



Building Authenticated and Responsive Networks that are Faster and More Efficient

Military Networking Protocol

Industry Day Briefing

Tim Gibson, Ph.D.

*You cannot make the network smarter
unless you give it more brains too*

mail.darpa.mil|arlington.virginia.us.northamerica

mail.mod.uk|london.uk.europe

18 December 2008

mail.usarmy.mil|4-54.Inf.194thArmdBde.XVIII Airborne Corps<user digital signature>,<user public key>, true machine IP & port, true machine name <digital signature>, <public key>

Distribution A: Approved for Public Release, Distribution Unlimited



Military Networking Protocol Concept

What we want to do with our networks



- Manage network priorities and bandwidth based on unit and mission
 - If 3rd Brigade is having problems, how do they get a higher network priority?
 - Today, they don't
- We want to know who is on the network
 - If someone is hacking the network, we want to go find them...
 - We cannot easily do this

Network Command and Control by unit
prioritization and bandwidth allocation

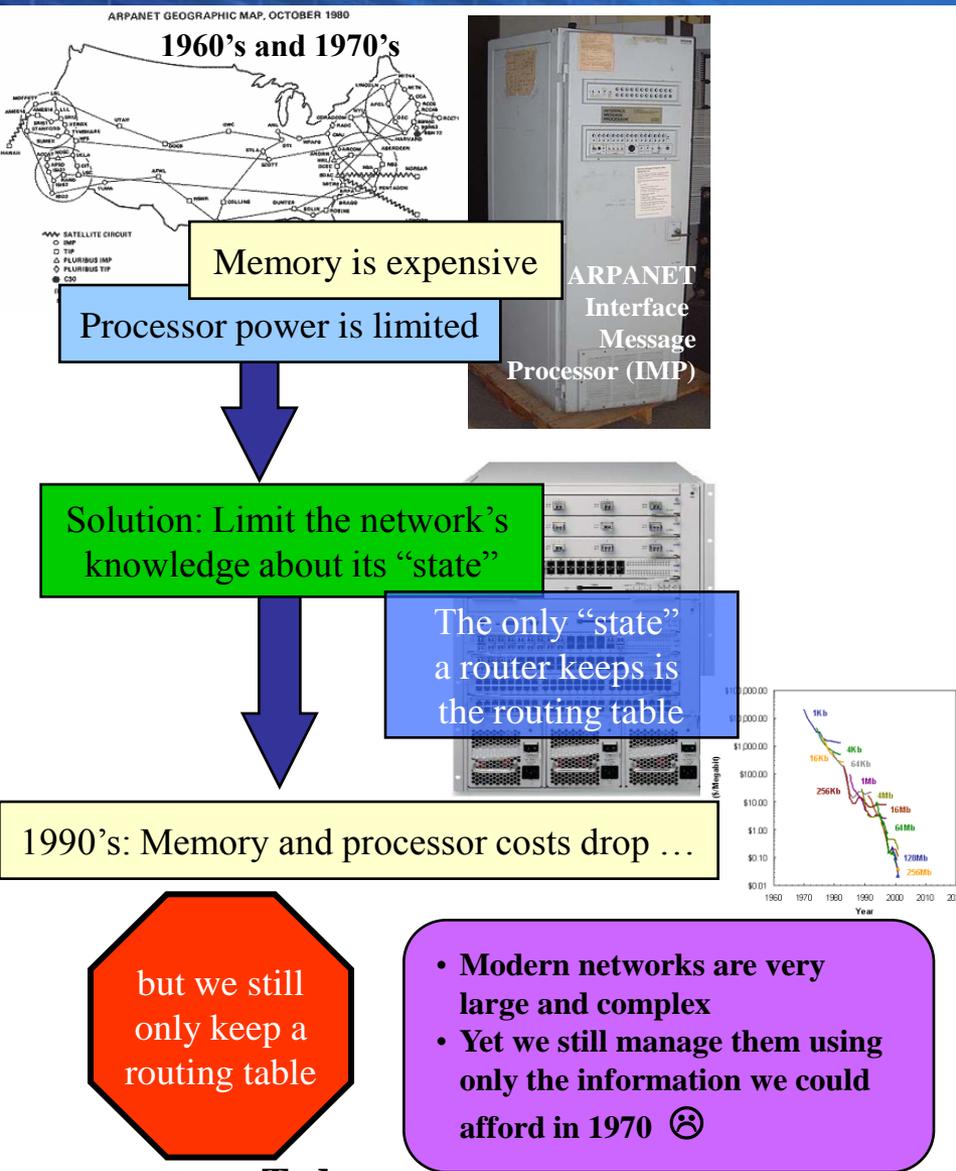
Full attribution

- The network hardware is already hard to configure
 - Let's not make it harder

Reduce manpower, training,
and procurement costs

We need to make configuring and managing the network easier
and manage by unit
and know who is using it

Deliver a network with military utility: management by command priorities,
full attribution, simple to configure



[192.168.001.213]

IP addresses are a hierarchical design ...

... but they are distributed randomly on a first come first served basis ... and they change over time ... and



they are pretty useless when trying to identify people

Basic network theory says you should have addressing identifiers for:

- The user
- The machine
- The routing indicator

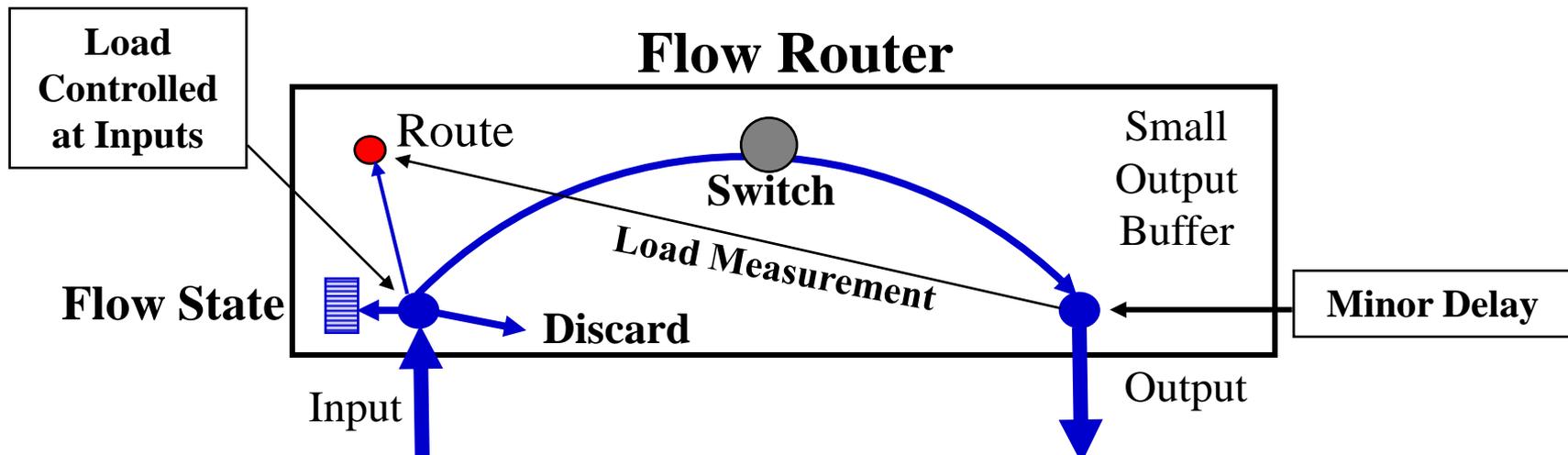
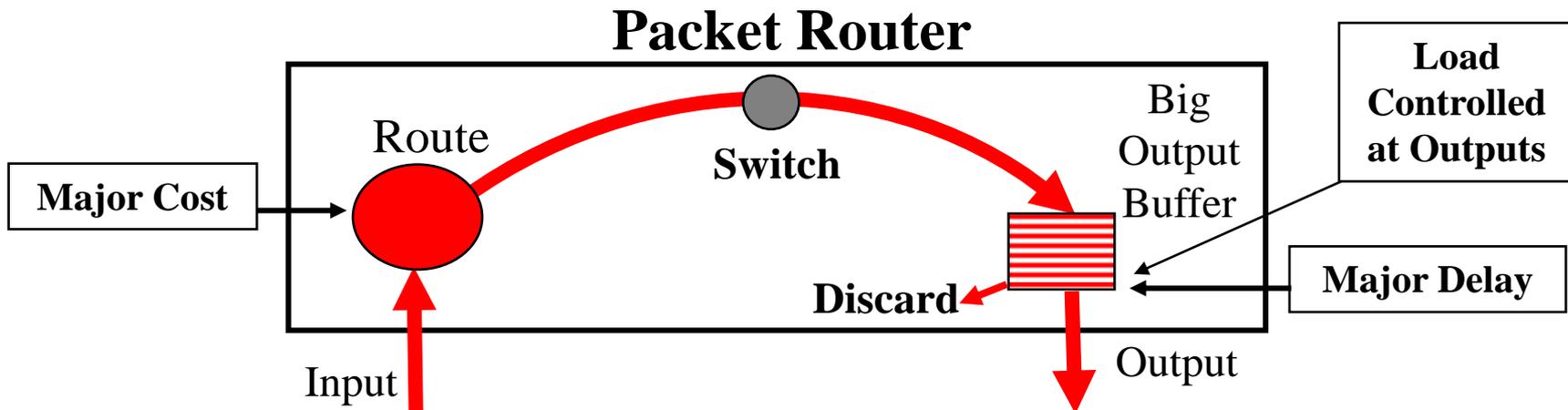
We use the IP address for all three and network address translation devices change the IP addresses!

Result → Having an IP address only gives you the region (e.g., Europe) and the provider (e.g., BT)



If only we could ...

- Tag some kind of information onto the flow so we could get some attribution without adding too much overhead ...
 - Why not use the data portion of a TCP connection request? Is there any reason we have to send headers and an empty data field?
 - This is one approach, there are likely others
- Manage individual flows with a router ...
 - We've been talking about managing individual flows for years, too bad we cannot actually make a flow router



By using faster processors and additional memory in each line card, the route engine can be less capable
 Router workload is distributed between the line cards and route engine

Distributed Computing: What a concept!



But ... it turns out we do we have flow routers

Comparison of Flow and Normal Routers



- Normal routers handle every packet independently
- “Flow” based on the source/destination and address/port and the protocol
- Flow routers were not feasible to make six years ago because of memory costs ... they are feasible now
- Using commodity processors (network processors and FPGAs) and cheaper memory, the routers are lighter (9x), smaller (12x), use less power (5x) and cost less (3.5x) than conventional routers

Manufacturer	Comparable Layer 3 Router	Anagran	Percent Improvement
Speed (4 x 10 Gbps full duplex cards)	40	40	
Cubic inches	4,000	714	82.2%
Weight (lbs)	100	24	76.0%
Gigabit Ethernet ports per RU	3.5	48	1371.4%
Price per Gigabit Ethernet port	\$5,000	\$1,667	66.7%
Watts	1,300	300	76.9%
Price	over \$250,000	\$80,000	over 70%
Watts / Gbps	32.5	7.5	76.9%
Estimated Cooling Cost (W*.8)	1,040	240	
Total Energy Cost (Watts / Gbps)	58.5	13.5	

Developed in the DARPA Control Plane program



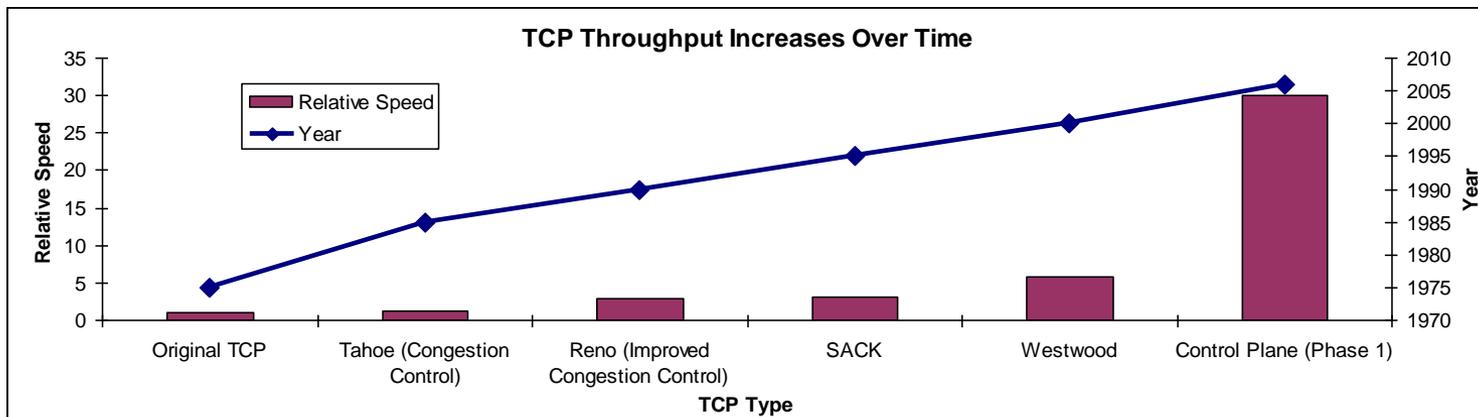


DARPA Control Plane Overview

Fundamental Issues and Results



- Control Plane addresses TCP/IP's fundamental design constraint:
 - Memory and processing power were expensive when TCP/IP was designed
 - “Talking to” the network requires too much memory, so we did not do it
 - TCP transmission speed entirely based upon maximum packet size, delay, and error → link speed is not a factor
 - Memory and processing power are now commodities
 - If you can gather information from the network you should be able to improve performance
 - The capability to “talk to” the network was Control Plane’s basic premise
- In 2003, increasing performance by a factor of ten seemed “DARPA Hard”
 - In thirty years, the Internet research community raised TCP/IP performance by a factor of five
- **“Talking to the network” opens unexpected possibilities**
 - **Control Plane Phase 1 exceeded the end of program Go/No-Go speed metric**
 - **Provides packet networks with circuit predictability and throughput**



Distribution A: Approved for Public Release, Distribution Unlimited



DARPA Control Plane Overview

Phase 2 Test Results for a Flow Based System



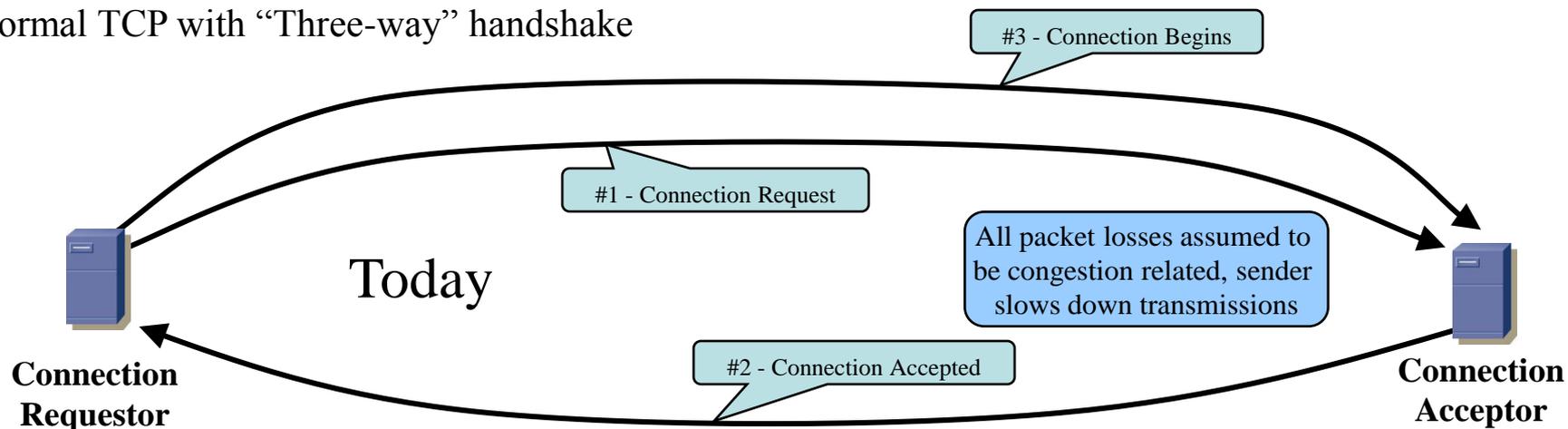
	Phase 2 Metrics	Hewlett-Packard Software with Anagran Flow Router
End-to-end throughput	6x	42.8x
Fairness to conventional traffic	Degrades < 5%	5x (400%) <u>improvement</u>
Multiplexing Throughput	65% for two links	70.5%
Additional users with same performance	2x	7.0x



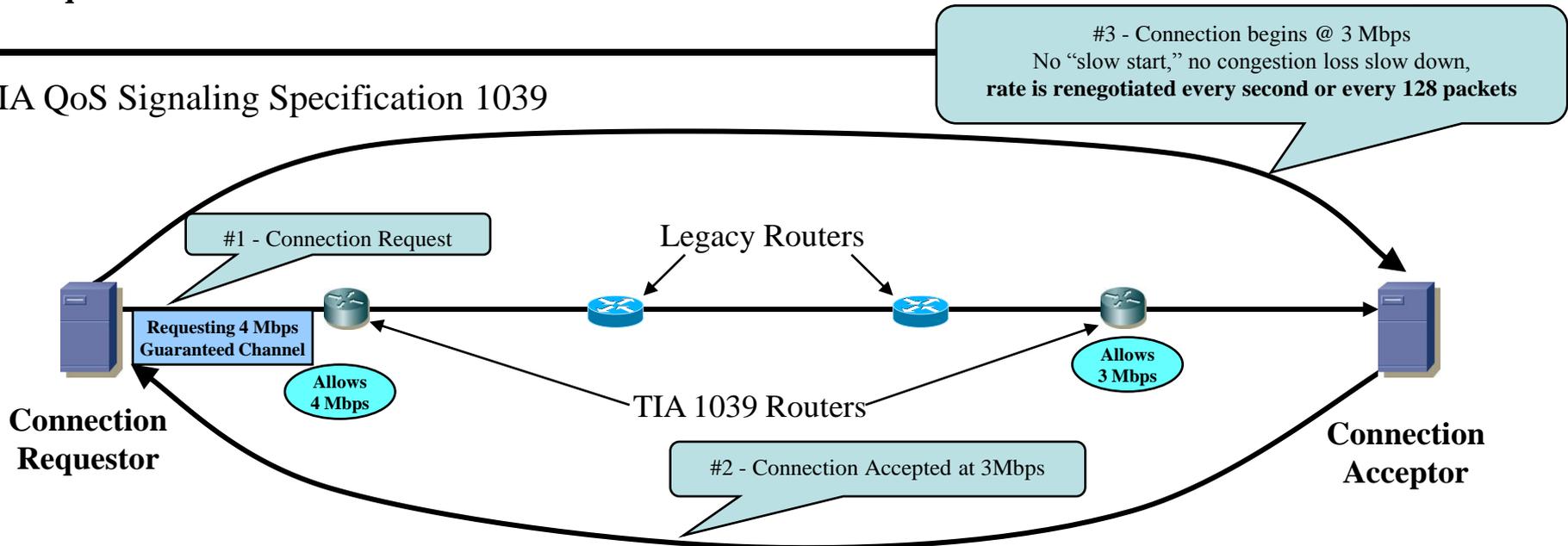
Hewlett-Packard and Anagran Solution –TIA and ITU specs Establishes an *Explicit Rate* that is constantly renegotiated



Normal TCP with “Three-way” handshake



TIA QoS Signaling Specification 1039





Signaling Specifications

TIA 1039 and ITU Documents Y.FLOWREQ and Q.FLOWSTATESIG



- Precedence (64+ levels)
- Pre-emption Priority (64+ levels)
- Delay Priority (64+ levels)
- Quality of Service
 - Rate is renegotiated every second or 128 packets (whichever comes first)
 - Mandatory Service Requirements
 - Available Bit Rate
 - Maximum Rate
- Burst Tolerance
- Charging Direction
- ITU Activity
 - Sponsored into the ITU by United Kingdom and British Telecom
 - Supported in the ITU by BT (UK), KT (Korea), NTT (Japan), China Telcom, Malaysian Telcom
 - Validated as a requirement by SG13 (Y.FLOWREQ), now in SG11 (Q.FLOWSTATESIG)

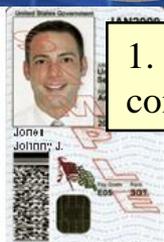
The TIA -1039 signaling specification is a standard and you may purchase it from the Telecommunications Industry Association (see: www.tia.org)



What's changed (and what hasn't)?

- ✓ Memory and processing power are much cheaper today than when TCP/IP was designed
- It is not feasible to eliminate the Internet Protocol addressing scheme and start from scratch
- **Providing attribution** or having role/identity based management is not practical **with just an IP address** → we keep trying and it **just doesn't work**
- The overhead of full attribution and identification data in every packet is impractical
- ✓ The overhead is manageable if you only send the identification data at the beginning of a data connection and update it with subsequent packets
 - Requires you to manage and track connections (*aka*, flows)
 - Tracking connections means tracking connection state → memory and processing
 - We do this today for completely different reasons and with totally dissimilar data in Control Plane ... but we know it works
- Result: A command and control system for the network should be possible by managing connections that contain identification and attribution data
 - The system should also be legacy IP transparent and compatible

... the key to making tomorrow's networks better is to use the things we have now that weren't available forty years ago: memory and processing power ... *Tim Gibson, DT07*



1. Users authenticate themselves to their communications or computing device

*Example: Johnny Jones, E4,
<digital signature>, <public key>,
true machine IP & port,
true machine name*

2. A local network device, called a Network Controller (NC)* is programmed with the organization and unit it “fronts for”

*Example: Tactical Command Post, 4-54 Inf, 194th
Armd Bde, XVIII Airborne Corps, US Army,
supporting 2nd Marine Division,
Location (optional): Iraq, NW, <digital signature>,
<public key>*



No special training or knowledge is needed to program the Network Controller



3. When a user makes a connection request, the network controller combines all the identity data in the new connection request

IP Hdr

TCP|UDP Hdr

Packet payload: Johnny Jones, E4, Tactical Command Post, 4-54 Inf, 194th Armd Bde, XVIII Airborne Corps, US Army, supporting 2nd Marine Division, Location (optional): Iraq, NW, <user digital signature>, <user public key>, true machine IP & port, true machine name <digital signature>, <public key>, Network Controller Name <digital signature>, <public key>

An initial connection request with attribution data

These packets pass through normal IP networks or a black core, allowing attribution and identification between “islands”

4. The NC at the other end decides whether it wants to accept the connection



5. Options once the connection is allowed and established:

- Log the connection
- Verify the connection
- Verify the connection’s path
- Periodically conduct challenge and response

Network Controllers replace most, if not all, conventional routers within the “controlled” network



Caveats to the MNP BAA and this presentation



- Do we have to team with Control Plane performers to have a successful proposal? **Absolutely not!**
- Do we have to use TIA-1039 or a related protocol?
 - No! TIA-1039 will need modifications to meet the MNP goals
 - Choosing or not choosing to use TIA-1039 is your choice and does **not** need to be explained or justified in your proposal

Regardless of what method you choose to meet the program's objectives ...
You **must** explain what you propose to do in detail!



- Do we have to use flow management in our proposal?
 - Absolutely not. While it has been demonstrated that flow management is now feasible, there are other techniques that may be capable of meeting the program's goals
- You should explain very thoroughly why your approach will work
 - Regardless of what technique you use
- MNP traffic will run on and through the Internet
 - Your proposal should explain how your work will address the standards community



What this program will deliver

- **A box** that replaces routers in tactical units and installations
 - Providing unit identification and managing priorities
 - Verifying attribution
 - Simpler to configure than conventional routers
- **Software** modifications to computer operating systems that work with “the box” and a user’s tokens to provide attribution

Why is it going to work

- New FPGA and software routers reduce experimentation and implementation costs
- DARPA Control Plane proved that stateful management of packet flows works
 - You probably cannot manage individual packets, there are just too many of them
 - ... but you can manage individual flows and connections (aggregations of packets)
 - **The current Control Plane solution does NOT address the MNP problem**
 - Control Plane does not address individual attribution, unit identification, manage network resources by unit, and it isn’t easier to configure
 - It does show we can do this ...
 - **There are other ways to do stateful flow management that should also be explored**

Tactical military network speeds don’t require a hardware router; neither do most commercial edge locations
You can do it with a laptop!



Program Metrics (Part 1)



Metric	Phase 1	Phase 2	Phase 3
Configure network controller (NC) with identity data (e.g., unit & location) → One time cost	5 minutes	Same	Same
Time to distribute network C2 instructions and have all network control devices in test respond (see scalability)	20 minutes	10 minutes	5 minutes
Network command level supported	Specific unit	“Part of unit*”	“Supporting unit**”
Scalability: Physical Network Controller devices tested	20	100	200
Network speeds supported	100 Mbps	1 Gbps	10 Gbps
Ability to allow or refuse connections: without attributions (i.e., a normal IP packet) or with attributions (i.e., one of the new packets)	Yes	Yes	Yes
Level of aggregation when filtering (allowing or refusing) connections with new attribution packets*	Specific individual Specific unit	“Part of unit*”	“Supporting unit**”
Cost—No particular number but the solution with the minimum cost will be given preference assuming all other metrics are met	Minimum	Minimum	Minimum

* “Part of a unit” means any unit that is part of a parent unit is included in parent unit instructions. For example, 3rd Brigade, 9th Infantry Division is “part of” the 9th Division

** “Supporting” units respond to commands given to units they support but are not “part of” the unit. For example, 3-3 Field Artillery is “part of” the Divisional Field Artillery, but it is direct “support of” 3rd Brigade, so priorities for 3rd Brigade can be inherited by 3-3 FA



Program Metrics (Part 2)



Metric	Phase 1	Phase 2	Phase 3
Priority levels supported	≥ 32	≥ 32	≥ 32
Generate all NC configuration files for an Army division (300–400 network controllers)	≤ 6 hours	≤ 3 hours	≤ 1 hour
NC boot-up time with unit ID and a pre-loaded configuration file	≤ 4 minutes	≤ 2 minutes	≤ 2 minutes
NC boot-up with unit ID and without a configuration file (requires fetching from another NC)	≤ 20 minutes	≤ 10 minutes	≤ 4 minutes
Scalability: Virtual devices tested	≥ 200	$\geq 1,000$	$\geq 10,000$
Speed degradation compared to network system without MNP	$\leq 5\%$	$\leq 2\%$	None
Attribution level tracked	Individual	Individual	Individual
Connection mistrust level supported	Log Verify connection with other NC	Tunable challenge response on the connection	Verify path
Connection type supported	Connection oriented (TCP)	Connection (TCP) and Connectionless (UDP)	Connection (TCP) and Connectionless (UDP)
Client software	---	---	Win & Linux
Ability to provide unit level functionality for attribution and prioritization without client (end host) modification	Yes	Yes	Yes



- Metric: Time to distribute network C2 instructions and have all network control devices in test respond is X minutes
 - Must the devices all change their prioritization scheme simultaneously? No
 - Must the configuration be changed simultaneously? No ... but you cannot crash, disrupt, or partition the network
- Network command level supported:
 - Specific unit, “Part of unit,” “Supporting unit”
- Level of aggregation when filtering (allowing or refusing) connections with new attribution packets:
 - Specific individual, Specific unit, “Part of unit,” or “Supporting unit”
- Connection mistrust level supported:
 - Log, Verify connection with other Network controllers, Tunable challenge response for the connection, Verify the path
- Ability to provide unit level functionality for attribution and prioritization without client (end host) modification



BAA Topic Areas



- Two topic areas:
 - **Technical Development**
 - Developing network controllers and supporting software
 - Includes network attribution and prioritization schemes, command and control system, self-configuration
 - **Testing and Security Verification**
- Proposers applying to the *Testing and Security Verification* area may not apply to the *Technical Development* area
- Agent: SPAWAR-SSC San Diego, CA



Change #1 to the BAA



- AMENDMENT 1 to DARPA-BAA-09-11 Military Networking Protocol (MNP) Military Networking Protocol
 - The purpose of Amendment 1 is make the following changes summarized and detailed below:
 - Page 19, Section 4.3.2.2 Volume II, Cost Proposal, is replaced in its entirety with the following:

4.3.2.2 Volume II, Cost Proposal – {No Page Limit}

Cover sheet. Format to be followed using the template provided as APPENDIX 2 to this announcement. Detailed cost breakdown to include:

(1) Total program cost broken down by ...

- Total change is four pages long



Expansion of the MNP BAA #1

(What is Gibson really looking for?)



- **Section 1.2: “The MNP program is not developing technology to replace encryption (e.g., IP-Sec, HAIPE, VPN, etc.) nor are key management, key distribution, or key revocation program requirements”**
- Why not? Well, we may not need it ...
 - Military networks are normally link or IP layer encrypted
- MNP Network Controllers may be implemented in software on commodity hardware or FPGA based devices
 - There are issues with certifying software or FPGA based encryption devices
- MNP Network Controllers will be deployed on large numbers
 - There are trust and scalability issues with certifying scalable distributed key management systems
- Assume you have a hardware token
 - Attribution: **REQUIRED**
 - OPSEC Handshake: “Should be capable of ...”
 - Authentication and Non-Repudiation: Very nice, your call
 - Network Administrator selectable packet encryption: Very nice, your call

NSA certifiable encryption:
Not part of this program



Expansion of the MNP BAA #2

(What is Gibson really looking for?)



- **3.2 COST SHARING/MATCHING ...**
- **Cost sharing is not required for this particular program;**
however, cost sharing will be carefully considered where there is an applicable statutory condition relating to the selected funding instrument (e.g., for any Other Transactions under the authority of 10 U.S.C. § 2371)
- **Cost sharing is encouraged where there is a reasonable probability of a potential commercial application** related to the proposed research and development effort
- If you decide to do cost sharing, make sure you clearly state how you are doing it (manpower, equipment, etc.) and its value
 - For example, do not use “at cost” or discounted manpower rates in the Cost Proposal and expect reviewers to recognize this as a cost share
 - **Specific information is required on the cover sheets**



Expansion of the MNP BAA #3

(What is Gibson really looking for?)



• Transition

- Section 4.3.1.1 Volume I, Technical and Management Proposal ...
 - *Proposals should address the proposer's plans for technology transition and commercialization in detail. Transitioning the MNP into a commercially available product is important to the government and is addressed in the evaluation criteria ...*
- We really want this capability and these devices; assume it is going to happen!
 - Address manufacturing , support, and sales in the proposal
 - A good plan: Manufacturing partner on the team and **participating** in Phase 1
 - A 'not as good' plan: Letter from a manufacturer's company officer that says. "If you pass the Phase 1 DARPA metrics we will consider whether it is in our commercial interests to possibly participate in future phases ..."
- Teaming with large legacy network and router manufacturers
 - **Network Controllers provide a major shift in network operations and economics**
 - If you have a network equipment manufacturer on your team, your proposal should address why developing, manufacturing, and selling MNP Network Controllers **fits the network equipment manufacturer's long-term business plan**

MNP is a SECRET program; products may become ITAR restricted **commercial sales** items



Expansion of the MNP BAA #4

(What is Gibson really looking for?)



- Section 4.3.1: Proposal Format
 - The Technical and Management Proposal (Volume 1) shall not exceed sixty (60) pages
 - **You get 60 pages, there are no page number requirements for the individual sections**
 - Do not whine, I am giving you more flexibility
- Section 4.3.1, sub-Section II, paragraph F
 - In addition to naming key personnel, proposals will include key persons' Domicile (City and State) and every location (City, State, and Distance from Domicile) where each person will work at least 25% of their time
 - I have no problem with teams located in one location
 - I have no problem with distributed teams
 - Distributed team management mechanisms should be addressed in the proposal's management plan
 - **I do have problems with distributed teams that are represented as being in one location and have no management plan (yes, this has happened)**

Explain what you are doing, how it works, and how you will manage your work



Expansion of the MNP BAA #5

(What is Gibson really looking for?)



- **Section 6.10.4 Earned Value Management (EVM)**

- DARPA will use **commercial** standards of Earned Value Management (EVM) to manage this program
- Proposers selected for funding must be prepared to use—and possibly make changes to—their internal EVM reporting procedures
- If a proposer selected for funding does not use EVM, at a minimum the following must be tracked and provided: “fully loaded” cost per month per major task; milestones or tasks projected for completion per month per major task
- Large parts of MNP program cost will likely be labor, particularly in the early phases
 - **Using EVM will assist in the early identification of instances in which the performer is “on budget” but behind deliverables (*i.e.*, actually behind schedule and over budget)**

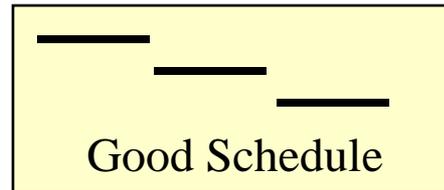


Expansion of the MNP BAA #6

(What is Gibson really looking for?)



- How many phases do you expect?
 - Three
- Can we just have one or two long phases instead?
 - Three
- How long should each phase last and how long will the program be?
 - It is up to you, but do NOT do this →
- How much money does DARPA have allocated for this program?
 - More than enough to fund the best proposal(s)





Military Networking Protocol Security



- This program is **SECRET**
 - Collateral SECRET is—by definition—NOFORN
 - The Security Classification Guide (SCG) is FOUO and is available upon receipt of your CAGE code and Security POC
 - **Be safe: Get the SCG and read it!**
 - Your submission may be classified
 - If so, request a DD254 in accordance with the BAA
- Discussion Points
 - Large portions of the program are unclassified
 - Effectively all basic and applied research is unclassified, to include authentication and attribution methods
 - Academic researchers without clearances should be able to participate
 - What is classified?
 - Unique capabilities, some performance and testing results, all implementation software, all vulnerabilities
 - **Specifics are in the security classification guide: get it and read it!**



Military Networking Protocol Publications



- MNP is developing an attributable networking protocol for military data networks
 - **The MNP program is classified** but includes some unclassified research
- All publications—classified and unclassified—by all performers and sub-contractors will require publication review prior to publication
 - Both DoD Instruction 5230.27 (Subject: Presentation of DoD-Related Scientific and Technical Papers at Meetings) and USD-ATL Memo on “Contracted fundamental Research” dated 26 June 2008 say:
 - *“Contracted Fundamental Research ... shall not be considered fundamental in those rare and exceptional circumstances where the 6.2-funded effort presents a high likelihood of disclosing performance characteristics of military systems ...”*
 - DARPA Instruction #65, Clearance of DARPA Information for Public Release
 - *If a potential awardee does not wish to participate because DARPA requires pre-publication review, or places restrictions on public access, then other sources are to be sought ...*
- Contract Primes: Ensure potential academic performers allow publication review before teaming with them
- Contract primes should plan on reviewing all publications for their team and providing DARPA with a written assessment based on the MNP SCG of why any proposed publication is unclassified or classified
 - Expect to see this requirement in the contract

If an academic institution's policies will not allow publication review or participation in a program with potential export restrictions, they should not part of this program



Writing for the proposal for the reviewers



- Reviewers are government employees with technical backgrounds
- They are not necessarily buzz-word compliant
 - Spell out acronyms the first time
 - Do not make up new and cute terms because you think it will make your proposal easier to remember → It actually does make it easier to remember ... be careful what you ask for
- Be consistent and precise in your terminology
 - The devices we are making are called Network Controllers (NC)
 - Not routers, firewalls, or dynamic hypervisor enabled high-speed network data handling devices (DHEHSNDHD) ...
 - There may be different types of Network Controllers in your design
 - That's fine → Explain why different types are needed, what the differences are, and keep the names simple and logical
 - The other thing we are making is host level software



Other things to know about the reviewers



- We will likely receive 10–20 proposals, each with up to 60 pages
 - That is 600–1,200 pages of technical material
- Reading a proposal normally requires 2–3 hours
 - Reviewers often read proposals singly, or block a day and read several in a session
 - If the proposal is poorly written it is hard to understand
 - If we do not fully understand what you are saying, we have to either ask for clarification through the Contracting Officer or figure it out on our own
 - You do not want either ...
- A suggestion
 - Give your proposal to someone with no involvement in your team and have them read it for two hours
 - Have them tell you—without prodding or coaching—what they think you are proposing to do

- Developing a system that
 - Provides attribution to the individual user,
 - Pairs that attribution with a unit-level ID,
 - Enabling user/unit attribution,
 - Command and control of network resources
 - Over existing encrypted military communications systems

By

- Developing novel network controllers (**a box**) and new host network **software**
 - We need a network command and control system, not another authentication, encryption, multi-level security system
- Key challenges for this program are in developing:
 - The attribution scheme and supporting protocols
 - Network equipment that automatically configures itself
 - A true networked command and control system for the network

We already have these ... what are we using them for?

- ✓ Signing email
- ✗ Actually protecting the network ☹️



Leveraging the good aspects of Defense Department networking infrastructure ...

- memory, processing power, widespread user authentication

... and avoiding the things that always complicate deployment

- full encryption and key management for everything

- What are we making?

Boxes

- What else are we making?

Software for the boxes and the hosts

- The boxes are called?

Network Controllers



Tim Gibson, Ph.D.
DARPA Strategic Technology Office
3701 North Fairfax Drive
Arlington, VA 22203
Tel 703-526-4768
Fax 703-516-8784
timothy.gibson@darpa.mil