth**

© 2005 Cisco Systems, Inc. All rights reserved.

Summary

- **Review your current protection schemes**
  - Identify gaps and areas of exposure
  - Develop a plan for protection
- **Next steps:**
  1. Begin to classify network traffic
  2. Use classification data and platform mix to determine appropriate protection schemes
- **Start planning your deployments!**
  - Can be difficult but certainly worthwhile!
  - Many customers have widespread deployments and have seen the benefits

© 2005 Cisco Systems, Inc. All rights reserved.

Interesting Links

- **iACL deployment guide**

  http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

- **rACL deployment guide**

  http://www.cisco.com/warp/public/707/racl.html

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1829/products_feature_guide09186a00805e9255.html#wp1047803

- **CoPP deployment guide**

  http://http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guide09186a008052446b.html

- **Cisco Network Foundation Protection (NFP)**

  http://http://www.cisco.com/en/US/products/ps6642/products_ios_protocol_group_home.html

- **SP security archive**

  ftp://ftp-eng.cisco.com/cons/isp/security/

- **NANOG**

  http://www.nanog.org/previous.html

  http://www.nanog.org/ispsecurity.html

© 2005 Cisco Systems, Inc. All rights reserved.